Guide de l'utilisateur

AWS Hub de sécurité



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

AWS Hub de sécurité: Guide de l’utilisateur

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

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Que sont Security Hub et Security Hub CSPM ? 1
AWS Hub de sécurité 2
Caractéristiques 2
Intégrations 3
Accès à Security Hub 4
Concepts 5
Estimateur de coûts 10
Accès par type de compte 11
Conditions préalables 12
Configurer l'accès intercompte 13
Utilisation de l'estimateur de coûts 16
Remarques importantes 24
Informations connexes 25
Activation de Security Hub 25
Activez Security Hub pour AWS Organisation 26
Activez Security Hub dans un compte autonome 28
Désignation d'un administrateur délégué 30
Création de la politique d'administrateur délégué 31
Gestion de la configuration des comptes des membres 32
Supprimer un administrateur délégué 38
Re-enabling Hub de sécurité 39
Recommandations 40
Couverture du compte 41
Page de couverture du compte 42
Widget de couverture de sécurité 44
Plan étendu 44
Autorisations pour le plan prolongé 44
Inscription aux partenaires du plan Extended 45
Désinscription auprès d'un partenaire 46
Cross-Region agrégation 46
Types de données agrégées 46
Agrégation pour les comptes d'administrateur et de membre 49
Règles d'automatisation et agrégation interrégionale 49
Activer l'agrégation 50

Révision des paramètres d'agrégation 51
Actualisation des paramètres d'agrégation 51
Supprimer l'agrégation 52
Intégration avec Azure 53
Comment AWS Config est utilisé 55
Informations supplémentaires 55
Conditions préalables 56
Configuration d'Azure 58
Configuration de Security Hub 69
Supprimer un connecteur Azure 82
Tableau de bord récapitulatif 83
Considérations 83
Widgets disponibles 84
Filtres disponibles 98
Affichage des détails relatifs aux ressources dans Security Hub 100
Format de recherche : OCSF 101
Présentation de l'OCSF 101
Ressources connexes 101
AWS extension pour OCSF 102
Résultats de couverture 124
Résultats de couverture pour AWS Hub de sécurité CSPM 125
Résultats de couverture pour Amazon GuardDuty 125
Résultats de couverture pour Amazon Inspector 126
Résultats de couverture pour Amazon Macie 126
Suppression des résultats de couverture 127
Inventaire de l'IA 127
Conditions préalables à la découverte d'IA auto-hébergée 128
Types de ressources d'IA pris en charge 128
Trouver des ressources d'IA à partir de la page Ressources 129
Utilisation de la page d'inventaire de l'IA 130
Considérations 131
Accès à l'inventaire de l'IA avec l'API 132
Constatations d'exposition 134
Comment fonctionnent les résultats d'exposition 134
Composantes d'une constatation d'exposition 135
Classification de gravité 137

Avantages des résultats d'exposition 137
Sources des résultats d'exposition 138
Bonnes pratiques 138
Ressources prises en charge 139
Caractéristiques prises en charge 140
Génération de résultats d'exposition 143
Déterminer le niveau de gravité d'un résultat d'exposition 147
Révision des résultats d'exposition 149
Graphique de la trajectoire d'attaque potentielle 151
Corriger les résultats d'exposition 152
Résultats des accès non utilisés 264
Comment fonctionne l'analyse des accès non utilisés 264
Types de recherche d'accès non utilisés 265
Service-linked analyseur 265
Affichage des résultats d'accès non utilisés 266
Accès non utilisé aux résultats d'exposition 266
Recommandations de politique pour les autorisations non utilisées 267
Tarification 267
Recommandations politiques 267
Comment fonctionnent les recommandations politiques 267
Qui peut générer des recommandations 268
Cycle de vie des recommandations 268
Cas d'erreur 269
Utilisation de la console 269
Référence des API 269
Numérisation réseau 270
Types de ressources pris en charge 270
Activer la numérisation réseau 271
Comment fonctionne la numérisation réseau 272
Résultats de l'analyse réseau 273
Scannez les preuves 276
Exclusion de ressources de la numérisation 276
Ports pris en charge 277
Multi-cloud soutien 277
Disponibilité dans les Régions 277
Désactiver la numérisation réseau 277

Automatisations 278
Règles d'automatisation 279
EventBridge règles d'automatisation 298
Third-party intégrations 3
Jira Cloud 308
ServiceNow 314
Principales politiques de KMS pour les intégrations de billetterie 322
Tester les intégrations de billetterie 325
Application MCP (version préliminaire) 328
Exemples d'applications MCP 328
Concepts clés 332
Conditions préalables 333
Configuration du serveur MCP 334
Utilisation de Connector Diagnostics 334
Outils disponibles 335
Surveillance de l'utilisation et des coûts 336
Qui peut accéder à la page d'utilisation 336
Synthèse des coûts liés à l'organisation et au compte 337
Vue Capacités 338
Vue Compte 339
Stratégies d'optimisation des coûts 340
Ressources connexes 340
Désactivation de Security Hub 341
Désactivation de Security Hub pour un seul compte 341
Désactivation de Security Hub au sein d'une organisation 341
Sécurité 344
Protection des données 345
Gestion des identités et des accès 348
Validation de conformité 383
Résilience 383
Sécurité de l'infrastructure 384
Points de terminaison de VPC (AWS PrivateLink) 384
Journalisation des appels d'API 386
Informations sur le Security Hub dans CloudTrail 386
Exemple : entrées du fichier journal de Security Hub 388
AWS Hub de sécurité CSPM 391

Avantages du Security Hub CSPM 392
Accès à Security Hub CSPM 393
Services connexes 395
Essai gratuit, utilisation et tarification de Security Hub CSPM 395
Affichage des détails d'utilisation 396
Informations de tarification 396
Concepts 396
Activation de Security Hub CSPM 403
Vérification des autorisations nécessaires 403
Activation de Security Hub CSPM avec l'intégration des organisations 403
Activation manuelle de Security Hub CSPM 405
Prochaines étapes : gestion de la posture et intégrations 407
Configuration AWS Config 408
Configuration locale 415
Configuration centrale 416
Gestion de plusieurs comptes 466
Gérer des comptes avecAWS Organizations 467
Gestion manuelle des comptes sur invitation 468
Recommandations pour les environnements multi-comptes 468
Gérer des comptes avec AWS Organizations 470
Gestion des comptes par invitation 487
Actions autorisées par les comptes administrateur et membre 502
Effet des actions du compte sur les données 509
Agrégation des données entre les régions 512
Types de données agrégées 513
Agrégation pour les comptes d'administrateur et de membre 515
Configuration et agrégation centralisées 516
Activer l'agrégation 517
Révision des paramètres d'agrégation 519
Actualisation des paramètres d'agrégation 521
Arrêt de l'agrégation 523
Normes 524
Référence aux normes 526
Activation d'une norme 626
Révision des détails d'une norme 633
Désactivation des normes activées automatiquement 637

Désactivation d'une norme 638
Contrôles 641
Vue consolidée des contrôles 642
Score de sécurité récapitulatif pour les contrôles 643
Référence des contrôles 644
Autorisations pour configurer les contrôles 1613
Contrôles d'activation 1614
Désactivation des commandes 1623
Contrôles de sécurité et scores 1635
Catégories de contrôle 1712
Révision des détails des contrôles 1716
Contrôles de filtrage et de tri 1719
Paramètres de contrôle 1720
Examen et gestion des résultats des contrôles 1736
Intégrations 1764
Révision d'une liste d'intégrations 1765
Faciliter le flux des résultats d'une intégration 1767
Désactiver le flux de résultats d'une intégration 1768
Visualisation des résultats d'une intégration 1769
Service AWS intégrations 1770
Third-party intégrations 1793
Intégrations de produits personnalisées 1828
Intégration à Azure 1830
Comment AWS Config est utilisé 1832
Types de connecteurs 1832
Conditions préalables 1833
Configuration d'Azure 1835
Configuration du Security Hub CSPM 1842
Supprimer un connecteur Azure 1864
Résultats 1865
BatchImportFindings pour trouver des prestataires 1867
BatchUpdateFindings pour les clients 1870
Révision des détails et de l'historique des découvertes 1874
Filtrage des résultats 1879
Regroupement des résultats 1882
Définition de l'état des résultats dans le flux de travail 1883

Envoi de résultats à une action personnalisée 1886
Format de recherche : ASFF 1887
Informations 2185
Examiner les informations et agir en fonction de celles-ci 2186
Informations gérées 2189
Informations personnalisées 2200
Automatisations 2208
Règles d'automatisation 2209
Réponse et remédiation automatisées 2236
Tableau de bord récapitulatif 2254
Widgets disponibles pour le tableau de bord Summary 2254
Filtrer le tableau de bord 2258
Personnalisation du tableau de bord 2260
Limites régionales 2261
Cross-Region restrictions d'agrégation 2261
Disponibilité des intégrations par région 2262
Disponibilité des normes par région 2264
Disponibilité des contrôles par région 2265
Limites régionales en matière de contrôles 2265
Création de ressources avec CloudFormation 2545
Security Hub (CSPM) etCloudFormationmodèles 2546
En savoir plus surCloudFormation 2547
Abonnement aux annonces 2547
Format du message Amazon SNS 2552
Désactivation du Security Hub CSPM 2554
Sécurité 2557
Protection des données 2558
Gestion des identités et des accès 2559
Validation de conformité 2597
Résilience 2597
Sécurité de l'infrastructure 2598
Points de terminaison de VPC (AWS PrivateLink) 2598
Journalisation des appels d'API 2600
Informations CSPM du Security Hub dans CloudTrail 386
Exemple : entrées du fichier journal CSPM du Security Hub 388
Balisage de ressources 2604

Principes fondamentaux du balisage 2604
Utilisation de balises dans les politiques IAM 2606
Ajout de balises à des ressources 2607
Modification des balises pour les ressources 2610
Révision des balises pour les ressources 2612
Suppression de balises de ressources 2615
Quotas 2617
Quotas maximaux 2617
Quotas tarifaires 2617
Historique de la documentation 2618
..... mmdccxliv

Que sont Security Hub et Security Hub CSPM ?

AWSSecurity Hub et AWS Security Hub CSPM Services AWS protègent votre environnement cloud. Les services se complètent mutuellement. Lorsqu'ils sont utilisés ensemble, ils fournissent des informations précieuses sur le niveau de sécurité de votre AWS environnement.

Security Hub CSPM fournit une vue complète de votre niveau de sécurité et vous aide à évaluer votre environnement cloud par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub fournit une expérience unifiée qui vous aide à hiérarchiser les problèmes de sécurité critiques et à y répondre. Les résultats du Security Hub CSPM sont automatiquement acheminés vers Security Hub, où ils sont corrélés aux résultats d'autres services de sécurité, tels qu'Amazon Inspector, afin de générer des risques. Cela vous permet d'identifier les risques les plus critiques de votre environnement. Security Hub fournit également des fonctionnalités de flux de travail automatisés, qui vous aident à intégrer les résultats du Security Hub CSPM dans vos flux de travail opérationnels.

La meilleure pratique consiste à activer les deux services. Vous pouvez activer Security Hub CSPM sans activer Security Hub si votre objectif principal est d'identifier les erreurs de configuration et d'évaluer votre niveau de sécurité. Toutefois, si vous activez Security Hub sans activer Security Hub CSPM, Security Hub ne peut pas utiliser les résultats du Security Hub CSPM pour fournir des informations sur les risques et les expositions dans votre environnement. AWS Pour une expérience optimale, nous recommandons non seulement d'activer Security Hub et Security Hub CSPM, mais également d'activer les autres services de sécurité suivants : Amazon GuardDuty, Amazon Inspector et Amazon Macie.

Présentation de AWS Hub de sécurité

AWS Security Hub est une solution de sécurité cloud unifiée qui donne la priorité à vos problèmes de sécurité critiques et vous aide à y répondre à grande échelle. Security Hub détecte les problèmes de sécurité en corrélant et en enrichissant automatiquement les signaux de sécurité provenant de sources multiples. Ces sources incluent la gestion de la posture, la gestion des vulnérabilités (Amazon Inspector), les données sensibles (Amazon Macie) et la détection des menaces (Amazon GuardDuty). Utilisez Security Hub pour hiérarchiser les risques actifs dans votre environnement cloud grâce à des analyses automatisées et à des informations contextuelles. Grâce à des visualisations intuitives, Security Hub transforme les signaux de sécurité complexes en informations exploitables, ce qui vous permet de prendre rapidement des décisions éclairées concernant votre sécurité. Security Hub inclut également des flux de réponse automatisés pour vous aider à remédier aux risques, à améliorer la productivité de votre équipe et à minimiser les interruptions opérationnelles.

Caractéristiques

Solution de sécurité unifiée

Bénéficiez d'une plus grande visibilité sur votre environnement cloud grâce à une gestion centralisée au sein d'une solution de sécurité cloud unifiée.

Informations de sécurité exploitables

Obtenez des informations de sécurité exploitables grâce à des analyses avancées pour en savoir plus sur les risques de sécurité associés à votre environnement.

Temps de réponse réduits

Rationalisez les temps de réponse grâce à des flux de travail automatisés et à un système de billetterie intégré.

Constatations d'exposition

Security Hub met en corrélation les résultats des contrôles CSPM de Security Hub, d'Amazon Inspector et d'autres outils Services AWS pour détecter les expositions associées aux ressources. AWS

Analyse des accès non utilisés

Security Hub identifie automatiquement les rôles, les utilisateurs, les clés d'accès et les autorisations IAM qui n'ont pas été utilisés au cours d'une période rétrospective de 90 jours. Lorsque vous activez Security Hub, le service crée un analyseur d'accès IAM lié au service dans votre compte. Les résultats d'accès non utilisés vous aident à mettre en œuvre l'accès au moindre privilège en mettant en évidence les principaux IAM surprovisionnés. En cas de détection d'autorisations non utilisées, Security Hub peut générer des recommandations de politique de moindre privilège qui vous indiquent une politique de remplacement limitée.

Les résultats sont formatés dans l'Open Cybersecurity Schema Framework (OCSF)

Security Hub génère des résultats dans OCSF et reçoit des résultats dans OCSF à partir de Security Hub CSPM et d'autres entités : Services AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Tableau de bord

La console Security Hub fournit une vue complète de vos expositions, de vos menaces, de votre couverture de sécurité et de vos ressources, ainsi qu'une visualisation interactive appelée graphique du chemin d'attaque, qui montre comment les attaquants potentiels peuvent accéder aux ressources associées à une détection d'exposition et en prendre le contrôle.

Intégrations avec des produits tiers

Vous pouvez améliorer votre niveau de sécurité grâce aux intégrations de Security Hub. Par exemple, si vous utilisez Jira Cloud ouServiceNow ITSM, vous pouvez utiliser cette fonctionnalité pour créer des tickets à partir des résultats.

Intégrations

Security Hub reçoit les résultats suivants Services AWS.

- AWS Hub de sécurité CSPM
- Amazon GuardDuty
- Amazon Inspector

- Amazon Macie
- Analyseur d'accès IAM

Accès à Security Hub

Security Hub est disponible dans la plupart des AWS régions. Pour obtenir la liste des régions dans lesquelles Security Hub est actuellement disponible, consultez la section Points de terminaison et quotas Security Hub dans le Références générales AWS. Pour plus d'informations sur la gestion Régions AWS de votre compte Compte AWS, consultez la section Spécifier les éléments que Régions AWS votre compte peut utiliser dans le Guide de Gestion de compte AWS référence.

Vous pouvez activer Security Hub pour des comptes individuels ou des comptes de votre organisation. Dans chaque région, vous pouvez accéder à Security Hub et l'utiliser de l'une des manières suivantes :

Console Security Hub

La console Security Hub est une interface basée sur un navigateur que vous pouvez utiliser pour créer et gérer AWS des ressources. Cette console vous permet d'accéder à votre compte, à vos données et à vos ressources.

API Security Hub

L'API Security Hub vous donne un accès programmatique à votre compte, à vos données et à vos ressources. Vous pouvez envoyer des requêtes HTTPS directement à Security Hub.

AWS CLI

Avec le AWS CLI, vous pouvez exécuter des commandes sur la ligne de commande de votre système pour effectuer des tâches et créer des scripts qui exécutent des tâches. Dans certains cas, elle AWS CLI peut s'avérer plus utile que la console Security Hub.

AWS SDK

AWSLes SDK se composent de bibliothèques et d'exemples de code pour divers langages de programmation et plates-formes (C++, Go, Java, .NET et Python). Ils fournissent un accès programmatique à Security Hub et à d'autres applications Services AWS dans la langue de votre choix et peuvent vous aider à gérer des tâches telles que la gestion des erreurs, la signature des demandes et les nouvelles tentatives.

Concepts de Security Hub

Dans Security Hub, nous nous appuyons sur AWS des concepts et une terminologie communs et utilisons ces termes supplémentaires.

Compte

Le AWS compte standard contenant vos AWS ressources. Connectez-vous AWS à votre AWS compte pour activer Security Hub.

Si votre compte est inscrit AWS Organizations, votre organisation désigne un compte administrateur Security Hub. Ce compte peut activer d'autres comptes d'organisation en tant que comptes de membres.

Une organisation ne peut avoir qu'un seul compte administrateur. Un compte ne peut pas être à la fois un compte administrateur et un compte membre.

Security Hub prend en charge les comptes suivants :

- Compte de gestion de l'organisation : AWS compte qui administre une AWS organisation.
- Compte administrateur délégué : AWS compte qui gère l'utilisation d'un Service AWS pour une AWS organisation.
- Compte de membre : AWS compte membre d'une AWS organisation.
- Compte autonome : AWS compte non AWS Organizations activé.

Compte administrateur

Ce type de AWS compte permet de consulter les résultats des comptes membres associés.

Ce type de AWS compte devient un compte administrateur lorsqu'il est désigné par un compte de gestion de l'organisation comme compte administrateur de Security Hub. Le compte administrateur de Security Hub peut activer n'importe quel compte d'organisation en tant que compte membre et peut également inviter d'autres comptes à devenir des comptes membres.

Une organisation ne peut avoir qu'un seul compte administrateur. Un compte ne peut pas être à la fois un compte administrateur et un compte membre.

Région d'agrégation

Une région d'agrégation vous permet de visualiser les résultats de sécurité de plusieurs sources Régions AWS dans une seule fenêtre.

La région d'agrégation est l' Région AWS endroit où vous pouvez consulter et gérer les résultats. Les résultats sont agrégés dans la région d'agrégation à partir des régions liées. Les résultats mis à jour sont reproduits dans toutes les régions.

Dans la région d'agrégation, le tableau de bord et les pages d'inventaire incluent les données de toutes les régions liées. La page d'automatisations ne peut être utilisée que pour définir des règles d'automatisation dans la région d'agrégation. Third-party les intégrations de billetterie ne peuvent être configurées que dans la région d'agrégation.

Résultat archivé

Une découverte dont le statut est de`ARCHIVED`. Ces résultats indiquent que le fournisseur de la découverte ou le client qui étudie la découverte estime que celle-ci n'est plus pertinente.

Les prestataires de services de recherche peuvent archiver les résultats qu'ils créent. Les clients peuvent archiver tous les résultats qui, selon eux, ne sont plus pertinents en utilisant l'BatchUpdateFindingsV2API Security Hub ou en mettant à jour le statut dans la console Security Hub.

Dans la console Security Hub, les paramètres de filtre par défaut excluent les résultats archivés des listes et des tableaux de recherche. Vous pouvez mettre à jour les filtres pour inclure les résultats archivés. Si vous récupérez des résultats à l'aide de l'opération GetFindings V2, l'opération extrait à la fois les résultats archivés et les résultats actifs. L'exemple suivant montre comment exclure des résultats archivés des résultats.

```
{
    "StringFilters":
    [
        {
            "FieldName": "status",
            "Filter":
            {
                "Value": "Archived",
                "Comparison": "EQUALS"
            }
        }
    ]
}
```

Cross-Region agrégation

L'agrégation des résultats et des ressources des régions liées à une région d'agrégation. Vous pouvez consulter toutes vos données depuis la région d'agrégation et mettre à jour les résultats de la région d'agrégation.

Compte administrateur délégué

Dans AWS Organizations, le compte administrateur délégué d'un service est capable de gérer l'utilisation d'un service pour l'organisation.

Dans Security Hub, le compte administrateur de Security Hub est également le compte d'administrateur délégué pour Security Hub. Lorsque le compte de gestion de l'organisation désigne pour la première fois le compte administrateur de Security Hub, Security Hub appelle les organisations pour faire de ce compte le compte d'administrateur délégué.

Le compte de gestion de l'organisation doit ensuite choisir le compte d'administrateur délégué comme compte d'administrateur de Security Hub dans toutes les régions.

Exposure

Les expositions sont des faiblesses plus générales des contrôles de sécurité, des erreurs de configuration ou d'autres domaines susceptibles d'être exploités par des menaces actives.

Voici des exemples d'expositions :

- Plan de contrôle mal configuré pour une ressource.
- Présence d'une vulnérabilité logicielle présentant un fort potentiel d'exploitabilité.
- Ressource accessible au public (réseau ou API).

Détection de l'exposition

Type de résultat qui décrit une exposition présente dans votre environnement. Un résultat d'exposition inclut des traits et des signaux. Un signal peut comprendre un ou plusieurs types de caractéristiques d'exposition. AWS Security Hub génère une détection d'exposition lorsque des signaux provenant de AWS Security Hub CSPM, d'Amazon Inspector, d'Amazon GuardDuty, d'Amazon Macie ou d'autres AWS services indiquent la présence d'une exposition. Une ressource peut être impliquée dans un ou plusieurs résultats d'exposition. Si une ressource n'a pas de caractéristiques d'exposition ou si ses caractéristiques sont insuffisantes, Security Hub ne génère pas de résultat d'exposition pour cette ressource.

Voici un exemple de découverte d'exposition : une instance EC2 accessible depuis Internet et présentant des vulnérabilités logicielles présentant une forte probabilité d'exploitation.

Résultat

Enregistrement observable d'une vérification de sécurité ou d'une détection liée à la sécurité. Security Hub génère et met à jour les résultats en les corrélant avec d'autres résultats de sécurité. C'est ce que l'on appelle les résultats d'exposition. Les résultats peuvent également provenir d'intégrations avec d'autres produits Services AWS et des produits tiers.

Détecter l'ingestion

L'importation des résultats dans Security Hub. La détection d'événements d'ingestion inclut à la fois de nouvelles découvertes et des mises à jour des résultats existants.

Région liée

Lorsque vous activez l'agrégation interrégionale, une région liée est une région qui regroupe les résultats et l'inventaire des ressources dans la région d'agrégation.

Dans une région liée, le tableau de bord et les pages d'inventaire ne contiennent que des résultats à ce sujet Région AWS.

Cadre de schéma de cybersécurité ouvert (OCSF)

L'Open Cybersecurity Schema Framework (OCSF) est un effort collaboratif AWS et open source réalisé par des partenaires de premier plan du secteur de la cybersécurité. L'OCSF fournit un schéma standard pour les événements de sécurité courants, définit des critères de version pour faciliter l'évolution du schéma et inclut un processus d'auto-gouvernance pour les producteurs et les consommateurs de journaux de sécurité. Pour plus d'informations, consultez les résultats de l'OCSF dans Security Hub.

Compte membre

Et Compte AWS qui a autorisé un compte administrateur à consulter ses résultats et à y donner suite. Ce type de compte Compte AWS devient un compte de membre lorsque le compte administrateur de Security Hub l'active en tant que compte de membre.

Signal

Une découverte qui contribue à une constatation d'exposition. Un signal peut être considéré comme un résultat contributif. Un signal peut provenir de Security Hub CSPM ou d'une autre source AWS Config Services AWS, telle qu'Amazon Inspector.

Service-linked enregistreur de configuration

Type d' AWS Config enregistreur utilisé pour enregistrer des données de configuration sur des ressources spécifiques à un service. Security Hub utilise ces enregistreurs dans le cadre d'une

approche axée sur les événements afin d'obtenir des éléments de configuration des ressources pour la couverture de l'analyse de l'exposition, les rapports d'inventaire des ressources et les évaluations du contrôle de gestion de la posture. Cette fonctionnalité est fournie à tous les clients de Security Hub dans le cadre de la tarification du plan Essential. Une fois que vous avez activé Security Hub, les enregistreurs de configuration liés aux services suivants sont créés dans votre compte :

- Dans chaque Compte AWS et Région AWS, un enregistreur de configuration lié à un service nommé `AWSConfigurationRecorderForSecurityHubAssets` est créé.
- Pour les types de ressources globaux, un enregistreur de configuration lié à un service supplémentaire nommé `AWSConfigurationRecorderForSecurityHubAssetsGlobal` est créé dans le fichier us-east-1. Région AWS
- Si Security Hub et Security Hub CSPM sont tous deux activés dans un Compte AWS et Région AWS, un enregistreur de configuration lié à un service nommé est créé. `AWSConfigurationRecorderForSecurityHubCSPM`

Pour plus d'informations, consultez les sections Considérations relatives aux enregistreurs de configuration liés aux services et Ressources régionales et mondiales relatives à l'enregistrement.

Service-linked analyseur

Analyseur d'accès IAM créé et géré par Security Hub pour vous. Lorsque vous activez Security Hub, il crée automatiquement un analyseur d'accès non utilisé lié à un service afin d'identifier les rôles IAM, les utilisateurs, les clés d'accès et les autorisations qui n'ont pas été utilisés au cours d'une période rétrospective de 90 jours. L'analyseur fonctionne dans l'est des États-Unis (Virginie du Nord) car l'IAM est un service mondial. Security Hub reproduit les résultats d'accès non utilisés dans toutes les régions dans lesquelles vous avez activé Security Hub. Il n'est pas nécessaire d'activer séparément IAM Access Analyzer ni de prendre d'autres mesures. Cette fonctionnalité est fournie à tous les clients de Security Hub dans le cadre de la tarification du plan Essential. Vous pouvez consulter l'analyseur lié à un service dans la console IAM Access Analyzer, mais vous ne pouvez ni le modifier ni le supprimer tant que Security Hub est activé. Security Hub supprime l'analyseur lorsque vous désactivez le service dans toutes les régions d'un. Compte AWS Pour de plus amples informations, veuillez consulter the section called "Résultats des accès non utilisés".

Trait

Écart de sécurité qui entraîne une constatation d'exposition. Les types de traits incluent l'assumabilité, la mauvaise configuration, l'accessibilité, les données sensibles et la

vulnérabilité. Un trait est associé à un signal, et un signal peut contenir plusieurs traits. Par exemple, un contrôle CSPM Security Hub indique qu'une politique gérée par le client autorise le contrôle d'accès administratif. Ce signal contient un trait de mauvaise configuration.

Résultats des accès non utilisés

Résultat qui identifie un rôle, un utilisateur, une clé d'accès ou un ensemble d'autorisations IAM qui n'a pas été utilisé au cours d'une période rétrospective de 90 jours. Security Hub génère les résultats d'accès non utilisés à l'aide d'un analyseur d'accès IAM lié à un service. Il existe quatre types de résultats d'accès non utilisés : les rôles IAM non utilisés, les clés d'accès utilisateur IAM non utilisées, les mots de passe utilisateur IAM non utilisés et les autorisations non utilisées.

AWS Estimateur des coûts de Security Hub

L'estimateur des coûts de Security Hub est une fonctionnalité de console qui fournit des estimations des fonctionnalités de Security Hub dans votre AWS environnement. L'estimateur de coûts vous indique quels sont vos coûts de service individuels pour AWS Security Hub CSPM, Amazon Inspector et Amazon GuardDuty et quels seraient vos coûts estimés dans Security Hub avec les plans tarifaires simplifiés de Security Hub. Vous pouvez ajuster l'utilisation estimée et le nombre de ressources en fonction de votre AWS utilisation afin d'améliorer la précision de votre estimation. L'estimateur de coûts est disponible dans toutes les régions où Security Hub est disponible.

L'estimateur de coûts estime les coûts mensuels des fonctionnalités de sécurité à l'aide de deux modèles de tarification :

- Tarification des services individuels : payez séparément pour chaque fonctionnalité de sécurité (GuardDuty, Amazon Inspector, Security Hub CSPM).
- Tarification simplifiée de Security Hub : tarification unifiée sur 3 plans tarifaires, plan Essentials avec tarification par ressource, analyse des menaces avec tarification par événement et par Go de journaux, et analyse du code Lambda avec tarification par ressource.

L'estimateur utilise les AWS Cost Explorer données lorsqu'elles sont disponibles. Lorsque les données de Cost Explorer ne sont pas disponibles, vous pouvez saisir manuellement les données d'utilisation. Les estimations de coûts sont basées sur l'utilisation observée et fournie par l'utilisateur, ainsi que sur les informations de tarification publiques. Les estimations peuvent ne pas refléter les remises accordées aux entreprises.

Les principaux avantages de l'estimateur de coûts sont les suivants :

- Découvrez comment le coût d'une tarification unifiée, lors de l'activation de Security Hub, se compare au coût d'un service individuel sans activation de Security Hub
- Estimez les coûts avant d'activer les fonctionnalités
- Ajustez les paramètres d'utilisation pour modéliser différents scénarios
- Exportez les estimations au format PDF pour examen par les parties prenantes

Accès par type de compte

> **Note**
>
> Pour les comptes d'administrateur délégué et de membre, l'estimateur de coûts s'ouvre en mode édition par défaut, ce qui vous permet de saisir immédiatement les données d'utilisation. Le compte de gestion et les comptes autonomes s'ouvrent en mode affichage lorsque les données de Cost Explorer sont disponibles.

Cette fonctionnalité récupère automatiquement des informations sur l'utilisation passée réelle afin d'estimer le coût de certains types de comptes. Consultez le tableau suivant pour plus de détails sur chacun des types de comptes et les données disponibles pour chaque type de compte.

Autorisations d'accès par type de compte

Type de compte	Données de Cost Explorer	Saisie de données	Scope
Compte de gestion (MA)	Auto-populated	Dérogation manuelle disponible	Organization-wide
Administrateur délégué (DA)	Auto-populated via un rôle multicompte*	Dérogation manuelle disponible	Organization-wide
Member Account	Auto-populated via un rôle multicompte*	Dérogation manuelle disponible	Organization-wide
Compte autonome (SA)	Auto-populated	Dérogation manuelle disponible	Compte unique

* Nécessite la configuration du rôle IAM entre comptes dans le compte de gestion. Voir Configurer l'accès intercompte la section ci-dessous.

Conditions préalables

Autorisations IAM requises

Pour utiliser toutes les fonctionnalités de l'estimateur de coûts, votre responsable IAM doit disposer des autorisations suivantes :

Autorisations IAM requises pour Cost Estimator

Opération API	Service	Objectif
`ce:GetCostAndUsage`	AWS Explorateur de coûts	Récupérez l'historique des données d'utilisation et de coûts
`pricing:GetProducts`	AWS Tarification	Consultez les tarifs actuels
`organizations:ListAccounts`	AWS Organisations	Compter les comptes dans l'organisation
`organizations:DescribeOrganization`	AWS Organisations	Déterminer le type de compte
`securityhub:ListOrganizationAdminAccounts`	Hub de sécurité	Répertorier les comptes d'administration de
`iam:GetRole`	IAM	Vérifier l'existence d'un rôle entre comptes (compte de gestion uniquement) *
`sts:AssumeRole`	IAM	Assumez un rôle multicompte (administrator/Member compte délégué uniquement) **

* Obligatoire uniquement pour les utilisateurs du compte de gestion afin de vérifier le statut des rôles entre comptes.

** Obligatoire uniquement pour les comptes d'administrateur délégué et de membre de l'organisation utilisant un accès multicompte.

Exigences supplémentaires

Cost Explorer

Doit être activé pour le remplissage automatique des données (délai de traitement de 24 heures après l'activation).

Configurer l'accès intercompte

Les comptes d'administrateur délégué et de membre peuvent accéder aux AWS Cost Explorer données à l'échelle de l'organisation à partir du compte de gestion en configurant un rôle IAM inter-comptes. Cette configuration permet à ces comptes d'afficher les données d'utilisation réelles sans passer au compte de gestion.

Conditions préalables

Les éléments et informations suivants sont nécessaires avant de configurer l'accès entre comptes pour l'estimateur des coûts :

- Le compte de gestion doit être AWS Cost Explorer activé.
- Autorisations IAM pour créer des rôles dans le compte de gestion.
- Connaissance de l'administrateur délégué ou de l'identifiant du compte de membre auquel l'accès intercomptes sera accordé.

Étapes de configuration

L'estimateur de coûts fournit des instructions de configuration guidées directement dans la console. Pour accéder aux instructions, accédez à la page de l'estimateur des coûts à l'adresse https://console.aws.amazon.com/securityhub/v2/home #/CostEstimator dans le compte de gestion de votre organisation. Localisez la section Cross-account d'accès et suivez les étapes décrites pour configurer le rôle multicompte.

Configuration du rôle

L'accès entre comptes à l'estimateur de coûts nécessite la configuration d'un rôle IAM avec une politique de confiance et une politique d'autorisations. Le rôle inter-comptes doit être créé dans le compte de gestion avec la configuration suivante :

Nom du rôle (nom exact requis) — AwsSecurityHubCostEstimatorCrossAccountRole

Politique de confiance recommandée :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
            "AWS": "arn:aws:iam::{ACCOUNT_ID}:role/{ROLE_NAME}"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Modifiez la politique en remplaçant les valeurs suivantes dans l'exemple de stratégie :

- Remplacez-le *{ACCOUNT_ID}* par l'identifiant de compte d'administrateur délégué ou de membre auquel vous accordez l'accès entre comptes.
- Remplacez-le *{ROLE_NAME}* par le nom du rôle IAM dans le compte d'administrateur délégué ou de membre auquel vous accordez l'accès.

Politique d'autorisations recommandée :

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

```
    ]
}
```

> **Note**
>
> La politique de confiance restreint l'accès à un compte et à un rôle spécifiques. Seul le principal IAM spécifié peut assumer ce rôle, empêchant ainsi tout accès non autorisé.

Vérification

Après avoir créé le rôle dans le compte de gestion, procédez comme suit pour vérifier que la configuration fonctionne.

1. Connectez-vous à l'administrateur délégué ou au compte de membre.
2. Accédez à l'estimateur de coûts de Security Hub à l'adresse #/CostEstimator https://console.aws.amazon.com/securityhub/v2/home
3. La page devrait automatiquement :
    a. Détectez le compte de gestion de votre organisation.
    b. Assumez le rôle multicompte.
    c. Chargez les données de Cost Explorer pour les utiliser à l'échelle de l'organisation.

En cas de succès, les données d'utilisation réelles apparaissent à la place des champs de saisie manuelle.

Résolution des problèmes

Cette section couvre les problèmes courants et les solutions qui peuvent survenir lors de la configuration de l'accès entre comptes.

Les données d'utilisation de l'organisation ne sont pas disponibles pour ce compte

Cette alerte indique que le rôle multicompte n'est pas accessible. Les causes possibles de cette alerte sont les suivantes :

1. Le rôle n'existe pas : le compte de gestion n'a pas encore créé le rôle.

- Solution : contactez l'administrateur de votre compte de gestion pour créer le rôle en suivant les instructions de configuration.

2. Incompatibilité du nom du rôle : le nom du rôle ne correspond pas exactement.
   - Solution : vérifiez que le nom du rôle est`AwsSecurityHubCostEstimatorCrossAccountRole`.
3. Politique de confiance incorrecte : la politique de confiance n'autorise pas votre compte à assumer ce rôle.
   - Solution : vérifiez que la politique de confiance inclut votre identifiant de compte et le nom de votre rôle.
4. AssumeRole Autorisation manquante : votre responsable IAM n'`sts:AssumeRole`a pas accès.
   - Solution : contactez votre administrateur pour ajouter une `sts:AssumeRole` autorisation.

Pour consulter les instructions de configuration détaillées : choisissez Afficher les instructions dans l'alerte pour ouvrir une fenêtre modale contenant des instructions étape par étape et des modèles de politiques.

Solution : vous pouvez toujours utiliser l'estimateur de coûts en saisissant manuellement les valeurs d'utilisation en mode édition.

Utilisation de l'estimateur de coûts

Accès à l'estimateur de coûts

Pour accéder à l'estimateur de coûts depuis la page d'accueil de Security Hub

1. Connectez-vous à votre AWS compte à l'aide des informations d'identification du compte de gestion ou d'administrateur délégué de votre AWS organisation. Ouvrez la console Security Hub dans la région us-east-1 à l'adresse. https://console.aws.amazon.com/securityhub/v2/home
2. Sur la page d'accueil, localisez la fiche tarifaire.
3. Choisissez Estimer le coût.

Pour accéder à l'estimateur de coûts pendant les étapes d'activation et de configuration de Security Hub

1. Accédez à la tarification sur la nouvelle carte Security Hub de l'interface d'intégration.
2. Choisissez Afficher les estimations.

Pour accéder à l'estimateur des coûts depuis les GuardDuty consoles Amazon Inspector ou Security Hub CSPM

1. Accédez au tableau de bord ou à la page de résumé du service.
2. Choisissez Comparer les prix dans la fiche d'informations sur les prix.

Comprendre l'interface de l'estimateur de coûts

Mise en page

La page de l'estimateur de coûts contient trois sections principales :

- Section de présentation — Explique les avantages de la gestion unifiée de la sécurité et de l'optimisation des coûts.
- Informations sur les prix : panneau extensible avec des catégories de fonctionnalités et des niveaux de prix.
- Tableau de comparaison des prix : comparaison Side-by-side des coûts avec les détails des capacités.

Tableau de comparaison des prix

L'en-tête du tableau inclut des commandes de view/edit mode et une option de réinitialisation. Le tableau affiche les coûts dans deux colonnes :

- Services individuels — Coûts actuels ou estimés pour des services de sécurité distincts.
- Security Hub — Coûts estimés à l'aide d'un modèle de tarification simplifié.

Région de tarification

La première colonne affiche des informations contextuelles relatives à la tarification, y compris une note indiquant que les estimations utilisent la tarification us-east-1 pour les calculs. Un badge indique que les remises destinées aux entreprises ne sont pas incluses dans les estimations.

Affichage des estimations de coûts

Lorsque vous utilisez l'estimateur de coûts, vous pouvez consulter, modifier, réinitialiser et exporter des estimations.

L'estimateur de coûts s'ouvre en mode affichage par défaut.

Pour consulter les estimations de coûts

1. Accédez à l'estimateur de coûts à l'aide de l'une des méthodes décrites dans. Accès à l'estimateur de coûts
2. Consultez le total des coûts mensuels dans la ligne récapitulative.
3. Passez en revue les groupes de capacités et leur ventilation détaillée des coûts.
4. Choisissez les noms des fonctionnalités pour afficher les descriptions dans une fenêtre contextuelle.

Sources de données en mode affichage

L'estimateur affiche des données provenant de plusieurs sources, indiquées par des libellés :

- Par défaut : données AWS Cost Explorer datant des 30 derniers jours.
- $-/mo — Données sur les coûts non disponibles (affichées lorsque l'accès à Cost Explorer n'est pas disponible).
- Utilisation personnalisée — User-entered valeurs.
- Non activé : indique quand les autorisations de Cost Explorer n'existent pas.

Account-specific comportement

Ce qui suit décrit le fonctionnement de l'estimateur de coûts sur différents types de comptes et de configurations.

Comptes d'administrateur délégué et de membre

Avec l'accès multicompte configuré :

- Les données de Cost Explorer sont disponibles pour une utilisation à l'échelle de l'organisation.
- S'ouvre en mode affichage par défaut (comme dans le compte de gestion). Vous pouvez passer en mode édition pour modifier les estimations.

Sans accès multi-comptes configuré :

- L'alerte s'affiche : « Les données d'utilisation de l'organisation ne sont pas disponibles pour ce compte ».
- S'ouvre en mode édition par défaut pour la saisie manuelle.
- Choisissez Afficher les instructions dans l'alerte pour obtenir des conseils de configuration.

Compte de gestion

Avec la création d'un rôle multicompte :

- la section « Cross-account accès » affiche l'état configuré.
- Affiche les politiques de vérification recommandées.
- Fournit un lien pour afficher le rôle dans la console IAM.

Sans création d'un rôle inter-comptes :

- la section « Cross-account accès » affiche le guide de configuration.
- Fournit des instructions étape par étape avec des politiques préremplies.
- Lien direct vers la console IAM pour la création de rôles.

Impossible de vérifier le statut du rôle :

- S'il n'y a aucune autorisation d'appel`iam:GetRole`, la console ne peut pas déterminer si vous avez créé le rôle nécessaire.
- Affiche « Impossible de vérifier » avec le message d'erreur correspondant.

Compte autonome

Sans création d'un rôle inter-comptes :

- Aucune modification du comportement existant.
- Les données de Cost Explorer sont disponibles lorsque cette option est activée.
- S'ouvre en mode affichage par défaut.

Modifier les valeurs d'utilisation

Le mode Édition vous permet de modifier les valeurs des dimensions et de consulter les mises à jour des coûts en temps réel.

Pour modifier les valeurs d'utilisation

1. Choisissez Modifier dans l'en-tête du tableau.
2. Entrez des valeurs dans les champs de saisie des dimensions.
3. Consultez automatiquement les coûts mis à jour.
4. Choisissez Afficher pour revenir au mode d'affichage.

> **Important**
>
> - Les modifications ne sont pas enregistrées lorsque vous quittez la page d'estimation des coûts
> - Les estimations modifiées utilisent la tarification us-east-1 (Virginie du Nord) et n'incluent pas les remises destinées aux entreprises
> - L'édition en mode « Afficher le coût actuel uniquement » revient automatiquement au mode estimé

Réinitialisation de l'estimateur

Cette action efface toutes les valeurs personnalisées et recharge les données par défaut depuis Cost Explorer.

Pour rétablir les valeurs par défaut de toutes les valeurs

1. Choisissez Réinitialiser dans l'en-tête du tableau.
2. Dans la boîte de dialogue de confirmation, choisissez Réinitialiser.

Exportation des estimations

Dans l'estimateur de coûts, les données de votre estimation peuvent être exportées vers un fichier PDF.

Pour exporter des estimations de coûts

1. Assurez-vous d'être en mode affichage.
2. Choisissez Télécharger le PDF dans l'en-tête de la page.

Le PDF se télécharge automatiquement avec le nom de fichier :`SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`.

Résolution des problèmes

Cette section couvre les problèmes courants et les solutions qui peuvent survenir lors de l'utilisation de l'estimateur de coûts.

Aucune donnée Cost Explorer disponible

Problème

L'alerte affiche « Aucune donnée de coût disponible pour votre compte ».

Solutions par type de compte

La solution dépend de votre type de compte :

Solutions pour les données manquantes de Cost Explorer

Type de compte	Solution
Compte de gestion	Activez Cost Explorer et attendez 24 heures pour le traitement des données

Type de compte	Solution
Administrateur délégué	Contactez l'administrateur du compte de gestion pour demander l'accès
Member Account	Contactez le compte de gestion ou l'administrateur délégué pour y accéder
Compte autonome	Activez Cost Explorer et attendez 24 heures pour le traitement des données

Solution

Entrez des valeurs personnalisées en mode édition.

Cross-account l'accès ne fonctionne pas

Problème

Le compte administrateur délégué ou membre affiche l'alerte « Les données d'utilisation de l'organisation ne sont pas disponibles pour ce compte ».

Passez en revue les causes courantes suivantes et leurs solutions :

Cross-account le rôle n'existe pas dans le compte de gestion

Contactez l'administrateur du compte de gestion pour créer le rôle. L'estimateur de coûts fournit des instructions de configuration guidées pour les utilisateurs des comptes de gestion.

Le nom du rôle ne correspond pas exactement

Nom de rôle obligatoire :`AwsSecurityHubCostEstimatorCrossAccountRole`. Vérifiez que le nom du rôle dans la console IAM correspond exactement (distinction majuscules/minuscules).

La politique de confiance n'autorise pas votre compte

Vérifiez que le principal de la politique de confiance inclut votre identifiant de compte et le nom de votre rôle. Format :`arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`.

AssumeRole Autorisation manquante

Vérifiez que votre responsable IAM est `sts:AssumeRole` autorisé. Contactez votre AWS administrateur pour ajouter cette autorisation.

Solution :

Entrez des valeurs personnalisées en mode édition pour estimer manuellement les coûts sans les données de Cost Explorer.

Obtenir des instructions détaillées

- Choisissez Afficher les instructions dans l'alerte pour ouvrir un modal contenant :
  - Step-by-step conseils de configuration
  - Modèles de politique Pre-populated
  - Conseils de dépannage spécifiques à votre erreur

Erreurs d'autorisation

Problème

Erreur « Accès refusé » pour des opérations d'API spécifiques.

Pour résoudre les erreurs d'autorisation

1. Notez l'opération refusée dans le message d'erreur (par exemple,`ce:GetCostAndUsage`).
2. Choisissez Copier pour copier les détails de l'erreur.
3. Envoyez les détails de l'erreur à votre AWS administrateur.
4. Demandez les autorisations IAM requises répertoriées dans. Autorisations IAM requises

> **Note**
>
> Vous pouvez toujours utiliser le mode édition pour saisir des valeurs manuelles lorsque les autorisations sont manquantes, sauf lorsque l'accès à l'API de tarification est refusé (empêche toutes les estimations de coûts).

La fonctionnalité indique « Non activée »

Problème

La fonctionnalité affiche le statut « Non activé ».

Explication

Ce statut apparaît lorsque vous avez accès à Cost Explorer mais que la fonctionnalité n'est pas active actuellement. Si vous voyez plutôt $-/mo, cela signifie que les données de Cost Explorer ne sont pas disponibles pour votre type de compte.

Pour consulter les estimations de coûts

1. Choisissez Modifier pour passer en mode édition.
2. Entrez les valeurs de dimension de la capacité.
3. Consultez les estimations de coûts mises à jour.

La capacité indique « Non applicable »

Problème

La fonctionnalité affiche « Non applicable » dans la colonne Services individuels.

Explication

Cette fonctionnalité n'est disponible que via la tarification simplifiée de Security Hub, et non en tant que service autonome.

Les coûts modifiés ne correspondent pas à Cost Explorer

Problème

Les coûts modifiés diffèrent des valeurs d'origine de Cost Explorer.

Explication

Les estimations modifiées utilisent les taux de tarification us-east-1 (Virginie du Nord) et n'incluent pas les remises destinées aux entreprises. Les données de Cost Explorer reflètent les coûts réels avec les remises applicables.

Remarques importantes

- Les estimations sont basées sur l'utilisation observée et fournie par l'utilisateur, ainsi que sur les informations publiques sur les prix. Les coûts réels peuvent varier en fonction des modèles d'utilisation et des contrats d'entreprise
- Rétrospective sur 30 jours : les données de Cost Explorer reflètent les 30 derniers jours d'utilisation
- Région de tarification — Toutes les estimations utilisent les taux US-east-1 (Virginie du Nord)

- Aucune incidence sur les paramètres : les modifications apportées à l'estimateur n'ont aucune incidence sur les configurations actuelles de votre Security Hub ou de vos services
- Réductions pour les entreprises : les estimations modifiées n'incluent pas les remises pour les entreprises ; seules les données de Cost Explorer reflètent les coûts actualisés réels
- Actualisation des données : les données de Cost Explorer sont mises à jour quotidiennement ; actualisez la page pour voir les données les plus récentes

Informations connexes

- AWS Tarification de Security Hub
- AWS Guide de l'utilisateur de Cost Explorer
- AWS Référence de l'API de tarification
- Activation de Security Hub

Activation de Security Hub

Vous pouvez activer Security Hub pour n'importe quel utilisateur Compte AWS. Cette section de la documentation décrit toutes les étapes nécessaires pour activer Security Hub pour une AWS organisation ou un compte autonome.

Pour une brève démonstration de l'activation de Security Hub, regardez la vidéo suivante : Procédure pas à pas et démo d'intégration de Security Hub.

Activez Security Hub pour AWS Organisation

Cette section comprend trois étapes :

- À l'étape 1, le compte de gestion de AWS l'organisation désigne un administrateur délégué pour son AWS organisation, crée la politique d'administrateur délégué et active éventuellement Security Hub pour son propre compte.
- À l'étape 2, l'administrateur délégué de l'organisation active Security Hub pour son propre compte.
- À l'étape 3, l'administrateur délégué de l'organisation configure tous les comptes membres de l'organisation, pour Security Hub et les autres services de sécurité pris en charge.

Étape 1. Délégation d'un compte administrateur et activation facultative de Security Hub dans AWS compte de gestion de l'organisation

> **Note**
>
> Effectuez cette étape dans une région du compte de gestion de l'organisation.

Lorsque vous attribuez le compte d'administrateur délégué pour Security Hub, le compte que vous pouvez choisir pour votre administrateur délégué dépend de la façon dont vous avez configuré un administrateur délégué pour Security Hub CSPM. Si vous avez configuré un administrateur délégué pour Security Hub CSPM et que ce compte n'est pas le compte de gestion de l'organisation, ce compte est automatiquement défini comme administrateur délégué de Security Hub et aucun compte différent ne peut être choisi. Si le compte administrateur délégué pour Security Hub CSPM est défini comme compte de gestion de l'organisation ou ne l'est pas du tout, vous pouvez choisir le compte à attribuer comme compte d'administrateur délégué Security Hub, à l'exception du compte de gestion de l'organisation.

Pour plus d'informations sur la désignation d'un administrateur délégué dans Security Hub, consultez la section Désignation d'un compte administrateur délégué dans Security Hub. Pour plus d'informations sur la création de la politique d'administrateur délégué dans Security Hub, voir Création de la stratégie d'administrateur délégué dans Security Hub.

Pour désigner un administrateur pour Security Hub

1. Connectez-vous à votre AWS compte à l'aide des informations d'identification du compte de gestion de votre AWS organisation. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Sur la page d'accueil de Security Hub, choisissez Security Hub, puis choisissez Commencer.
3. Dans la section Administrateur délégué, choisissez un compte administrateur en fonction des options proposées. Il est recommandé de faire appel au même administrateur délégué pour tous les services de sécurité afin d'assurer une gouvernance cohérente.
4. Cochez la case Accès sécurisé. Le choix de cette option permet à votre compte d'administrateur délégué de configurer certaines fonctionnalités, telles que la protection contre les GuardDuty programmes malveillants, sur les comptes des membres. Si vous décochez cette option, Security Hub ne peut pas activer ces fonctionnalités en votre nom et vous devez les activer directement via le service auquel la fonctionnalité est associée.
5. (Facultatif) Pour activer le compte, cochez la case pour activer Security Hub pour votre AWS compte.
6. Pour la politique d'administrateur délégué, choisissez l'une des options suivantes pour ajouter la déclaration de politique.

    a. (Option 1) Choisissez Mettre à jour ceci pour moi. Cochez la case située sous la déclaration de politique pour confirmer que Security Hub crée automatiquement une politique de délégation accordant toutes les autorisations requises à l'administrateur délégué.

    b. (Option 2) Choisissez Je veux le joindre manuellement. Choisissez Copier et joindre. Dans la AWS Organizations console, sous Administrateur délégué pour AWS Organizations, choisissez Déléguer et collez la politique de ressources dans l'éditeur de stratégie de délégation. Choisissez Create Policy (Créer une politique). Ouvrez l'onglet dans lequel vous vous trouvez dans la console Security Hub.
7. Choisissez Configurer.

Étape 2. Activez Security Hub dans le compte administrateur délégué

Le compte administrateur délégué effectue cette étape. Une fois que le compte de gestion de AWS l'organisation a désigné un administrateur délégué pour son organisation, l'administrateur délégué doit activer Security Hub pour son propre compte avant de l'activer pour l'ensemble de l' AWS organisation.

Pour activer Security Hub dans le compte administrateur délégué

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Sur la page d'accueil de Security Hub, choisissez Commencer.
3. La section sur les fonctionnalités de sécurité décrit les fonctionnalités qui sont automatiquement activées et incluses dans le prix de base par ressource de Security Hub.
4. (Facultatif) Pour les balises, déterminez si vous souhaitez ajouter une paire clé-valeur à la configuration du compte.
5. Choisissez Activer Security Hub pour terminer l'activation de Security Hub.
6. (Recommandé) Dans la fenêtre contextuelle, choisissez Configurer mon organisation et passez à l'étape 3.

Étape 3. Créez une politique qui active Security Hub dans tous les comptes des membres

Après avoir activé Security Hub dans le compte administrateur délégué d'une organisation, vous devez créer une politique qui définit les services et fonctionnalités qui sont activés dans les comptes des membres de l'organisation. Pour plus d'informations, consultez Activation d'une configuration avec un type de politique.

Une fois que vous avez activé Security Hub, les ressources suivantes sont créées dans votre compte :

- Un rôle lié à un service appelé. AWSServiceRoleForSecurityHubV2
- Service-linked enregistreurs de configuration. Consultez l'Service-linked enregistreur dans la documentation des concepts de Security Hub pour plus de détails.
- Un analyseur lié à un service. Consultez l'Service-linked analyseur dans la documentation des concepts de Security Hub pour plus de détails.

Activez Security Hub dans un compte autonome

Cette procédure explique comment activer Security Hub dans un compte autonome. Un compte autonome est un compte Compte AWS qui n'a pas activé AWS les organisations.

Pour activer Security Hub dans un compte autonome

1. Connectez-vous à votre AWS compte à l'aide des informations d'identification de votre compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Sur la page d'accueil de Security Hub, choisissez Commencer.
3. Dans la section Capacités de sécurité, effectuez l'une des opérations suivantes :
   a. (Option 1) Choisissez Activer toutes les fonctionnalités. Cela active toutes les fonctionnalités essentielles du Security Hub, l'analyse des menaces et les fonctionnalités supplémentaires.
   b. (Option 2) Choisissez Personnaliser les fonctionnalités. Sélectionnez les fonctionnalités à activer dans les sections Gestion de la sécurité, Analyse des menaces et Gestion des vulnérabilités. Vous ne pouvez désélectionner aucune fonctionnalité faisant partie des fonctionnalités essentielles du plan Security Hub.
4. Dans la section Régions, choisissez Activer toutes les régions ou Activer des régions spécifiques. Si vous choisissez Activer toutes les régions, vous pouvez déterminer si vous souhaitez activer automatiquement les nouvelles régions. Si vous choisissez Activer des régions spécifiques, vous devez choisir les régions que vous souhaitez activer.
5. (Facultatif) Pour les balises de ressources, ajoutez des balises sous forme de paires clé-valeur pour vous aider à identifier facilement la configuration.
6. Choisissez Enable Security Hub (Activer le hub de sécurité).

Après avoir activé Security Hub, les ressources suivantes sont créées dans chaque compte sur lequel vous avez activé le service :

- Un rôle lié à un service appelé. AWSServiceRoleForSecurityHubV2
- Service-linked enregistreurs de configuration. Consultez l'Service-linked enregistreur dans la documentation des concepts de Security Hub pour plus de détails.
- Un analyseur lié à un service. Consultez l'Service-linked analyseur dans la documentation des concepts de Security Hub pour plus de détails.

Désignation d'un administrateur délégué dans Security Hub

Dans le compte de gestion de AWS l'organisation, vous pouvez désigner un administrateur délégué pour votre organisation. Il est recommandé de faire appel au même administrateur délégué pour tous les services de sécurité afin d'assurer une gouvernance cohérente.

La procédure décrite dans cette rubrique décrit comment désigner un administrateur délégué dans Security Hub. Cela suppose que vous avez déjà activé Security Hub mais que vous n'avez pas désigné d'administrateur délégué au cours du processus d'activation.

Considérations

Lorsque vous désignez un administrateur délégué dans Security Hub, tenez compte des points suivants :

- Le compte de gestion de AWS l'organisation peut se désigner comme administrateur délégué dans Security Hub CSPM, mais ne peut pas se désigner comme administrateur délégué dans Security Hub. Dans ce scénario, le compte de gestion doit désigner un autre Compte AWS administrateur délégué dans Security Hub.
- Si le compte de gestion de AWS l'organisation désigne un administrateur délégué dans Security Hub CSPM, cet administrateur délégué devient automatiquement l'administrateur délégué dans Security Hub. Dans ce scénario, Security Hub autorise uniquement cette personne Compte AWS à agir en tant qu'administrateur délégué.

> **Note**
>
> La suppression de l'administrateur délégué via la console Security Hub CSPM, la console Security Hub ou l' AWS Organizations API le supprime des deux services. Lorsque l'administrateur délégué est retiré de Security Hub CSPM, la configuration centrale se désactive automatiquement.

Désignation d'un administrateur délégué après avoir activé Security Hub

Cette procédure doit être exécutée par le compte de gestion de l' AWS organisation. Il suppose que le compte de gestion de AWS l'organisation a précédemment activé Security Hub mais n'a pas désigné d'administrateur délégué pendant le flux de travail d'activation.

> **Note**
>
> Une fois cette procédure terminée, vous devez créer une politique permettant à l'administrateur délégué de votre organisation de configurer Security Hub et d'effectuer des actions spécifiques dans AWS Organizations. Pour plus d'informations, consultez la section Création de la politique d'administrateur délégué dans Security Hub.

Pour désigner un administrateur délégué dans Security Hub

1. Connectez-vous à votre AWS compte à l'aide des informations d'identification du compte de gestion de votre organisation, puis ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Général.
3. Dans Administrateur délégué, choisissez Configurer. Sélectionnez l'une des options proposées Comptes AWS ou entrez le Compte AWS numéro à 12 chiffres de l'administrateur délégué Compte AWS que vous souhaitez désigner comme administrateur délégué de votre organisation. Choisissez Enregistrer.

Création de la politique d'administrateur délégué dans Security Hub

Le compte de gestion de AWS l'organisation peut créer une politique permettant à l'administrateur délégué de configurer Security Hub et d'effectuer des actions spécifiques dans AWS Organizations. La procédure décrite dans cette rubrique décrit comment créer la politique. Une fois la procédure terminée, vous pouvez autoriser Security Hub à créer la politique pour vous ou la créer manuellement. Autorisez Security Hub à créer la politique, sauf si vous souhaitez la personnaliser pour un cas d'utilisation particulier.

Effectuez cette procédure uniquement si le compte de gestion de l'organisation a activé Security Hub et désigné un administrateur délégué, mais a ignoré la création de la politique pendant le flux de travail d'activation. Pour plus d'informations sur la mise à jour de cette politique, voir Mettre à jour une stratégie de délégation basée sur les ressources AWS Organizations dans le Guide de l'AWS Organizations utilisateur.

> **Note**
>
> Une fois cette procédure terminée, l'administrateur délégué peut créer une politique pour gérer les comptes des membres de votre organisation. Pour plus d'informations, voir Création d'une politique en tant qu'administrateur délégué pour gérer les comptes des membres.

Pour créer la politique d'administrateur délégué

1. Connectez-vous à votre AWS compte à l'aide des informations d'identification du compte de gestion de votre organisation. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Général.
3. Pour la politique d'administrateur délégué, effectuez l'une des opérations suivantes :
   - Choisissez Create Policy (Créer une politique). Cochez la case située sous la déclaration de politique pour confirmer que Security Hub crée automatiquement une politique de délégation accordant toutes les autorisations requises à l'administrateur délégué.
   - Ouvrez la politique. Choisissez Copier et joindre. Dans la AWS Organizations console, sous Administrateur délégué pour AWS Organizations, choisissez Déléguer et collez la politique de ressources dans l'éditeur de stratégie de délégation. Choisissez Create Policy (Créer une politique). Ouvrez l'onglet dans lequel vous vous trouvez dans la console Security Hub, puis choisissez Configurer.

Gestion de la configuration des comptes des membres dans un AWS Organisation

L'administrateur délégué d'une AWS organisation peut configurer les fonctionnalités de sécurité pour les comptes des membres et les régions. Deux types de configurations sont disponibles : les politiques et les déploiements. Les politiques génèrent AWS les politiques des organisations pour les comptes et les régions pour AWS Security Hub et Amazon Inspector. Les déploiements sont une action ponctuelle visant à activer une fonctionnalité de sécurité sur des comptes et des régions sélectionnés pour Amazon GuardDuty et AWS Security Hub CSPM. Contrairement aux politiques, vous ne pouvez ni afficher ni modifier les déploiements et les déploiements ne s'appliquent pas aux comptes récemment activés. Comme alternative, des fonctionnalités d'activation automatique pour

les nouveaux comptes de membres sont disponibles sur Amazon GuardDuty et AWS Security Hub CSPM.

Catalogue de configuration de Security Hub

Le catalogue de configuration de Security Hub propose plusieurs options pour vous aider à configurer les comptes de votre AWS organisation en fonction des fonctionnalités de sécurité fournies par Security Hub.

Les options disponibles dans le catalogue de configuration de Security Hub sont les suivantes.

Security Hub (fonctionnalités essentielles et supplémentaires)

Il s'agit de la configuration recommandée pour déployer Security Hub.

Type : Politique et déploiements

Description : cette configuration active les fonctionnalités essentielles de gestion de la sécurité, de gestion de la posture, d'analyse des menaces et de gestion des vulnérabilités de Security Hub. Il permet éventuellement d'activer des fonctionnalités supplémentaires.

Analyse des menaces à partir de GuardDuty

Type : Déploiement

Description : Activez certaines GuardDuty fonctionnalités Amazon pour surveiller, analyser et traiter en permanence les sources de AWS données et les journaux dans votre AWS environnement.

Gestion de la posture à partir de AWS Hub de sécurité CSPM

Type : Déploiement

Description : Cette configuration active les normes et les contrôles de Security Hub CSPM, qui détectent lorsque vos AWS comptes et vos ressources s'écartent des meilleures pratiques de sécurité.

Gestion des vulnérabilités depuis Amazon Inspector

Type : Politique

Description : Cette configuration active certaines fonctionnalités d'Amazon Inspector qui détectent automatiquement les charges de travail, les instances, les images de conteneurs et d'autres ressources, et les analyse pour détecter les vulnérabilités et l'exposition du réseau.

Activation d'une configuration avec un type de politique

La procédure suivante décrit comment créer une configuration avec un type de politique pour les comptes de votre AWS organisation. Pour créer une politique de configuration, vous devez d'abord créer la politique d'administrateur délégué dans le compte de gestion de AWS l'organisation. Pour plus d'informations sur la création de la politique d'administrateur délégué dans Security Hub, voir Création de la stratégie d'administrateur délégué dans Security Hub.

Pour créer une politique qui active et désactive les comptes des membres

1. Connectez-vous à l'aide de votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis sélectionnez Configurations.
3. Choisissez un élément avec un type de politique ou de stratégie et de déploiement dans le catalogue de configuration. Pour configurer complètement Security Hub, choisissez Security Hub (fonctionnalités essentielles et supplémentaires).
4. Sur la page Configurer Security Hub, dans la section Détails, entrez le nom et la description de la politique.
5. Dans la section Fonctionnalités de sécurité, choisissez l'une des options suivantes :
   - Activez toutes les fonctionnalités : active toutes les fonctionnalités essentielles de Security Hub, l'analyse des menaces et les fonctionnalités supplémentaires.
   - Personnalisation des fonctionnalités : sélectionnez les fonctionnalités dans les sections Gestion de la sécurité, Analyse des menaces et Gestion des vulnérabilités. Vous ne pouvez pas désélectionner les fonctionnalités qui font partie du plan Security Hub Essential.
6. Dans la section Sélection du compte, choisissez l'une des options suivantes :
   - Toutes les unités et tous les comptes organisationnels — Applique la configuration à l'ensemble de votre organisation.
   - Unités et comptes organisationnels spécifiques — Utilisez la barre de recherche ou l'arborescence de la structure organisationnelle pour sélectionner les unités organisationnelles et les comptes auxquels la politique s'applique.
   - Aucune unité organisationnelle ni aucun compte — N'applique la configuration à aucune unité organisationnelle ni à aucun compte.
7. Dans la section Régions, choisissez l'une des options suivantes :

- Activer toutes les régions : choisissez éventuellement d'activer automatiquement les nouvelles régions.
- Désactiver toutes les régions — Choisissez éventuellement si vous souhaitez désactiver automatiquement les nouvelles régions.
- Spécifier les régions : choisissez les régions à activer et à désactiver.

8. (Facultatif) Pour les paramètres avancés, consultez la section Opérateurs d'héritage dans le Guide de AWS Organizations l'utilisateur.
9. (Facultatif) Pour les balises de ressources, ajoutez des balises sous forme de paires clé-valeur pour vous aider à identifier la configuration.
10. Choisissez Suivant.
11. Vérifiez vos modifications, puis choisissez Appliquer.

    L'état de configuration de votre politique s'affiche en haut de la page Politiques. Chaque fonctionnalité fournit un état indiquant si elle a été configurée avec succès ou si son déploiement a échoué. En cas de panne, cliquez sur le lien de défaillance pour obtenir plus de détails. Pour consulter la politique en vigueur au niveau du compte, consultez l'onglet Organisation de la page Configurations.

Activation d'une configuration avec un type de déploiement

La procédure suivante décrit comment créer une configuration avec un type de déploiement pour les comptes de votre AWS organisation.

Pour créer un déploiement qui active les comptes membres

1. Connectez-vous à l'aide de votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis sélectionnez Configurations.
3. Choisissez un élément avec un type de déploiement dans le catalogue de configuration.
4. Dans la section Fonctionnalités de sécurité, sélectionnez les fonctionnalités de sécurité à activer.
5. Dans la section Sélection du compte, choisissez l'une des options suivantes :

- Toutes les unités et tous les comptes de l'organisation : applique le déploiement à l'ensemble de votre organisation.
- Unités et comptes organisationnels spécifiques : utilisez la barre de recherche ou l'arborescence de la structure organisationnelle pour sélectionner les unités organisationnelles et les comptes auxquels le déploiement s'applique.
- Aucune unité organisationnelle ni aucun compte : n'applique le déploiement à aucune unité organisationnelle ni à aucun compte.

6. Dans la section Régions, choisissez l'une des options suivantes :

- Activer toutes les régions : choisissez éventuellement d'activer automatiquement les nouvelles régions.
- Désactiver toutes les régions — Choisissez éventuellement si vous souhaitez désactiver automatiquement les nouvelles régions.
- Spécifier les régions : choisissez les régions à activer et à désactiver.

7. Choisissez Configurer.

Modifier une politique de configuration

Vous pouvez modifier les fonctionnalités, les régions et les comptes associés à une politique de configuration. Lorsque vous ouvrez une politique pour la modifier, la console affiche la configuration actuelle.

> **Note**
>
> Les modifications s'appliquent uniquement aux fonctionnalités que vous sélectionnez dans la politique mise à jour. Les fonctionnalités non sélectionnées conservent leur configuration existante pour les comptes et les régions de la politique.

Pour modifier une politique de configuration

1. Connectez-vous à l'aide de votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis sélectionnez Configurations.

3. Dans l'onglet Stratégies configurées, cliquez sur le bouton radio correspondant à la stratégie que vous souhaitez modifier, puis choisissez Modifier.
4. Dans la section Capability, choisissez l'une des options suivantes :
   - Configurer et activer toutes les fonctionnalités : active toutes les fonctionnalités de la politique.
   - Sélectionnez des fonctionnalités individuelles et choisissez Activer , Désactiver ou Personnaliser pour chacune d'entre elles.
5. Dans la section Sélection du compte, choisissez l'une des options suivantes :
   - Toutes les unités et tous les comptes de l'organisation : applique la politique à l'ensemble de votre organisation.
   - Unités et comptes organisationnels spécifiques — Utilisez la barre de recherche ou l'arborescence de la structure organisationnelle pour sélectionner les unités organisationnelles et les comptes auxquels la politique s'applique.
   - Aucune unité organisationnelle ni aucun compte : supprime la politique de toutes les cibles.
6. Dans la section Régions, configurez les régions auxquelles la politique s'applique. Les options dépendent de vos sélections de capacités.

   Si vous avez choisi d'activer toutes les fonctionnalités :

   - Pour toutes les fonctionnalités sélectionnées : définit la même configuration de région pour toutes les fonctionnalités.
   - Par capacité : vous permet de choisir les régions individuellement pour chaque capacité.

   Choisissez ensuite Activer toutes les régions (avec la possibilité d'activer automatiquement les nouvelles régions) ou Activer dans certaines régions pour sélectionner des régions spécifiques.

   Si vous avez choisi des actions mixtes (activer, désactiver ou personnaliser) pour des fonctionnalités individuelles :

   - Si toutes les fonctionnalités sélectionnées partagent la même action, choisissez Dans toutes les fonctionnalités sélectionnées pour définir les régions de manière uniforme. Pour définir les régions pour chaque fonctionnalité individuellement, choisissez Par capacité.
   - Si les fonctionnalités ont des actions différentes, vous devez attribuer des régions à chaque capacité individuellement.

- Pour les fonctionnalités dotées de l'action Personnaliser, choisissez Parmi toutes les fonctionnalités sélectionnées afin de définir les régions de manière uniforme pour toutes les fonctionnalités. Pour configurer les régions séparément pour chaque fonctionnalité, choisissez Par capacité.

7. Choisissez Suivant.
8. Examinez vos modifications, puis choisissez Update (Mettre à jour). La politique mise à jour configure les comptes cibles.

Supprimer une politique de configuration

Vous pouvez supprimer une politique de configuration. Lorsque vous supprimez une politique, le service supprime tous les comptes et unités organisationnelles qui y sont rattachés.

Pour supprimer une politique de configuration

1. Connectez-vous à l'aide de votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis sélectionnez Configurations.
3. Dans l'onglet Stratégies configurées, sélectionnez la stratégie que vous souhaitez supprimer, puis choisissez Supprimer.
4. Entrez `delete` dans la case de confirmation, puis choisissez Supprimer.

Supprimer le compte administrateur délégué dans Security Hub

Vous pouvez supprimer le compte administrateur délégué dans la console Security Hub à tout moment. Toutefois, cette action supprime l'administrateur délégué de Security Hub et de Security Hub CSPM. Nous vous recommandons d'effectuer cette action uniquement lorsque vous l'avez confirmée avec votre compte de sécurité.

> **Note**
>
> Si vous utilisez un compte autre que le compte de gestion de l'organisation en tant qu'administrateur délégué CSPM de Security Hub, le supprimer via la console Security Hub CSPM ou via l' AWS Organizations API le supprime également de Security Hub.

De même, si vous supprimez l'administrateur délégué de Security Hub via la console ou l' AWS Organizations API Security Hub, il est également supprimé de Security Hub CSPM. Lorsque l'administrateur délégué est retiré de Security Hub CSPM, la configuration centrale se désactive automatiquement.

Pour supprimer le compte d'administrateur délégué

1. Connectez-vous à votre AWS compte à l'aide des informations d'identification du compte de gestion de votre organisation. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Général.
3. Dans Administrateur délégué, choisissez Supprimer l'administrateur délégué. Dans la boîte de dialogue de confirmation, saisissez Supprimer, puis choisissez Supprimer.

Re-enabling Hub de sécurité

Avant de réactiver Security Hub sur des comptes précédemment désactivés à l'aide d'une politique Security Hub, vous devez d'abord détacher la politique de désactivation. Si vous tentez de réactiver Security Hub alors qu'une politique de désactivation est toujours associée au compte ou à l'unité organisationnelle, la politique de désactivation annule l'activation et Security Hub reste désactivé.

Pour supprimer la politique de désactivation de Security Hub pour une organisation ou un compte

1. Connectez-vous à l'aide de votre AWS compte à l'aide des informations d'identification du compte de gestion de votre organisation. Ouvrez la AWS Organizations console à l'adresse https://console.aws.amazon.com/organizations/v2/home.
2. Dans le panneau de navigation, choisissez AWS des comptes.
3. Si la politique de désactivation actuelle de Security Hub s'appliquait à l'ensemble de votre organisation, choisissez Root dans la section Structure organisationnelle. Si la politique de désactivation actuelle de Security Hub concerne des comptes spécifiques, choisissez le compte spécifique dans la structure organisationnelle, puis suivez les étapes restantes pour chaque compte.
4. Dans l'onglet Politiques, recherchez la section intitulée Politiques de Security Hub.
5. Cliquez sur le bouton radio à côté de la politique qui désactive Security Hub. Choisissez Détacher.

Après avoir détaché la politique de votre organisation ou de vos comptes, vous pouvez réactiver Security Hub. Consultez la section Gestion de la configuration des comptes des membres dans une AWS organisation pour plus de détails sur la réactivation de Security Hub.

Recommandations du Security Hub

Les services de sécurité suivants AWS envoient les résultats à Security Hub au format OCSF. Après avoir activé Security Hub, activez-les Services AWS pour plus de sécurité.

Hub de sécurité CSPM

Lorsque vous activez Security Hub CSPM, vous obtenez une vue complète de votre état de sécurité dans. AWS Cela vous permet d'évaluer votre environnement par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Bien que vous puissiez démarrer avec Security Hub sans activer Security Hub CSPM, l'activation de Security Hub CSPM permet à Security Hub de corréler les signaux de sécurité provenant de Security Hub CSPM afin d'améliorer la gestion de votre posture.

Si vous activez Security Hub CSPM, nous vous recommandons également d'activer la norme AWS Foundational Security Best Practices pour votre compte. Cette norme consiste en un ensemble de contrôles qui détectent lorsque vous Comptes AWS et vos ressources s'écartent des meilleures pratiques de sécurité. Lorsque vous activez la norme des meilleures pratiques de sécurité AWS fondamentales pour votre compte, AWS Security Hub CSPM active automatiquement tous ses contrôles, y compris les contrôles pour les types de ressources suivants :

- Contrôles des comptes
- Contrôles Amazon DynamoDB
- Contrôles Amazon Elastic Compute Cloud
- Gestion des identités et des accès AWS contrôles (IAM)
- AWS Lambda contrôles
- Contrôles Amazon Relational Database Service (Amazon RDS)
- Contrôles d'Amazon Simple Storage Service

Vous pouvez désactiver toutes les commandes de cette liste. Toutefois, si vous désactivez l'un de ces contrôles, vous ne pourrez pas recevoir de résultats d'exposition pour les ressources prises en charge. Pour plus d'informations sur les contrôles qui s'appliquent à la norme AWS Foundational

Security Best Practices, consultez la norme AWS Foundational Security Best Practices v1.0.0 (FSBP).

GuardDuty

Lorsque vous activez cette option GuardDuty, vous pouvez consulter toutes vos menaces et vos résultats en matière de couverture de sécurité dans le tableau de bord de la console Security Hub. Si vous l'activez GuardDuty, l'envoi de données à Security Hub au format OCSF commence GuardDuty automatiquement.

Amazon Inspector

Lorsque vous activez Amazon Inspector, vous pouvez consulter toutes vos expositions et vos résultats en matière de couverture de sécurité sur le tableau de bord de la console Security Hub. Si vous activez Amazon Inspector, Amazon Inspector commence automatiquement à envoyer des données à Security Hub au format OCSF.

Nous vous recommandons d'activer le scan Amazon EC2 et le scan standard Lambda. Lorsque vous activez l'analyse Amazon EC2, Amazon Inspector analyse les instances Amazon EC2 de votre compte pour détecter les vulnérabilités des packages et les problèmes d'accessibilité réseau. Lorsque vous activez l'analyse standard Lambda, Amazon Inspector analyse les fonctions Lambda pour détecter les vulnérabilités logicielles liées aux dépendances des packages. Pour plus d'informations, consultez la section Activation d'un type de scan dans le guide de l'utilisateur d'Amazon Inspector.

Macie

Lorsque vous activez Macie, vous pouvez détecter des expositions supplémentaires pour vos compartiments Amazon S3. Nous vous recommandons de configurer la découverte automatique des données sensibles, afin que Macie puisse évaluer quotidiennement votre inventaire de compartiments Amazon S3.

Couverture du compte dans Security Hub

La page de couverture du compte indique les comptes et les régions de votre organisation sur lesquels Security Hub et ses fonctionnalités de sécurité intégrées sont activées. Ces fonctionnalités incluent des services tels qu'Amazon Inspector, Amazon GuardDuty, AWS Security Hub CSPM et Amazon Macie. Utilisez cette page pour identifier les lacunes en matière de couverture et suivre l'adoption des fonctionnalités au sein de votre organisation.

Page de couverture du compte

Sur la page de couverture du compte, vous pouvez consulter les statistiques de couverture agrégées. Utilisez l'onglet Comptes pour obtenir des informations détaillées au niveau du compte et l'onglet Résultats de couverture pour examiner les écarts de couverture spécifiques.

Pour accéder au Security Hub Couverture du compte page

1. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Paramètres, choisissez Couverture du compte.

Section d'aperçu

La section Vue d'ensemble affiche les mesures de couverture de sécurité agrégées pour tous les comptes surveillés. Pour les comptes d'administrateur délégué, cette section affiche les détails relatifs à l'activation de Security Hub au sein de l'organisation, offrant ainsi une visibilité sur la couverture de tous les comptes membres. Cette visualisation de haut niveau indique le pourcentage de comptes dotés de Security Hub et chaque fonctionnalité de sécurité activée, offrant ainsi une vue complète de votre niveau de sécurité. Vous pouvez sélectionner le pourcentage de couverture du Security Hub pour consulter la répartition des comptes activés par région. Vous pouvez sélectionner chaque pourcentage de capacité pour filtrer les résultats de couverture en fonction de cette fonctionnalité.

Les pourcentages de la section Vue d'ensemble sont déterminés à l'aide des calculs suivants :

- Activation du Security Hub = (nombre de paires de comptes et de régions dans lesquelles Security Hub est activé) ÷ (Nombre total de comptes de votre organisation × Régions dans lesquelles Security Hub est disponible)
- Couverture des services = (Nombre de paires de comptes activés et de régions configurées dans lesquelles la fonctionnalité est activée) ÷ (Nombre total de paires de comptes activés et de régions configurées, dans les régions configurées où le compte est activé et la fonctionnalité est disponible)

Régions configurées

Pour la configuration d'une région d'origine, les régions configurées incluent la région d'origine et les régions associées. Pour toutes les autres configurations, les régions configurées se réfèrent uniquement à la région actuelle.

Onglet Comptes

Cet onglet est uniquement disponible dans le compte d'administrateur délégué du Security Hub. Utilisez l'onglet Comptes pour analyser la couverture spécifique au compte. La colonne Security Hub indique le nombre de régions dans lesquelles Security Hub est activé pour chaque compte. Cette colonne ne s'affiche pas lors de l'affichage de l'onglet dans Régions facultatives (régions désactivées par défaut). Chaque fonctionnalité de sécurité affiche un pourcentage de couverture qui, lorsqu'il est sélectionné, révèle une ventilation détaillée des fonctionnalités individuelles et leur pourcentage de couverture au sein de cette fonctionnalité. Lorsque vous sélectionnez ces pourcentages, Security Hub filtre les résultats pour afficher la couverture de cette fonctionnalité et de ce compte.

Les pourcentages figurant dans l'onglet Comptes sont déterminés à l'aide du calcul suivant :

Couverture de l'onglet Comptes = (Nombre de régions dans lesquelles la fonctionnalité est activée) ÷ (Régions dans lesquelles la fonctionnalité est disponible)

Dans plusieurs cas, le pourcentage de couverture peut être égal à 0 % :

- Security Hub n'étant pas activé dans le compte, aucun résultat de couverture n'est ingéré.
- Security Hub attend que les résultats de couverture soient générés.

Onglet des résultats de couverture

L'onglet Résultats relatifs à la couverture répertorie les informations relatives aux fonctionnalités de sécurité activées ou désactivées sur l'ensemble de vos comptes et de vos régions. Ces résultats permettent d'identifier les domaines dans lesquels la couverture de sécurité peut être améliorée. Chaque résultat indique le titre du résultat, le compte et la région concernés, ainsi que le statut actuel. Chaque recherche comporte également un lien de configuration qui vous dirige vers le service individuel où vous pouvez gérer la configuration pour cette fonctionnalité, ou vers la page de configuration du Security Hub où vous pouvez mettre à jour vos configurations pour les services de sécurité.

Vous pouvez supprimer les résultats de couverture présentant le statut Non couvert si cette fonctionnalité de sécurité n'est pas applicable à la combinaison compte-région. Security Hub exclut les résultats supprimés du calcul du pourcentage de couverture de sécurité.

Pour plus d'informations sur les résultats de couverture et sur la manière de les supprimer, consultez la section Résultats de couverture dans Security Hub.

Widget de couverture de sécurité

La couverture du compte peut également être consultée via le widget Couverture de sécurité dans le tableau de bord récapitulatif du Security Hub. Pour plus d'informations, consultez la section Widget de couverture de sécurité.

Forfait Security Hub Extended

Avec le plan Security Hub Extended, vous pouvez protéger l'ensemble du parc de votre entreprise sur le cloud, les terminaux, le réseau, l'identité, les données, la messagerie et le navigateur. Utilisez AWS Security Hub comme centre d'une expérience d'opérations de sécurité intégrée. Avec le plan Security Hub Extended, vous pouvez sélectionner des solutions partenaires qui répondent à vos besoins en matière de sécurité et souscrire à une tarification flexible en fonction de l'utilisation, sans investissement initial ni engagement à long terme. Vous pouvez ajouter ou supprimer des solutions partenaires en fonction de l'évolution des besoins de votre entreprise.

Le plan Security Hub Extended est disponible pour tous les clients qui ont activé le plan Security Hub Essentials. Les frais liés au forfait Security Hub Extended apparaissent sur votre AWS facture mensuelle avec AWS en tant que vendeur officiel.

La tarification du plan Security Hub Extended pour toutes les solutions est disponible dans l'onglet Plan étendu de la page de détails des tarifs de Security Hub.

Autorisations pour le plan Security Hub Extended

Pour souscrire à un produit partenaire dans le cadre du plan Security Hub Extended, vous devez disposer des autorisations suivantes, en plus de vos autorisations Security Hub :

- `aws-marketplace:ViewSubscriptions`
- `aws-marketplace:Subscribe`

Pour vous désabonner d'un produit partenaire dans le cadre du plan Security Hub Extended, vous devez disposer des autorisations suivantes, en plus de vos autorisations Security Hub :

- `license-manager:ListReceivedLicenses`
- `aws-marketplace:ListAgreementCharges`
- `aws-marketplace:Unsubscribe`

Pour plus d'informations sur les autorisations de AWS Marketplace, consultez la section Contrôle de l'accès aux abonnements AWS Marketplace dans le Guide d'achat de AWS Marketplace.

Consulter les partenaires du plan Extended et s'y inscrire

Le plan Security Hub Extended est accessible via le compte administrateur délégué Security Hub ou des comptes autonomes. Sur la page du plan Security Hub Extended, vous pouvez consulter les détails de chaque partenaire, initier un abonnement à une solution partenaire et commencer le processus d'intégration à la solution de chaque partenaire via la page d'intégration du partenaire.

Pour accéder au plan Security Hub Extended et souscrire au produit d'un partenaire

1. Connectez-vous à la console de AWS gestion à l'aide des informations d'identification de votre compte administrateur délégué ou autonome.
2. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
3. Dans le volet de navigation, choisissez Gestion, puis choisissez Plan étendu.
4. Pour chaque solution partenaire à laquelle vous souhaitez vous inscrire, choisissez Afficher le produit.
5. Consultez le détail des prix du produit, puis choisissez S'abonner lorsque vous êtes prêt à démarrer le processus d'intégration au produit partenaire.
6. Une fois le processus d'inscription terminé, choisissez Configurer votre compte pour être redirigé vers la page d'inscription du partenaire.
7. Fournissez les informations nécessaires pour la page d'inscription du partenaire et suivez les étapes suivantes, fournies par le partenaire, pour terminer les étapes d'intégration.

> **Important**
>
> La solution partenaire ne vous est pas facturée tant que vous n'avez pas terminé le processus d'intégration du produit partenaire.

Désinscription auprès d'un partenaire du plan Extended

Si vous ne souhaitez plus utiliser une solution partenaire du plan étendu, vous pouvez vous désabonner de la liste des partenaires.

Pour vous désabonner d'une solution partenaire, suivez les instructions de la section Annulation de votre abonnement SaaS dans le Guide d'achat de AWS Marketplace.

> **Important**
>
> Outre l'annulation de votre abonnement, suivez toutes les étapes supplémentaires requises pour la solution partenaire, en fonction de la façon dont vous l'avez configurée pour votre entreprise.

Comprendre l'agrégation interrégionale dans Security Hub

Lorsque vous activez l'agrégation entre régions dans Security Hub, vous désignez une région d'origine. La région d'origine rassemble les résultats, les ressources et les tendances d'une ou de plusieurs régions liées. Vous pouvez ensuite gérer toutes les données de sécurité depuis une seule région.

Supposons que vous définissiez USA Est (Virginie du Nord) comme région d'origine, et USA Ouest (Oregon) et USA Ouest (Californie du Nord) comme régions liées. Lorsque vous consultez la page des résultats dans l'est des États-Unis (Virginie du Nord), vous pouvez voir les résultats des trois régions. Les mises à jour de ces résultats sont également prises en compte dans les trois régions.

Types de données agrégées

Lorsque l'agrégation interrégionale est activée avec une ou plusieurs régions liées, Security Hub réplique les données suivantes des régions liées vers la région d'origine. Cela se produit dans tous les comptes pour lesquels l'agrégation interrégionale est activée.

- Résultats
- Ressources
- Tendances

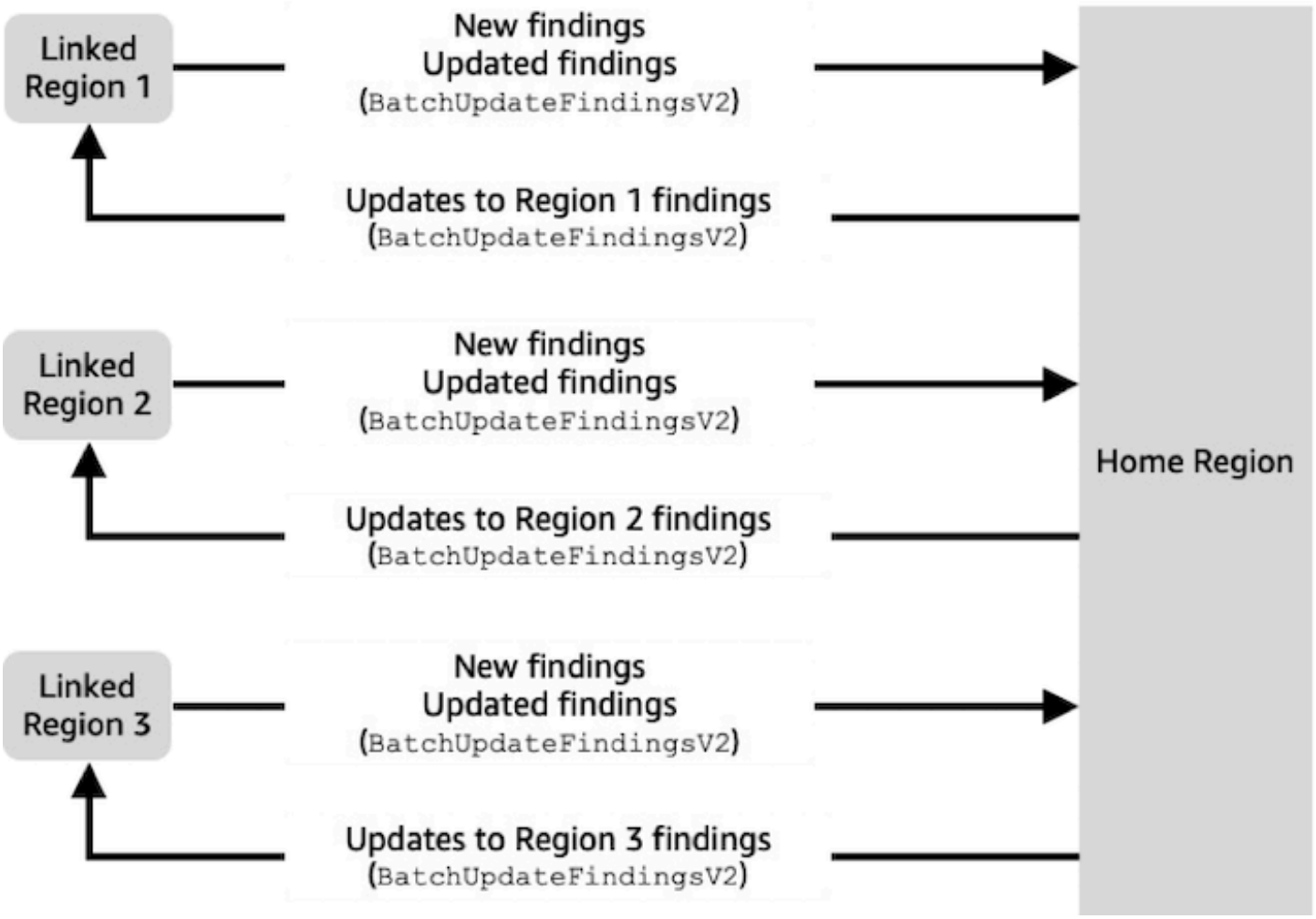
Outre les nouvelles données de la liste précédente, Security Hub reproduit également les mises à jour de ces données entre les régions liées et la région d'origine. Les mises à jour effectuées dans une région liée sont répliquées dans la région d'origine. Les mises à jour effectuées dans la région d'origine sont répliquées dans la région liée. S'il existe des mises à jour contradictoires dans la région d'origine et dans la région liée, la mise à jour la plus récente est utilisée.

Les résultats qui existaient dans une région au moment où celle-ci devient une région liée ne sont pas répliqués dans la région d'origine, sauf en cas de mise à jour des résultats. Une fois qu'une région est liée à une région d'origine, il existe une différence dans les résultats entre la région d'origine et la région liée jusqu'à ce que les résultats de la région liée soient mis à jour ou qu'ils expirent.

Toutes les ressources qui existaient dans une région au moment où celle-ci devient une région liée sont répliquées dans la région d'origine, généralement dans les 24 à 48 heures suivant la liaison de la région à une région d'origine.

Lorsque vous supprimez une région liée, tous les résultats ou ressources de cette région restent dans la région d'origine jusqu'à ce que la découverte ou la ressource soit épuisée.

Les données sur les tendances sont basées sur les résultats et les ressources disponibles dans la région visée par la tendance. Les données relatives aux tendances dans une région d'origine reflètent l'état actuel des résultats et des ressources qui ont été synchronisés avec la région d'origine.



Cross-Region l'agrégation n'augmente pas le coût de Security Hub. Vous n'êtes pas facturé lorsque Security Hub reproduit de nouvelles données ou des mises à jour.

Dans la région d'origine, la page Résumé fournit un aperçu de vos résultats actifs et de vos ressources dans les régions liées.

Security Hub regroupe uniquement les données provenant des régions où Security Hub est activé sur un compte. Security Hub n'est pas automatiquement activé pour un compte en fonction de la configuration d'agrégation interrégionale.

Il est possible d'activer l'agrégation entre régions sans qu'aucune région liée ne soit sélectionnée. Dans ce cas, aucune réplication des données n'a lieu.

Agrégation pour les comptes d'administrateur et de membre

Les comptes autonomes et les comptes d'administrateur peuvent configurer l'agrégation entre régions. Si elle est configurée par un administrateur, la présence du compte administrateur est essentielle pour que l'agrégation interrégionale fonctionne dans les comptes administrés. Si le compte administrateur est supprimé ou dissocié d'un compte de membre, l'agrégation interrégionale s'arrête pour ce compte de membre. Toutefois, si le compte membre possédait sa propre configuration d'agrégation interrégionale avant d'être associé à un administrateur, cette configuration redevient effective.

Lorsqu'un compte administrateur permet l'agrégation entre régions, Security Hub réplique les données générées par le compte administrateur dans toutes les régions liées vers la région d'origine. En outre, Security Hub identifie les comptes de membres associés à cet administrateur, et chaque compte de membre hérite des paramètres d'agrégation interrégionaux de l'administrateur. Security Hub reproduit les données générées par un compte de membre dans toutes les régions liées vers la région d'origine.

L'administrateur peut accéder aux résultats de sécurité de tous les comptes membres des régions administrées et les gérer. En outre, l'administrateur peut consulter l'inventaire des ressources de tous les comptes membres des régions administrées.

En tant que compte membre de Security Hub, vous devez être connecté à la région d'origine pour consulter les données agrégées de votre compte provenant de toutes les régions associées. Les comptes membres ne sont pas autorisés à consulter les données des autres comptes membres et ne sont pas autorisés à appeler les `GetAggregatorV2` API `CreateAggregatorV2DeleteAggregatorV2`, et.

Règles d'automatisation et agrégation interrégionale

Lorsque l'agrégation interrégionale est activée, les règles d'automatisation ne peuvent être créées que dans la région d'origine définie. Toute règle que vous définissez s'applique à toutes les régions liées, sauf si vos critères de règle s'appliquent à des régions spécifiques. Vous devez créer des règles d'automatisation distinctes pour toute région qui n'est pas une région liée.

Toutes les règles créées dans la région d'origine, avant d'activer l'agrégation interrégionale, s'appliquent automatiquement aux régions liées. Les règles créées précédemment dans les régions liées ne s'appliqueront plus une fois qu'un agrégateur sera créé. Les règles définies dans les régions liées reprennent leur application une fois que l'agrégateur est supprimé ou que la région n'est plus liée.

Activation de l'agrégation entre régions

Vous devez activer l'agrégation interrégionale à partir de la AWS région que vous souhaitez désigner comme région d'origine.

Pour activer l'agrégation entre régions, vous devez créer une ressource Security Hub appelée agrégateur de recherche. La ressource d'agrégation de recherche spécifie votre région d'origine et les régions associées (le cas échéant).

Vous ne pouvez pas utiliser une AWS région désactivée par défaut comme région d'origine. Pour obtenir la liste des régions désactivées par défaut, consultez la section Activation d'une région dans la référence AWS générale.

Lorsque vous activez l'agrégation entre régions, vous choisissez de spécifier une ou plusieurs régions liées si vous le souhaitez. L'activation de l'agrégation entre régions n'active pas Security Hub dans cette région. Pour activer Security Hub dans une région, reportez-vous à la section Création d'une politique en tant qu'administrateur délégué chargé de gérer les comptes des membres dans le guide de l'utilisateur de Security Hub.

Pour activer l'agrégation entre régions (console)

1. À partir du compte administrateur ou dans un compte autonome, ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home
2. À l'aide du sélecteur de AWS région, connectez-vous à la région que vous souhaitez utiliser comme région d'agrégation.
3. Dans le menu de navigation de Security Hub, choisissez Paramètres, puis Général.
4. Dans la section Cross-Region d'agrégation, choisissez Configurer.
5. Par défaut, la région d'origine est définie sur Aucune région d'agrégation.
6. Sous Région d'origine, sélectionnez l'option permettant de désigner la région actuelle comme région d'origine.
7. Si vous le souhaitez, pour les régions liées, sélectionnez les régions à partir desquelles vous souhaitez agréger les données.
8. Choisissez Enregistrer.

Révision des paramètres d'agrégation entre régions

Vous pouvez consulter la configuration d'agrégation interrégionale actuelle dans AWS Security Hub depuis n'importe quelle AWS région dans le compte administrateur ou dans un compte autonome. Les comptes membres ne peuvent pas afficher la configuration d'agrégation interrégionale. La configuration inclut la région d'origine et les régions liées (le cas échéant).

Suivez les étapes pour afficher vos paramètres d'agrégation interrégionaux actuels

Pour afficher les paramètres d'agrégation entre régions (console)

1. Ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Paramètres, puis Général.
3. Si l'agrégation entre régions n'est pas activée, la page Général affiche l'option permettant d'activer l'agrégation entre régions. Seuls les comptes d'administrateur et les comptes autonomes peuvent activer l'agrégation entre régions.
4. Si l'agrégation entre régions est activée, l'onglet Régions affiche les informations suivantes :
   - La Région d'accueil
   - S'il faut regrouper automatiquement les résultats, les ressources et les tendances des nouvelles régions prises en charge par Security Hub et dans lesquelles vous avez choisi de participer
   - La liste des régions liées (si certaines sont sélectionnées)

Mise à jour des paramètres d'agrégation entre régions

Vous pouvez mettre à jour vos paramètres actuels d'agrégation interrégionale dans AWS Security Hub en modifiant les régions liées ou la région d'origine actuelle.

Les modifications apportées à l'agrégation interrégionale ne sont pas mises en œuvre pour une région optionnelle tant que vous n'avez pas activé cette région dans votre AWS compte. Les régions qui AWS ont été introduites le 20 mars 2019 ou après cette date sont des régions facultatives.

Lorsque vous arrêtez d'agréger les données d'une région liée, AWS Security Hub ne supprime aucune donnée agrégée existante de cette région qui est accessible dans la région d'origine.

Vous ne pouvez pas utiliser les procédures de mise à jour décrites dans cette section pour modifier la région d'origine. Pour modifier la région d'origine, vous devez effectuer les opérations suivantes :

1. Supprimez la configuration d'agrégation interrégionale actuelle. Pour obtenir des instructions, veuillez consulter the section called “Supprimer l'agrégation”.
2. Choisissez la région dans laquelle vous souhaitez devenir la nouvelle région d'origine.
3. Activez l'agrégation entre régions. Pour obtenir des instructions, veuillez consulter the section called “Activer l'agrégation”.

Vous devez mettre à jour la configuration d'agrégation interrégionale à partir de la région d'origine actuelle.

Pour modifier les régions associées (console)

1. À partir du compte administrateur ou d'un compte autonome, ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Connectez-vous à la région d'agrégation actuelle.
3. Dans le menu de navigation de Security Hub, choisissez Paramètres, puis Général.
4. Pour Cross-Region l'agrégation, choisissez Modifier.
5. Pour les régions liées, mettez à jour les régions liées sélectionnées.
6. Choisissez Enregistrer.

Suppression de l'agrégation entre régions

Si vous ne souhaitez pas que AWS Security Hub regroupe les données, vous pouvez supprimer votre agrégateur de recherche. Vous pouvez également conserver votre agrégateur de recherche mais ne lier aucune AWS région à la région d'origine en mettant à jour l'agrégateur existant pour qu'aucune région liée ne soit sélectionnée.

Pour modifier votre région d'origine, vous devez supprimer votre agrégateur de recherche actuel et en créer un nouveau.

Lorsque vous supprimez votre agrégateur de recherche, Security Hub arrête d'agréger les données. Il ne supprime aucune donnée agrégée existante de la région d'origine.

Supprimer l'agrégateur de recherche (console)

Vous pouvez supprimer votre agrégateur de recherche de la région d'origine actuelle uniquement.

Dans les régions autres que la région d'origine, le panneau Recherche d'agrégation de la console Security Hub affiche un message indiquant que vous devez modifier la configuration dans la région d'origine. Choisissez ce message pour afficher un lien permettant de passer à la région d'origine.

Pour arrêter l'agrégation entre régions (console)

1. Ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Assurez-vous d'être connecté à votre région d'origine actuelle.
3. Dans le menu de navigation de Security Hub, choisissez Paramètres, puis Général.
4. Dans la Cross-Region section Agrégation, choisissez Modifier.
5. Sous Région d'agrégation, choisissez Aucune région d'agrégation.
6. Choisissez Enregistrer.
7. Dans la boîte de dialogue de confirmation, dans le champ de confirmation, tapez**`Confirm`**.
8. Choisissez Confirmer.

Intégrer Security Hub à Microsoft Azure

Pour surveiller vos ressources Microsoft Azure, vous pouvez intégrer Microsoft Azure à AWS Security Hub. Security Hub active ensuite automatiquement la gestion de la posture et la gestion des vulnérabilités pour votre environnement Azure et génère des résultats et d'autres données sur votre environnement. Vous n'avez pas besoin d'activer les services de sécurité Azure : toutes les fonctionnalités sont assurées par. AWS Plus précisément, le service vous fournit les éléments suivants :

CIS Microsoft Azure Foundations Benchmark v4.0 et meilleures pratiques Azure Foundational

Contrôles de conformité automatisés par rapport à la norme CIS Azure v4.0 et à la norme Azure Foundational Best Practices. Ces normes couvrent les contrôles d'identité, de mise en réseau, de stockage, de journalisation et de base de données.

Gestion de la vulnérabilité

Amazon Inspector analyse automatiquement vos machines virtuelles Azure, vos applications fonctionnelles et les images de conteneurs Azure Container Registry (ACR) à la recherche de vulnérabilités logicielles via le connecteur lié à un service.

> **Note**
>
> L'analyse des machines virtuelles nécessite la configuration d'Amazon EC2 Systems Manager dans la même région. Pour plus de détails sur la configuration, consultez la documentation Amazon Inspector relative à l'intégration d'Azure.

Corrélation d'exposition

Détection automatique des ressources Azure exposées en fonction de l'accessibilité du réseau, de l'accès public et des combinaisons de mauvaises configurations.

Alertes de détection des menaces Microsoft Defender pour le cloud

Si vous configurez l'exportation continue d'Azure Defender vers l'Event Hub, Security Hub ingère les alertes de détection des menaces de Defender for Cloud et les mappe au format Open Cybersecurity Schema Framework (OCSF). Ils apparaissent à côté de votre gestion de la posture et de vos résultats de vulnérabilité dans la console Security Hub.

Inventaire des actifs

Un inventaire complet de vos ressources Azure découvertes grâce à l'intégration, visible dans la console Security Hub à côté de vos AWS ressources.

Format OCSF

Security Hub génère tous les résultats au format Open Cybersecurity Schema Framework (OCSF), fournissant un schéma cohérent entre AWS les résultats d'Azure.

Pour créer l'intégration, vous devez connecter votre environnement Azure à Security Hub en suivant le processus suivant :

1. Vous configurez votre environnement Azure avec un enregistrement d'application, des informations d'identification fédérées, des attributions de rôles Azure et une infrastructure Event Hub.
2. À l'aide de la console Security Hub, vous créez un connecteur pour l'intégration. Vous spécifiez votre ID de locataire Azure, votre ID client d'application, votre étendue de surveillance et la région Event Hub.
3. Security Hub crée les rôles et les ressources liés aux services nécessaires dans votre. Compte AWS

4. AWS Config collecte les données de configuration des ressources à partir de votre environnement Azure.

   AWS Config est utilisé en interne pour collecter les données de configuration des ressources. Contrairement à AWS la gestion de la posture, dans laquelle vous devez explicitement activer AWS Config et payer pour l'enregistrement, Azure Posture Management gère AWS Config automatiquement. Vous n'avez pas besoin d'activer AWS Config séparément, de configurer un enregistreur ou de payer séparément pour AWS Config l'utilisation. Ces coûts sont inclus dans la tarification de votre Security Hub.
5. Security Hub commence à recevoir les données de configuration des ressources et les événements du journal d'activité de votre environnement Azure.
6. Security Hub génère des informations sur la gestion de la posture et les vulnérabilités de votre environnement Azure.

Comment ? AWS Config est utilisé

AWS Config est utilisé en interne pour collecter les données de configuration des ressources et détecter les modifications dans votre environnement Azure. Le connecteur gère cela automatiquement. Vous n'avez pas besoin d'activer AWS Config séparément, de configurer un enregistreur ou de payer pour AWS Config l'utilisation. Ces coûts sont inclus dans la tarification de votre Security Hub pour les ressources Azure.

Informations supplémentaires

Lorsque vous créez l'intégration, Security Hub crée également automatiquement les intégrations liées aux services correspondantes dans Security Hub CSPM et Amazon Inspector. Ces intégrations liées à des services garantissent que l'étendue de vos contrôles CSPM et de vos analyses de vulnérabilité de l'inspecteur correspond à la portée que vous définissez dans Security Hub. Si vous souhaitez modifier la portée, vous devez effectuer les modifications dans le Security Hub. Vous ne pouvez pas modifier une intégration liée à un service directement dans Security Hub CSPM ou Inspector.

Vous pouvez également créer une intégration Azure directement dans Security Hub CSPM et spécifier des paramètres de portée indépendants. L'intégration CSPM fonctionne alors indépendamment de l'intégration Security Hub et peut avoir une portée d'abonnement Azure et de région Azure différentes.

Pour plus d'informations sur l'estimation et le calcul des coûts liés à l'intégration de Security Hub à Azure, consultez AWS la rubrique Tarification de Security Hub.

Rubriques

- Conditions requises pour intégrer Security Hub à Microsoft Azure
- Configuration de Microsoft Azure pour l'intégrer à Security Hub
- Configuration de Security Hub pour l'intégrer à Microsoft Azure
- Supprimer un connecteur Microsoft Azure dans Security Hub

Conditions requises pour intégrer Security Hub à Microsoft Azure

Avant d'intégrer Microsoft Azure à AWS Security Hub, effectuez les tâches suivantes dans votre environnement AWS et dans Azure. Cela permet de garantir que vous et Security Hub disposez des ressources et des autorisations dont vous avez besoin pour surveiller vos ressources Azure.

Rubriques

- Prérequis pour AWS
- Prérequis pour Microsoft Azure

Prérequis pour AWS

Vérifiez que vous avez les éléments suivants dans votre Compte AWS :

AWS Security Hub activé

Security Hub doit être activé à Compte AWS l' Région AWS endroit où vous souhaitez créer le connecteur. Vous devez activer Security Hub avant de créer un connecteur Azure.

AWS Security Hub CSPM activé

Security Hub CSPM doit être activé dans le même Compte AWS et. Région AWS L'intégration Azure repose sur Security Hub CSPM pour l'évaluation de la configuration des ressources.

Autorisations IAM de la console

Le principal IAM qui crée le connecteur doit disposer des autorisations suivantes :

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

IAM Outbound Identity Federation activée

Vous devez activer IAM Outbound Identity Federation dans votre. Compte AWS Cette fonctionnalité permet aux AWS services de s'authentifier auprès de fournisseurs d'identité externes (tels que Microsoft Entra ID) à l'aide d'informations d'identification fédérées plutôt que de secrets de longue durée.

Après avoir activé Outbound Identity Federation, notez l'URL de l'émetteur du jeton. Cette URL suit le format suivant :

```
https://uuid.tokens.sts.global.api.aws
```

Vous aurez besoin de cette URL pour configurer les informations d'identification fédérées dans Azure.

Prérequis pour Microsoft Azure

Vérifiez que vous disposez des éléments suivants dans votre environnement Azure :

Locataire Azure

Vous devez disposer d'un locataire Azure dans le cloud commercial Azure. Azure Government et Azure China ne sont pas pris en charge.

Disponibilité du journal des identifiants Microsoft Entra

L'enregistrement des ressources nécessite les journaux d'audit Microsoft Graph et les journaux de connexion de votre client Microsoft Entra ID. Certains journaux Microsoft Entra ID nécessitent une licence Microsoft Entra ID P1 ou P2.

Si le locataire ne dispose pas des journaux requis, l'enregistrement des ressources peut signaler des défaillances partielles. L'enregistrement de l'application et les attributions de rôles Azure ne fournissent pas les données de journal manquantes.

Rôle d'administrateur global

Vous devez disposer du rôle d'administrateur global dans Microsoft Entra ID pour configurer l'environnement Azure. Ce rôle est requis pour enregistrer des applications, accorder l'autorisation de l'administrateur aux autorisations de l'API Microsoft Graph, attribuer des rôles RBAC au niveau du groupe de gestion racine du locataire et configurer les paramètres de diagnostic pour les journaux d'audit Entra ID.

Outre Global Administrator, vous avez besoin des rôles Azure RBAC suivants pour créer les ressources requises par l'intégration :

- Administrateur d'accès utilisateur (ou propriétaire) au niveau de l'étendue racine (`/`) : pour attribuer des rôles RBAC au niveau du groupe de gestion racine du locataire.
- Contributeur (ou propriétaire) des politiques de ressources au sein du groupe de gestion racine du locataire : pour créer les définitions et les attributions des politiques Azure qui automatisent les paramètres de diagnostic et les mesures correctives.
- Contributeur (ou propriétaire) au niveau de l'abonnement qui héberge l'Event Hub, pour créer l'espace de noms Event Hub et les ressources associées.

> **Note**
>
> Dans de nombreuses organisations, l'administrateur global Azure et l'administrateur AWS de la sécurité sont des personnes différentes. La configuration d'Azure peut être effectuée indépendamment à l'aide du script de configuration généré.

Une fois ces tâches terminées, vous êtes prêt à configurer votre environnement Azure.

Configuration de Microsoft Azure pour l'intégrer à Security Hub

Après avoir effectué les tâches préalables, vous pouvez configurer votre environnement Microsoft Azure pour prendre en charge l'intégration avec AWS Security Hub. Pour vous aider à le faire, la console Security Hub génère un script de configuration personnalisé en fonction de votre configuration.

Pour générer le script de configuration

1. Ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/advanced/home ? region=us-est-1. .
2. Dans le volet de navigation, choisissez Intégrations.
3. Choisissez Créer un connecteur Azure.
4. Terminez la configuration du connecteur (ID du locataire, étendue et nom), puis copiez le script de configuration généré.

Pour exécuter le script, utilisez l'interface de ligne de commande Azure et authentifiez-vous avec un compte d'administrateur global (`az login`).

Lorsque vous exécutez le script, il exécute une série de tâches. Les sections suivantes décrivent chaque tâche exécutée par le script. Si votre organisation restreint l'exécution des scripts, vous pouvez effectuer ces tâches manuellement, en vous servant de cette rubrique comme guide. Après avoir configuré votre environnement Azure, vous pouvez configurer Security Hub pour l'intégrer à Azure.

Les étapes 1 à 7 configurent la base partagée utilisée par toutes les fonctionnalités de Security Hub : enregistrement de l'application, informations d'identification fédérées, attributions de rôles Azure, autorisations Microsoft Graph, Event Hub et exportation des journaux. Étapes 8 à 10 : configurez les ressources Azure supplémentaires pour des fonctionnalités spécifiques :

- Gestion des vulnérabilités (Amazon Inspector) : configure l'exportation des événements du référentiel Azure Container Registry (ACR) et une identité gérée attribuée par le système sur vos machines virtuelles Azure.
- Détection des menaces (Microsoft Defender pour le cloud) : configure Microsoft Defender pour le cloud afin d'exporter en continu les alertes de sécurité vers l'Event Hub.

> **Note**
>
> Un seul enregistrement d'application Azure est partagé entre les services AWS de sécurité. Si vous utilisez également Security Hub CSPM ou Amazon Inspector pour Azure, ils utilisent le même enregistrement d'application. Il n'est pas nécessaire de créer des inscriptions distinctes pour chaque AWS service.

Tâches

- Étape 1 : enregistrer une application Azure
- Étape 2 : Création d'un responsable de service
- Étape 3 : Configuration des informations d'identification fédérées
- Étape 4 : Attribuer des rôles RBAC
- Étape 5 : Configuration des autorisations de l'API Microsoft Graph
- Étape 6 : configurer Azure Event Hub
- Étape 7 : Configuration du journal d'activité et exportation du journal d'audit Entra ID
- Étape 8 : Configuration de l'exportation d'Azure Container Registry
- Étape 9 : Activer une identité gérée sur les machines virtuelles Azure

- Étape 10 : Exporter les alertes Microsoft Defender pour le cloud

Étape 1 : enregistrer une application Azure

Enregistrez une nouvelle application dans Microsoft Entra ID. Cette application sert d'identité AWS utilisée pour s'authentifier auprès de votre environnement Azure à l'aide d'informations d'identification fédérées. Aucun secret client n'est requis.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Notez l'ID de l'application (client) de la sortie (l'`appId`attribut). Vous fournirez cette valeur lors de la création du connecteur dans la console Security Hub.

Étape 2 : Création d'un responsable de service

Créez un principal de service pour l'application enregistrée. Vous utilisez les attributions de rôles Azure pour accorder des autorisations au responsable du service. Le responsable du service exécute des actions dans votre environnement Azure.

```
$ az ad sp create --id application-client-id
```

Où se *`application-client-id`* trouve l'ID de l'application (client) de l'étape précédente.

Définissez l'URI de l'ID d'application lors de l'enregistrement sur`api://`*`application-client-id`*. AWS nécessite cet identifiant pour échanger des jetons fédérés avec l'application. Sans cet URI, il est AWS impossible de générer une audience de jetons fédérés valide et toutes les fonctionnalités ne parviennent pas à s'authentifier auprès d'Azure.

```
$ az ad app update \
  --id application-client-id \
  --identifier-uris "api://application-client-id"
```

Étape 3 : Configuration des informations d'identification fédérées

Configurez les informations d'identification fédérées sur l'application pour AWS permettre l'authentification sans secret client. Cela permet d'établir une relation de confiance OIDC entre AWS et Azure. Aucun secret ou identifiant de longue durée n'est stocké.

L'intégration de Security Hub Azure s'authentifie à l'aide d'un rôle AWS IAM par fonctionnalité : découverte de la configuration des ressources, gestion des vulnérabilités et détection des menaces. Ajoutez un identifiant d'identité fédéré pour chaque rôle afin que chaque fonctionnalité puisse s'authentifier auprès d'Azure. AWS crée automatiquement les rôles liés aux services lorsque vous créez le connecteur. Le rôle `Inspector2SSMFederationRole` utilisé pour l'analyse des machines virtuelles n'est pas lié à un service ; vous le créez dans le cadre de la configuration de l'analyse des machines virtuelles Amazon Inspector, décrite à l'étape 9.

Capacité	Objet (ARN du rôle IAM)
Découverte de la configuration des ressources (AWS Config)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty`
Gestion des vulnérabilités (Inspector)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/thirdparty.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2ThirdParty`
Gestion des vulnérabilités : analyse des machines virtuelles (Amazon EC2 Systems Manager)	`arn:aws:iam::` *`account-id`* `:role/Inspector2SSMFederationRole-` *`tenant-id`*
Détection des menaces (Security Hub)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/securityhubv2.amazonaws.com/AWSServiceRoleForSecurityHubV2`

Exécutez la commande suivante une fois pour chaque sujet du tableau précédent, en modifiant les `subject` valeurs `name` et à chaque fois. Les `audiences` valeurs `issuer` et sont les mêmes pour chaque titre d'identification.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "credential-name",
    "issuer": "token-issuer-url",
    "subject": "service-linked-role-arn",
```

```
    "audiences": ["api://AzureADTokenExchange"],
    "description": "AWS federation for Security Hub Azure integration"
  }'
```

Valeurs clés :

- Émetteur : URL de l'émetteur de votre jeton provenant de l'IAM Outbound Identity Federation. Cela suit le format`https://uuid.tokens.sts.global.api.aws`.
- Objet : ARN de rôle IAM figurant dans le tableau précédent. *`tenant-id`*Dans le rôle Amazon EC2 Systems Manager, il s'agit de votre ID de locataire Azure.
- Audience — `api://AzureADTokenExchange` (valeur standard pour la fédération des identités de la charge de travail).
- Nom : n'importe quel nom unique au sein de l'application.

Étape 4 : Attribuer des rôles RBAC

Attribuez les rôles intégrés suivants au responsable du service :

- Reader : accorde un accès en lecture seule à toutes les ressources Azure, afin que Security Hub puisse découvrir et évaluer les configurations de vos ressources. Attribuez ce rôle à la portée racine (`/`).
- Contributeur : accorde l'accès en écriture dont Amazon Inspector a besoin pour analyser vos machines virtuelles Azure, vos applications fonctionnelles et vos images de conteneurs à la recherche de vulnérabilités. Attribuez ce rôle au niveau du groupe de gestion racine du locataire, qui le propage à chaque abonnement du locataire.
- Récepteur de données Azure Event Hubs : AWS permet de lire les événements depuis l'Event Hub. Attribuez ce rôle au niveau du groupe de gestion racine du locataire.

> **Attribuer Reader à la portée racine**
>
> Assurez-vous d'attribuer le rôle Reader à la portée racine (`/`), et non à l'étendue du groupe de gestion racine du locataire. Security Hub lit les ressources d'attribution de rôles Azure à tous les niveaux, y compris les attributions définies à la racine du locataire. Une attribution Reader au niveau du groupe de gestion racine ne couvre pas les affectations dont la portée est limitée. Sans elle`/`, les lectures échouent avec une erreur d'autorisation et le connecteur peut entrer dans un état dégradé.

Le contributeur accorde un accès à l'écriture à l'ensemble du locataire

Le rôle de contributeur dans la portée du groupe de gestion racine du locataire confère un accès en écriture hautement privilégié à l'échelle du locataire à vos ressources Azure. Security Hub a besoin de cet accès pour qu'Amazon Inspector puisse analyser vos ressources informatiques à la recherche de vulnérabilités. Par exemple, Inspector utilise les autorisations d'exécution de commandes de machine virtuelle fournies par Contributor. Grâce à Amazon EC2 Systems Manager Automation, Inspector exécute des commandes sur vos machines virtuelles Azure pour installer et utiliser l'agent VM Scanner.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Contributor" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

Root-scope l'affectation nécessite un accès élevé

L'attribution d'un rôle à la portée racine (/) nécessite un accès élevé. Si l'attribution d'un rôle échoue, vérifiez que la gestion des accès pour les ressources Azure est définie sur Oui dans Microsoft Entra ID > Propriétés. Déconnectez-vous puis reconnectez-vous pour actualiser votre jeton.

Supprimer l'élévation temporaire de la racine

L'activation de la gestion des accès pour les ressources Azure confère à l'administrateur connecté le rôle d'administrateur de l'accès utilisateur à la racine (/), qui peut gérer l'accès à tous les abonnements et groupes de gestion du locataire. Une fois l'intégration terminée,

redéfinissez Gestion de l'accès pour les ressources Azure sur Non dans Microsoft Entra ID > Propriétés, enregistrez et déconnectez-vous afin que cette élévation ne reste pas active.

Étape 5 : Configuration des autorisations de l'API Microsoft Graph

Accordez les autorisations d'API Microsoft Graph suivantes (type d'application) à l'application, puis accordez le consentement de l'administrateur :

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Étape 6 : configurer Azure Event Hub

AWS Config utilise un Azure Event Hub pour recevoir des notifications en temps quasi réel concernant les modifications de configuration des ressources dans votre environnement Azure. Le script de configuration crée l'infrastructure Event Hub et l'étiquette à des fins de découverte. La découverte d'Event Hub utilise une résolution basée sur les balises : Security Hub recherche une balise dans l'espace de noms Event Hub dont le format permet `AWSConfig-account-id-region` d'identifier l'instance d'Event Hub appropriée pour votre intégration.

```
$ az group create \
```

```
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Après avoir créé le hub d'événements, balisez l'espace de noms à découvrir et attribuez le rôle de récepteur de données. Utilisez `az tag update` with `--operation merge` pour conserver toutes les autres balises de l'espace de noms (comme la balise de découverte de détection des menaces de l'étape 10) :

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> Dans le format tag`AWSConfig-account-id-region`, `account-id` il s'agit de votre Compte AWS identifiant à 12 chiffres et `region` de l' Région AWS endroit où vous créez

le connecteur (par exemple,`us-east-1`). Ces valeurs identifient Compte AWS la région propriétaire de cette intégration d'Event Hub.

Configuration des touches :

- Namespace SKU — Standard (obligatoire pour les groupes de consommateurs).
- Nom du hub d'événements —`activitylog`.
- Groupe de consommateurs —`AWSConfig`.
- Tag — `AWSConfig-`*`account-id`*`-`*`region`* avec valeur`activitylog`. Ce tag permet AWS Config de découvrir automatiquement l'Event Hub.
- Attribution de rôle : récepteur de données Azure Event Hubs dans l'espace de noms.

Pour la détection des menaces, la configuration crée également un `defender-alerts` Event Hub distinct avec un groupe de `AWSSecurityHub` consommateurs et ajoute une deuxième balise de découverte au format `AWSSecurityHub-`*`account-id`*`-`*`region`* qui identifie les hubs que Security Hub lit directement. Pour plus d'informations, reportez-vous à l'étape 10.

Étape 7 : Configuration du journal d'activité et exportation du journal d'audit Entra ID

Configurez Azure pour exporter les journaux d'activité et les journaux d'identification Microsoft Entra vers l'Event Hub.

Exportation du journal d'activité :

Configurez les paramètres de diagnostic de chaque abonnement pour exporter les journaux d'activité vers l'Event Hub. Le script de configuration le configure automatiquement pour tous les abonnements surveillés. Les journaux d'activité capturent l'activité au niveau de l'abonnement, y compris les attributions de rôles et les modifications de ressources.

Exportation du journal des identifiants Microsoft Entra :

Configurez les paramètres de diagnostic sur Microsoft Entra ID pour exporter les journaux vers le même Event Hub. Accédez à Microsoft Entra ID > Surveillance > Paramètres de diagnostic > Ajouter un paramètre de diagnostic. Activez AuditLogs SignInLogs, et NonInteractiveUserSignInLogs, et acheminez-les vers votre Event Hub.

Étape 8 : Configuration de l'exportation d'Azure Container Registry

Security Hub analyse les images de vos conteneurs Azure Container Registry (ACR) à la recherche de vulnérabilités via Amazon Inspector. Pour ce faire, Inspector a besoin que les événements du référentiel ACR soient exportés vers un Event Hub situé dans la même région Azure que le registre. Pour la configuration de l'exportation ACR, consultez la section Configuration d'Amazon Inspector pour l'intégrer à Microsoft Azure dans le guide de l'utilisateur d'Amazon Inspector.

Étape 9 : Activer une identité gérée sur les machines virtuelles Azure

Security Hub analyse vos machines virtuelles Azure via Inspector. Une identité gérée attribuée par le système doit être activée pour chaque machine virtuelle Azure cible. Pour ajouter automatiquement cette identité à vos machines virtuelles, attribuez deux politiques Azure qui utilisent l'`modify`effet au niveau du groupe de gestion racine du locataire :

- Pour une machine virtuelle qui n'a aucune identité, la politique ajoute une identité gérée attribuée par le système.
- Pour une machine virtuelle qui ne possède qu'une identité attribuée par l'utilisateur, la politique ajoute une identité gérée attribuée par le système tout en préservant les identités attribuées aux utilisateurs existantes.

Une machine virtuelle qui possède déjà une identité gérée attribuée par le système reste inchangée. Comme les politiques utilisent `modify` cet effet, elles ajustent l'identité en place sans redéployer la machine virtuelle.

Inspector utilise Amazon EC2 Systems Manager Automation pour déployer et gérer l'agent Inspector VM Scanner sur vos machines virtuelles Azure. Cela nécessite une configuration supplémentaire AWS, notamment un fournisseur d'identité IAM OIDC pour Microsoft Entra ID et plusieurs rôles IAM. Pour la configuration complète de l'analyse des machines virtuelles, consultez la section Configuration d'Amazon Inspector pour l'intégrer à Microsoft Azure dans le guide de l'utilisateur d'Amazon Inspector.

Étape 10 : Exporter les alertes Microsoft Defender pour le cloud

Security Hub ingère les alertes de détection des menaces de Microsoft Defender for Cloud et les mappe au format Open Cybersecurity Schema Framework (OCSF). Pour diffuser ces alertes, créez un hub d'`defender-alerts`événements dédié et configurez Microsoft Defender pour Cloud pour y exporter en permanence les alertes de sécurité.

Dans l'espace de noms Event Hub de l'étape 6, créez l'`defender-alerts`Event Hub, un groupe de `AWSSecurityHub` consommateurs auquel Security Hub pourra lire, et une règle d'autorisation de signature d'accès partagé (SAS) à portée de hub avec l'autorisation d'envoi utilisée par Microsoft Defender for Cloud pour envoyer des alertes :

```
$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "defender-alerts" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "AWSSecurityHub"

$ az eventhubs eventhub authorization-rule create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "DefenderExportSend" \
  --rights Send
```

Fusionnez ensuite une deuxième balise de découverte dans l'espace de noms afin que Security Hub découvre le `defender-alerts` hub. Utilisez `az tag update` with `--operation merge` pour conserver la balise de `AWSConfig` découverte de l'étape 6 :

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSSecurityHub-account-id-region=defender-alerts"
```

Enfin, configurez l'exportation continue de Microsoft Defender for Cloud du type de données Alertes de sécurité vers l'`defender-alerts`Event Hub. Dans le portail Azure, accédez à Microsoft Defender for Cloud > Paramètres d'environnement, sélectionnez l'abonnement, choisissez Exportation continue > Event Hub, sélectionnez Alertes de sécurité, puis choisissez `defender-alerts` Event Hub et la règle `DefenderExportSend` SAS.

> **Note**
>
> Si vous configurez l'exportation continue par programmation (via l'API Azure Resource Manager, un modèle ARM ou Azure Policy) plutôt que depuis le portail, authentifiez l'exportation vers l'Event Hub à l'aide de la chaîne de connexion `DefenderExportSend` SAS. Récupérez-le avec `az eventhubs eventhub authorization-rule keys list` pour la `DefenderExportSend` règle et définissez-le comme chaîne de connexion de l'action d'exportation. Pour plus d'informations, consultez la section Configurer l'exportation continue dans la documentation Microsoft Azure.

> **Note**
>
> Une fois ces tâches terminées, attendez environ 15 à 30 minutes pour que la configuration soit effective. Vérifiez ensuite que votre Event Hub reçoit des messages (la IncomingMessages métrique) avant de créer le connecteur dans Security Hub.

Configuration de Security Hub pour l'intégrer à Microsoft Azure

Après avoir effectué les tâches préalables et configuré votre environnement Microsoft Azure, vous pouvez configurer AWS Security Hub pour l'intégrer à Azure. Pour configurer Security Hub afin de l'intégrer à Azure, vous devez créer un connecteur. Vous pouvez créer le connecteur à partir d'un compte administrateur délégué ou du compte de gestion. Une fois le connecteur créé, les événements suivants se produisent :

1. Security Hub valide les informations d'identification Azure et la connectivité à votre environnement Azure. Ce processus peut prendre plusieurs minutes.
2. Security Hub crée des connecteurs liés à des services dans Security Hub CSPM et Amazon Inspector. Ces connecteurs garantissent que les contrôles de gestion de la posture et l'analyse des vulnérabilités correspondent à la portée que vous avez définie dans Security Hub.
3. AWS Config commence à découvrir les ressources Azure à l'aide des informations d'identification fédérées.
4. Security Hub active automatiquement la norme CIS Microsoft Azure Foundations Benchmark v4.0 et la norme Azure Foundational Best Practices dans CSPM pour vos ressources Azure.

5. Les premiers résultats commencent à apparaître dans les 15 à 30 minutes pour les ressources contenant des événements du journal d'activité. L'évaluation complète de toutes les ressources existantes peut prendre jusqu'à 24 heures.

Rubriques

- Création d'un connecteur Azure
- Ajuster la portée d'un connecteur Azure
- Vérifier l'état d'un connecteur Azure
- Résoudre les problèmes liés à un connecteur Azure
- Comment Security Hub gère les ressources et trouve les identifiants

Création d'un connecteur Azure

Pour créer un connecteur Microsoft Azure pour votre environnement, effectuez les étapes suivantes à l'aide de la console AWS Security Hub ou de l'API.

1. Ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/advanced/home ? region=us-est-1. .
2. Dans le volet de navigation, choisissez Intégrations.
3. Choisissez Créer un connecteur Azure.
4. Dans la section Fonctionnalités de sécurité, choisissez si vous souhaitez que la fonction d'analyse réseau soit activée. Cette fonctionnalité est activée par défaut pour le compte sur lequel vous activez l'intégration Azure et peut être décochée avant de terminer la configuration de votre connecteur. Si une politique d'organisation bloque cette fonctionnalité pour votre compte, elle n'apparaît pas comme une option. Pour plus d'informations, consultez la section Analyse du réseau dans Security Hub.
5. Pour Azure Tenant ID, entrez votre identifiant de locataire Microsoft Entra ID. Vous pouvez le trouver sur le portail Azure sous Microsoft Entra ID > Propriétés > Tenant ID.
6. Pour l'ID de l'application (client), entrez l'ID de l'application Azure que vous avez enregistrée lors de la configuration de l'environnement Azure.
7. Configurez des paramètres supplémentaires et l'étendue du connecteur en procédant comme suit :

    - Dans le champ Nom, entrez un nom unique pour le connecteur. Le nom peut contenir jusqu'à 50 caractères alphanumériques et peut inclure des traits d'union.

> **Note**
>
> Le nom du connecteur ne peut pas être modifié après sa création.

- Dans le champ Description, entrez éventuellement une brève description du connecteur. La description peut contenir jusqu'à 200 caractères.

> **Important**
>
> Les noms et les descriptions sont utilisés pour identifier votre contenu. N'y incluez pas d'informations sensibles, confidentielles ou personnellement identifiables (PII).

- Pour les abonnements, choisissez Tous les abonnements pour surveiller tous les abonnements actuels et futurs du locataire, ou Abonnements spécifiques pour surveiller uniquement les abonnements que vous spécifiez. Si vous choisissez de ne surveiller que des abonnements spécifiques, entrez l'identifiant de chacun d'entre eux.
- Pour les régions, choisissez Toutes les régions pour surveiller les ressources dans toutes les régions Azure, ou Régions spécifiques pour surveiller uniquement les régions que vous spécifiez.

> **Note**
>
> Si vous avez déjà créé un connecteur dans Security Hub CSPM ou Amazon Inspector pour le même locataire Azure, la portée du connecteur dans Security Hub doit inclure les mêmes abonnements et régions que le connecteur dans Security Hub CSPM ou Amazon Inspector.

> **Note**
>
> Les contrôles qui évaluent les ressources Microsoft Entra ID et Microsoft Graph nécessitent l'inclusion de l'étendue de la région globale dans votre configuration d'intégration. Si vous sélectionnez uniquement des régions Azure spécifiques, ces contrôles ne génèrent pas de résultats.

8. Vérifiez la configuration du connecteur.

> **Note**
>
> Si vous envisagez d'utiliser Amazon Inspector pour l'analyse des machines virtuelles Azure, vous devez créer les rôles IAM requis. Pour en savoir plus, consultez the section called "Rôles IAM pour l'analyse des machines virtuelles".

9. Lorsque vous avez fini de saisir et de vérifier les paramètres, choisissez Créer un connecteur.

Rôles IAM pour l'analyse des machines virtuelles Azure via Amazon Inspector

Pour activer l'analyse des vulnérabilités via Amazon Inspector, vous devez créer les ressources IAM suivantes dans votre Compte AWS.

Fournisseur d'identité IAM OIDC

Créez un fournisseur d'identité IAM OIDC pour Microsoft Entra ID avec la configuration suivante :

- URL de l'émetteur : `https://sts.windows.net/tenant-id/`
- Liste des identifiants clients : `api://app-id`, `api://AzureADTokenExchange`
- Empreinte numérique : chaîne de 40 caractères composée uniquement de zéros (`0`répétée 40 fois). AWS STS valide les jetons via le point de terminaison JWKS plutôt que la valeur de l'empreinte numérique.

Inspector2VmScannerRole-*tenant-id*

Utilisé par l'agent Amazon Inspector VM Scanner qui s'exécute sur les machines virtuelles Azure pour envoyer la télémétrie de numérisation à Amazon Inspector. Ce rôle utilise la fédération d'identité Web OIDC via le fournisseur Microsoft Entra ID d'identité.

Politique de confiance :

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

```
                "Federated": "arn:aws:iam::account-id:oidc-provider/
sts.windows.net/tenant-id/"
            },
            "Action": "sts:AssumeRoleWithWebIdentity"
        }
    ]
}
```

Étiquettes :

- `inspector-managed` = `true`

Politique d'autorisation (TelemetryPolicy) :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2-telemetry:*",
            "Resource": "*"
        }
    ]
}
```

Inspector2SSMFederationRole-***tenant-id***

Active la fédération OIDC vers Azure pour une authentification sécurisée entre les clouds. Ce rôle est assumé par le AssumeRole et DispatchRole, et par Amazon EC2 Systems Manager, pour obtenir des jetons d'identité Web pour les opérations Azure.

Politique de confiance :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "sts:AssumeRole",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalTag/caller": "SSM"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
                        "arn:aws:iam::account-id:role/Inspector2SSMDispatchRole-tenant-
id"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Politique d'autorisation (FederationPolicy) :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "sts:IdentityTokenAudience": [
                        "api://AzureADTokenExchange"
                    ]
                }
            },
            "Action": [
                "sts:GetWebIdentityToken",
                "sts:TagGetWebIdentityToken"
            ],
            "Resource": "*",
            "Effect": "Allow"
```

```
        }
    ]
}
```

Étiquettes :

- `caller` = `SSM`
- `inspector-managed` = `true`

Inspector2SSMAssumeRole-*tenant-id*

Exécute Amazon EC2 Systems Manager Automation pour intégrer les machines virtuelles Azure en tant qu'instances gérées. Ce rôle crée et gère les activations hybrides, transmet les rôles à Amazon EC2 Systems Manager et extrait les documents d'automatisation.

Politique de confiance :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Politique d'autorisation (AssumeRolePolicy) :

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

```
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/
AmazonEC2RunCommandRoleForManagedInstances",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateActivation",
                "ssm:DeleteActivation",
                "ssm:DescribeActivations",
                "ssm:DescribeInstanceInformation",
                "ssm:PutConfigurePackageResult",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:AddTagsToResource",
            "Resource": [
                "arn:aws:ssm:*:account-id:activation/*",
                "arn:aws:ssm:*:account-id:managed-instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetDocument",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:*:document/AWS-InstallSsmAgentOnAzure",
                "arn:aws:ssm:*::document/AmazonInspector2-InspectorVmScanner"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ssm:GetCloudConnector",
            "Resource": "*"
        }
    ]
}
```

Étiquettes :

- `caller` = `SSM`
- `AzureTenantId` = *`tenant-id`*
- `AzureApplicationId` = *`app-id`*
- `inspector-managed` = `true`

Inspector2SSMDispatchRole-***`tenant-id`***

Corrige les cibles des machines virtuelles Azure et distribue l'installation de l'agent Amazon Inspector VM Scanner via Amazon EC2 Systems Manager Automation. Ce rôle lance les exécutions d'automatisation et les transmet AssumeRole à Amazon EC2 Systems Manager.

Politique de confiance :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Politique d'autorisation (DispatchPolicy) :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:account-id:automation-execution/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:ListCloudConnectors",
                "ssm:GetCloudConnector",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Étiquettes :

- `caller` = `SSM`
- `inspector-managed` = `true`

Prérequis pour l'analyse des machines virtuelles

L'URI de l'ID d'application pour l'enregistrement de l'application Azure doit être défini sur`api://app-id`.

Une identité gérée attribuée par le système doit être activée pour chaque machine virtuelle Azure que vous souhaitez scanner. Pour attribuer automatiquement une identité gérée aux nouvelles machines virtuelles, utilisez une DeployIfNotExists politique dans votre environnement Azure.

Une fois le connecteur créé, Security Hub commence à surveiller votre environnement Azure. Vous pouvez vérifier l'état du connecteur sur la page Intégrations.

Ajuster la portée d'un connecteur Azure

Après avoir créé un connecteur Microsoft Azure, vous pouvez ajuster la portée du connecteur en modifiant les abonnements Azure ou les régions Azure qu'il surveille. Les modifications de périmètre prennent généralement effet dans un délai de 15 à 30 minutes pour les ressources contenant des événements du journal d'activité. L'évaluation complète des abonnements Azure récemment ajoutés peut prendre jusqu'à 24 heures.

Avant de régler la portée d'un connecteur, tenez compte des points suivants :

- Lorsque vous modifiez la portée d'un connecteur dans Security Hub, les connecteurs liés aux services associés dans Security Hub CSPM et Amazon Inspector sont automatiquement mis à jour en conséquence.
- La portée d'un connecteur Security Hub ne peut jamais être inférieure à celle de n'importe quel connecteur géré par le client existant dans Security Hub CSPM ou Amazon Inspector pour le même locataire Azure.
- Si vous ajoutez une région au périmètre du connecteur, vous devez réexécuter le script de configuration pour provisionner l'infrastructure Event Hub dans la nouvelle région. La configuration actuelle de votre Event Hub n'est pas affectée.

Vérifier l'état d'un connecteur Azure

Vous pouvez vérifier l'état d'un connecteur Microsoft Azure à tout moment pour vous assurer que Security Hub reçoit des données de votre environnement Azure.

Pour vérifier l'état d'un connecteur

1. Ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/advanced/home ? region=us-est-1. .
2. Dans le volet de navigation, choisissez Intégrations et sélectionnez votre connecteur Azure.
3. Vérifiez que l'état du connecteur indique Actif. Si le connecteur indique Actif, la vérification est terminée. S'il affiche un statut différent, consultezthe section called "Résoudre les problèmes liés à un connecteur".
4. Accédez à Résultats et filtrez par `ResourceCloudProviders = Azure` pour confirmer que les résultats sont générés pour vos ressources Azure.
5. Consultez la page Normes de sécurité pour confirmer que la norme CIS Azure v4.0 affiche les contrôles en statut PASSED ou FAILED (pas tous NO_DATA).

> **Note**
>
> L'état de santé du connecteur est finalement constant. Lorsqu'un problème d'autorisation ou de configuration survient, l'état du connecteur passe rapidement à Dégradé avec un message exploitable. Cependant, une fois le problème résolu, le retour à l'état Connecté peut prendre jusqu'à 24 heures.
>
> - Un état dégradé après une correction récente n'indique pas nécessairement un problème persistant.
> - Pour une visibilité en temps réel des échecs d'enregistrement, vérifiez les CloudWatch métriques dans l'espace de noms.

Résoudre les problèmes liés à un connecteur Azure

Si vous rencontrez des problèmes avec votre connecteur, consultez les problèmes courants et les solutions suivants.

L'état du connecteur n'est pas sain

Ce problème se produit généralement si les informations d'identification fédérées ne sont pas configurées correctement dans Azure.

Pour résoudre ce problème, vérifiez que l'URL de l'émetteur du jeton et l'ARN du sujet de vos informations d'identification fédérées Azure correspondent aux vôtres Compte AWS.

Aucun résultat après 30 minutes

Ce problème peut se produire si l'Event Hub ne reçoit pas de journaux d'activité.

Pour résoudre ce problème, vérifiez que les paramètres de diagnostic sont configurés sur vos abonnements Azure et que l'espace de noms Event Hub est correctement balisé. `AWSConfig-`*`account-id`*`-`*`region`*

Toutes les commandes affichent NO_DATA

Ce problème peut survenir si le connecteur est désactivé ou si vous AWS Config ne pouvez pas accéder à votre environnement Azure.

Pour résoudre ce problème, vérifiez que le connecteur est activé et que le principal du service possède le rôle de lecteur au niveau du groupe de gestion racine du locataire.

Impossible d'enregistrer certaines ressources Azure

L'erreur peut se produire pour l'une des raisons suivantes :

- L'environnement Azure ne répond pas aux conditions requises pour l'enregistrement des ressources.
- L'enregistrement de l'application ne nécessite pas le consentement de l'administrateur pour les autorisations de l'API Microsoft Graph.
- L'attribution du rôle de lecteur ne couvre pas tous les domaines d'application requis.
- Le locataire Microsoft Entra ID ne dispose pas des données de journal requises.

Pour corriger l'erreur, procédez comme suit :

1. Pour vérifier que votre environnement répond à toutes les exigences, consultez la section Prérequis pour Microsoft Azure.
2. Vérifiez que l'enregistrement de l'application dispose des autorisations requises pour l'API Microsoft Graph avec le consentement de l'administrateur.

3. Vérifiez que le responsable du service possède le rôle de lecteur dans l'étendue du groupe de gestion racine du locataire.

Les résultats apparaissent uniquement pour certains abonnements

Ce problème peut se produire si l'exportation du journal d'activité n'est pas configurée pour tous les abonnements cibles.

Pour résoudre ce problème, vérifiez que les paramètres de diagnostic couvrent tous les abonnements inclus dans le champ d'application du connecteur.

Comment Security Hub gère les ressources et trouve les identifiants

En activant votre intégration Azure pour AWS Security Hub, les identifiants de recherche de ressources et de sécurité d'autres fournisseurs de cloud sont stockés dans AWS Config Security Hub et dans d'autres AWS services (selon les besoins) sous forme de métadonnées liées à la gestion de la configuration des ressources correspondante et des données de recherche de sécurité collectées auprès des autres fournisseurs de cloud. Ces identifiants ne constituent pas votre contenu. N'y incluez pas d'informations sensibles, confidentielles ou personnellement identifiables.

Les identifiants suivants de votre environnement cloud connecté sont stockés et utilisés par pour fournir des AWS fonctionnalités de sécurité multicloud :

- Identifiants de ressources : ID de locataire Azure, ID d'abonnement, emplacement (région), ID de ressource (ID ou noms de groupes de ressources, fournisseur de ressources, type de ressource)
- Identifiants de détection de sécurité : identificateurs uniques attribués à chaque résultat de sécurité généré par le service de détection.

Les relations entre ces identifiants, y compris la manière dont les ressources sont liées les unes aux autres et la manière dont les résultats sont liés aux ressources, sont également stockées sous forme de métadonnées de service. AWS utilise ces identifiants pour la corrélation des ressources, l'association des résultats aux ressources, la journalisation des opérations des services et la déduplication.

Supprimer un connecteur Microsoft Azure dans Security Hub

Après avoir créé un connecteur Microsoft Azure dans AWS Security Hub, vous pouvez le supprimer à tout moment. Si vous supprimez un connecteur, Security Hub cesse d'effectuer des contrôles de gestion de la posture et de surveiller les vulnérabilités pour votre environnement Azure. Security

Hub cesse également de générer de nouvelles découvertes et d'autres données concernant votre environnement. Vos résultats existants sont conservés pendant 90 jours. L'inventaire des ressources reste tel qu'il était lorsque le connecteur a été supprimé et est supprimé au bout de 90 jours.

Lorsque vous supprimez un connecteur, Security Hub supprime automatiquement les connecteurs liés aux services associés dans AWS Security Hub CSPM et Amazon Inspector. Security Hub ne supprime pas l'enregistrement de l'application Azure et l'infrastructure Event Hub dans votre environnement Azure. Vous devez les supprimer manuellement, directement dans Microsoft Azure. Pour savoir comment procéder, consultez la section Supprimer une application dans la documentation Microsoft Azure.

Pour supprimer un connecteur Azure

1. Ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/advanced/home ? region=us-est-1. .
2. Dans le volet de navigation, choisissez Intégrations.
3. Sélectionnez le connecteur que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer).
5. Lorsque vous y êtes invité, confirmez que vous souhaitez supprimer le connecteur.

> **Important**
>
> Si vous supprimez un connecteur et en créez un nouveau dans les 6 heures, la détection des ressources peut prendre jusqu'à 6 heures. Planifiez la suppression et la recréation du connecteur en conséquence.

Travailler dans le tableau de bord récapitulatif de Security Hub

Le tableau de bord récapitulatif de la console Security Hub affiche une vue d'ensemble de vos expositions, menaces, ressources et couverture de sécurité sur l'ensemble des widgets de sécurité. Vous pouvez personnaliser le tableau de bord en ajoutant et en supprimant des widgets et en créant et en appliquant des ensembles de filtres pour récupérer les données de chaque widget.

Considérations

Avant d'interagir avec le tableau de bord, tenez compte des points suivants :

- Les personnalisations telles que les ensembles de filtres enregistrés ou les modifications apportées à la disposition des widgets sont enregistrées automatiquement.
- Les données sont automatiquement actualisées chaque fois que vous ouvrez le tableau de bord.
- Si vous configurez l'agrégation entre régions, le tableau de bord inclut les résultats de toutes vos régions associées (lorsque vous consultez le tableau de bord dans votre région d'origine).

Tenez compte des points suivants si votre compte est un compte d'administrateur délégué pour une organisation, un compte de membre d'une organisation ou un compte autonome.

- Les personnalisations effectuées par un compte administrateur délégué seront enregistrées indépendamment des personnalisations effectuées par les comptes membres. Les personnalisations peuvent inclure des ensembles de filtres enregistrés ou des modifications de la disposition des widgets.
- Si votre compte est le compte d'administrateur délégué d'une organisation, les données incluent les résultats relatifs à votre compte et aux comptes des membres.
- Si votre compte est un compte de membre d'une organisation ou un compte autonome, les données incluent les résultats uniquement pour votre compte.

Il est recommandé de ne pas inclure d'informations confidentielles, sensibles ou personnellement identifiables (PII) dans les ensembles de filtres enregistrés, les widgets personnalisés ou d'autres champs de texte libre connexes.

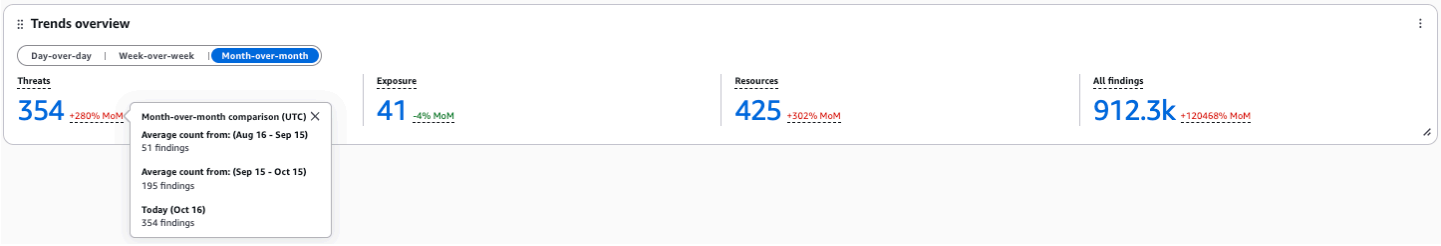
Widgets disponibles

Vous pouvez interagir avec différents widgets dans les onglets Exécutif et Triage du tableau de bord Résumé. L'onglet Exécutif comprend des widgets qui affichent les données relatives aux tendances relatives à vos expositions, à vos menaces et à vos ressources, ainsi que le widget Couverture de sécurité pour vous aider à suivre la couverture de votre compte en fonction des différentes fonctionnalités de sécurité. L'onglet Triage comprend des widgets qui affichent un résumé de vos expositions, de vos menaces et de vos ressources. Cependant, vous pouvez ajouter des widgets, supprimer des widgets et gérer la position de chaque widget dans les deux onglets pour personnaliser votre expérience.

Widgets de tendances

Les widgets suivants affichent les données relatives aux tendances relatives à vos expositions, à vos menaces et à vos ressources, afin que vous puissiez les analyser au fil du temps.

Widget de présentation des tendances



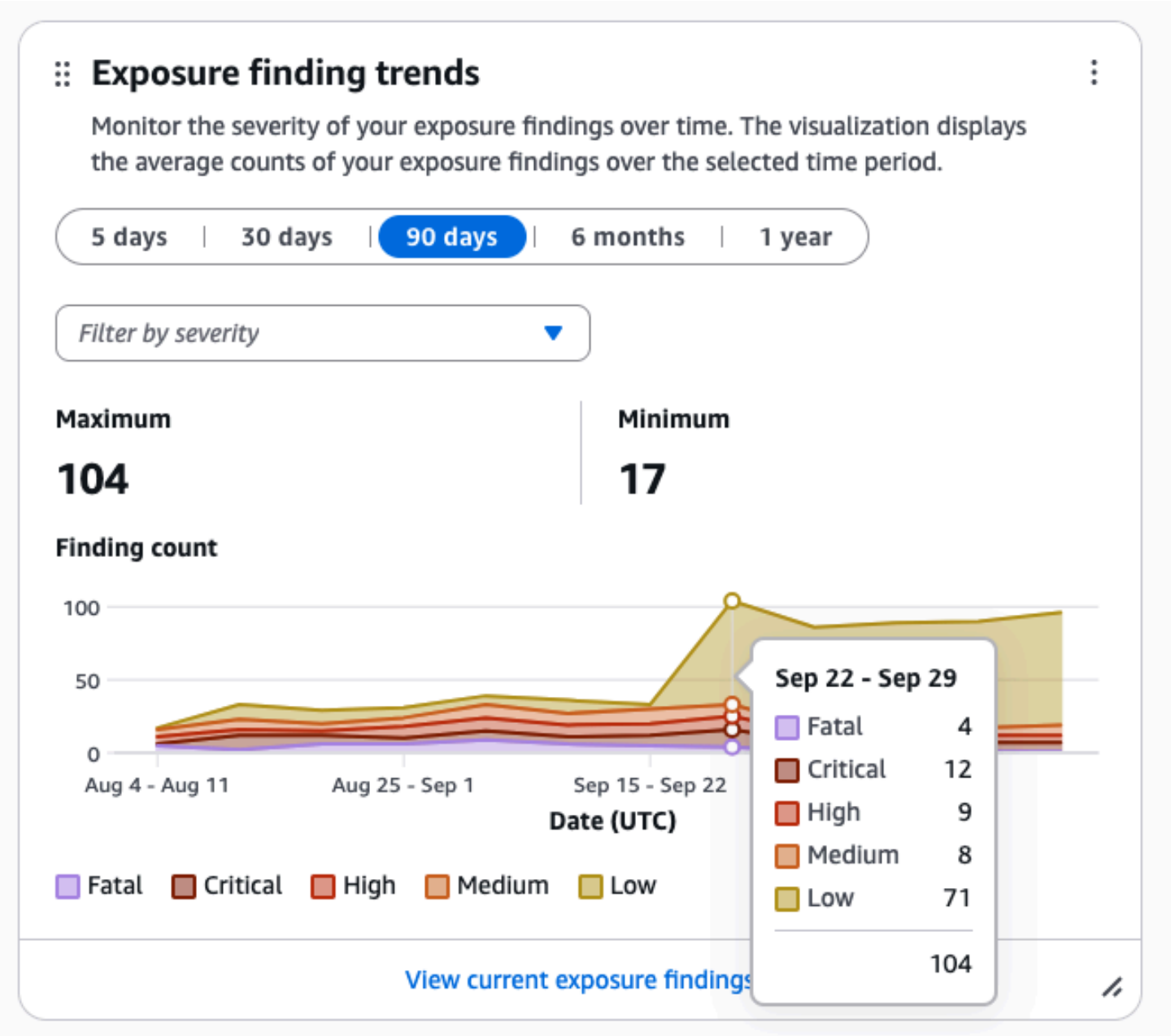
Ce widget affiche un aperçu de vos expositions, de vos menaces, de vos ressources et de vos résultats au cours des périodes suivantes :

- Month-over-monthreflète le décompte d'une période à l'autre au cours des deux derniers mois.
- Week-over-weekreflète le décompte d'une période à l'autre au cours des deux dernières semaines.
- Day-over-dayreflète le décompte d'une période à l'autre au cours des deux derniers jours.

Le chiffre à côté du pourcentage reflète le décompte moyen d'une période à l'autre à ce jour. Le choix de ce numéro vous dirige vers le tableau de bord correspondant dans la console. Si vous accédez à un autre tableau de bord qui affiche des données de tendances, celui-ci affiche uniquement les données relatives aux tendances des 90 derniers jours ou de la période la mieux adaptée si votre compte ne contient pas de résultats ou de ressources datant de plus de 30 jours.

> **Note**
>
> Pour recevoir des données dans ce widget, vous devez activer les services de sécurité suivants :
>
> - AWS Security Hub CSPM — Pour recevoir des données sur les expositions
> - Amazon Inspector — Pour recevoir des données sur les expositions
> - GuardDuty— Pour recevoir des données sur les menaces

Widget de recherche des tendances d'exposition



Ce widget affiche la gravité de vos résultats d'exposition au cours des périodes suivantes :

- 5 jours
- 30 jours
- 90 jours
- 6 mois
- 1 an

La visualisation affiche le nombre moyen de vos résultats au cours de la période sélectionnée.

Filtres de gravité

Vous pouvez mettre à jour le graphique en incluant ou en excluant les filtres de gravité suivants :

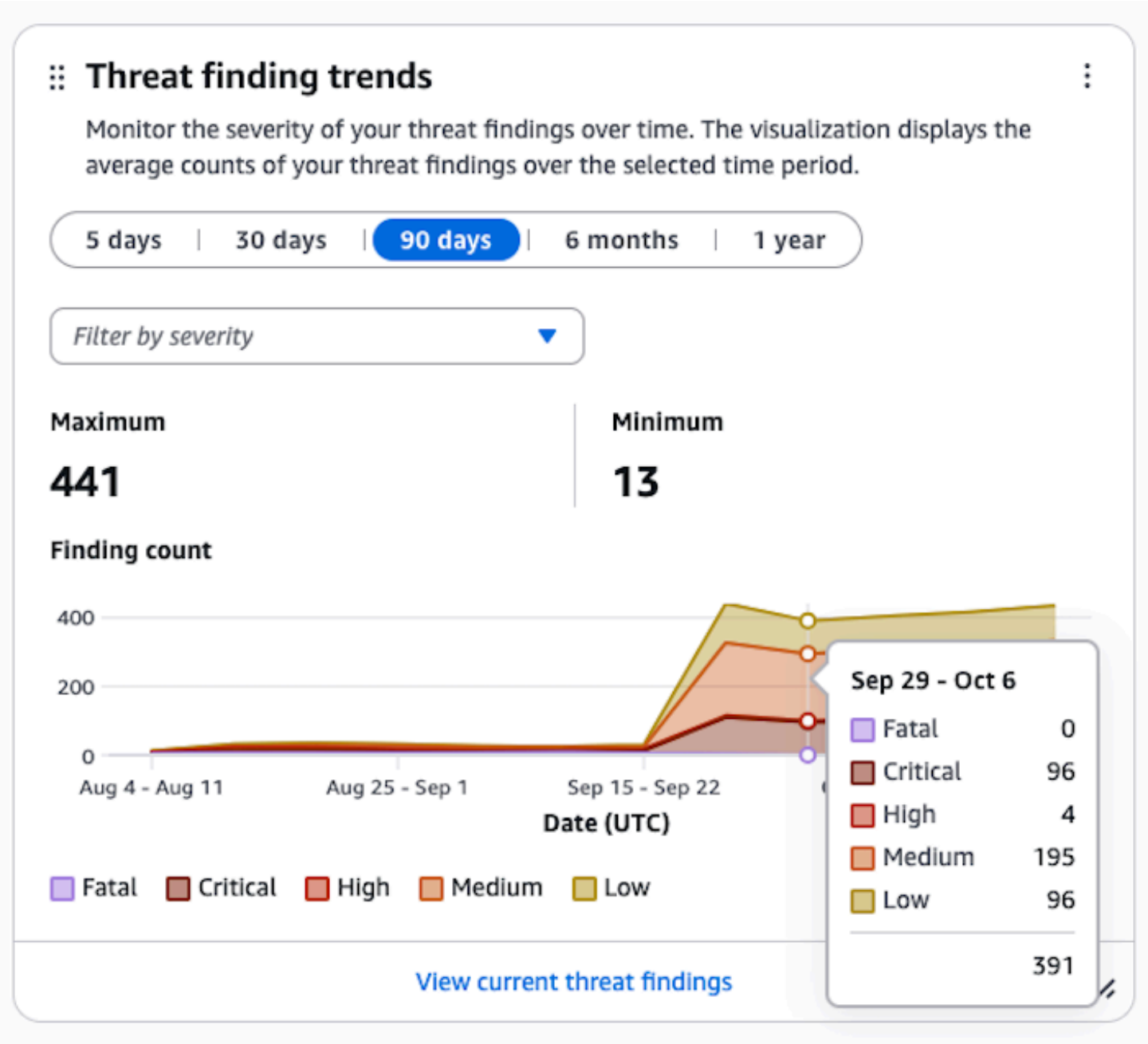
- Fatale
- Critical (Critique)
- Élevée
- Moyenne
- Faible
- Informatif
- Autre
- Inconnu

Les filtres de sévérité appliqués apparaissent en bas de la visualisation dans différentes cases. Vous pouvez passer la souris sur la visualisation pour consulter le nombre moyen de résultats obtenus à des moments spécifiques. Vous pouvez également consulter le nombre moyen de résultats correspondant à chaque filtre de gravité appliqué.

Vous pouvez choisir Afficher tous les résultats d'exposition actuels pour être redirigé vers le tableau de bord de l'exposition. Par défaut, le tableau de bord Exposure affiche uniquement les données relatives aux tendances des 90 derniers jours. Si votre compte ne contient aucun résultat d'exposition datant de plus de 30 jours, le tableau de bord affiche les données relatives aux tendances en fonction de la période la mieux adaptée.

> **Note**
>
> Pour recevoir des données dans ce widget, vous devez activer Amazon Inspector et Security Hub CSPM.

Widget de tendances de détection des menaces



Ce widget affiche la gravité des menaces détectées au cours des périodes suivantes :

- 5 jours
- 30 jours
- 90 jours
- 6 mois
- 1 an

La visualisation affiche le nombre moyen de vos résultats au cours de la période sélectionnée.

Filtres de gravité

Vous pouvez mettre à jour le graphique en incluant ou en excluant les filtres de gravité suivants :

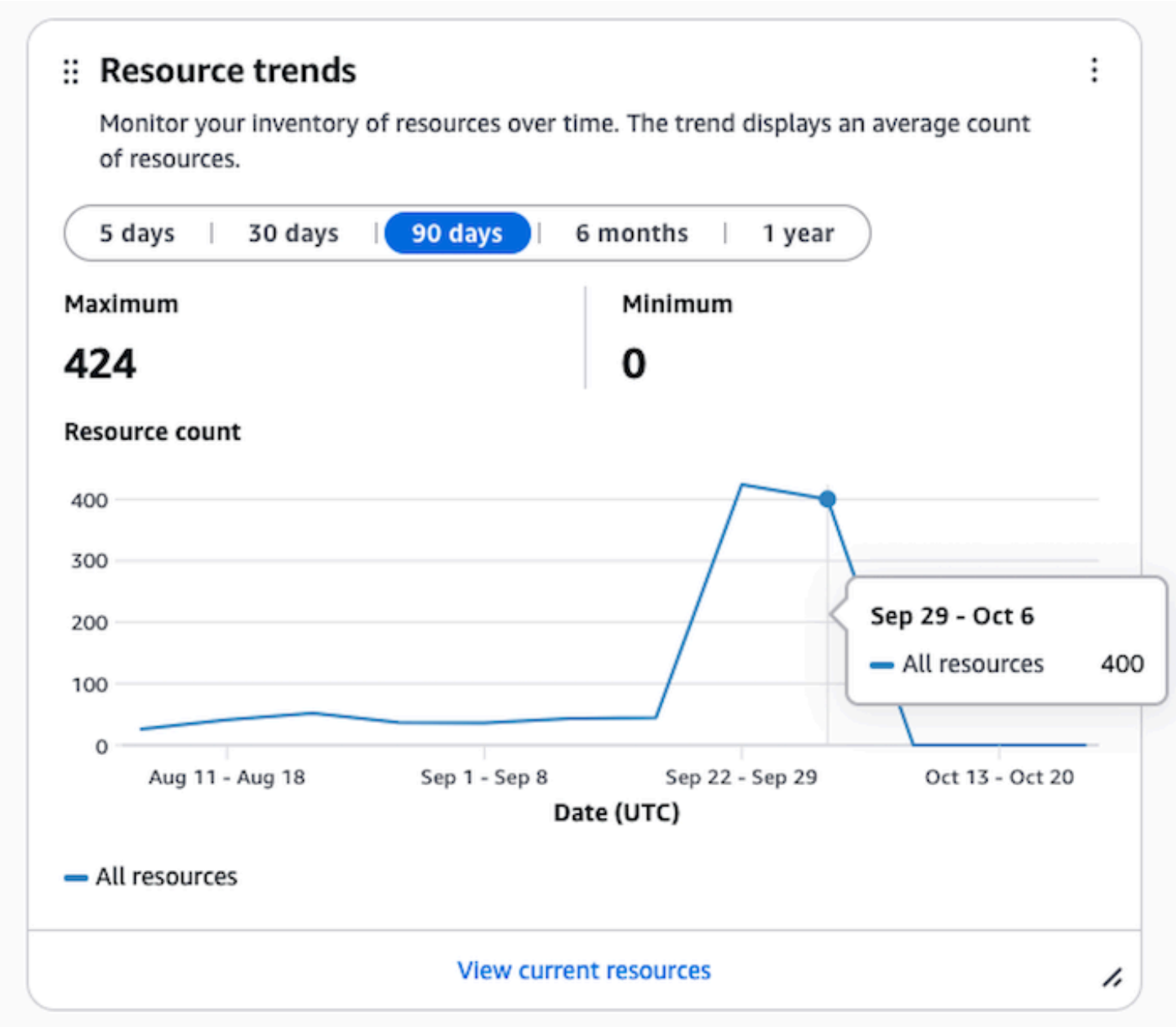
- Fatale
- Critical (Critique)
- Élevée
- Moyenne
- Faible
- Informatif
- Autre
- Inconnu

Les filtres de sévérité appliqués apparaissent en bas de la visualisation dans différentes cases. Vous pouvez passer la souris sur la visualisation pour consulter le nombre moyen de résultats obtenus à des moments spécifiques. Vous pouvez également consulter le nombre moyen de résultats correspondant à chaque filtre de gravité appliqué.

Vous pouvez choisir Afficher toutes les menaces actuelles pour être redirigé vers le tableau de bord Exposure. Par défaut, le tableau de bord des menaces affiche uniquement les données relatives aux tendances des 90 derniers jours. Si votre compte ne contient aucune information concernant une menace datant de plus de 30 jours, le tableau de bord affiche les données relatives aux tendances en fonction de la période la mieux adaptée.

> **Note**
>
> Pour recevoir des données dans ce widget, vous devez l'activer GuardDuty.

Widget de tendances en matière



Ce widget affiche un inventaire de vos ressources au cours des périodes suivantes :

- 5 jours
- 30 jours
- 90 jours
- 6 mois
- 1 an

La visualisation affiche le nombre moyen de vos ressources sur la période sélectionnée. Vous pouvez passer la souris sur la visualisation pour consulter le nombre moyen de ressources pour des moments spécifiques.

Vous pouvez choisir Afficher les ressources actuelles pour être redirigé vers le tableau de bord des ressources. Par défaut, le tableau de bord Ressources affiche uniquement les données relatives aux tendances des 90 derniers jours. Si votre compte ne contient pas de ressources datant de plus de 30 jours, le tableau de bord affiche les données relatives aux tendances en fonction de la période la mieux adaptée.

Ce widget affiche un inventaire de vos ressources au cours des périodes suivantes :

- 5 jours
- 30 jours
- 90 jours
- 6 mois
- 1 an

Conservation des données en fonction des tendances

Security Hub conserve les données relatives aux tendances pendant un an pour toutes les Comptes AWS applications où Security Hub est activé. Une fois que les données relatives aux tendances ont été conservées pendant un an, elles sont supprimées de Security Hub.

Les données de tendances relatives aux comptes d'administrateur délégué et aux comptes autonomes sont supprimées après la désactivation de Security Hub ou en cas de résiliation des comptes.

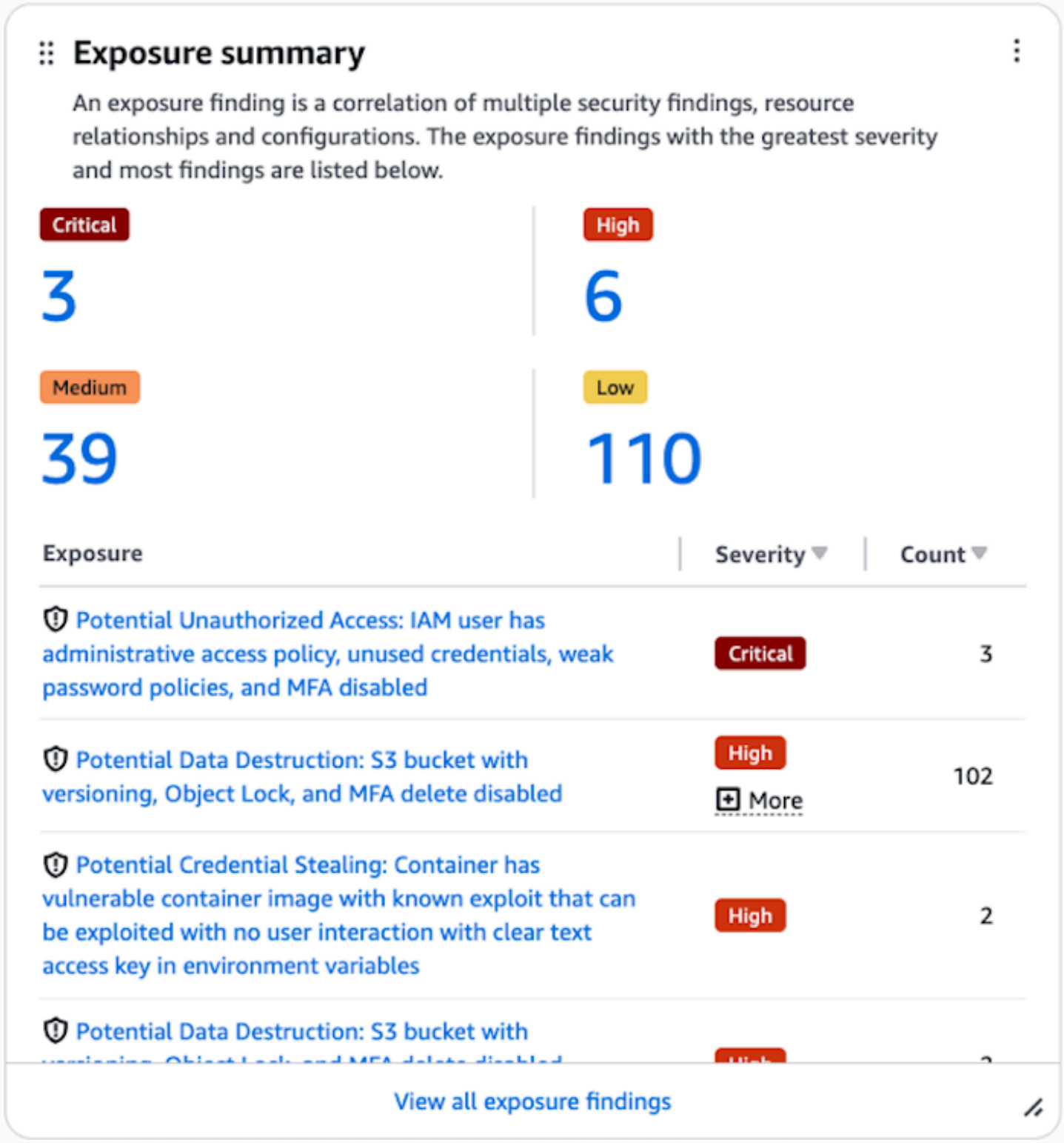
Scénarios de conservation des données relatives aux tendances pour les comptes membres sur lesquels Security Hub est activé :

- Si le compte d'un membre quitte son organisation, Security Hub conserve les données relatives aux tendances, jusqu'au moment où le compte a quitté l'organisation, pendant un an.
- Si Security Hub est désactivé pour un compte membre, Security Hub conserve les données relatives aux tendances, jusqu'à la date de désactivation du compte, pendant un an.
- Si le compte d'un membre est résilié, Security Hub dissocie les données relatives aux tendances du compte clôturé (par exemple, en effaçant l'identifiant du compte résilié) et conserve le reste des données de tendances pendant un an.

Widgets récapitulatifs

Les widgets suivants présentent un résumé de vos expositions, de vos menaces et de vos ressources.

Widget récapitulatif des expositions

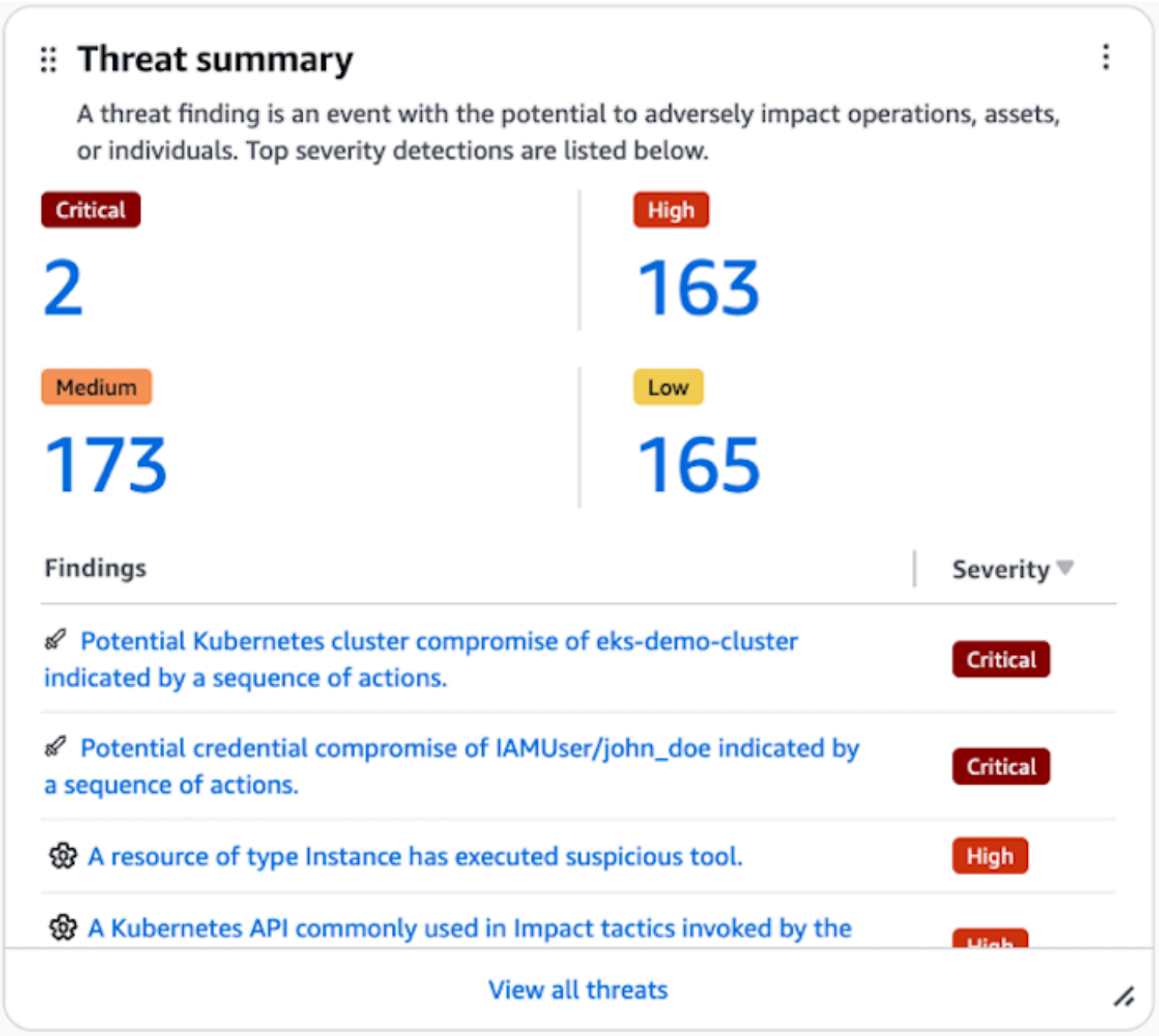


Ce widget affiche vos expositions par niveau de gravité. Une exposition est basée sur une analyse des résultats et des caractéristiques de Security Hub et d'autres services AWS de sécurité, tels

qu'Amazon Inspector. La liste des expositions de ce widget est limitée aux huit expositions les plus graves. Les expositions les plus graves apparaissent en premier dans la liste. Si deux expositions ou plus sont de gravité égale, la liste regroupe automatiquement ces expositions après les expositions les plus récentes. En choisissant Afficher toutes les expositions, vous êtes redirigé vers le tableau de bord des expositions.

> **Note**
>
> Pour recevoir des données dans ce widget, vous devez activer Amazon Inspector et Security Hub CSPM.

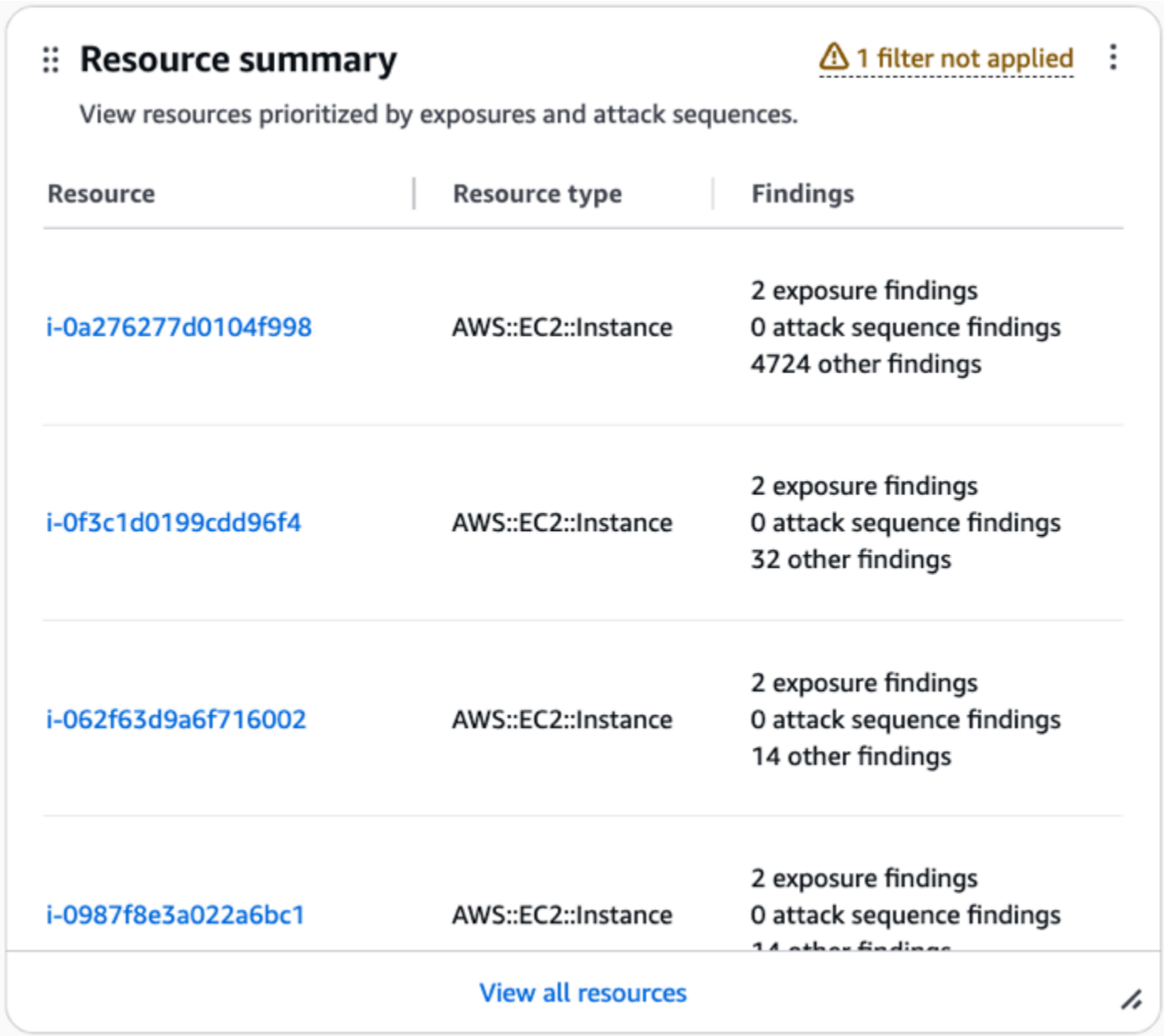
Widget récapitulatif des menaces



Ce widget affiche vos menaces par niveau de gravité. Une menace fait référence à une activité malveillante ou suspecte susceptible de compromettre la sécurité de votre environnement. La liste des menaces de ce widget est limitée aux huit menaces les plus graves. Les menaces les plus graves apparaissent en premier dans la liste. Si deux menaces ou plus sont de gravité égale, la liste regroupe automatiquement ces menaces par rapport aux menaces les plus récentes. Choisissez Afficher toutes les menaces pour accéder au tableau de bord des menaces.

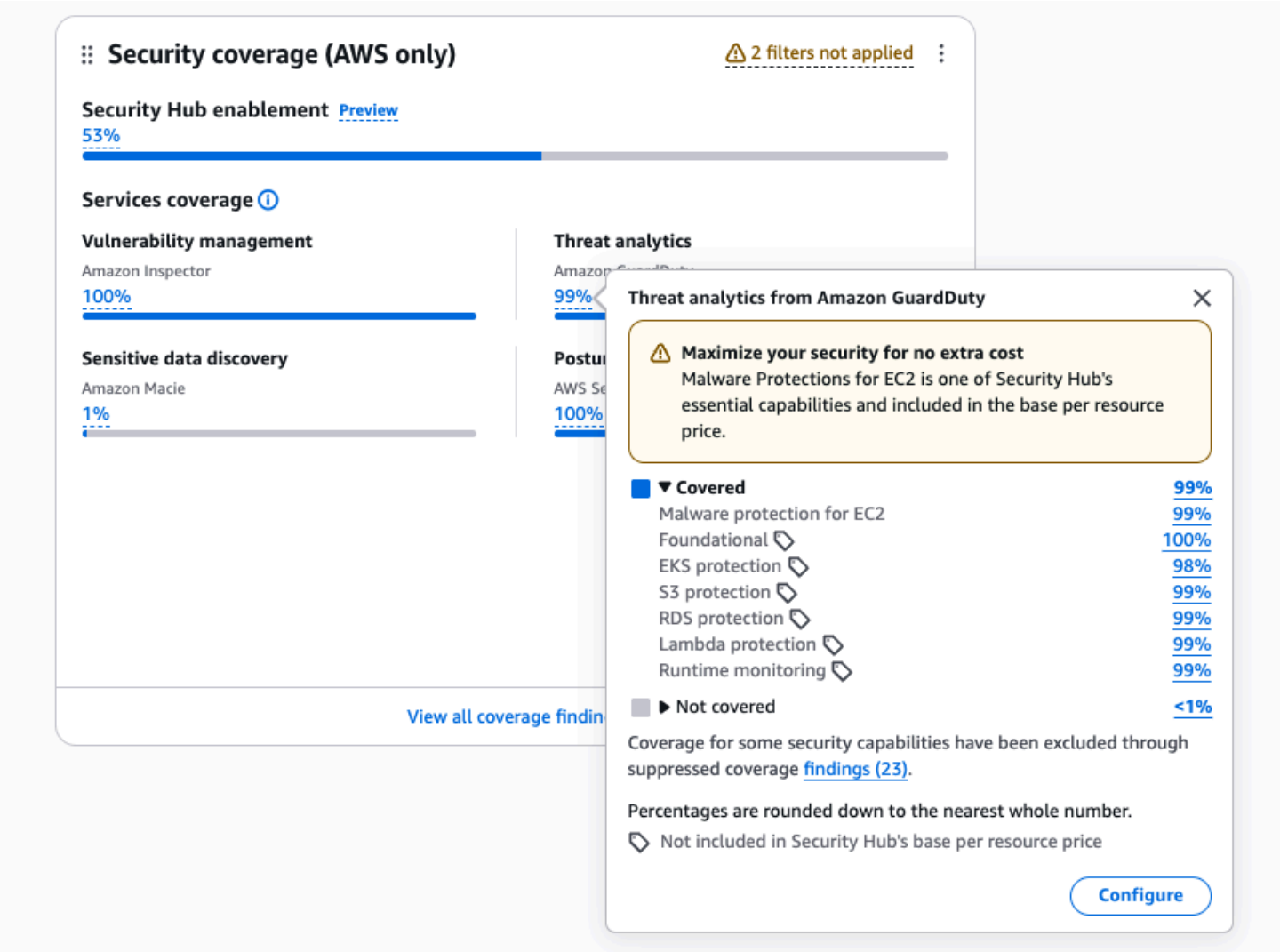
> **Note**
>
> Pour recevoir des données dans ce widget, vous devez l'activer GuardDuty.

Widget récapitulatif des ressources



Ce widget affiche les ressources par type et les résultats associés aux ressources. Les ressources sont classées par ordre de priorité en fonction des expositions et des séquences d'attaques. Choisir Afficher toutes les ressources vous dirige vers le tableau de bord des ressources.

Widget de couverture de sécurité



Le widget affiche un résumé de la couverture de votre compte pour les fonctionnalités de sécurité suivantes :

- Gestion des vulnérabilités par Amazon Inspector
- Détection des menaces par Amazon GuardDuty
- Découverte de données sensibles par Amazon Macie
- Gestion de la posture par AWS Security Hub CSPM

Dans les comptes d'administrateur délégué, le widget affiche également la couverture du compte pour l'activation de Security Hub.

Chaque élément de couverture affiche un pourcentage représentant l'activation de cette fonctionnalité sur vos comptes. Le choix d'un pourcentage affiche les détails relatifs à la couverture de cette capacité. Le choix du pourcentage d'activation de Security Hub affiche un panneau latéral. Le panneau indique le nombre de comptes activés dans chaque région de votre organisation.

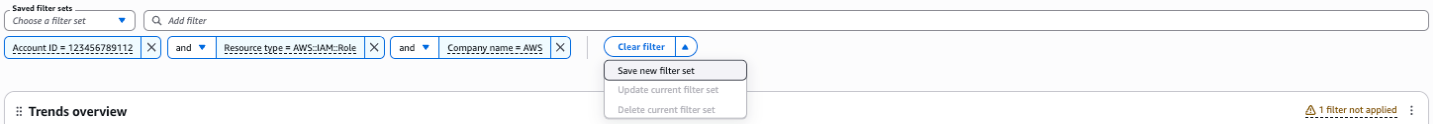
Dans la section Couverture des services, les pourcentages représentent la proportion de contrôles de couverture réussis pour chaque capacité de sécurité. Ces contrôles concernent les comptes et les régions dans lesquels Security Hub est activé. Le choix d'un pourcentage de couverture affiche une fenêtre contextuelle qui classe chaque fonctionnalité comme Couverte (vérification réussie) ou Non couverte (échec de la vérification). Les pourcentages sont arrondis au nombre entier inférieur le plus proche. Le choix d'un pourcentage dans la fenêtre contextuelle ouvre la page des résultats de couverture avec des détails sur les résultats qui constituent ce pourcentage. Choisissez Configurer pour ouvrir le service individuel dans lequel vous pouvez gérer la configuration de cette fonctionnalité, ou pour ouvrir la page des configurations de Security Hub où vous pouvez mettre à jour vos configurations pour les services de sécurité.

Si l'un de vos résultats de couverture dans Security Hub est supprimé, le widget affiche un message vous informant que la couverture a été exclue : La couverture des fonctionnalités de sécurité a été exclue par le biais de résultats de couverture supprimés.

Pour plus d'informations sur l'affichage et la suppression des résultats de couverture, voir Résultats de couverture dans Security Hub.

Filtres disponibles

Vous pouvez appliquer des filtres aux widgets de sécurité à l'aide de la barre de filtre Ajouter.



Les filtres sont organisés selon les catégories suivantes :

- Filtres partagés : s'applique à tous les widgets de sécurité
- Filtres de recherche : s'applique aux widgets de sécurité qui affichent des données de recherche
- Filtres de ressources : s'applique aux widgets de sécurité qui affichent les données relatives aux ressources

Vous pouvez créer un ensemble de filtres en connectant des filtres à l'aide des opérateurs et/ou, puis en choisissant Enregistrer un nouveau jeu de filtres dans la liste déroulante.

Filtres appliqués au widget Tendances de recherche d'exposition et au widget Tendances de détection des menaces

Actuellement, les filtres pris en charge pour ces widgets sont les suivants :

- ID de compte
- Trouver le nom de la classe
- Type de résultat
- Nom du produit
- Région
- Statut

Filtres appliqués au widget Tendances des ressources

Actuellement, les filtres pris en charge pour ce widget sont les suivants :

- ID de compte
- Région
- Catégorie de ressources
- Type de ressource

Filtres non appliqués aux widgets



Si un widget ne prend pas en charge de filtre, celui-ci n'est pas appliqué au widget. Dans ce cas, le widget affiche un message d'avertissement vous indiquant combien de filtres n'ont pas été appliqués et répertorie les noms des filtres qu'il ne prend pas en charge.

Affichage des détails relatifs aux ressources dans Security Hub

La page Ressources permet de suivre les ressources communes à votre compte et à votre organisation. Vous pouvez accéder à la page Ressources de la console Security Hub en choisissant Ressources dans le volet de navigation. L'avantage de la page Ressources est qu'elle vous permet de surveiller votre niveau de sécurité, d'organiser vos ressources et de consulter les informations les concernant. Lorsque vous choisissez un type de ressource, vous pouvez consulter toutes les ressources associées à ce type de ressource. Vous pouvez consulter tous les résultats associés à une ressource. Les types de ressources disponibles sur la page Ressources incluent toutes les ressources de vos comptes couvertes par les services AWS de sécurité qui fournissent des résultats à Security Hub.

> **Note**
>
> L'administrateur délégué peut consulter toutes les ressources associées aux comptes des membres. Si vous avez configuré une page d'accueil Région AWS, vous pouvez consulter toutes les ressources qu'elle contient Région AWS depuis Linked Régions AWS.

Si vous choisissez une ressource, vous pouvez consulter les détails de cette ressource. Ces informations incluent le nom, l'ID, l'ARN, le type et la catégorie de la ressource. Vous pouvez consulter l'ID de compte associé à la ressource, la date de création de la ressource (horodatage) et l'endroit où elle a été créée (Région AWS). Vous pouvez également consulter les détails de configuration supplémentaires concernant la ressource. Ces informations se trouvent dans un extrait JSON que vous pouvez copier.

Si vous passez de l'onglet Vue d'ensemble à l'onglet Résultats, vous pouvez consulter tous les résultats associés à la ressource. L'onglet Résultats indique le nom de chaque résultat, le type de chaque résultat et la gravité de chaque résultat. Vous pouvez regrouper les résultats par différents champs et rechercher des résultats à l'aide de filtres. Si vous choisissez un résultat, vous pouvez consulter un aperçu du résultat, qui comprend des informations sur la conformité et la manière de résoudre les problèmes associés à ce résultat. L'onglet Traits affiche chaque trait qui a été identifié à propos de la ressource. Vous pouvez consulter les caractéristiques contributives qui ont été utilisées pour créer un indicateur d'exposition pour la ressource. Vous pouvez également consulter les traits contextuels, qui sont d'autres éléments de sécurité identifiés pour la ressource mais qui n'ont pas directement contribué aux résultats d'exposition. Si vous revenez à la ressource, vous pouvez choisir Ouvrir la ressource pour vérifier son type dans la console. Par exemple, si la ressource est une ressource IAM, vous pouvez l'ouvrir dans la console IAM.

La page des ressources vous propose différentes manières d'organiser et de rechercher des ressources. Vous pouvez regrouper les ressources par type. Par exemple, vous pouvez regrouper les ressources par ID de compte, type de recherche Région AWS, catégorie de ressource, nom de ressource et type de ressource. Les filtres rapides vous permettent de passer en revue les ressources par catégorie, par compte et par type de recherche.

Security Hub et Open Cybersecurity Schema Framework (OCSF)

Security Hub utilise l'Open Cybersecurity Schema Framework (OCSF) comme format standard pour toutes les informations de sécurité. Cette rubrique décrit l'OCSF et la manière dont Security Hub l'implémente.

Présentation de l'OCSF

Les résultats de Security Hub sont formatés à l'aide de l'OCSF (Open Cybersecurity Schema Framework). OCSF est un projet open source qui fournit un cadre extensible pour le développement de schémas, ainsi qu'un schéma de sécurité de base indépendant des fournisseurs. Les fournisseurs et autres producteurs de données peuvent adopter et étendre le schéma pour leurs domaines spécifiques. Les producteurs de données peuvent cartographier différents schémas pour aider les équipes de sécurité à simplifier l'ingestion et la normalisation des données, afin que les data scientists et les analystes puissent travailler avec un langage commun pour la détection et l'investigation des menaces. L'objectif est de fournir une norme ouverte, adoptée dans n'importe quel environnement, application ou solution, tout en complétant les normes et processus de sécurité existants.

Le framework comprend des types de données, un dictionnaire d'attributs et une taxonomie. Bien que cela ne soit pas limité à la cybersécurité ou aux événements, l'accent est d'abord mis sur les schémas d'événements de cybersécurité. L'OCSF est indépendant du format de stockage, des méthodes de collecte de données et des processus ETL.

Security Hub prend actuellement en charge les résultats de la version 1.6 du schéma OCSF.

Ressources connexes

Pour plus d'informations sur l'OCSF et sa mise en œuvre, consultez les ressources suivantes :

- Documentation publique de l'OCSF
- Documentation sur l'utilisation de l'extension OCSF

- Référence du schéma de base de l'OCSF
- Registre des extensions OCSF

AWS extension pour OCSF

Les schémas OCSF peuvent être étendus en ajoutant de nouveaux attributs, objets, catégories, profils et classes d'événements. Un schéma est l'agrégation d'entités et d'extensions de schéma de base.

Les extensions d'OCSF permettent à un fournisseur ou à un client particulier de compléter un schéma existant en ajoutant des attributs pour fournir une personnalisation spécifique au domaine, améliorer l'interopérabilité des données et ajouter un contexte plus détaillé pour l'analyse de sécurité.

L' AWS extension pour Open Cybersecurity Schema Framework (OCSF) fournit des définitions d'attributs pour les ressources cloud dans les événements OCSF. Cette extension ajoute un `cloud_resources` profil qui étend l'`resource_details`objet OCSF avec des attributs de ressources spécifiques au cloud. Grâce à ces attributs, les équipes de sécurité peuvent analyser les configurations des ressources, les vulnérabilités potentielles et les métadonnées de détection des menaces.

Objet **`resource_details`** étendu

L' AWS extension étend l'`resource_details`objet avec les attributs mentionnés dans la liste des références d'attributs ci-dessous. Ces attributs garantissent une identification et une classification appropriées des ressources cloud auprès des différents fournisseurs au sein de cadres d'événements standardisés.

AWS Extension pour la référence d'attribut OCSF

Les sections Attributs de base et Objets spécifiques aux ressources fournissent des exemples de chacun des attributs qui font partie de l'extension AWS OCSF de resource_details.

Chacune des définitions d'attributs contient un statut OCSF décrivant sa relation actuelle avec le schéma OCSF public :

- Existant : cet attribut figurait déjà dans la norme OCSF resource_details et fait désormais partie de l'extension. AWS
- Nouveau : L'attribut ne fait pas partie de l'OCSF et a été introduit dans le cadre de l' AWS extension. Il n'existe pas dans le schéma OCSF de base.

- Ajouté à resource_details : L'attribut est défini dans OCSF mais ne fait pas partie de resource_details.

Attributs de base

Il s'agit d'attributs fondamentaux utilisés pour l'identification des ressources, leur localisation et les métadonnées de base. Ils se composent de types de données simples tels que des chaînes, des horodatages et des tableaux.

Partition nuageuse

Partition cloud sur laquelle se trouve la ressource.

Exigence

Recommandée

Type

Chaîne

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "cloud_partition": "aws"
    }
  ]
}
```

ID du compte du propriétaire

Identifiant de compte à 12 chiffres auquel appartient la ressource.

Exigence

Recommandée

Type

Chaîne

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      }
    }
  ]
}
```

Type de ressource

Type de AWS CloudFormation ressource qui identifie le service et la ressource spécifiques.

Exigence

Obligatoire

Type

Chaîne

Format

Doit respecter AWS CloudFormation la convention de dénomination des types de ressources : `AWS::<Service>::<ResourceType>`

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "type": "AWS::EC2::Instance"
    }
  ]
}
```

Identificateur de ressource

Identifiant unique de la ressource cloud (par exemple, i-1234567890abcdef0).

Exigence

Recommandée

Type

Chaîne

Format

Il doit s'agir d'un identifiant de ressource valide. Longueur minimale de 1. Longueur maximale de 768.

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "uid": "i-1234567890abcdef0"
    }
  ]
}
```

Identifiant de ressource alternatif

L'identifiant unique de la ressource cloud, généralement l'Amazon Resource Name (ARN).

Exigence

Recommandée

Type

Chaîne

Format

Il doit s'agir d'un AWS ARN valide. Les modèles courants incluent :

- `"arn:partition:service:region:account-id:resource-id"`
- `"arn:partition:service:region:account-id:resource-type/resource-id"`
- `"arn:partition:service:region:account-id:resource-type:resource-id"`

Remarque : Certains services tels que S3 utilisent des variantes telles que arn:aws:s3 : :bucket-name (sans région ni identifiant de compte).

Statut de l'OCSF

Existing

Exemples

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
  ]
}
```

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:s3:::my-bucket-name"
    }
  ]
}
```

Nom de la ressource

Le nom unique de la ressource cloud.

Exigence

Recommandée

Type

Chaîne

Format

User-created noms dont les valeurs dépendront de l'environnement.

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "name": "My-Server-1"
    }
  ]
}
```

Région nuageuse

La AWS région où se trouve la ressource.

Exigence

Recommandée

Type

Chaîne

Format

Identifiant de région cloud valide (par exemple, us-east-1, eu-west-1, ap-southeast-2)

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "region": "us-west-2"
    }
  ]
}
```

Heure de création de la ressource

Heure à laquelle la ressource a été créée.

Exigence

Recommandée

Type

Horodatage

Format

Horodatage Unix en millisecondes depuis l'époque (1er janvier 1970, 00:00:00 UTC)

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "created_time": 1762019193000
    }
  ]
}
```

Étiquettes

Key-value paires pour les métadonnées et l'organisation des ressources.

Exigence

Recommandée

Type

Tableau d'objets key:value

Format

Un objet générique permettant de définir un couple clé:valeur.

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "tags": [
        {
          "name": "Environment",
          "value": "Production"
        },
        {
          "name": "Owner",
          "value": "SecurityTeam"
        }
      ]
    }
  ]
}
```

Adresse IP

Adresse IP associée à l'instance au format IPv4 ou IPv6.

Exigence

Facultatif

Type

Chaîne

Format

Adresse IPv4 ou IPv6 valide

Statut de l'OCSF

Existing

Exemple

```
{
  "resources": [
    {
      "ip": "10.0.1.25"
    }
  ]
}
```

Adresses IP

Tableau d'adresses IP (IPv4 ou IPv6) associées à l'appareil. Il peut s'agir d'adresses IP publiques et privées.

Exigence

Facultatif

Type

Tableau d'adresses IP

Statut de l'OCSF

Nouveau

Exemple

```
{
  "resources": [
    {
      "ip_addresses": ["10.0.1.25", "52.12.34.56"]
    }
```

```
  ]
}
```

UID EN PVC

L'ID VPC où se trouve la ressource.

Exigence

Facultatif

Type

Chaîne

Format

Identifiant VPC (par exemple, vpc-12345678900)

Statut de l'OCSF

Ajouté à `resource_details`

Exemple

```
{
  "resources": [
    {
      "vpc_uid": "vpc-0a1b2c3d4e5f6g7h8"
    }
  ]
}
```

Exemple d'objet de ressource avec des attributs de base

```
{
  "resources": [
    {
      "cloud_partition": "aws",
      "owner": {
        "account": {
          "uid": "123456789012"
        }
```

```
      },
      "region": "us-east-1",
      "type": "AWS::EC2::NetworkInterface",
      "uid": "eni-03e6c892dd45e836c",
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-03e6c892dd45e836c",
      "zone": "us-east-1f",
      "vpc_uid": "vpc-0ef6045717b0362f6"
    }
  ]
}
```

Objets spécifiques à une ressource

Il s'agit d'objets imbriqués complexes qui fournissent des informations détaillées sur des types de ressources et des services spécifiques. Chaque objet contient plusieurs champs et sous-objets avec une configuration et des métadonnées spécifiques au service.

Appareil

Attributs d'instance cloud améliorés pour les ressources de calcul, notamment les détails de chiffrement, les informations d'image, le profil d'instance et l'heure de lancement.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Ajouté à`resource_details`. Consultez la définition de l'objet du périphérique OCSF.

AWS L'extension ajoute les attributs suivants à cet objet :

- `encryption_details`- Les détails de cryptage de la ressource
- `image`- Informations sur l'image
- `instance_profile`- Le profil d'instance IAM à associer à l'instance
- `launch_time`- L'heure à laquelle l'instance a été lancée

- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource

Exemple

```
{
  "device": {
    "image": {
      "uid": "ami-99999999",
      "name": "LoadTestAMI-Current"
    },
    "instance_profile": {
      "uid": "LoadTestingInstanceProfileId",
      "uid_alt": "arn:aws:iam::012345678999:instance-profile/generated"
    },
    "launch_time": 1762019193000,
    "launch_time_dt": "2025-08-02T02:05:06Z",
    "model": "m3.xlarge",
    "network_interfaces": [
      {
        "ip": "198.51.100.0",
        "security_groups": [
          {
            "name": "LoadTestingSecurityGroupName",
            "uid": "LoadTestingSecurityId"
          }
        ],
        "uid": "eni-abcdef12"
      }
    ],
    "type": "Virtual",
    "type_id": 6,
    "uid": "i-99999999"
  }
}
```

Interface réseau

Détails et configuration de l'interface réseau, y compris les pièces jointes et les groupes de sécurité.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Ajouté à`resource_details`. Consultez la définition de l'objet de l'interface réseau OCSF.

AWS L'extension ajoute les attributs suivants à cet objet :

- `attachments`- Informations sur les pièces jointes de l'interface réseau
- `security_groups`- Tableau d'identifiants uniques de groupes de sécurité
- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource

Exemple

```
{
  "network_interface": {
    "uid": "eni-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a1b2c3d4e5f6g7h8",
    "name": "prod-web-server-eni",
    "attachments": [
      {
        "uid": "eni-attach-0abcd1234efgh5678",
        "instance_uid": "i-0123456789abcdef0",
        "name": "/dev/eth0",
        "state": "attached",
        "attach_time": 1762019193000
      }
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "web-server-sg"
      },
      {
        "uid": "sg-9i8h7g6f5e4d3c2b1",
        "name": "ssh-access-sg"
      }
    ]
  }
```

```
}
```

Dispositif de stockage

Informations sur le périphérique de stockage, y compris les pièces jointes, le cryptage et les informations de capture d'écran.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Nouveau

L'objet du périphérique de stockage inclut les attributs suivants :

- `name`- Le nom du périphérique de stockage
- `uid`- L'identifiant unique du périphérique de stockage
- `attachments`- Les pièces jointes du périphérique de stockage
- `encryption_details`- La clé de chiffrement du périphérique de stockage
- `is_encrypted`- Si le périphérique de stockage est crypté (obligatoire)
- `snapshot_id`- L'identifiant du snapshot du périphérique de stockage
- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource

Exemple

```
{
  "storage_device": {
    "is_encrypted": false,
    "name": "LocalVolumeDeviceName1",
    "snapshot_id": "snap-12345678901234567",
    "uid": "vol-09d5050dea915943d",
    "uid_alt": "arn:aws:ec2:us-west-2:123456789000:volume/vol-09d5050dea915943d"
  }
}
```

Base de données

Attributs d'instance de base de données, notamment le type de moteur, le point de terminaison et les informations utilisateur.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Ajouté à`resource_details`. Consultez la définition de l'objet de la base de données OCSF.

AWS L'extension ajoute les attributs suivants à cet objet :

- `cluster_uid`- L'identifiant du cluster de base de données
- `db_endpoint`- Le point final de la base de données
- `encryption_details`- Les détails du chiffrement de la base de données
- `engine`- Le nom du moteur de base de données (par exemple, mysql)
- `is_encrypted`- Si la base de données est cryptée
- `is_iam_authentication`- Si l'authentification IAM est activée
- `is_public`- Si la base de données est accessible au public
- `port`- Le numéro de port de la base de données
- `security_groups`- Tableau de groupes de sécurité VPC associés à l'instance de base de données
- `snapshot_details`- Les détails de l'instantané de la base de données
- `status`- L'état de la base de données (par exemple, disponible)
- `subnet_group`- Un groupe de sous-réseaux de base de données est un ensemble de sous-réseaux d'un VPC
- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource
- `user`- L'utilisateur de la base de données
- `version`- La version de la base de données

Exemple

```
{
  "database": {
    "cluster_uid": "SampleDBClusterId",
    "engine": "mysql",
    "is_iam_authentication": true,
    "is_public": false,
    "type": "Relational",
    "type_id": 1,
    "uid": "SampleDBId",
    "version": "13.6"
  }
}
```

cluster de bases de données

Attributs d'instance de base de données, notamment le type de moteur, le point de terminaison et les informations utilisateur.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Nouveau

L'objet de base de données inclut les attributs suivants :

- `uid`- L'identifiant unique du cluster de bases de données
- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource
- `name`- Le nom du cluster de bases de données
- `status`- L'état du cluster de bases de données
- `engine`- Le moteur associé au cluster
- `version`- La version du cluster de base de données

- `cluster_members`- Liste des instances de base de données qui font partie du cluster
- `security_groups`- Tableau des groupes de sécurité associés au cluster
- `is_encrypted`- Si le cluster de bases de données est chiffré
- `is_iam_authentication`- Si l'authentification IAM est activée
- `encryption_details`- Les détails du chiffrement du cluster de bases de données
- `subnet_group`- Le groupe de sous-réseaux associé au cluster
- `port`- Le numéro de port du cluster de base de données
- `zones`- Liste des zones de disponibilité
- `db_endpoint`- Point de terminaison du cluster de bases de données
- `snapshot_details`- Détails de l'instantané de la base de données

Exemple


```
{
  "db_cluster": {
    "uid": "production-aurora-cluster",
    "uid_alt": "arn:aws:rds:us-east-1:123456789012:cluster:production-aurora-cluster",
    "name": "production-aurora-cluster",
    "status": "available",
    "engine": "aurora-mysql",
    "version": "8.0.mysql_aurora.3.04.0",
    "cluster_members": [
      "instance-1",
      "instance-2"
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "db-security-group"
      }
    ],
    "is_encrypted": true,
    "is_iam_authentication": true,
    "encryption_details": {
      "key_uid": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    },
    "subnet_group": {
      "uid": "production-db-subnet-group"
```

```
    },
    "port": 3306,
    "zones": [
      "us-east-1a",
      "us-east-1b",
      "us-east-1c"
    ],
    "db_endpoint": {
      "name": "production-aurora-cluster.cluster-abc123xyz.us-
east-1.rds.amazonaws.com",
      "port": 3306
    }
  }
}
```

Fonction cloud

Attributs des fonctions cloud pour les fonctions sans serveur, notamment le gestionnaire, les couches et la configuration d'exécution.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Nouveau

L'objet de fonction cloud inclut les attributs suivants :

- `name`- Le nom de la fonction cloud
- `uid`- L'identifiant unique de la fonction cloud
- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource
- `encryption_details`- Les détails du cryptage de la fonction cloud
- `handler`- La méthode du code de fonction qui traite les événements
- `layers`- La liste des couches fonctionnelles du cloud contenant du code ou des données supplémentaires

- `runtime`- L'environnement spécifique à la langue des fonctions cloud
- `security_groups`- Tableau de groupes de sécurité associés à la fonction cloud
- `subnet_info_list`- Détails sur les sous-réseaux associés à la fonction cloud
- `user`- Informations sur l'entité IAM qui accorde à cloud_function l'autorisation d'accéder aux services
- `version`- La version avec fonction cloud
- `vpc_uid`- L'identifiant unique du VPC si la fonction cloud se trouve dans un VPC

Exemple

```
{
  "cloud_function": {
    "name": "my-lambda-function",
    "uid": "my-lambda-function",
    "uid_alt": "arn:aws:lambda:us-east-1:123456789012:function:my-lambda-function",
    "handler": "index.handler",
    "runtime": "python3.11",
    "version": "$LATEST",
    "layers": [
      {
        "name": "my-layer",
        "uid_alt": "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1",
        "version": "1"
      }
    ],
    "security_groups": [
      {
        "name": "lambda-security-group",
        "uid": "sg-0123456789abcdef0"
      }
    ],
    "subnet_info_list": [
      {
        "uid": "subnet-0a1b2c3d4e5f6g7h8"
      }
    ],
    "vpc_uid": "vpc-0ef6045717b0362f6"
  }
}
```

Seau à données

Compartiment S3 ou attributs de stockage de données.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Ajouté à`resource_details`. Consultez la définition de l'objet OCSF Databucket.

Remarque : Cet objet est ajouté à resource_details par l'extension. AWS L'objet Databucket OCSF de base est utilisé sans attributs supplémentaires.

Exemple

```
{
  "databucket": {
    "type": "S3",
    "type_id": 1,
    "uid": "my-bucket-name"
  }
}
```

Image

Informations d'image pour les ressources de calcul, y compris les détails de la plate-forme et de l'utilisation.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Ajouté à`resource_details`. Consultez la définition de l'objet OCSF Image.

AWS L'extension ajoute les attributs suivants à cet objet :

- `platform`- La plateforme du système d'exploitation de l'image
- `in_use_count`- Nombre de ressources utilisant cette image

Exemple

```
{
  "image": {
    "uid": "ami-0abcdef1234567890",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:image/ami-0abcdef1234567890",
    "name": "my-custom-ami",
    "platform": "AMAZON_LINUX_2",
    "in_use_count": 2
  }
}
```

Informations sur le sous-réseau

Informations sur le sous-réseau où se trouve la ressource.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Nouveau

L'objet d'informations de sous-réseau inclut les attributs suivants :

- `uid`- L'identifiant unique du sous-réseau
- `uid_alt`- Nom de ressource Amazon (ARN) de la ressource
- `name`- Le nom du sous-réseau
- `zone`- La zone de disponibilité
- `ip_count`- Le nombre d'adresses IP dans le sous-réseau

- `cidr_block`- Le bloc CIDR du sous-réseau
- `is_default`- S'il s'agit du sous-réseau par défaut
- `is_public`- Si le sous-réseau est accessible au public
- `state`- L'état du sous-réseau
- `vpc_uid`- L'ID du VPC où se trouve le sous-réseau

Exemple

```
{
  "subnet_info": {
    "uid": "subnet-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-0a1b2c3d4e5f6g7h8",
    "name": "production-web-subnet-1a",
    "zone": "us-east-1a",
    "ip_count": 251,
    "cidr_block": "10.0.1.0/24",
    "is_default": false,
    "is_public": true,
    "state": "available",
    "vpc_uid": "vpc-0123456789abcdef0"
  }
}
```

Utilisateur

Attributs utilisateur IAM, y compris les profils d'instance et les politiques.

Exigence

Facultatif

Type

Objet

Statut de l'OCSF

Ajouté à`resource_details`. Consultez la définition de l'objet utilisateur OCSF.

L'objet utilisateur inclut les attributs suivants :

- `instance_profiles`- Liste des profils d'instance associés à une instance cloud
- `policies`- Politiques qui attribuent des autorisations aux utilisateurs, aux groupes, aux rôles et aux ressources

Exemple

```
{
  "user": {
    "type_id": 1,
    "uid": "AIDACKCEVSQ6C2EXAMPLE",
    "uid_alt": "arn:aws:iam::123456789012:user/developers/john.doe",
    "name": "john.doe",
    "type": "User",
    "groups": [
      {
        "name": "Developers"
      },
      {
        "name": "ReadOnlyAccess"
      }
    ],
    "policies": [
      {
        "name": "AmazonS3ReadOnlyAccess"
      },
      {
        "name": "AmazonEC2ReadOnlyAccess"
      }
    ]
  }
}
```

Résultats de couverture dans Security Hub

Les résultats de couverture pour Security Hub fournissent une visibilité sur les fonctionnalités de AWS sécurité activées et sur les éventuelles lacunes de couverture dans un compte autonome ou sur les comptes des membres d'une organisation. Les résultats de couverture permettent actuellement de signaler quels services et fonctionnalités sont activés pour Amazon GuardDuty, Amazon Inspector, Amazon Macie et AWS Security Hub CSPM. Ces résultats apparaissent dans le

widget Couverture de sécurité du tableau de bord Security Hub, avec la possibilité d’accéder à des vues plus détaillées par capacité de sécurité spécifique.

Limitations

- Pour les comptes de membres, les informations de couverture sont agrégées entre les différents liens Régions AWS, mais uniquement pour ce compte de membre.
- Les informations de couverture ne sont pas affichées pour les comptes qui ne sont pas intégrés à Security Hub.

Résultats de couverture pour AWS Hub de sécurité CSPM

Les résultats de la couverture CSPM de Security Hub évaluent si une norme de sécurité qualifiée pour la gestion de la posture est activée sur un compte. L'activation de n'importe quelle norme CSPM de Security Hub sera éligible, à l'exception des normes de balisage AWS Control Tower des ressources.

La détection des normes activées par défaut lors de l'activation de Security Hub CSPM peut prendre jusqu'à 24 heures.

Résultats de couverture pour Amazon GuardDuty

GuardDuty les résultats de couverture permettent de déterminer si elle GuardDuty est activée et quelles GuardDuty fonctionnalités sont activées dans un Compte AWS :

- GuardDuty Protection contre les programmes malveillants pour Amazon EC2 : analyse les instances Amazon EC2 à la recherche de programmes malveillants potentiels.
- GuardDuty Protection Amazon EKS : surveille les journaux d'audit de Kubernetes pour détecter les menaces dans les clusters Amazon EKS.
- GuardDuty Protection Lambda : analyse les appels de fonctions Lambda à la recherche de menaces potentielles.
- GuardDuty Protection Amazon S3 : analyse les événements de données pour détecter les menaces potentielles pesant sur les compartiments Amazon S3.
- GuardDuty Protection Amazon RDS : surveille les menaces qui pèsent sur les bases de données Amazon RDS.
- GuardDuty Surveillance de l'exécution : fournit une surveillance en temps réel du comportement d'exécution dans les instances Amazon EC2.

- GuardDuty Couverture de base : GuardDuty fonctionnalités de base qui sont automatiquement activées lorsqu'elles GuardDuty sont activées.

> **Note**
>
> Pour GuardDuty la couverture de base, les résultats de couverture indiquant que la fonctionnalité est désactivée ne sont GuardDuty généralement pas activés dans le compte pour la recherche de couverture.

Cela peut prendre jusqu'à 24 heures pour que les mises à jour de GuardDuty la couverture soient répercutées sur tous les comptes des membres d'une organisation.

Résultats de couverture pour Amazon Inspector

Les résultats de la couverture d'Amazon Inspector évaluent si Amazon Inspector est activé et quelles fonctionnalités sont activées sur un compte :

- Inspector EC2 Scanning : analyse les instances Amazon EC2 à la recherche de vulnérabilités.
- Inspector ECR Scanning : analyse les images des conteneurs Amazon ECR à la recherche de vulnérabilités.
- Inspector Lambda Standard Scanning : analyse les fonctions Lambda à la recherche de vulnérabilités.
- Inspecteur Lambda Code Scanning : analyse les fonctions du code Lambda pour détecter les vulnérabilités du code.

Résultats de couverture pour Amazon Macie

Les résultats de la couverture de Macie évaluent si Macie est activé dans les domaines suivants : Comptes AWS

- Couverture de découverte automatisée des données sensibles par Macie : évalue en permanence votre parc de données Amazon S3 pour détecter les données sensibles.

Les mises à jour de la découverte automatique des données sensibles par Macie peuvent prendre jusqu'à 24 heures pour que les résultats de couverture soient répercutés sur tous les comptes membres d'une organisation.

Suppression des résultats de couverture

Par défaut, les résultats de la couverture de sécurité évaluent quelles fonctionnalités Amazon GuardDuty, Amazon Inspector, Amazon Macie et AWS Security Hub CSPM sont activées pour un compte et une région. Si certaines fonctionnalités de sécurité ne s'appliquent pas à vous ou constituent un risque accepté, vous pouvez utiliser la fonction de suppression pour supprimer les résultats de couverture de la même manière que tous les autres résultats. Lorsqu'un résultat de couverture est supprimé, il n'est pas inclus dans les calculs de couverture du widget de couverture de sécurité. Le widget affiche le message suivant : La couverture des fonctionnalités de sécurité a été exclue en raison de résultats de couverture supprimés. Le message inclut le nombre de résultats supprimés.

Pour supprimer une détection de couverture dans Security Hub

1. Lorsque vous consultez le widget de couverture de sécurité, choisissez le lien correspondant au pourcentage de couverture.
2. Dans la fenêtre contextuelle de couverture, choisissez Afficher les résultats de couverture. Chaque résultat dont le statut est Nouveau décrit un écart de couverture observé.
3. Cochez la case à côté de chaque résultat que vous souhaitez supprimer.
4. En haut de la page, choisissez Mettre à jour le statut, puis sélectionnez Supprimé.
5. Dans la boîte de dialogue Définir le statut sur Supprimé, entrez éventuellement une note détaillant la raison du changement de statut. Choisissez ensuite Définir le statut.

Inventaire de l'IA dans Security Hub

L'inventaire de l'IA dans AWS Security Hub fournit une vue unifiée de vos ressources d'intelligence artificielle (IA) et d'apprentissage automatique (ML) dans votre AWS environnement. Utilisez l'inventaire de l'IA pour identifier les charges de travail d'IA non autorisées, comprendre où l'IA fonctionne et comment elle a été découverte, et hiérarchiser les ressources qui nécessitent un examen de sécurité plus approfondi. Security Hub organise les ressources d'IA en deux types de découverte :

- Géré : ressources d'IA AWS fournies sous forme de service géré. Security Hub découvre ces ressources à partir d'éléments de AWS Config configuration. Les types de ressources gérées incluent un sous-ensemble pris en charge d'Amazon Bedrock, Amazon Bedrock AgentCore et Amazon. SageMaker
- Self-hosted— Ressources d'IA qui ne sont pas fournies sous forme de service géré. Les exemples incluent les modèles open source, les agents et les serveurs d'inférence qui s'exécutent sur votre propre ordinateur. Security Hub détecte ces ressources à partir de signaux provenant des instances Amazon Elastic Compute Cloud (Amazon EC2) et des images Amazon Elastic Container Registry (Amazon ECR). Les signaux incluent les résultats de la nomenclature logicielle Amazon Inspector (SBOM) et l'activité du GuardDuty DNS d'Amazon.

Les comptes administrateurs peuvent consulter les ressources d'IA de tous les comptes activés de leur organisation. Les comptes des membres ne peuvent consulter que les ressources d'IA de leur propre compte.

Conditions préalables à la découverte d'IA auto-hébergée

La découverte de ressources d'IA gérées ne nécessite aucune configuration supplémentaire au-delà de l'activation de Security Hub. Pour découvrir les ressources d'IA auto-hébergées, vous devez également activer celles Services AWS qui fournissent les signaux contributifs :

- Amazon Inspector — Activez Amazon Inspector (avec Security Hub Essentials) pour générer des SBOM. Security Hub utilise ces SBOM pour détecter les modèles auto-hébergés, les points de terminaison d'inférence et les agents. Pour les instances Amazon EC2, activez le scan basé sur un agent avec le mode de numérisation amélioré, le scan sans agent ou le scan hybride. Agent-based l'analyse sans mode de numérisation amélioré ne produit pas l'inventaire logiciel complet requis par la détection des ressources par l'IA. Pour les images Amazon ECR, Amazon Inspector fournit des SBOM par le biais de la numérisation d'images de conteneurs.
- Amazon GuardDuty — Activez cette option GuardDuty pour que Security Hub puisse utiliser l'activité DNS pour détecter les points de terminaison IA externes appelés par vos instances Amazon EC2.

Types de ressources d'IA pris en charge

Lors de sa disponibilité générale, Security Hub prend en charge les types de ressources d'IA auto-hébergées suivants. Security Hub utilise un système de détection basé sur la confiance pour

les ressources d'IA auto-hébergées. Chaque détection est ancrée à un signal principal, tel qu'un composant SBOM. Security Hub met ensuite en corrélation des signaux supplémentaires pour établir la confiance avant qu'une ressource n'apparaisse dans votre inventaire. Security Hub affiche uniquement les ressources qui atteignent le seuil de confiance, ce qui permet de minimiser les faux positifs. Chaque ressource utilise un `ResourceType` avec le `SelfHosted::AI::` préfixe.

- Modèles (`SelfHosted::AI::Model`) — Modèles Hugging Face et Ollama. Security Hub détecte les modèles uniquement dans les répertoires de cache de modèles par défaut (tels que les caches Hugging Face et Ollama) et dans les chemins personnalisés que vous configurez pour le scan par Amazon Inspector.
- Points de terminaison d'inférence (`SelfHosted::AI::InferenceEndpoint`) : logiciels de service de modèles pris en charge, tels que vLLM, Ollama, Triton, Text Generation Inference (TGI), SGlang, llama.cpp, LocalAI, BentoML, Xinference, Ray Serve et GPT4all. TorchServe
- Agents (`SelfHosted::AI::Agent`) — OpenClaw agents.
- Points de terminaison externes (`SelfHosted::AI::ExternalEndpoint`) : domaines de service d'IA externes appelés par vos instances Amazon EC2. Security Hub tient à jour une liste d'autorisations des domaines de services d'IA connus, tels qu'OpenAI, Anthropic, Cohere, Mistral et d'autres grands fournisseurs d'IA, et détecte quand vos instances leur adressent des requêtes DNS. Les points de terminaison externes sont détectés uniquement à partir de l'activité GuardDuty DNS sur Amazon EC2.

Les ressources d'IA gérées sont un sous-ensemble pris en charge des types d'éléments de SageMaker configuration Amazon Bedrock, Amazon Bedrock AgentCore et Amazon, chacun avec une catégorie de `AI/ML` ressource.

Trouver des ressources d'IA à partir de la page Ressources

La page Ressources répertorie toutes les ressources de votre environnement. Pour les ressources d'IA, vous pouvez utiliser les fonctionnalités suivantes pour identifier les charges de travail d'IA et les hôtes qui les exécutent :

- Les AI/ML ressources gérées affichent une icône d'IA à côté de la ressource. Cliquez sur l'icône pour afficher une description.
- Les ressources hôtes qui exécutent des ressources d'IA auto-hébergées, telles que les instances Amazon EC2, affichent un badge de comptage d'IA auto-hébergées. Les hôtes ne disposant pas de ressources d'IA auto-hébergées n'affichent pas de badge.

- Utilisez le filtre rapide pour afficher uniquement les hôtes contenant des ressources d'IA auto-hébergées.
- Pour explorer un hôte, choisissez l'hôte pour ouvrir son panneau détaillé, choisissez l'onglet Ressources d'IA, puis choisissez Afficher tout pour voir les ressources d'IA auto-hébergées détectées sur cet hôte.

Utilisation de la page d'inventaire de l'IA

La page d'inventaire de l'IA met l'accent sur les ressources d'IA de votre organisation. Chaque ressource de cette page appartient à la catégorie de `AI/ML` ressources. Cette page présente les ressources d' AWS IA gérées et les ressources d'IA auto-hébergées dans votre environnement. Les sections suivantes décrivent les principaux composants de la page.

Barre de résumé

La barre de résumé affiche le nombre total d'actifs d'IA et une ventilation par type de découverte, qu'ils soient auto-hébergés ou gérés. Il affiche également une ventilation par sous-catégorie, telle que le modèle ou l'agent. Choisissez la valeur d'une statistique pour afficher les informations complémentaires dans le tableau.

Regroupement, filtrage et recherche

Le tableau d'inventaire AI regroupe les ressources par type de ressource par défaut. Vous pouvez modifier le groupement ou le supprimer pour obtenir une vue aplanie de toutes les ressources. Les champs de regroupement disponibles incluent l'ID canonique, le type de ressource hôte, le type de découverte, l'ID de compte et le type de ressource.

L'ID canonique identifie la nature d'une ressource, quel que soit son emplacement d'exécution. Par exemple, deux instances Amazon EC2 qui exécutent le même modèle Hugging Face partagent le même identifiant canonique, ce qui vous permet de retrouver tous les déploiements d'un modèle spécifique au sein de votre organisation.

> **Note**
>
> Les groupements d'ID canonique et de type de ressource hôte ne s'appliquent qu'aux ressources auto-hébergées. Lorsque vous les regroupez en fonction de ces champs, les ressources d'IA gérées n'apparaissent pas dans les résultats car elles ne possèdent pas ces

attributs. Utilisez le type de découverte ou les groupements de types de ressources pour voir ensemble les ressources gérées et auto-hébergées.

Les filtres rapides permettent de filtrer par sous-catégorie de ressources ou par type de découverte. Les filtres de propriétés prennent en charge des champs supplémentaires, notamment le type de ressource hôte et l'ID canonique pour les ressources auto-hébergées.

Détails des ressources et signaux contributifs

Choisissez une ligne de ressources pour ouvrir le panneau de détails. Pour les ressources gérées, le panneau affiche la configuration des ressources au format JSON. Pour les ressources auto-hébergées, le panneau affiche les signaux contributifs utilisés par Security Hub pour détecter la ressource. Ces signaux incluent la source de détection et les détails des signaux individuels, tels que les composants SBOM et le logiciel d'inférence associé à un modèle, ou le domaine DNS d'un point de terminaison externe.

Intégration à la ressource hôte

Pour une ressource d'IA auto-hébergée, le panneau détaillé affiche la ressource hôte sur laquelle Security Hub l'a détectée. Pour voir toutes les ressources d'IA auto-hébergées sur le même hôte, filtrez le tableau en fonction de la ressource hôte. Avec cette vue, vous pouvez passer d'une ressource auto-hébergée individuelle à son hôte et passer en revue les ressources d'IA adjacentes sur cet hôte.

Considérations

L'inventaire de l'IA présente les limites suivantes en termes de disponibilité générale :

- Self-hosted Les ressources d'IA ne contiennent aucune découverte dans cette version. Security Hub indique le nombre de résultats uniquement pour les ressources d'IA gérées.
- Self-hosted La détection par IA est prise en charge uniquement sur les instances Amazon EC2 et les images Amazon ECR. AWS Lambda les fonctions et autres types de calcul ne sont pas pris en charge.
- Security Hub n'attribue pas les images Amazon ECR à un hôte parent dans cette version. Le nombre d'IA des hôtes ne les inclut donc pas.
- Security Hub détecte les points de terminaison externes uniquement à partir de l'activité GuardDuty DNS sur Amazon EC2. Dans cette version, Security Hub n'attribue pas les appels provenant

de AWS Fargate, Amazon AWS Lambda SageMaker, Amazon EKS ou d'autres systèmes informatiques gérés par des services.

Accès à l'inventaire de l'IA avec l'API

Vous pouvez récupérer les données d'inventaire de l'IA par programmation avec le GetResourcesV2 et GetResourcesStatisticsV2les opérations.

Pour les AI/ML ressources, la `GetResourcesV2` réponse inclut les `DiscoveryType` champs `ResourceSubCategory` et. Le `DiscoveryType` champ indique si une ressource est `Managed` ou`SelfHosted`. Pour les ressources d'IA auto-hébergées et leurs ressources hôtes, la réponse inclut également `ResourceInfo` une `AIDetails` structure.

Self-hosted Les ressources d'IA utilisent un `ResourceType` avec le `SelfHosted::AI::` préfixe. Les types pris en charge sont les suivants :

- `SelfHosted::AI::Model`
- `SelfHosted::AI::Agent`
- `SelfHosted::AI::InferenceEndpoint`
- `SelfHosted::AI::ExternalEndpoint`

La `AIDetails` structure relie une ressource d'IA auto-hébergée à son hôte à l'aide des `HostResourceType` champs `HostResourceGuid` et. Le `CanonicalId` champ identifie la nature d'une ressource, indépendamment de l'endroit où elle est déployée, afin que vous puissiez agréger des ressources identiques sur plusieurs hôtes. L'identifiant canonique utilise le `type/identifier` format suivant :

- Pour les modèles ML : `model/<purl>` (par exemple,`model/pkg:huggingface/meta-llama/llama-3-8b`)
- Pour les points de terminaison et les agents d'inférence : un format `type/asset-identifier-name`
- Pour les points de terminaison externes : le domaine normalisé (par exemple,) `api.*.openai.com`

Sur une ressource hôte, telle qu'une instance Amazon EC2, les `SelfHostedAI*ResourceCount` champs et le `SelfHostedTotalAIResourceCount` champ contiennent le nombre de ressources d'IA auto-hébergées détectées sur l'hôte.

> **Note**
>
> Lorsque vous utilisez `GetResourcesV2` et filtrez par`ResourceSubCategory`, vous devez également inclure un `ResourceCategory` filtre. Définissez la comparaison `EQUALS` et la valeur sur`AI/ML`. Cette exigence s'applique également lorsque vous regroupez par `ResourceSubCategoryResourceInfo.AIDetails.HostResourceType`, ou `ResourceInfo.AIDetails.CanonicalId` dans`GetResourcesStatisticsV2`. Dans le cas contraire, l'opération renvoie un`ValidationException`.
> L'exemple suivant montre une combinaison de filtres valide :

```
{
    "Filters": {
        "CompositeFilters": [
            {
                "Operator": "AND",
                "StringFilters": [
                    {
                        "FieldName": "ResourceCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "AI/ML"
                        }
                    },
                    {
                        "FieldName": "ResourceSubCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "Model"
                        }
                    }
                ]
            }
        ]
    }
}
```

Résultats d’exposition dans Security Hub

Un résultat d'exposition dans Security Hub représente la corrélation de plusieurs signaux de sécurité qui identifient les risques de sécurité potentiels dans votre AWS environnement. Les résultats de l'exposition vous aident à comprendre et à hiérarchiser les risques de sécurité. Ils analysent automatiquement les combinaisons de vulnérabilités, de configurations, de menaces et de relations entre les ressources. Un résultat d'exposition inclut des traits et des signaux. Un signal peut comprendre un ou plusieurs types de caractéristiques d'exposition. Security Hub génère une détection d'exposition lorsque des signaux provenant de Security Hub CSPM, Amazon Inspector GuardDuty, Macie ou d'autres AWS services indiquent la présence d'une exposition. Une ressource peut être la principale ressource dans tout au plus une constatation d'exposition. Si une ressource n'a pas de caractéristiques d'exposition ou si ses caractéristiques sont insuffisantes, Security Hub ne génère pas de résultat d'exposition pour cette ressource.

Comment fonctionnent les résultats d'exposition

Security Hub génère des résultats d'exposition en :

Analyse des signaux provenant de plusieurs services AWS de sécurité

Security Hub collecte et analyse en permanence les signaux de sécurité provenant de plusieurs services AWS de sécurité. Il intègre les résultats GuardDuty pour la détection des menaces, Amazon Inspector pour l'évaluation des vulnérabilités, Security Hub CSPM pour les vérifications de configuration et Macie pour l'exposition de données sensibles. Ces signaux sont traités par des moteurs de corrélation avancés afin d'identifier les risques de sécurité potentiels.

Évaluation des configurations et des relations entre les ressources

Le système effectue une évaluation détaillée des configurations des ressources par rapport aux meilleures pratiques de sécurité. Il examine les paramètres spécifiques au service, les exigences de conformité et les contrôles de sécurité. Cette analyse permet d'identifier les erreurs de configuration susceptibles d'entraîner des failles de sécurité lorsqu'elles sont combinées à d'autres facteurs.

Évaluation de l'accessibilité du réseau

L'évaluation de l'accessibilité du réseau est un élément crucial des résultats en matière d'exposition. Le système évalue à la fois l'exposition à Internet et les chemins d'accès au réseau interne. Il analyse les configurations des groupes de sécurité et les paramètres ACL du

réseau afin de déterminer les vecteurs d'attaque potentiels. Cette analyse permet d'identifier les ressources susceptibles d'être exposées par inadvertance à un accès non autorisé.

Corrélation des problèmes de sécurité connexes

Le moteur de corrélation cartographie les relations entre les AWS ressources, analyse la façon dont elles interagissent et identifie les implications potentielles en matière de sécurité. Il examine les autorisations, les rôles et les modèles d'accès aux ressources IAM afin de comprendre le contexte de sécurité plus large. Ce processus permet d'identifier les risques de sécurité qui peuvent exister en raison de la combinaison de configurations individuelles apparemment innocentes.

Composantes d'une constatation d'exposition

Chaque résultat d'exposition inclut :

Titre et description du risque de sécurité potentiel

Chaque découverte d'exposition comprend un titre descriptif clair qui indique immédiatement la nature du risque de sécurité. La description fournit des informations détaillées sur l'impact potentiel sur la sécurité, les ressources affectées et le contexte général de l'exposition. Ces informations aident les équipes de sécurité à comprendre et à évaluer rapidement le risque.

Classification de gravité (critique, élevée, moyenne, faible)

- La gravité critique indique qu'une attention immédiate est requise en raison de la forte probabilité d'exploitation et de l'impact potentiel significatif. Ces résultats représentent généralement des vulnérabilités facilement détectables et exploitables.
- Une gravité élevée suggère qu'une attention prioritaire est requise, avec une probabilité d'exploitation modérée à élevée et un impact potentiel important. Ces résultats peuvent être relativement faciles à exploiter mais peuvent nécessiter des conditions spécifiques.
- Une gravité moyenne indique qu'une attention planifiée est requise, avec une probabilité d'exploitation plus faible et un impact potentiel modéré. Ces résultats nécessitent généralement des méthodes d'exploitation plus complexes.
- Une faible gravité suggère qu'une attention de routine est nécessaire, avec un potentiel d'exploitation limité et un impact mineur. Ces résultats sont généralement difficiles à exploiter et présentent un risque minimal.

Caractéristiques contributives qui ont conduit à l'exposition

Les caractéristiques contributives représentent les principaux facteurs qui ont conduit à la constatation de l'exposition. Il s'agit notamment des vulnérabilités de sécurité directes, des problèmes de configuration, des conditions d'exposition du réseau et des paramètres d'autorisation des ressources. Chaque caractéristique fournit des détails spécifiques sur la manière dont elle contribue au risque de sécurité global.

Visualisation de la trajectoire d'attaque potentielle et du rayon d'explosion

La visualisation de la trajectoire d'attaque potentielle et du rayon d'explosion fournit un diagramme interactif montrant comment les attaquants potentiels pourraient exploiter l'exposition identifiée. Il mappe les relations entre les ressources, les chemins réseau et les chemins d'élévation de privilèges aux ressources en aval qui sont potentiellement accessibles par un attaquant si l'exposition est exploitée.

Conseils de remédiation détaillés

Chaque découverte d'exposition comprend des conseils de remédiation détaillés avec des mesures spécifiques et réalisables pour faire face aux risques identifiés. Ce guide inclut des recommandations sur les meilleures pratiques, des étapes de correction de configuration et des actions prioritaires. Les recommandations sont adaptées au scénario d'exposition spécifique et prennent en compte les AWS services concernés.

Détails de configuration des ressources

Configuration de la ressource au moment de la création de la découverte ainsi que configuration actuelle de la ressource dans le tableau de bord de l'inventaire des ressources de Security Hub.

Caractéristiques contextuelles fournissant un contexte de sécurité supplémentaire

Les traits contextuels sont des marqueurs de sécurité supplémentaires qui ont été identifiés par Security Hub mais qui n'ont pas été utilisés pour créer un résultat d'exposition.

Les informations d'accès non utilisées provenant d'IAM Access Analyzer peuvent apparaître sous forme de caractéristiques contextuelles dans les résultats d'exposition. Lorsqu'un rôle IAM associé à une ressource possède des autorisations non utilisées, Security Hub inclut ces informations en tant que caractéristique contextuelle dans la vue détaillée de l'exposition. Par exemple, si une instance Amazon EC2 présente une vulnérabilité logicielle et que le rôle IAM qui lui est associé comporte 47 autorisations inutilisées sur 5 services, le résultat d'exposition indique les autorisations inutilisées comme contexte supplémentaire. Cela vous permet de comprendre le rayon d'action potentiel : une ressource vulnérable dotée d'un rôle IAM trop privilégié présente un risque plus élevé qu'une

ressource dotée des autorisations les moins privilégiées, car une ressource compromise pourrait utiliser ces autorisations non utilisées pour augmenter l'accès.

Les types de ressources suivants peuvent afficher des caractéristiques contextuelles d'accès non utilisées dans leurs résultats d'exposition :

- Instances Amazon Elastic Compute Cloud
- AWS Lambda fonctions
- Services Amazon Elastic Container Service
- Clusters Amazon Elastic Kubernetes Service
- Utilisateurs IAM (directement)

Classification de gravité

Les résultats d'exposition sont classés en fonction de :

- Facilité de découverte
- Facilité d'exploitation
- Probabilité d'exploitation
- Sensibilisation du public
- Incidence potentielle

Pour plus d'informations, voir Classification de gravité des résultats d'exposition.

Avantages des résultats d'exposition

- Analyse manuelle réduite grâce à la corrélation automatique : les résultats d'exposition réduisent considérablement le temps et les efforts nécessaires à l'analyse de la sécurité grâce à une corrélation automatique et à une hiérarchisation intelligente des risques. Security Hub surveille en permanence votre AWS environnement, identifiant et corrélant automatiquement les risques de sécurité qui pourraient ne pas être détectés lors d'un examen manuel.
- Vue hiérarchisée des risques de sécurité : Security Hub utilise des algorithmes sophistiqués d'évaluation des risques pour hiérarchiser les expositions en fonction de la gravité, de l'impact, de la criticité des ressources et de la probabilité d'exploitation. Cela permet aux équipes de sécurité de concentrer leurs efforts sur les risques les plus importants en premier lieu, améliorant ainsi l'efficacité des opérations de sécurité.

Sources des résultats d'exposition

Les résultats relatifs à l'exposition intègrent des données provenant de :

- GuardDuty L'intégration d'Amazon fournit des fonctionnalités de détection continue des menaces dans le cadre des résultats d'exposition. Il surveille les activités malveillantes, les compromissions potentielles des comptes et les anomalies comportementales. Le système intègre les résultats de ces menaces dans l'analyse plus large de l'exposition, ce qui permet d'identifier les cas où les menaces se combinent à d'autres problèmes de sécurité pour créer des risques importants.
- Amazon Inspector fournit des données cruciales d'évaluation des vulnérabilités aux résultats d'exposition. Il fournit des informations détaillées sur l'accessibilité du réseau, les vulnérabilités logicielles et les violations des meilleures pratiques de sécurité. Cette intégration permet de comprendre comment les vulnérabilités peuvent être exploitées par le biais de voies d'attaque identifiées.
- AWS Security Hub CSPM garantit que la conformité de la configuration et les normes de sécurité sont prises en compte dans l'analyse des expositions. Il évalue les ressources par rapport aux contrôles de sécurité établis et aux meilleures pratiques, fournissant ainsi une base pour comprendre les risques liés à la configuration.
- Amazon Macie améliore les résultats en matière d'exposition grâce à des fonctionnalités de découverte et de classification des données sensibles. Il identifie l'emplacement des données sensibles dans votre AWS environnement et évalue les risques potentiels en matière de confidentialité, ce qui permet de comprendre l'impact potentiel des expositions identifiées.

Bonnes pratiques

- Passez régulièrement en revue les résultats de l'exposition : une gestion efficace de l'exposition nécessite des processus d'évaluation structurés. Les organisations devraient procéder à des examens quotidiens des expositions critiques, à des évaluations hebdomadaires de l'état général des expositions, à une analyse mensuelle des tendances et à des évaluations trimestrielles de la posture de sécurité. Cette approche à plusieurs niveaux garantit une attention appropriée aux risques immédiats et aux tendances de sécurité à long terme.
- Priorisez les expositions critiques et de gravité élevée : la réussite de la gestion des expositions dépend d'une hiérarchisation efficace des risques. Les organisations doivent d'abord se concentrer sur les expositions critiques tout en tenant compte de la criticité des ressources et de l'impact commercial. Cette approche basée sur les risques permet de garantir que les efforts de sécurité correspondent aux priorités de l'entreprise et de maximiser la réduction des risques.

- Mettre en œuvre les mesures correctives recommandées : La correction de l'exposition doit suivre une approche systématique. Les organisations doivent mettre en œuvre avec soin les étapes de correction recommandées, conserver une documentation détaillée des modifications, effectuer des tests approfondis des modifications et valider l'efficacité des correctifs mis en œuvre. Cette approche méthodique permet d'atténuer les risques avec succès tout en évitant les conséquences imprévues.
- Configurez des règles de réponse automatisées : l'optimisation de la valeur des résultats d'exposition nécessite une automatisation efficace. Les organisations doivent mettre en œuvre des règles de réponse automatisées, configurer les notifications appropriées, établir des flux de travail efficaces et maintenir des pistes d'audit complètes. Cette automatisation permet de garantir une réponse cohérente et rapide aux expositions identifiées tout en réduisant les efforts manuels.

Types de ressources pris en charge pour les résultats d'exposition dans Security Hub

AWS Security Hub génère des résultats d'exposition pour les types de AWS ressources suivants :

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`
- `AWS::SageMaker::NotebookInstance`

Si vous disposez d'un connecteur Azure, Security Hub génère également des résultats d'exposition pour les types de ressources Azure suivants :

- `microsoft.app/containerapps`
- `microsoft.compute/virtualmachines`
- `microsoft.containerservice/managedclusters`
- `microsoft.documentdb/databaseaccounts`

- `microsoft.graph/user`
- `microsoft.sql/servers/databases`
- `microsoft.storage/storageaccounts/blobservices/containers`
- `microsoft.web/sites`

Security Hub génère un résultat d'exposition par ressource principale. Si une ressource n'a pas de caractéristiques d'exposition ou si ses caractéristiques sont insuffisantes, Security Hub ne génère pas de résultat d'exposition pour cette ressource.

Types de traits pris en charge dans Security Hub

AWS Security Hub génère un résultat d'exposition lorsque les résultats de contrôle CSPM de AWS Security Hub et les résultats générés par d'autres sites pris en charge Services AWS, tels qu'Amazon Inspector, contiennent des caractéristiques d'exposition pour une ressource. Le tableau suivant fournit des informations sur les types de traits pris en charge.

Type de trait	Description	Source	Ressources touchées
Assumabilité	Indique une ressource avec des autorisations distribuées Gestion des identités et des accès AWS	Configuration des ressources à partir de AWS Config	AWS ressources avec Gestion des identités et des accès AWS rôles associés
Impact	Indique le rayon d'explosion potentiel si la ressource est compromise, en fonction des autorisations effectives des Gestion des identités et des accès AWS principaux acteurs associés, y compris la possibilité de créer et de modifier des ressources	Analyse efficace des autorisations des Gestion des identités et des accès AWS principaux associés	AWS ressources associées à Gestion des identités et des accès AWS des identités
Mauvaise configuration	Indique une ressource mal configurée	AWS Résultats des contrôles CSPM de Security Hub,	Tous les types de ressources

Type de trait	Description	Source	Ressources touchées
		résultats des GuardDuty menaces Amazon et informations sur la confirmation des ressource s dans. AWS Config	
Accessibilité	Indique les chemins réseau ouverts vers une ressource	AWS Résultats des contrôles CSPM de Security Hub, résultats des GuardDuty menaces Amazon et résultats de l'accessibilité du réseau Amazon Inspector.	Instances Amazon EC2, clusters Amazon EKS, fonctions Lambda et compartiments Amazon S3
Données sensibles	Indique qu'une ressource contient des données sensibles	Conclusions de données sensibles de Macie	Compartiments Amazon S3

Type de trait	Description	Source	Ressources touchées
Vulnérabilité	Indique qu'une ressource présente une faiblesse qui pourrait être exploitée par une source de menace.	Résultats de la vulnérabilité des packages Amazon Inspector et du logiciel malveillant GuardDuty Amazon Amazon EC2.	Instances Amazon EC2, services Amazon ECS, clusters Amazon EKS et fonctions Lambda

Chaque trait peut être associé à plusieurs titres qui fournissent des détails sur l'exposition affectant la ressource. Par exemple, vous pouvez voir un titre Exploit Available pour le trait de vulnérabilité dans les détails d'une découverte d'exposition EC2.

Impact et autorisations effectives

Le trait Impact décrit le rayon d'explosion potentiel d'une exposition, c'est-à-dire les ressources en aval qu'un attaquant pourrait atteindre et compromettre si la ressource principale utilisée pour détecter l'exposition est compromise. Pour déterminer l'impact, Security Hub analyse les autorisations effectives des principaux Gestion des identités et des accès AWS (IAM) associés à la ressource.

Les autorisations effectives sont les autorisations dont dispose réellement un responsable une fois que Security Hub a évalué ses politiques basées sur l'identité ainsi que les politiques basées sur les ressources des ressources auxquelles il peut accéder. Étant donné que les autorisations effectives tiennent compte à la fois de ce qui est accordé à un mandant et de ce que les ressources cibles autorisent, elles reflètent plus précisément les actions que peut effectuer un mandant que les seules politiques basées sur l'identité.

À l'aide d'autorisations efficaces, Security Hub trace les voies d'élévation de privilèges depuis la ressource principale vers les autres ressources de votre environnement. Chaque chemin est une chaîne de ressources connectées par les autorisations qui permettent à un attaquant de passer d'une ressource à l'autre. Lorsque Security Hub identifie un chemin concret vers une ressource existante, il affiche ce chemin dans le cadre du trait Impact. L'impact prend également en compte les autorisations au-delà de ces chemins, telles que la possibilité d'invoquer Services AWS pour

créer ou modifier d'autres ressources. Vous pouvez consulter ces trajectoires dans le graphique des trajectoires d'attaque potentielles et réduire votre rayon d'explosion en supprimant les autorisations inutiles. Pour de plus amples informations, veuillez consulter Visualisation des expositions dans Security Hub à l'aide du graphique de la trajectoire d'attaque potentielle.

Génération de résultats d'exposition

Security Hub génère des résultats d'exposition en temps quasi réel. Au fur et à mesure que de nouveaux résultats de sécurité sont ingérés et que les résultats existants sont mis à jour, Security Hub génère ou met à jour les résultats d'exposition en temps quasi réel. Security Hub génère un résultat d'exposition par identifiant de ressource.

Security Hub ne publie pas les résultats d'exposition pour les types de ressources non étayés par les résultats d'exposition. Lorsqu'une ressource possède un nombre et une combinaison de caractéristiques significatifs, Security Hub génère un résultat d'exposition. Le nombre et la combinaison de caractéristiques déterminent également le niveau de gravité de l'exposition constatée.

Détection de l'exposition par échantillon

AWS Security Hub normalise les résultats d'exposition dans l'Open Cybersecurity Schema Framework (OCSF).

Détection de l'exposition par échantillon

Dans l'échantillon de résultats d'exposition suivant, le `related_events` paramètre contient des détails propres au résultat d'exposition, tels que les résultats contributifs. Les résultats contributifs sont les caractéristiques et les signaux associés à un résultat d'exposition. Un seul résultat contributif peut inclure un ou plusieurs traits. Le `observables` paramètre identifie la ressource associée à la découverte contributive. Ce paramètre peut être différent du `resources` paramètre qui identifie la ressource associée à la constatation de l'exposition.

```
{
    "activity_id": 1,
    "activity_name": "Create",
    "category_name": "Findings",
    "category_uid": 2,
    "class_name": "Detection Finding",
    "class_uid": 2004,
    "cloud": {
        "account": {
```

```
            "uid": "123456789012",
            "name": "production-application"
        },
        "cloud_partition": "aws",
        "provider": "AWS",
        "region": "us-east-1"
    },
    "finding_info": {
        "analytic": {
            "name": "Exposure",
            "type": "Rule",
            "type_id": 1,
            "uid": "0.0.1"
        },
        "created_time_dt": "2024-11-15T21:39:26.337224100Z",
        "desc": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
        "related_events_count": 3,
        "related_events": [
            {
                "tags": [
                    {
                        "name": "Vulnerability",
                        "values": [
                            "Attack Vector Network",
                            "EPSS Level >= High",
                            "EPSS Level >= Medium",
                            "Exploit Available",
                            "No Privileges Required",
                            "No User Interaction Required",
                            "Vulnerable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
```

```
                    }
                ],
                "type": "Finding",
                "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
                "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
            },
            {
                "tags": [
                    {
                        "name": "Reachability",
                        "values": [
                            "Publicly Invocable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title":  "Lambda function policies should prohibit public access",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
            },
            {
                "tags": [
                    {
                        "name": "Misconfiguration",
                        "values": [
                            "Deployed outside VPC"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
```

```
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "Lambda functions should be in a VPC",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        ],
        "title": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "types": [
            "Exposure/Potential Impact/Resource Hijacking"
        ],
        "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
    },
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "LambdaProdStack"
                },
```

```
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
LambdaProdStack/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],
    "severity": "Critical",
    "severity_id": 5,
    "impact": "High",
    "impact_id": 3,
    "likelihood": "Very High",
    "likelihood_id": 5,
    "status": "New",
    "status_id": 1,
    "time": 1731706766337,
    "time_dt": "2024-11-15T21:39:26.337224100Z",
    "type_name": "Detection Finding: Create",
    "type_uid": 200401,
    "vendor_attributes": {
        "severity_id": 5,
        "severity": "Critical"
    }
}
```


Déterminer le niveau de gravité d'un résultat d'exposition

AWS Security Hub attribue à chaque exposition une gravité par défaut de`CRITICAL`, `HIGHMEDIUM`, ou`LOW`. Les résultats d'exposition dont la gravité est de ne `INFORMATIONAL` sont pas publiés. Security Hub détermine la gravité d'une découverte d'exposition en combinant deux dimensions, la probabilité et l'impact, sur une matrice de risques. La probabilité reflète la facilité avec laquelle l'exposition peut être exploitée, et l'impact reflète l'ampleur des dommages si elle est exploitée.

Dans les cas où l'impact ne peut être déterminé pour une ressource, la gravité est basée uniquement sur la probabilité.

Matrice des risques

Le tableau suivant montre comment la probabilité et l'impact se combinent pour produire la gravité finale d'un résultat d'exposition. La probabilité établit une gravité de référence, et l'impact l'ajuste : un impact élevé augmente la gravité d'un niveau (plafonné à`CRITICAL`), un impact moyen laisse la gravité inchangée et un impact faible réduit la gravité d'un niveau (plafonné à). `INFORMATIONAL` L'impact n'ajuste que la gravité établie par la probabilité. L'impact à lui seul ne permet pas de déterminer l'exposition.

Matrice du risque de gravité

Probabilité ↓/Impact →	Faible	Medium	Élevée
Très élevé	ÉLEVÉ	CRITIQUE	CRITIQUE
Élevée	MOYEN	ÉLEVÉ	CRITIQUE
Modérées	FAIBLE	MOYEN	ÉLEVÉ
Faible	INFORMATIF	FAIBLE	MOYEN

> **Note**
>
> Une faible probabilité combinée à un faible impact entraîne une gravité de`INFORMATIONAL`. Security Hub ne publie pas les résultats d'exposition d'une telle gravité. Ils n'apparaissent donc pas sur la page Expositions ni dans les GetFindingsV2 résultats.

Probabilité

La probabilité mesure la facilité avec laquelle une exposition peut être exploitée, en fonction des caractéristiques contributives présentes sur la ressource, telles que l'assumabilité, la mauvaise configuration, l'accessibilité, les données sensibles et la vulnérabilité. Security Hub utilise plusieurs caractéristiques pour évaluer la probabilité, notamment les suivantes :

- Sensibilisation : mesure dans laquelle l'exposition n'est pas théorique, mais comporte des exploits accessibles au public ou automatisés.
- Facilité de découverte : si des outils automatisés, tels qu'une analyse des ports ou une recherche sur Internet, sont disponibles pour découvrir la ressource à risque.

- Facilité d'exploitation : facilité avec laquelle un acteur de la menace peut exploiter l'exposition. Par exemple, s'il existe des chemins réseau ouverts ou des métadonnées mal configurées, un acteur malveillant peut plus facilement exploiter cette exposition.
- Probabilité d'exploitation — Probabilité que l'exposition soit exploitée au cours des 30 prochains jours. Ce facteur correspond au système de notation des exploits (EPSS).

Impact

L'impact mesure l'ampleur des dommages causés à votre environnement si l'exposition est exploitée. Par exemple, une exposition peut entraîner une perte de responsabilité, une perte de disponibilité, une perte de confidentialité en raison de l'exposition de données ou une perte d'intégrité due à une corruption de données.

Pour évaluer l'impact, Security Hub analyse les autorisations effectives des Gestion des identités et des accès AWS principaux associés à la ressource afin de déterminer les actions Services AWS qu'un attaquant pourrait invoquer. Il identifie également les ressources existantes qu'un attaquant pourrait atteindre et compromettre en augmentant les privilèges. Pour de plus amples informations, veuillez consulter Impact et autorisations effectives.

Révision des résultats d'exposition

Vous pouvez consulter tous vos résultats d'exposition dans la console Security Hub et à l'aide de l'GetFindingsV2API. La page Expositions de la console Security Hub affiche tous les résultats d'exposition active. Les résultats d'exposition sont classés par gravité décroissante. Vous pouvez filtrer vos résultats d'exposition en ajoutant et en supprimant des filtres à l'aide de la barre de recherche Ajouter un filtre. Vous pouvez regrouper les résultats de votre exposition dans le menu déroulant Grouper par liste déroulante. Vous pouvez également filtrer les résultats de votre exposition à l'aide du menu Filtres rapides.

Informations détaillées sur les résultats d'exposition

Vous pouvez consulter de nombreux détails pour déterminer l'exposition. Ces informations sont réparties entre les onglets de la console Security Hub. L'onglet Aperçu fournit des informations clés sur le résultat de l'exposition. L'onglet Caractéristiques répertorie les caractéristiques et les signaux associés à un résultat d'exposition. L'onglet Ressources fournit des informations sur les ressources et les balises de ressources associées à une découverte d'exposition. La liste suivante fournit des descriptions des détails relatifs à la détection de l'exposition.

- Titre de la recherche : titre de la constatation d'exposition.
- Niveau de gravité : niveau de gravité du résultat d'exposition. Security Hub utilise le nombre et la combinaison de caractéristiques d'une ressource pour déterminer le niveau de gravité d'un résultat d'exposition. Le niveau de gravité peut être `CRITICAL`,`HIGH`,`MEDIUM`, ou`LOW`. Security Hub ne publie pas de résultats d'exposition d'une gravité de`INFORMATIONAL`. Vous pouvez le mettre à jour `Severity` via la console Security Hub ou à l'aide de l'BatchUpdateFindingsV2API.
- Description : description du résultat d'exposition.
- Type : nom du type de détection d'exposition. Par exemple, le nom peut ressembler`Exposure/ Potential Impact/Resource Hijacking`.
- Compte : identifiant de l' Compte AWS endroit où le résultat d'exposition a été généré.
- Âge : indique depuis combien de temps le détecteur d'exposition est actif.
- Heure de création : horodatage qui indique la date de création de la détection d'exposition.
- Heure modifiée : horodatage qui indique la date de dernière mise à jour du résultat d'exposition.
- Région — L' Région AWS endroit où le résultat d'exposition a été généré.
- Nom du produit : nom du produit qui a généré le résultat d'exposition. Il s'agira toujours de la détection d'exposition de Security Hub.
- Nom de l'entreprise : nom de la société qui a généré le résultat d'exposition. Ce sera toujours le cas AWS.
- Nom de l'activité : nom de la dernière activité effectuée par rapport à la découverte.
- État : statut de ce résultat d'exposition.
- Identifiant de découverte : identifiant unique associé au résultat d'exposition.
- Trajectoire d'attaque potentielle (console uniquement) : visualisation interactive montrant comment les attaquants potentiels peuvent accéder aux ressources associées à une découverte d'exposition et en prendre le contrôle. Pour de plus amples informations, veuillez consulter Visualisation des expositions dans Security Hub à l'aide du graphique de la trajectoire d'attaque potentielle.
- Traits — Identifie les types de traits et les titres de traits associés à la découverte de l'exposition. Dans la console Security Hub, vous pouvez afficher les caractéristiques par type de caractéristique ou par signal. Cela vous permet d'analyser les résultats contributifs dans le contexte de l'exposition associée.
- Assainissement — Liens vers la documentation de remédiation spécifique aux caractéristiques identifiées lors de l'exposition.
- Ressources — Identifie la ressource associée à la découverte de l'exposition.

Examiner les détails des résultats d'exposition

Cette rubrique explique comment consulter les informations relatives aux résultats d'exposition dans la console AWS Security Hub et à l'aide de l'API.

Consulter les informations relatives à une détection d'exposition dans la console Security Hub

Pour afficher les détails d'une détection d'exposition dans la console Security Hub

1. Connectez-vous à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Exposures.
3. Choisissez un indicateur d'exposition dont vous souhaitez afficher les détails.

Révision des détails d'une découverte d'exposition à l'aide de l'API

Vous pouvez consulter les résultats d'exposition à l'aide de GetFindingsV2 l'API ou du AWS CLI. Vous pouvez filtrer tous les résultats d'exposition à l'aide du `metadata.product.feature.uid` champ contenant la `security-hub/Exposure` valeur. Pour de plus amples informations, veuillez consulter GetFindingsV2.

Exemple de commande

L' AWS CLI exemple suivant permet de récupérer les 10 derniers résultats d'exposition générés dans votre compte. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
aws securityhub get-findings-v2 \
--max-results '10' \
--filter '{"CompositeFilters": [{"StringFilters":
 [{"FieldName":"metadata.product.feature.uid","Filter": {"Value":"security-hub/
Exposure","Comparison":"EQUALS"}} ]}]}'
```

Visualisation des expositions dans Security Hub à l'aide du graphique de la trajectoire d'attaque potentielle

Le graphique du chemin d'attaque potentiel est une visualisation interactive qui montre comment les attaquants potentiels peuvent accéder aux ressources associées à une découverte d'exposition et en prendre le contrôle. Vous pouvez accéder à ce graphique uniquement dans la console Security Hub

depuis la page Exposures. Lorsque vous consultez les détails d'une détection d'exposition, l'onglet Aperçu inclut une section intitulée Trajectoire d'attaque potentielle et Rayon d'explosion.

Le graphique du chemin d'attaque indique la ressource principale sur laquelle l'exposition a été générée, le chemin réseau (le cas échéant) et les ressources en aval qu'un attaquant pourrait atteindre en augmentant les autorisations. Lorsque Security Hub identifie des voies d'escalade de privilèges concrètes entre la ressource principale et les autres ressources de votre environnement, il les affiche sous forme de rayon de propagation du graphique. Chaque nœud représente une ressource, et les connexions entre les nœuds indiquent les autorisations qui permettent à un attaquant de passer d'une ressource à l'autre.

Dans cette section de l'onglet Aperçu, vous pouvez choisir et faire glisser AWS des ressources dans le graphique de la trajectoire d'attaque potentielle. Vous pouvez vous concentrer sur des zones spécifiques du graphique de la trajectoire d'attaque à l'aide des icônes de zoom avant et arrière. Vous pouvez développer le graphique de la trajectoire d'attaque en mode plein écran et en dehors du mode plein écran via l'icône plein écran. La légende code la ressource principale, la ressource concernée, les ressources du rayon d'explosion et le nombre de traits contributifs par couleur et affiche les catégories de traits et le nombre de traits dans le graphique de la trajectoire d'attaque. Vous pouvez consulter les détails d'une ressource en choisissant une ressource, puis en choisissant Afficher les détails de la ressource. Vous pouvez également copier l'identifiant et le Compte AWS numéro associés à une ressource. Les résultats d'exposition avec une caractéristique d'accessibilité montrent l'Internet public et le chemin réseau effondré dans le graphique du chemin d'attaque. Vous pouvez afficher ce détail en choisissant le nœud de chemin réseau réduit.

Pour afficher les ressources en aval et les chemins d'élévation de privilèges qui les relient, choisissez l'onglet Impact assessment. Chaque chemin indique la chaîne de ressources qu'un attaquant pourrait traverser et les autorisations spécifiques à chaque étape. Pour plus d'informations sur les caractéristiques d'impact et les autorisations effectives, consultezImpact et autorisations effectives.

Corriger les résultats d'exposition

Les rubriques de cette section décrivent les étapes de remédiation pour les résultats d'exposition dans différents Services AWS domaines.

Le `Remediation` champ du format OCSF contient deux champs : `remediation` et`references`.

```
"Remediation": {
    "Recommendation": {
        "remediation":{"desc":"String",
        "references":["string array"]}
```

```
    }
},
```

> **Note**
>
> Les conseils d'assainissement fournis dans les sections suivantes peuvent nécessiter des consultations supplémentaires auprès d'autres AWS ressources.

Corriger les expositions pour les tables DynamoDB

AWS Security Hub peut générer des résultats d'exposition pour les tables DynamoDB.

Sur la console Security Hub, la table DynamoDB impliquée dans la détection d'une exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration dans DynamoDB
  - La restauration instantanée de la table DynamoDB est désactivée
  - La table DynamoDB n'est pas couverte par un plan de sauvegarde

- La protection contre la suppression de la table DynamoDB est désactivée.

Caractéristiques de mauvaise configuration dans DynamoDB

Ce qui suit décrit les caractéristiques de configuration erronée et les étapes de correction pour les tables DynamoDB.

La restauration instantanée de la table DynamoDB est désactivée

Correction : activer la restauration instantanée de DynamoDB

La restauration instantanée de DynamoDB fournit des sauvegardes automatisées continues pour les données de vos tables DynamoDB. Pour plus d'informations sur la façon de restaurer une table DynamoDB à un moment donné, voir Restaurer une table DynamoDB à un moment donné dans le guide du développeur Amazon DynamoDB.

La table DynamoDB n'est pas couverte par un plan de sauvegarde

AWS Backup fournit un service centralisé permettant de configurer, de gérer et d'automatiser les sauvegardes entre les AWS services, y compris DynamoDB. Sans plan de sauvegarde, votre table ne dispose pas de sauvegardes planifiées et automatisées avec des périodes de conservation personnalisables, ce qui crée des risques de sécurité importants. Un attaquant pourrait corrompre ou supprimer les données de votre table de manière malveillante. Sans sauvegardes appropriées, il se peut que vous ne disposiez d'aucune option de restauration au-delà de la fenêtre de Point-in-Time restauration (si elle est activée), ce qui peut entraîner une perte de données permanente. Conformément aux meilleures pratiques en matière de protection des données, couvrez vos tables DynamoDB avec un plan de sauvegarde.

Remédiation : créer un plan de sauvegarde

Avant de créer un plan de sauvegarde, déterminez une fréquence de sauvegarde et des périodes de conservation appropriées pour vos données. Pour plus d'informations sur la création d'un plan de sauvegarde, voir Affecter des ressources à un plan de sauvegarde dans le AWS Backup Developer Guide.

La protection contre la suppression de la table DynamoDB est désactivée.

La protection contre la suppression empêche la suppression accidentelle de tables DynamoDB. Lorsque la protection contre la suppression est désactivée, les tables DynamoDB sont vulnérables à une suppression involontaire via des actions de console, des appels d'API, des commandes

CLI ou des processus automatisés. Cela peut exposer votre AWS environnement à une perte de données, car une entité non autorisée ayant accès à votre AWS environnement pourrait supprimer intentionnellement des tables, entraînant une interruption de service et une perte de données permanente. Conformément aux meilleures pratiques en matière de protection des données, activez la protection des données pour les tables DynamoDB.

Correction : activer la protection contre la suppression

Si vous gérez plusieurs tables, pensez à les utiliser CloudFormation pour mettre à jour les propriétés des tables en bloc. Vous pouvez modifier vos CloudFormation modèles pour inclure des `DeletionProtectionEnabled` propriétés et mettre à jour vos piles. Une fois la correction terminée, vérifiez que la protection contre la suppression est activée dans la liste déroulante Informations supplémentaires de l'onglet Paramètres du tableau.

Remédier aux expositions pour les instances EC2

AWS Security Hub peut générer des résultats d'exposition pour les instances Amazon Elastic Compute Cloud (EC2).

Sur la console Security Hub, l'instance EC2 impliquée dans la détection d'une exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration pour les instances EC2
  - L'instance EC2 permet d'accéder à IMDS à l'aide de la version 1
  - L'instance Amazon EC2 possède un groupe de sécurité ou une liste ACL réseau qui autorise l'accès SSH ou RDP
  - L'instance Amazon EC2 possède un groupe de sécurité ouvert
- Caractéristiques d'accessibilité pour les instances EC2
  - L'instance EC2 est accessible via Internet
- Caractéristiques de vulnérabilité des instances EC2
  - L'instance EC2 présente des vulnérabilités logicielles exploitables par le réseau avec une forte probabilité d'exploitation
  - L'instance Amazon EC2 présente des vulnérabilités logicielles
  - L'instance EC2 possède un End-Of-Life système d'exploitation
  - L'instance EC2 contient des packages logiciels malveillants
  - L'instance EC2 contient des fichiers malveillants
- Caractéristiques d'impact pour les instances EC2
  - Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié
  - A une trajectoire d'escalade politique directe
  - A une voie de détournement de la politique de confiance
  - Possède un chemin de données vers un
  - Dispose d'un chemin de restriction supprimé
  - A un rôle de passe pour créer le chemin de l'exécuteur
  - Dispose d'un rôle d'échange (chemin d'exécuteur existant)
  - Dispose d'une voie d'escalade en chaîne de rôles
  - Possède un chemin d'exécution privilégié pour l'injection de code
  - A désactivé le chemin de la piste d'audit
  - A accès au chemin d'exécution existant
  - Dispose d'un parcours de création d'identifiants
  - Dispose d'un chemin d'accès aux données du rôle de passe
  - A un rôle de passe, une tâche, un chemin de détournement
  - Dispose d'un chemin d'accès aux données à saut unique

- Possède une capacité d'avancement

Caractéristiques de mauvaise configuration pour les instances EC2

Voici les caractéristiques des erreurs de configuration pour les instances EC2 et les étapes de correction suggérées.

L'instance EC2 permet d'accéder à IMDS à l'aide de la version 1

Les métadonnées d'instance sont des données relatives à votre instance Amazon EC2 que les applications peuvent utiliser pour configurer ou gérer l'instance en cours d'exécution. Le service de métadonnées d'instance (IMDS) est un composant sur instance utilisé par le code sur l'instance pour accéder en toute sécurité aux métadonnées d'instance. Si l'IMDS n'est pas correctement sécurisé, il peut devenir un vecteur d'attaque potentiel, car il permet d'accéder à des informations d'identification temporaires et à d'autres données de configuration sensibles. L'IMDSv2 fournit une protection renforcée contre l'exploitation grâce à une authentification orientée session, qui nécessite un jeton de session pour les demandes de métadonnées et limite la durée des sessions. Conformément aux principes de sécurité standard, configurez les instances Amazon EC2 pour utiliser IMDSv2 et désactivez IMDSv1.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Compatibilité des applications de test

Avant d'implémenter IMDSv2, testez votre instance pour vous assurer de sa compatibilité avec IMDSv2. Certaines applications ou certains scripts peuvent nécessiter IMDSv1 pour les fonctionnalités de base et nécessiter une configuration supplémentaire. Pour plus d'informations sur les outils et les chemins recommandés pour tester la compatibilité des applications, passez à l'utilisation de la version 2 du service de métadonnées d'instance dans le guide de l'utilisateur Amazon Elastic Compute Cloud.

Mettre à jour l'instance pour utiliser IMDSv2

Modifiez les instances existantes pour utiliser IMDSv2. Pour plus d'informations, consultez la section Modifier les options de métadonnées d'instance pour les instances existantes dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

Appliquer les mises à jour aux instances d'un groupe Auto Scaling

Si votre instance fait partie d'un groupe Auto Scaling, mettez à jour votre modèle de lancement ou votre configuration de lancement avec une nouvelle configuration, puis actualisez l'instance.

L'instance Amazon EC2 possède un groupe de sécurité ou une liste ACL réseau qui autorise l'accès SSH ou RDP

Les protocoles d'accès à distance tels que SSH et RDP permettent aux utilisateurs de se connecter à des instances Amazon EC2 et de les gérer depuis des emplacements externes. Lorsque les groupes de sécurité autorisent un accès illimité à ces protocoles depuis Internet, ils augmentent la surface d'attaque de vos instances Amazon EC2 en autorisant l'accès à Internet à votre instance. Conformément aux principes de sécurité standard, limitez l'accès à distance à des adresses ou à des plages IP spécifiques et fiables.

Correction : modifier les règles des groupes de sécurité

Limitez l'accès à vos instances Amazon EC2 à des adresses IP fiables spécifiques. Limitez l'accès SSH et RDP à des adresses IP fiables spécifiques ou utilisez la notation CIDR pour spécifier des plages IP (par exemple, 192.168.1). 0/24). Pour modifier les règles des groupes de sécurité, consultez la section Configurer les règles des groupes de sécurité dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

L'instance Amazon EC2 possède un groupe de sécurité ouvert

Les groupes de sécurité agissent comme des pare-feux virtuels pour vos instances Amazon EC2 afin de contrôler le trafic entrant et sortant. Les groupes de sécurité ouverts, qui permettent un accès illimité à partir de n'importe quelle adresse IP, peuvent exposer vos instances à un accès non autorisé. Conformément aux principes de sécurité standard, limitez l'accès des groupes de sécurité à des adresses IP et à des ports spécifiques.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Passez en revue les règles des groupes de sécurité et évaluez la configuration actuelle

Évaluez quels ports sont ouverts et accessibles à partir de larges plages d'adresses IP, telles que`(0.0.0.0/0 or ::/0)`. Pour obtenir des instructions sur l'affichage des détails des groupes de sécurité, consultez DescribeSecurityGroups le manuel Porting Assistant for .NET API Reference.

Modifier les règles des groupes de sécurité

Modifiez les règles de votre groupe de sécurité pour restreindre l'accès à des adresses IP ou à des plages d'adresses IP fiables spécifiques. Lorsque vous mettez à jour les règles de votre groupe de sécurité, pensez à séparer les exigences d'accès pour les différents segments du réseau en créant des règles pour chaque plage d'adresses IP source requise ou en limitant l'accès à des ports spécifiques. Pour modifier les règles des groupes de sécurité, consultez la section Configurer les règles des groupes de sécurité dans le guide de l'utilisateur Amazon EC2.

Caractéristiques d'accessibilité pour les instances EC2

Voici les caractéristiques d'accessibilité des instances EC2 et les étapes de correction suggérées.

L'instance EC2 est accessible via Internet

Les instances Amazon EC2 dont les ports sont accessibles depuis Internet peuvent exposer votre instance. L'accessibilité peut se faire via une passerelle Internet (y compris des instances situées derrière des équilibreurs de charge d'application ou des équilibreurs de charge classiques), une connexion d'appairage VPC ou une passerelle virtuelle VPN. Conformément aux principes de sécurité standard, mettez en œuvre des contrôles d'accès réseau au moindre privilège en limitant le trafic entrant aux seules sources et ports nécessaires.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Modifier ou supprimer les règles des groupes de sécurité

Dans l'onglet Ressources, ouvrez la ressource pour le groupe de sécurité Amazon EC2. Vérifiez si un accès à Internet est requis pour que l'instance fonctionne. Modifiez ou supprimez les règles des groupes de sécurité entrants qui autorisent un accès illimité (`0.0.0.0/0` ou `::/0`). Implémentez des règles plus restrictives en fonction de plages IP ou de groupes de sécurité spécifiques. Si un accès public limité est nécessaire, limitez l'accès aux ports et protocoles spécifiques nécessaires au fonctionnement de l'instance. Pour obtenir des instructions sur la gestion des règles des groupes de sécurité, consultez la section Configurer les règles des groupes de sécurité dans le guide de l'utilisateur Amazon EC2.

Mettre à jour les ACL réseau

Vérifiez et modifiez les listes de contrôle d'accès au réseau (ACL) associées au sous-réseau de l'instance. Vérifiez que les paramètres ACL correspondent aux modifications du groupe de sécurité et

n'autorisez pas involontairement l'accès public. Pour obtenir des instructions sur la modification des ACL réseau, consultez la section Utilisation des ACL réseau dans le guide de l'utilisateur Amazon VPC.

Autres méthodes d'accès

Envisagez les options suivantes pour d'autres méthodes d'accès :

- Utiliser la passerelle NAT pour la connectivité Internet sortante — Pour les instances de sous-réseaux privés nécessitant un accès à Internet (par exemple, pour télécharger des mises à jour), envisagez d'utiliser une passerelle NAT au lieu d'attribuer une adresse IP publique. Une passerelle NAT permet aux instances de sous-réseaux privés d'établir des connexions sortantes vers Internet tout en empêchant les connexions entrantes depuis Internet.
- Utilisez le gestionnaire de session de Systems Manager — Le gestionnaire de session fournit un accès shell sécurisé à vos instances Amazon EC2 sans avoir besoin de ports entrants, de gérer des clés SSH ou de gérer des hôtes bastion.
- Utilisez WAF et Elastic Load Balancing ou Application Load Balancer : pour les instances qui exécutent des applications Web, envisagez d'utiliser un LB associé à un AWS Web Application Firewall (WAF). Le LB peut être configuré pour permettre à vos instances de s'exécuter dans des sous-réseaux privés tandis que le LB s'exécute dans un sous-réseau public et gère le trafic Internet. L'ajout d'un WAF à votre équilibreur de charge fournit une protection supplémentaire contre les exploits Web et les robots.

Caractéristiques de vulnérabilité des instances EC2

Voici les caractéristiques de vulnérabilité des instances EC2 et les étapes de correction suggérées.

L'instance EC2 présente des vulnérabilités logicielles exploitables par le réseau avec une forte probabilité d'exploitation

Les packages logiciels installés sur les instances EC2 peuvent être exposés à des vulnérabilités et expositions communes (CVE). Les CVE critiques présentent des risques de sécurité importants pour votre AWS environnement. Les administrateurs non autorisés peuvent exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. Les vulnérabilités critiques présentant une forte probabilité d'exploitation constituent des menaces de sécurité immédiates, car le code d'exploitation est peut-être déjà accessible au public et utilisé activement par des attaquants ou des outils d'analyse automatisés. Corrigez ces vulnérabilités pour protéger votre instance.

Correction : mettre à jour les instances concernées

Consultez la section Références de l'onglet Vulnérabilité du trait. La documentation du fournisseur peut inclure des directives de correction spécifiques. Suivez les mesures correctives appropriées en suivant ces directives générales :

Utilisez Systems Manager Patch Manager pour appliquer des correctifs à la fois aux systèmes d'exploitation et aux applications. Patch Manager vous permet de sélectionner et de déployer automatiquement des correctifs de système d'exploitation et de logiciels sur de grands groupes d'instances. Si Patch Manager n'est pas configuré, mettez à jour manuellement le système d'exploitation de chaque instance concernée.

Mettez à jour les applications concernées vers leurs dernières versions sécurisées en suivant les procédures recommandées par le fournisseur. Pour gérer les mises à jour des applications sur plusieurs instances, pensez à utiliser Systems Manager State Manager pour maintenir la cohérence de votre logiciel. Si les mises à jour ne sont pas disponibles, envisagez de supprimer ou de désactiver l'application vulnérable jusqu'à la publication d'un correctif ou d'autres mesures d'atténuation, telles que la restriction de l'accès réseau à l'application ou la désactivation de fonctionnalités vulnérables.

Suivez les conseils de correction spécifiques fournis dans les résultats d'Amazon Inspector. Cela peut impliquer de modifier les règles des groupes de sécurité, de modifier les configurations d'instance ou d'ajuster les paramètres de l'application.

Vérifiez si l'instance fait partie d'Auto Scaling Group. AMI-replacement l'application de correctifs est effectuée sur des infrastructures immuables en mettant à jour l'ID AMI configuré pour déployer de nouvelles instances Amazon EC2 dans un groupe Auto Scaling. Si vous utilisez une custom/golden AMI, créez une instance avec la nouvelle AMI, puis personnalisez-la et créez une nouvelle AMI dorée. Pour plus d'informations, voir Mise à jour de l'AMI et application de correctifs (utilisation d'AMI patchées pour les groupes Auto Scaling).

Considérations futures

Pour éviter que cela ne se reproduise, envisagez de mettre en œuvre un programme de gestion des vulnérabilités. Amazon Inspector peut être configuré pour rechercher automatiquement les CVE sur vos instances. Amazon Inspector peut également être intégré à Security Hub pour des corrections automatiques. Envisagez de mettre en œuvre un calendrier d'application régulier des correctifs à l'aide des fenêtres de maintenance de Systems Manager afin de minimiser les interruptions de vos instances.

L'instance Amazon EC2 présente des vulnérabilités logicielles

Les packages logiciels installés sur les instances Amazon EC2 peuvent être exposés à des vulnérabilités et expositions courantes (CVE). Les CVE non critiques représentent des failles de sécurité dont la gravité ou l'exploitabilité sont inférieures à celles des CVE critiques. Bien que ces vulnérabilités présentent un risque immédiat moindre, les attaquants peuvent toujours exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités pour protéger votre instance contre les attaques.

Correction : mettre à jour les instances concernées

Utilisez AWS Systems Manager Patch Manager pour appliquer des correctifs aux systèmes d'exploitation. Patch Manager vous permet de sélectionner et de déployer automatiquement des correctifs de système d'exploitation et de logiciels sur de grands groupes d'instances. Si Patch Manager n'est pas configuré, mettez à jour manuellement le système d'exploitation de chaque instance concernée.

Mettez à jour les applications concernées vers leurs dernières versions sécurisées en suivant les procédures recommandées par le fournisseur. Pour gérer les mises à jour des applications sur plusieurs instances, pensez à utiliser AWS Systems Manager State Manager pour maintenir la cohérence de votre logiciel. Si les mises à jour ne sont pas disponibles, envisagez de supprimer ou de désactiver l'application vulnérable jusqu'à la publication d'un correctif ou d'autres mesures d'atténuation, telles que la restriction de l'accès réseau à l'application ou la désactivation de fonctionnalités vulnérables.

Suivez les conseils de correction spécifiques fournis dans les résultats d'Amazon Inspector. Cela peut impliquer de modifier les règles des groupes de sécurité, de modifier les configurations d'instance ou d'ajuster les paramètres de l'application.

Vérifiez si l'instance fait partie d'Auto Scaling Group. AMI-replacement l'application de correctifs est effectuée sur des infrastructures immuables en mettant à jour l'ID AMI configuré pour déployer de nouvelles instances Amazon EC2 dans un groupe Auto Scaling. Si vous utilisez une custom/golden AMI, créez une instance avec la nouvelle AMI, puis personnalisez-la et créez une nouvelle AMI dorée. Pour plus d'informations, voir Mise à jour de l'AMI et application de correctifs (utilisation d'AMI patchées pour les groupes Auto Scaling).

Considérations futures

Pour éviter que cela ne se reproduise, envisagez de mettre en œuvre un programme de gestion des vulnérabilités. Amazon Inspector peut être configuré pour rechercher automatiquement les CVE sur vos instances. Amazon Inspector peut également être intégré à Security Hub pour des corrections automatiques. Envisagez de mettre en œuvre un calendrier d'application régulier des correctifs à l'aide des fenêtres de maintenance de Systems Manager afin de minimiser les interruptions de vos instances.

L'instance EC2 possède un End-Of-Life système d'exploitation

L'instance EC2 exécute un système d'exploitation en fin de vie qui n'est plus pris en charge ni maintenu par le développeur d'origine. Cela expose l'instance à des failles de sécurité et à des attaques potentielles. Lorsque les systèmes d'exploitation arrivent en fin de vie, les fournisseurs cessent généralement de publier de nouveaux avis de sécurité. Les avis de sécurité existants peuvent également être supprimés des flux des fournisseurs. Par conséquent, Amazon Inspector pourrait arrêter de générer des résultats pour les CVE connus, ce qui créerait de nouvelles failles dans la couverture de sécurité.

Consultez la section Systèmes d'exploitation abandonnés dans le guide de l'utilisateur d'Amazon Inspector pour obtenir des informations sur les systèmes d'exploitation en fin de vie qui peuvent être détectés par Amazon Inspector.

Correction : mise à jour vers une version du système d'exploitation prise en charge

Effectuez la mise à jour vers une version compatible du système d'exploitation. Dans la recherche d'exposition, ouvrez la ressource pour accéder à la ressource concernée. Avant de mettre à jour la version du système d'exploitation de votre instance, créez un instantané ou une sauvegarde AMI au cas où vous auriez besoin de revenir en arrière. Passez ensuite en revue les versions disponibles dans Systèmes d'exploitation pris en charge dans le guide de l'utilisateur Amazon Inspector pour obtenir la liste des versions de systèmes d'exploitation actuellement prises en charge.

L'instance EC2 contient des packages logiciels malveillants

Les packages malveillants sont des composants logiciels contenant du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les packages malveillants constituent une menace active et critique pour votre instance, car les attaquants peuvent exécuter automatiquement du code malveillant sans exploiter de vulnérabilité. En suivant les meilleures pratiques de sécurité, supprimez les packages malveillants pour protéger votre instance contre d'éventuelles attaques.

Remédiation : suppression des packages malveillants

Consultez les détails du package malveillant dans la section Références de l'onglet Vulnérabilité du trait pour comprendre la menace. Supprimez les packages malveillants identifiés à l'aide du gestionnaire de packages approprié. Consultez l'outil de gestion des packages dans le guide de l'utilisateur d'Amazon Linux 2023 pour un exemple. Après avoir supprimé les packages malveillants, pensez à effectuer une analyse pour vous assurer que tous les packages susceptibles d'avoir été installés par le code malveillant ont été supprimés. Pour plus d'informations, consultez la section Démarrage de l'analyse des On-demand programmes malveillants GuardDuty dans le.

L'instance EC2 contient des fichiers malveillants

Les fichiers malveillants contiennent du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les fichiers malveillants constituent une menace active et critique pour votre instance, car les attaquants peuvent exécuter automatiquement du code malveillant sans exploiter de vulnérabilité. En suivant les meilleures pratiques de sécurité, supprimez les fichiers malveillants pour protéger votre instance contre d'éventuelles attaques.

Remédiation : supprimer les fichiers malveillants

Pour identifier le volume Amazon Elastic Block Store (Amazon EBS) spécifique qui contient des fichiers malveillants, consultez la section Ressources des détails de recherche de la caractéristique. Après avoir identifié le volume contenant le fichier malveillant, créez un instantané du volume avant d'apporter des modifications, puis supprimez les fichiers malveillants identifiés. Après avoir supprimé les fichiers malveillants, pensez à effectuer une analyse pour vous assurer que tous les fichiers susceptibles d'avoir été installés par le fichier malveillant ont été supprimés. Pour plus d'informations, consultez la section Démarrage de l'analyse des On-demand programmes malveillants GuardDuty dans le.

Caractéristiques d'impact pour les instances EC2

Les caractéristiques d'impact décrivent le rayon d'explosion potentiel d'une exposition. Security Hub analyse les autorisations effectives du Gestion des identités et des accès AWS principal associé à l'instance EC2 afin de déterminer les ressources en aval qu'un attaquant pourrait atteindre si l'instance est compromise. Chaque trait d'impact identifie un modèle d'escalade de privilèges spécifique. Pour réduire votre rayon d'action, passez en revue les chemins d'autorisation décrits dans chaque trait et supprimez tous les privilèges inutiles.

Conformément aux principes de sécurité standard, accordez le moindre privilège en ne fournissant que les autorisations requises pour effectuer une tâche. Remplacez les politiques générales par

des politiques restreintes qui n'accordent que les actions et les ressources spécifiques nécessaires. Pour identifier les autorisations non utilisées à supprimer, utilisez IAM Access Analyzer pour générer des recommandations en fonction de l'historique des accès. Pour plus d'informations, consultez les sections Constatations relatives à l'accès externe et inutilisé et Appliquer les autorisations de moindre privilège dans le guide de l'utilisateur IAM.

Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié

Le principal associé peut transmettre un rôle et injecter du code dans une ressource de calcul qui dispose déjà d'autorisations élevées. Cela permet au mandant de prendre le contrôle total de l'exécuteur testamentaire et d'effectuer toutes les actions autorisées par le rôle de l'exécuteur testamentaire.

A une trajectoire d'escalade politique directe

Le principal associé peut modifier directement les politiques IAM pour s'accorder des autorisations supplémentaires, augmentant ainsi ses propres privilèges sans ressources intermédiaires.

A une voie de détournement de la politique de confiance

Le principal associé peut modifier la politique de confiance d'un rôle IAM pour s'autoriser à assumer ce rôle, en obtenant les autorisations du rôle.

Possède un chemin de données vers un

Le principal associé peut chiffrer ou supprimer des données d'une manière susceptible d'être utilisée pour les rançongiciels, par exemple en chiffrant des objets Amazon S3 à l'aide d'une AWS KMS clé gérée par le client, puis en modifiant la politique relative aux clés.

Dispose d'un chemin de restriction supprimé

Le principal associé peut supprimer les restrictions de sécurité telles que les limites d'autorisation, les politiques de contrôle des services ou les instructions de refus de politiques basées sur les ressources, élargissant ainsi ce que peuvent faire les autres principaux ou la ressource elle-même.

A un rôle de passe pour créer le chemin de l'exécuteur

Le principal associé peut créer une nouvelle ressource de calcul (telle qu'une fonction Lambda ou une instance Amazon EC2) et lui transmettre un rôle privilégié, libérant ainsi ses propres autorisations via la nouvelle ressource.

Dispose d'un rôle d'échange (chemin d'exécuteur existant)

Le principal associé peut modifier le rôle IAM attaché à une ressource de calcul existante, en le remplaçant par un rôle plus privilégié pour augmenter l'accès.

Dispose d'une voie d'escalade en chaîne de rôles

Le principal associé peut assumer une séquence de rôles, chaque rôle de la chaîne bénéficiant d'autorisations progressivement plus larges, pour atteindre finalement un rôle hautement privilégié.

Possède un chemin d'exécution privilégié pour l'injection de code

Le principal associé peut injecter du code dans une ressource de calcul en cours d'exécution dotée d'autorisations élevées, en exécutant des opérations arbitraires sous le rôle privilégié de cette ressource.

A désactivé le chemin de la piste d'audit

Le principal associé peut désactiver les services de journalisation ou de surveillance CloudTrail, tels que la couverture efficace de ses traces pendant ou après une escalade.

A accès au chemin d'exécution existant

Le principal associé peut invoquer ou se connecter à une ressource de calcul existante et utiliser le rôle qui lui est attaché pour effectuer des actions privilégiées.

Dispose d'un parcours de création d'identifiants

Le principal associé peut créer de nouvelles informations d'identification à long terme (telles que des clés d'accès ou des profils de connexion) pour d'autres mandants, en établissant des chemins d'accès persistants qui survivent aux rotations de mots de passe ou aux expirations de session.

Dispose d'un chemin d'accès aux données du rôle de passe

Le principal associé peut créer une ressource de service et lui transmettre un rôle ayant accès à des données sensibles, en obtenant un accès indirect à ces données via la nouvelle ressource.

A un rôle de passe, une tâche, un chemin de détournement

Le principal associé peut transmettre un rôle à une tâche planifiée ou pilotée par un événement (telle qu'une fonction Lambda déclenchée par un événement), ce qui lui permet d'exécuter du code arbitraire avec les autorisations de ce rôle.

Dispose d'un chemin d'accès aux données à saut unique

Le principal associé peut accéder directement à des ressources de données sensibles (telles que des compartiments Amazon S3 ou des tables DynamoDB) via ses autorisations existantes, sans avoir besoin d'étapes d'escalade intermédiaires.

Possède une capacité d'avancement

Le principal associé dispose d'un chemin d'escalade des privilèges qui fait progresser ses capacités globales au-delà de ce que suggèrent ses autorisations directement attribuées. Il s'agit d'une classification générale pour les chemins qui ne correspondent pas à un modèle plus spécifique.

Remédier aux risques pour les services Amazon ECS

AWS Security Hub peut générer des résultats d'exposition pour les services Amazon Elastic Container Service (Amazon ECS).

Le service Amazon ECS impliqué dans la détection d'une exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la découverte. Vous pouvez récupérer ces informations sur les ressources sur la console Security Hub ou par programmation à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration pour les services Amazon ECS
  - Le service Amazon ECS utilise une définition de tâche qui permet aux conteneurs d'accéder aux systèmes de fichiers racine.
  - Le service Amazon ECS utilise une définition de tâche configurée pour partager l'espace de noms des processus d'un hôte
  - Le service Amazon ECS utilise une définition de tâche configurée avec des informations d'identification en texte clair dans les variables d'environnement.
  - Le service Amazon ECS possède un groupe de sécurité ouvert
  - Le service Amazon ECS possède des adresses IP publiques
  - Le service Amazon ECS utilise une définition de tâche configurée avec le mode réseau hôte activé.
- Caractéristiques d'accessibilité pour les services Amazon ECS
  - Le service Amazon ECS est accessible via Internet
- Caractéristiques de vulnérabilité des services Amazon ECS
  - Le service Amazon ECS contient un conteneur contenant des vulnérabilités logicielles exploitables par le réseau et présentant une forte probabilité d'exploitation
  - Le service Amazon ECS contient un conteneur présentant des vulnérabilités logicielles
  - Le service Amazon ECS possède un conteneur doté End-Of-Life d'un système d'exploitation
  - Le service Amazon ECS contient un conteneur contenant des packages logiciels malveillants.
- Caractéristiques d'impact pour les services Amazon ECS
  - Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié
  - A une trajectoire d'escalade politique directe
  - A une voie de détournement de la politique de confiance
  - Possède un chemin de données vers un
  - Dispose d'un chemin de restriction supprimé
  - A un rôle de passe pour créer le chemin de l'exécuteur
  - Dispose d'un rôle d'échange (chemin d'exécuteur existant)
  - Dispose d'une voie d'escalade en chaîne de rôles
  - Possède un chemin d'exécution privilégié pour l'injection de code
  - A désactivé le chemin de la piste d'audit
  - A accès au chemin d'exécution existant

- Dispose d'un parcours de création d'identifiants
- Dispose d'un chemin d'accès aux données du rôle de passe
- A un rôle de passe, une tâche, un chemin de détournement
- Dispose d'un chemin d'accès aux données à saut unique
- Possède une capacité d'avancement

Caractéristiques de mauvaise configuration pour les services Amazon ECS

Voici les caractéristiques de configuration erronées des services Amazon ECS et les étapes à suivre pour y remédier.

Le service Amazon ECS utilise une définition de tâche qui permet aux conteneurs d'accéder aux systèmes de fichiers racine.

Les conteneurs Amazon ECS ayant accès au système de fichiers racine de l'hôte peuvent potentiellement lire, modifier ou exécuter des fichiers critiques sur le système hôte. Cette configuration augmente le risque qu'un conteneur compromis soit utilisé pour accéder à des ressources ou les modifier en dehors de la portée prévue, exposant ainsi des données sensibles sur le système de fichiers hôte. Conformément aux principes de sécurité standard, accordez le moins de privilèges, ce qui signifie que vous n'accordez que les autorisations requises pour effectuer une tâche.

Correction : examen et modification des conteneurs ayant accès au système de fichiers hôte

Dans le résultat de l'exposition, identifiez l'ARN de définition de tâche. Ouvrez la définition de tâche dans la console Amazon ECS. Recherchez la section volumes dans la définition de tâche qui définit les mappages de chemins d'hôte.

Passez en revue la définition de la tâche pour déterminer si l'accès au système de fichiers hôte est requis pour la fonctionnalité du conteneur. Si l'accès au système de fichiers hôte n'est pas requis, créez une nouvelle révision de définition de tâche et supprimez toutes les définitions de volume qui utilisent des chemins d'hôte. Si l'accès au système de fichiers hôte est requis, pensez à configurer le conteneur pour qu'il utilise un système de fichiers en lecture seule afin d'empêcher toute modification non autorisée.

Le service Amazon ECS utilise une définition de tâche configurée pour partager l'espace de noms des processus d'un hôte

Les conteneurs Amazon ECS exécutés avec des espaces de noms exposés peuvent potentiellement accéder aux ressources du système hôte et à d'autres espaces de noms de conteneurs. Cette configuration pourrait permettre à un conteneur compromis d'échapper à sa limite d'isolation, en accédant à des processus, à des interfaces réseau ou à d'autres ressources en dehors de sa portée prévue.

Un espace de noms PID (Process ID) permet de séparer les processus. Il empêche les processus du système d'être visibles et permet de réutiliser les PID, y compris le PID 1. Si l'espace de noms PID de l'hôte est partagé avec des conteneurs, ceux-ci peuvent voir tous les processus du système hôte, ce qui réduit l'isolation au niveau des processus. Cela pourrait entraîner un accès non autorisé aux processus hôtes, y compris la possibilité de les manipuler et de les arrêter. Conformément aux principes de sécurité standard, maintenez une isolation appropriée de l'espace de noms pour les conteneurs.

Correction : mise à jour des définitions de tâches avec des espaces de noms exposés

Ouvrez l'onglet Ressources de l'exposition, identifiez la définition de la tâche avec l'espace de noms exposé. Ouvrez la définition de tâche dans la console Amazon ECS. Recherchez les paramètres PIDMode avec la valeur host, qui partageraient les espaces de noms des ID de processus avec l'hôte. Supprimez les paramètres PIDMode : host de vos définitions de tâches pour vous assurer que les conteneurs s'exécutent avec une isolation d'espace de noms appropriée.

Le service Amazon ECS utilise une définition de tâche configurée avec des informations d'identification en texte clair dans les variables d'environnement.

Les conteneurs Amazon ECS comportant des informations d'identification en texte clair dans les variables d'environnement exposent des informations d'authentification sensibles qui pourraient être compromises si un attaquant accédait à la définition de la tâche, à l'environnement du conteneur ou aux journaux du conteneur. Cela crée un risque de sécurité important, car les informations d'identification divulguées pourraient être utilisées pour accéder à d'autres AWS services ou ressources.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Remplacer les informations d'identification en texte clair

Dans la recherche d'exposition, identifiez la définition de la tâche à l'aide d'informations d'identification en texte clair. Ouvrez la définition de tâche dans la console Amazon ECS. Dans la définition du conteneur, recherchez les variables d'environnement qui contiennent des valeurs sensibles telles que des clés AWS d'accès, des mots de passe de base de données ou des jetons d'API.

Envisagez les alternatives suivantes pour transmettre les informations d'identification :

- Au lieu d'utiliser des clés AWS d'accès, utilisez les rôles d'exécution des tâches IAM et les rôles de tâches pour accorder des autorisations à vos conteneurs.
- Stockez les informations d'identification sous forme de secrets AWS Secrets Manager et référencez-les dans la définition de votre tâche.

Mise à jour les définitions de tâche

Créez une nouvelle révision de votre définition de tâche qui gère les informations d'identification de manière sécurisée. Mettez ensuite à jour votre service Amazon ECS pour utiliser la nouvelle révision de définition des tâches.

Le service Amazon ECS possède un groupe de sécurité ouvert

Les groupes de sécurité agissent comme des pare-feux virtuels pour vos tâches Amazon ECS afin de contrôler le trafic entrant et sortant. Les groupes de sécurité ouverts, qui permettent un accès illimité à partir de n'importe quelle adresse IP, peuvent exposer vos conteneurs à un accès non autorisé, augmentant ainsi le risque d'exposition à des outils d'analyse automatisés et à des attaques ciblées. Conformément aux principes de sécurité standard, limitez l'accès des groupes de sécurité à des adresses IP et à des ports spécifiques.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Passez en revue les règles des groupes de sécurité et évaluez la configuration actuelle

Ouvrez la ressource pour le groupe de sécurité Amazon ECS. Évaluez quels ports sont ouverts et accessibles à partir de larges plages d'adresses IP, telles que`(0.0.0.0/0 or ::/0)`.

Modifier les règles des groupes de sécurité

Modifiez les règles de votre groupe de sécurité pour restreindre l'accès à des adresses IP ou à des plages d'adresses IP fiables spécifiques. Lorsque vous mettez à jour les règles de votre groupe

de sécurité, pensez à séparer les exigences d'accès pour les différents segments du réseau en créant des règles pour chaque plage d'adresses IP source requise ou en limitant l'accès à des ports spécifiques.

Modifier les règles des groupes de sécurité

Envisagez les options suivantes pour d'autres méthodes d'accès :

- Session Manager fournit un accès shell sécurisé à vos instances Amazon EC2 sans avoir besoin de ports entrants, de gérer des clés SSH ou de gérer des hôtes bastion.
- Les NACL fournissent une couche de sécurité supplémentaire au niveau du sous-réseau. Contrairement aux groupes de sécurité, les NACL sont sans état et nécessitent la définition explicite de règles entrantes et sortantes.

Le service Amazon ECS possède des adresses IP publiques

Les services Amazon ECS auxquels des adresses IP publiques sont attribuées à leurs tâches sont directement accessibles depuis Internet. Bien que cela puisse être nécessaire pour les services qui doivent être accessibles au public, cela augmente la surface d'attaque et le risque d'accès non autorisé.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Identifier les services dotés d'adresses IP publiques

Dans la recherche d'exposition, identifiez le service Amazon ECS auquel des adresses IP publiques sont attribuées à ses tâches. Recherchez le `assignPublicIp` paramètre dont la valeur est égale `ENABLED` à dans la configuration du service.

Mise à jour les définitions de tâche

Créez une nouvelle révision de votre définition de tâche qui désactive les adresses IP publiques. Mettez ensuite à jour votre service Amazon ECS pour utiliser la nouvelle révision de définition des tâches.

Implémenter des modèles d'accès au réseau privé

Pour les instances qui exécutent des applications Web, pensez à utiliser un équilibreur de charge (LB). Le LB peut être configuré pour permettre à vos instances de s'exécuter dans des sous-réseaux privés tandis que le LB s'exécute dans un sous-réseau public et gère le trafic Internet.

Le service Amazon ECS utilise une définition de tâche configurée avec le mode réseau hôte activé.

Les conteneurs Amazon ECS exécutés en mode réseau hôte partagent l'espace de noms réseau avec l'hôte, ce qui permet un accès direct aux interfaces réseau, aux ports et aux tables de routage de l'hôte. Cette configuration contourne l'isolation réseau fournie par les conteneurs, exposant potentiellement les services exécutés sur le conteneur directement aux réseaux externes et permettant aux conteneurs de modifier les paramètres du réseau hôte. Conformément aux principes de sécurité standard, maintenez une isolation réseau appropriée pour les conteneurs.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Désactiver le mode réseau hôte

Dans la recherche d'exposition, identifiez la définition de la tâche avec le mode réseau hôte. Ouvrez la définition de tâche dans la console Amazon ECS. Recherchez le paramètre NetworkMode avec la valeur host dans la définition de la tâche.

Envisagez les options suivantes pour désactiver le mode réseau hôte :

- Le mode `awsvpc` réseau fournit le plus haut niveau d'isolation réseau en dotant chaque tâche de sa propre interface réseau élastique.
- Le mode `bridge` réseau assure l'isolation tout en autorisant les mappages de ports afin d'exposer des ports de conteneur spécifiques à l'hôte.

Mise à jour les définitions de tâche

Créez une nouvelle révision de votre définition de tâche à l'aide de la configuration du mode réseau mise à jour. Mettez ensuite à jour votre service Amazon ECS pour utiliser la nouvelle révision de définition des tâches.

Caractéristiques d'accessibilité pour les services Amazon ECS

Voici les caractéristiques d'accessibilité des services Amazon ECS et les étapes de correction suggérées.

Le service Amazon ECS est accessible via Internet

Un service Amazon ECS qui exécute des tâches sur un sous-réseau public est directement accessible depuis Internet. Cela augmente la surface d'attaque et le risque d'accès non autorisé. En suivant les principes de sécurité standard, exécutez des tâches sur des sous-réseaux privés et autorisez uniquement l'accès Internet dont votre service a besoin.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Exécuter des tâches sur un sous-réseau privé

Pour déplacer vos tâches hors d'un sous-réseau public, mettez à jour la configuration réseau correspondant à votre type de lancement :

- Pour Fargate, spécifiez des sous-réseaux privés dans la configuration réseau de votre service Amazon ECS et réglez-le sur. `assignPublicIp` `DISABLED` Amazon ECS héberge chaque tâche sur un sous-réseau privé et achemine son trafic sortant via une passerelle NAT que vous associez au sous-réseau.
- Pour EC2, lancez les instances de conteneur qui fournissent la capacité de votre cluster sur des sous-réseaux privés. Les tâches utilisent le réseau privé de l'hôte et acheminent le trafic sortant via une passerelle NAT.

Utiliser une passerelle NAT pour l'accès sortant

Pour les tâches d'un sous-réseau privé qui nécessitent un accès Internet sortant, utilisez une passerelle NAT. Vous pouvez utiliser une passerelle NAT pour permettre aux tâches de démarrer des connexions sortantes vers Internet et d'empêcher les connexions entrantes depuis Internet. Pour plus d'informations, consultez Connecter les applications Amazon ECS à Internet dans le manuel Amazon ECS Developer Guide.

Utiliser un équilibreur de charge pour l'accès entrant

Pour les services qui doivent accepter le trafic Internet, exécutez vos tâches sur des sous-réseaux privés à l'aide d'un équilibreur de charge qui s'exécute sur un sous-réseau public. Pour renforcer la protection contre les exploits Web et les robots, associez le AWS Web Application Firewall (WAF) à votre équilibreur de charge. Pour plus d'informations, consultez la section Utiliser l'équilibrage de charge pour distribuer le trafic du service Amazon ECS dans le guide du développeur Amazon ECS.

Caractéristiques de vulnérabilité des services Amazon ECS

Voici les caractéristiques de vulnérabilité d'Amazon ECS et les étapes de correction suggérées.

Le service Amazon ECS contient un conteneur contenant des vulnérabilités logicielles exploitables par le réseau et présentant une forte probabilité d'exploitation

1. Comprenez l'exposition

   Les résultats relatifs aux vulnérabilités des packages identifient les packages logiciels de votre AWS environnement qui sont exposés à des vulnérabilités et expositions courantes (CVE). Les attaquants peuvent exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. Les images de conteneurs ECR peuvent contenir des résultats de vulnérabilité de package.
2. Remédier à l'exposition
   a. Mettre à jour la version du package

      Passez en revue la découverte de la vulnérabilité du package pour votre image de conteneur ECR. Mettez à jour la version du package comme suggéré par Amazon Inspector. Pour plus d'informations, consultez la section Afficher les détails de vos résultats Amazon Inspector dans le guide de l'utilisateur Amazon Inspector. La section Remédiation des détails de la recherche dans la console Amazon Inspector vous indique les commandes que vous pouvez exécuter pour mettre à jour le package.

   b. Mettre à jour les images du conteneur de base

      Reconstruisez et mettez à jour régulièrement les images des conteneurs de base pour maintenir vos conteneurs à jour. Lorsque vous reconstruisez une image, n'incluez pas de composants inutiles pour réduire la surface d'attaque. Pour obtenir des instructions sur la reconstruction d'une image de conteneur, voir Reconstruire souvent vos images.

Le service Amazon ECS contient un conteneur présentant des vulnérabilités logicielles

Les packages logiciels installés sur les conteneurs Amazon ECS peuvent être exposés à des vulnérabilités et expositions courantes (CVE). Les vulnérabilités de faible priorité représentent des failles de sécurité dont la gravité ou l'exploitabilité sont moindres par rapport aux vulnérabilités hautement prioritaires. Bien que ces vulnérabilités présentent un risque immédiat moindre, les attaquants peuvent toujours exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Mettre à jour les images des conteneurs concernés

Consultez la section Références de l'onglet Vulnérabilité du trait. La documentation du fournisseur peut inclure des directives de correction spécifiques.

Appliquez les mesures correctives appropriées en suivant ces directives générales :

- Mettez à jour les images de vos conteneurs pour utiliser des versions corrigées des packages concernés.
- Mettez à jour les dépendances concernées dans votre application vers leurs dernières versions sécurisées.

Après avoir mis à jour votre image de conteneur, transférez-la dans votre registre de conteneurs et mettez à jour la définition de votre tâche Amazon ECS pour utiliser la nouvelle image.

Considérations futures

Pour renforcer davantage le niveau de sécurité de vos images de conteneurs, pensez à suivre les meilleures pratiques en matière de sécurité des tâches et des conteneurs d'Amazon ECS. Amazon Inspector peut être configuré pour rechercher automatiquement les CVE sur vos conteneurs. Amazon Inspector peut également être intégré à Security Hub pour des corrections automatiques. Envisagez de mettre en œuvre un calendrier d'application régulier des correctifs à l'aide des fenêtres de maintenance de Systems Manager afin de minimiser les perturbations de vos conteneurs.

Le service Amazon ECS possède un conteneur doté End-Of-Life d'un système d'exploitation

Le conteneur Amazon ECS repose sur un système d'exploitation en fin de vie qui n'est plus pris en charge ni maintenu par le développeur d'origine. Cela expose le conteneur à des failles de sécurité et à des attaques potentielles. Lorsque les systèmes d'exploitation arrivent en fin de vie, les fournisseurs cessent généralement de publier de nouveaux avis de sécurité. Les avis de sécurité existants peuvent également être supprimés des flux des fournisseurs. Par conséquent, Amazon Inspector pourrait arrêter de générer des résultats pour les CVE connus, ce qui créerait de nouvelles failles dans la couverture de sécurité.

Consultez la section Systèmes d'exploitation abandonnés dans le guide de l'utilisateur d'Amazon Inspector pour obtenir des informations sur les systèmes d'exploitation en fin de vie qui peuvent être détectés par Amazon Inspector.

Correction : mise à jour vers une version du système d'exploitation prise en charge

Effectuez la mise à jour vers une version compatible du système d'exploitation. Dans la recherche d'exposition, ouvrez la ressource pour accéder à la ressource concernée. Avant de mettre à jour la version du système d'exploitation dans l'image de votre conteneur, consultez les versions disponibles dans Systèmes d'exploitation pris en charge dans le guide de l'utilisateur Amazon Inspector pour obtenir la liste des versions de système d'exploitation actuellement prises en charge. Après avoir mis à jour votre image de conteneur, transférez-la dans votre registre de conteneurs et mettez à jour la définition de votre tâche Amazon ECS pour utiliser la nouvelle image.

Le service Amazon ECS contient un conteneur contenant des packages logiciels malveillants.

Les packages malveillants sont des composants logiciels contenant du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les packages malveillants constituent une menace active et critique pour les images de vos conteneurs Amazon ECS, car les attaquants peuvent exécuter automatiquement du code malveillant sans exploiter de vulnérabilité. En suivant les meilleures pratiques de sécurité, supprimez les packages malveillants pour protéger vos conteneurs contre d'éventuelles attaques.

Remédiation : suppression des packages malveillants

Consultez les détails du package malveillant dans la section Références de l'onglet Vulnérabilité du trait pour comprendre la menace. Supprimez les packages malveillants identifiés des images de vos conteneurs, puis reconstruisez-les. Pour plus d'informations, consultez ContainerDependency dans la AWS référence de l'API Amazon ECS.

Après avoir mis à jour votre image de conteneur, transférez-la dans votre registre de conteneurs et mettez à jour la définition de votre tâche Amazon ECS pour utiliser la nouvelle image. Pour plus d'informations, consultez la section Mise à jour d'une définition de tâche Amazon ECS à l'aide de la console dans le manuel AWS Amazon ECS Developer Guide.

Caractéristiques d'impact pour les services Amazon ECS

Les caractéristiques d'impact décrivent le rayon d'explosion potentiel d'une exposition. Security Hub analyse les autorisations effectives du Gestion des identités et des accès AWS principal associé au service Amazon ECS afin de déterminer les ressources en aval qu'un attaquant pourrait atteindre

si le service est compromis. Chaque trait d'impact identifie un modèle d'escalade de privilèges spécifique. Pour réduire votre rayon d'action, passez en revue les chemins d'autorisation décrits dans chaque trait et supprimez tous les privilèges inutiles.

Conformément aux principes de sécurité standard, accordez le moindre privilège en ne fournissant que les autorisations requises pour effectuer une tâche. Remplacez les politiques générales par des politiques restreintes qui n'accordent que les actions et les ressources spécifiques nécessaires. Pour identifier les autorisations non utilisées à supprimer, utilisez IAM Access Analyzer pour générer des recommandations en fonction de l'historique des accès. Pour plus d'informations, consultez les sections Constatations relatives à l'accès externe et inutilisé et Appliquer les autorisations de moindre privilège dans le guide de l'utilisateur IAM.

Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié

Le principal associé peut transmettre un rôle et injecter du code dans une ressource de calcul qui dispose déjà d'autorisations élevées. Cela permet au mandant de prendre le contrôle total de l'exécuteur testamentaire et d'effectuer toutes les actions autorisées par le rôle de l'exécuteur testamentaire.

A une trajectoire d'escalade politique directe

Le principal associé peut modifier directement les politiques IAM pour s'accorder des autorisations supplémentaires, augmentant ainsi ses propres privilèges sans ressources intermédiaires.

A une voie de détournement de la politique de confiance

Le principal associé peut modifier la politique de confiance d'un rôle IAM pour s'autoriser à assumer ce rôle, en obtenant les autorisations du rôle.

Possède un chemin de données vers un

Le principal associé peut chiffrer ou supprimer des données d'une manière susceptible d'être utilisée pour les rançongiciels, par exemple en chiffrant des objets Amazon S3 à l'aide d'une AWS KMS clé gérée par le client, puis en modifiant la politique relative aux clés.

Dispose d'un chemin de restriction supprimé

Le principal associé peut supprimer les restrictions de sécurité telles que les limites d'autorisation, les politiques de contrôle des services ou les instructions de refus de politiques basées sur les ressources, élargissant ainsi ce que peuvent faire les autres principaux ou la ressource elle-même.

A un rôle de passe pour créer le chemin de l'exécuteur

Le principal associé peut créer une nouvelle ressource de calcul (telle qu'une fonction Lambda ou une instance Amazon EC2) et lui transmettre un rôle privilégié, libérant ainsi ses propres autorisations via la nouvelle ressource.

Dispose d'un rôle d'échange (chemin d'exécuteur existant)

Le principal associé peut modifier le rôle IAM attaché à une ressource de calcul existante, en le remplaçant par un rôle plus privilégié pour augmenter l'accès.

Dispose d'une voie d'escalade en chaîne de rôles

Le principal associé peut assumer une séquence de rôles, chaque rôle de la chaîne bénéficiant d'autorisations progressivement plus larges, pour atteindre finalement un rôle hautement privilégié.

Possède un chemin d'exécution privilégié pour l'injection de code

Le principal associé peut injecter du code dans une ressource de calcul en cours d'exécution dotée d'autorisations élevées, en exécutant des opérations arbitraires sous le rôle privilégié de cette ressource.

A désactivé le chemin de la piste d'audit

Le principal associé peut désactiver les services de journalisation ou de surveillance CloudTrail, tels que la couverture efficace de ses traces pendant ou après une escalade.

A accès au chemin d'exécution existant

Le principal associé peut invoquer ou se connecter à une ressource de calcul existante et utiliser le rôle qui lui est attaché pour effectuer des actions privilégiées.

Dispose d'un parcours de création d'identifiants

Le principal associé peut créer de nouvelles informations d'identification à long terme (telles que des clés d'accès ou des profils de connexion) pour d'autres mandants, en établissant des chemins d'accès persistants qui survivent aux rotations de mots de passe ou aux expirations de session.

Dispose d'un chemin d'accès aux données du rôle de passe

Le principal associé peut créer une ressource de service et lui transmettre un rôle ayant accès à des données sensibles, en obtenant un accès indirect à ces données via la nouvelle ressource.

A un rôle de passe, une tâche, un chemin de détournement

Le principal associé peut transmettre un rôle à une tâche planifiée ou pilotée par un événement (telle qu'une fonction Lambda déclenchée par un événement), ce qui lui permet d'exécuter du code arbitraire avec les autorisations de ce rôle.

Dispose d'un chemin d'accès aux données à saut unique

Le principal associé peut accéder directement à des ressources de données sensibles (telles que des compartiments Amazon S3 ou des tables DynamoDB) via ses autorisations existantes, sans avoir besoin d'étapes d'escalade intermédiaires.

Possède une capacité d'avancement

Le principal associé dispose d'un chemin d'escalade des privilèges qui fait progresser ses capacités globales au-delà de ce que suggèrent ses autorisations directement attribuées. Il s'agit d'une classification générale pour les chemins qui ne correspondent pas à un modèle plus spécifique.

Corriger les risques pour les clusters Amazon EKS

AWS Security Hub peut générer des résultats d'exposition pour les clusters Amazon Elastic Kubernetes Service (Amazon EKS).

Le cluster Amazon EKS impliqué dans la détection d'une exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la découverte. Vous pouvez récupérer ces informations sur les ressources sur la console Security Hub ou par programmation à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration pour les clusters Amazon EKS
  - Le cluster Amazon EKS autorise l'accès public
  - Le cluster Amazon EKS utilise une version de Kubernetes non prise en charge
  - Le cluster Amazon EKS utilise des secrets Kubernetes non chiffrés
- Caractéristiques de vulnérabilité des clusters Amazon EKS
  - Le cluster Amazon EKS possède un conteneur contenant des vulnérabilités logicielles exploitables par le réseau et présentant une forte probabilité d'exploitation
  - Le cluster Amazon EKS possède un conteneur présentant des vulnérabilités logicielles
  - Le cluster Amazon EKS possède un conteneur avec un système End-Of-Life d'exploitation
  - Le cluster Amazon EKS possède un conteneur contenant des packages logiciels malveillants
  - Le cluster Amazon EKS contient des fichiers malveillants

Caractéristiques de mauvaise configuration pour les clusters Amazon EKS

Voici les caractéristiques de configuration erronées des clusters Amazon EKS et les étapes de correction suggérées.

Le cluster Amazon EKS autorise l'accès public

Le point de terminaison du cluster Amazon EKS est le point de terminaison que vous utilisez pour communiquer avec le serveur d'API Kubernetes de votre cluster. Par défaut, ce point de terminaison est public sur Internet. Les terminaux publics augmentent votre surface d'attaque et augmentent le risque d'accès non autorisé à votre serveur API Kubernetes, ce qui pourrait permettre aux attaquants d'accéder aux ressources du cluster ou de les modifier ou d'accéder à des données sensibles. Conformément aux meilleures pratiques de sécurité, limitez l'accès au point de terminaison de votre cluster Amazon EKS aux seules plages IP nécessaires.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Modifier l'accès aux terminaux

Dans la recherche d'exposition, ouvrez la ressource. Cela ouvre le cluster Amazon EKS concerné. Vous pouvez configurer votre cluster pour utiliser un accès privé, un accès public ou les deux.

Avec un accès privé, les requêtes d'API Kubernetes qui proviennent du VPC de votre cluster utilisent le point de terminaison VPC privé. Avec un accès public, les requêtes d'API Kubernetes provenant de l'extérieur du VPC de votre cluster utilisent le point de terminaison public.

Modifier ou supprimer l'accès public au cluster

Pour modifier l'accès aux points de terminaison d'un cluster existant, consultez la section Modification de l'accès aux points de terminaison du cluster dans le guide de l'utilisateur d'Amazon Elastic Kubernetes Service. Implémentez des règles plus restrictives en fonction de plages IP ou de groupes de sécurité spécifiques. Si un accès public limité est nécessaire, limitez l'accès à des plages de blocs CIDR spécifiques ou utilisez des listes de préfixes.

Le cluster Amazon EKS utilise une version de Kubernetes non prise en charge

Amazon EKS prend en charge chaque version de Kubernetes pendant une période limitée. L'exécution de clusters avec des versions de Kubernetes non prises en charge peut exposer votre environnement à des failles de sécurité, car les correctifs CVE cesseront d'être publiés pour les versions obsolètes. Les versions non prises en charge peuvent contenir des failles de sécurité connues qui peuvent être exploitées par des attaquants et ne disposent pas des fonctionnalités de sécurité qui peuvent être disponibles dans les versions les plus récentes. En suivant les meilleures pratiques de sécurité, maintenez votre version de Kubernetes à jour.

Correction : mettre à jour la version de Kubernetes

Dans la recherche d'exposition, ouvrez la ressource. Cela ouvre le cluster Amazon EKS concerné. Avant de mettre à jour votre cluster, consultez les versions disponibles dans le cadre du support standard dans le Guide de l'utilisateur d'Amazon Elastic Kubernetes Service pour obtenir la liste des versions de Kubernetes actuellement prises en charge.

Le cluster Amazon EKS utilise des secrets Kubernetes non chiffrés

Les secrets Kubernetes sont, par défaut, stockés en clair dans le magasin de données sous-jacent (etcd) du serveur API. Toute personne ayant accès à l'API ou à etcd peut récupérer ou modifier un secret. Pour éviter cela, vous devez crypter les secrets Kubernetes au repos. Si les secrets Kubernetes ne sont pas chiffrés, ils sont vulnérables à un accès non autorisé si etcd est compromis. Étant donné que les secrets contiennent souvent des informations sensibles telles

que des mots de passe et des jetons d'API, leur divulgation peut entraîner un accès non autorisé à d'autres applications et données. En suivant les meilleures pratiques de sécurité, chiffrez toutes les informations sensibles stockées dans les secrets Kubernetes.

Remédiation : chiffrez les secrets de Kubernetes

Amazon EKS prend en charge le chiffrement des secrets Kubernetes à l'aide de clés KMS via le chiffrement d'enveloppe. Pour activer le chiffrement des secrets Kubernetes pour votre cluster EKS, consultez la section Chiffrer les secrets Kubernetes avec KMS sur les clusters existants dans le guide de l'utilisateur Amazon EKS.

Caractéristiques de vulnérabilité des clusters Amazon EKS

Voici les caractéristiques de vulnérabilité des clusters Amazon EKS.

Le cluster Amazon EKS possède un conteneur contenant des vulnérabilités logicielles exploitables par le réseau et présentant une forte probabilité d'exploitation

Les packages logiciels installés sur les clusters Amazon EKS peuvent être exposés à des vulnérabilités et expositions courantes (CVE). Les CVE critiques présentent des risques de sécurité importants pour votre AWS environnement. Les utilisateurs non autorisés peuvent exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. Les vulnérabilités critiques présentant une forte probabilité d'exploitation constituent des menaces de sécurité immédiates, car le code d'exploitation est peut-être déjà accessible au public et utilisé activement par des attaquants ou des outils d'analyse automatisés. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités pour protéger votre instance contre les attaques.

Correction : mettre à jour les instances concernées

Mettez à jour les images de vos conteneurs vers des versions plus récentes qui incluent des correctifs de sécurité pour les vulnérabilités identifiées. Cela implique généralement de reconstruire vos images de conteneur avec des images de base ou des dépendances mises à jour, puis de déployer les nouvelles images sur votre cluster Amazon EKS.

Le cluster Amazon EKS possède un conteneur présentant des vulnérabilités logicielles

Les packages logiciels installés sur les clusters Amazon EKS peuvent être exposés à des vulnérabilités et expositions courantes (CVE). Les CVE non critiques représentent des failles de sécurité dont la gravité ou l'exploitabilité sont inférieures à celles des CVE critiques. Bien que ces vulnérabilités présentent un risque immédiat moindre, les attaquants peuvent toujours exploiter ces

vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités pour protéger votre instance contre les attaques.

Correction : mettre à jour les instances concernées

Mettez à jour les images de vos conteneurs vers des versions plus récentes qui incluent des correctifs de sécurité pour les vulnérabilités identifiées. Cela implique généralement de reconstruire vos images de conteneur avec des images de base ou des dépendances mises à jour, puis de déployer les nouvelles images sur votre cluster Amazon EKS.

Le cluster Amazon EKS possède un conteneur avec un système End-Of-Life d'exploitation

L'image du conteneur Amazon EKS repose sur un système d'exploitation en fin de vie qui n'est plus pris en charge ni maintenu par le développeur d'origine. Cela expose le conteneur à des failles de sécurité et à des attaques potentielles. Lorsque les systèmes d'exploitation arrivent en fin de vie, les fournisseurs cessent généralement de publier de nouveaux avis de sécurité. Les avis de sécurité existants peuvent également être supprimés des flux des fournisseurs. Par conséquent, Amazon Inspector pourrait arrêter de générer des résultats pour les CVE connus, ce qui créerait de nouvelles failles dans la couverture de sécurité.

Consultez la section Systèmes d'exploitation abandonnés dans le guide de l'utilisateur d'Amazon Inspector pour obtenir des informations sur les systèmes d'exploitation en fin de vie qui peuvent être détectés par Amazon Inspector.

Correction : mise à jour vers une version du système d'exploitation prise en charge

Effectuez la mise à jour vers une version compatible du système d'exploitation. Dans la recherche d'exposition, ouvrez la ressource pour accéder à la ressource concernée. Avant de mettre à jour la version du système d'exploitation dans l'image de votre conteneur, consultez les versions disponibles dans Systèmes d'exploitation pris en charge dans le guide de l'utilisateur Amazon Inspector pour obtenir la liste des versions de système d'exploitation actuellement prises en charge. Après avoir mis à jour l'image de votre conteneur, reconstruisez et redéployez vos conteneurs sur le cluster Amazon EKS.

Le cluster Amazon EKS possède un conteneur contenant des packages logiciels malveillants

Les packages malveillants sont des composants logiciels contenant du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les packages malveillants constituent une menace active et critique pour votre cluster Amazon EKS, car

les attaquants peuvent exécuter automatiquement du code malveillant sans exploiter de vulnérabilité. En suivant les meilleures pratiques de sécurité, supprimez les packages malveillants pour protéger votre cluster contre d'éventuelles attaques.

Remédiation : suppression des packages malveillants

Consultez les détails du package malveillant dans la section Références de l'onglet Vulnérabilité du trait pour comprendre la menace. Supprimez les packages malveillants identifiés des images de vos conteneurs. Supprimez ensuite les pods contenant l'image compromise.

Mettez à jour vos déploiements Kubernetes pour utiliser les images de conteneur mises à jour. Déployez ensuite vos modifications et redéployez vos pods.

Le cluster Amazon EKS contient des fichiers malveillants

Les fichiers malveillants contiennent du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les fichiers malveillants constituent une menace active et critique pour votre cluster, car les attaquants peuvent exécuter automatiquement du code malveillant sans exploiter de vulnérabilité. En suivant les meilleures pratiques de sécurité, supprimez les fichiers malveillants pour protéger votre cluster contre d'éventuelles attaques.

Remédiation : supprimer les fichiers malveillants

Pour identifier le volume Amazon Elastic Block Store (Amazon EBS) spécifique qui contient des fichiers malveillants, consultez la section Ressources des détails de recherche de la caractéristique. Après avoir identifié le volume contenant le fichier malveillant, supprimez les fichiers malveillants identifiés. Après avoir supprimé les fichiers malveillants, pensez à effectuer une analyse pour vous assurer que tous les fichiers susceptibles d'avoir été installés par le fichier malveillant ont été supprimés. Pour plus d'informations, consultez la section Démarrage de l'analyse des On-demand programmes malveillants GuardDuty dans le.

Remédier aux risques auxquels sont exposés les utilisateurs d'IAM

AWS Security Hub peut générer des résultats d'exposition pour les utilisateurs Gestion des identités et des accès AWS (IAM).

Sur la console Security Hub, l'utilisateur IAM impliqué dans la détection d'une exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Les meilleures pratiques IAM vous recommandent de créer des rôles IAM ou d'utiliser la fédération avec un fournisseur d'identité pour accéder à l' AWS aide d'informations d'identification temporaires au lieu de créer des utilisateurs IAM individuels. Si cette option convient à votre organisation et à votre cas d'utilisation, passez aux rôles ou à la fédération au lieu d'utiliser des utilisateurs IAM. Pour plus d'informations, consultez la section IAM users (Utilisateurs IAM) dans le IAM User Guide (Guide de l'utilisateur IAM).

Table des matières

- Caractéristiques de mauvaise configuration pour les utilisateurs IAM
  - L'authentification multifacteur n'est pas activée pour l'utilisateur IAM
  - Le AWS le compte de l'utilisateur IAM a des politiques de mot de passe faibles
  - L'utilisateur IAM possède des clés d'accès non pivotées
  - L'utilisateur IAM dispose d'une politique qui autorise un accès illimité au déchiffrement de la clé KMS
- Caractéristiques d'accès non utilisées pour les utilisateurs IAM
- Caractéristiques d'impact pour les utilisateurs d'IAM
  - Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié
  - A une trajectoire d'escalade politique directe
  - A une voie de détournement de la politique de confiance

- Possède un chemin de données vers un
- Dispose d'un chemin de restriction supprimé
- A un rôle de passe pour créer le chemin de l'exécuteur
- Dispose d'un rôle d'échange (chemin d'exécuteur existant)
- Dispose d'une voie d'escalade en chaîne de rôles
- Possède un chemin d'exécution privilégié pour l'injection de code
- A désactivé le chemin de la piste d'audit
- A accès au chemin d'exécution existant
- Dispose d'un parcours de création d'identifiants
- Dispose d'un chemin d'accès aux données du rôle de passe
- A un rôle de passe, une tâche, un chemin de détournement
- Dispose d'un chemin d'accès aux données à saut unique
- Possède une capacité d'avancement

Caractéristiques de mauvaise configuration pour les utilisateurs IAM

Voici les caractéristiques des erreurs de configuration pour les utilisateurs IAM et les étapes à suivre pour y remédier.

L'authentification multifacteur n'est pas activée pour l'utilisateur IAM

Multi-factor l'authentification (MFA) ajoute une couche de protection supplémentaire en plus du nom d'utilisateur et du mot de passe. Lorsque l'authentification multifacteur est activée et qu'un utilisateur IAM se connecte à un AWS site Web, il est invité à saisir son nom d'utilisateur, son mot de passe et un code d'authentification sur son appareil AWS MFA. Le mandataire d'authentification doit posséder un dispositif qui émet une clé sensible au temps et connaître des informations d'identification. Sans MFA, si le mot de passe d'un utilisateur est compromis, un attaquant obtient un accès complet aux AWS autorisations de l'utilisateur. Conformément aux principes de sécurité standard, activez l'authentification multifacteur pour tous les comptes et utilisateurs qui y ont Console de gestion AWS accès.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Passez en revue les types de MFA

AWS prend en charge les types de MFA suivants :

- Clés d'accès et clés de sécurité
- Applications d'authentification virtuelle
- Jetons TOTP matériels

Bien que l'authentification à l'aide d'un appareil physique fournisse généralement une protection de sécurité plus stricte, l'utilisation de tout type d'authentification multifacteur est plus sûre que la désactivation de l'authentification multifacteur.

Activer MFA

Pour activer le type d'authentification multifacteur adapté à vos besoins, consultez l'authentification AWS multifacteur dans IAM dans le guide de l'utilisateur IAM. Suivez les étapes correspondant au type d'authentification multifacteur spécifique que vous souhaitez implémenter. Pour les organisations qui gèrent de nombreux utilisateurs, vous souhaiterez peut-être renforcer l'utilisation de l'authentification multifacteur en exigeant que l'authentification multifacteur accède à des ressources sensibles.

Le AWS le compte de l'utilisateur IAM a des politiques de mot de passe faibles

Les politiques relatives aux mots de passe contribuent à la protection contre les accès non autorisés en imposant des exigences de complexité minimales pour les mots de passe des utilisateurs IAM. Sans politiques strictes en matière de mots de passe, il existe un risque accru que les comptes des utilisateurs soient compromis par le biais de devinettes de mots de passe ou d'attaques par force brute. Conformément aux principes de sécurité standard, mettez en œuvre une politique de mot de passe robuste pour garantir que les utilisateurs créent des mots de passe complexes difficiles à deviner.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Configurez une politique de mot de passe robuste

Accédez au tableau de bord IAM et accédez aux paramètres du compte. Vérifiez les paramètres actuels de la politique de mot de passe de votre compte, notamment la longueur minimale, les types de caractères requis et les paramètres d'expiration du mot de passe.

Suivez au minimum ces bonnes pratiques lors de la définition de votre politique en matière de mots de passe :

- Nécessite au moins une majuscule.
- Nécessite au moins une lettre minuscule.
- Nécessite au moins un symbole.
- Il faut au moins un numéro.
- Nécessite au moins huit caractères.

Considérations supplémentaires en matière de sécurité

Envisagez ces mesures de sécurité supplémentaires en plus d'une politique de mot de passe robuste :

- Le MFA ajoute une couche de sécurité supplémentaire en exigeant une forme d'authentification supplémentaire. Cela permet d'empêcher tout accès non autorisé, même si les informations d'identification sont compromises.
- Configuration d'éléments de condition pour limiter quand et comment les autorisations administratives peuvent être utilisées en fonction de facteurs tels que l'adresse IP source ou l'âge du MFA.

L'utilisateur IAM possède des clés d'accès non pivotées

Les clés d'accès se composent d'un identifiant de clé d'accès et d'une clé d'accès secrète qui permettent un accès programmatique aux AWS ressources. Lorsque les clés d'accès restent inchangées pendant de longues périodes, elles augmentent le risque d'accès non autorisé si elles sont compromises. Conformément aux meilleures pratiques de sécurité, alternez les clés d'accès tous les 90 jours afin de minimiser la possibilité pour les attaquants d'utiliser des informations d'identification compromises.

Remédiation : rotation des clés d'accès

Dans la recherche d'exposition, ouvrez la ressource. Cela ouvre la fenêtre des détails de l'utilisateur. Pour alterner les clés d'accès, voir Gérer les clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

L'utilisateur IAM dispose d'une politique qui autorise un accès illimité au déchiffrement de la clé KMS

AWS KMS vous permet de créer et de gérer des clés cryptographiques utilisées pour protéger vos données. Les politiques IAM qui autorisent des autorisations de AWS KMS déchiffrement illimitées (par exemple, `kms:Decrypt` ou`kms:ReEncryptFrom`) sur toutes les clés KMS peuvent entraîner un accès non autorisé aux données si les informations d'identification d'un utilisateur IAM sont compromises. Si un attaquant accède à ces informations d'identification, il est susceptible de déchiffrer toutes les données chiffrées de votre environnement, y compris des données sensibles. Conformément aux meilleures pratiques de sécurité, implémentez le principe du moindre privilège en limitant les autorisations de AWS KMS déchiffrement aux seules clés spécifiques dont les utilisateurs ont besoin pour leurs fonctions professionnelles.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Implémentation d'un accès sur la base du moindre privilège

Dans la recherche d'exposition, ouvrez la ressource. Cela ouvre la fenêtre IAM Policy. Recherchez les autorisations dans KMS qui autorisent KMS:Decrypt `kms:ReEncryptFrom` ou `KMS:*` avec une spécification de ressource de. `"*"`

Mettez à jour la politique pour limiter les autorisations de AWS KMS déchiffrement aux seules clés spécifiques nécessaires. Modifiez la politique pour remplacer la `"*"` ressource par les ARN spécifiques des AWS KMS clés requises.

Considérations relatives à la configuration sécurisée

Envisagez d'ajouter des conditions pour restreindre davantage le moment où ces autorisations peuvent être utilisées. Par exemple, vous pouvez limiter les opérations de déchiffrement à des points de terminaison VPC spécifiques ou à des plages d'adresses IP sources. Vous pouvez également configurer des politiques clés pour restreindre davantage les personnes autorisées à utiliser des clés KMS spécifiques.

Caractéristiques d'accès non utilisées pour les utilisateurs IAM

Lorsqu'un utilisateur IAM dispose d'autorisations, de clés d'accès ou de mots de passe inutilisés, Security Hub peut les inclure en tant que caractéristiques contextuelles dans les résultats d'exposition de cet utilisateur. Ces caractéristiques sont générées par l'analyseur d'accès IAM géré par les services et fournissent un contexte supplémentaire sur la posture de sécurité de l'utilisateur. Les

caractéristiques d'accès non utilisées ne sont pas la principale cause de la découverte d'exposition, mais elles indiquent que l'utilisateur dispose de plus d'autorisations que nécessaire, ce qui augmente l'impact potentiel si ses informations d'identification sont compromises.

Pour les autorisations non utilisées en particulier, vous pouvez générer une recommandation de politique de moindre privilège qui vous indique une politique de remplacement limitée. Pour de plus amples informations, veuillez consulter the section called "Recommandations politiques".

Caractéristiques d'impact pour les utilisateurs d'IAM

Les caractéristiques d'impact décrivent le rayon d'explosion potentiel d'une exposition. Security Hub analyse les autorisations effectives du Gestion des identités et des accès AWS principal associé à l'utilisateur IAM afin de déterminer les ressources en aval qu'un attaquant pourrait atteindre si l'utilisateur IAM est compromis. Chaque trait d'impact identifie un modèle d'escalade de privilèges spécifique. Pour réduire votre rayon d'action, passez en revue les chemins d'autorisation décrits dans chaque trait et supprimez tous les privilèges inutiles.

Conformément aux principes de sécurité standard, accordez le moindre privilège en ne fournissant que les autorisations requises pour effectuer une tâche. Remplacez les politiques générales par des politiques restreintes qui n'accordent que les actions et les ressources spécifiques nécessaires. Pour identifier les autorisations non utilisées à supprimer, utilisez IAM Access Analyzer pour générer des recommandations en fonction de l'historique des accès. Pour plus d'informations, consultez les sections Constatations relatives à l'accès externe et inutilisé et Appliquer les autorisations de moindre privilège dans le guide de l'utilisateur IAM.

Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié

Le principal associé peut transmettre un rôle et injecter du code dans une ressource de calcul qui dispose déjà d'autorisations élevées. Cela permet au mandant de prendre le contrôle total de l'exécuteur testamentaire et d'effectuer toutes les actions autorisées par le rôle de l'exécuteur testamentaire.

A une trajectoire d'escalade politique directe

Le principal associé peut modifier directement les politiques IAM pour s'accorder des autorisations supplémentaires, augmentant ainsi ses propres privilèges sans ressources intermédiaires.

A une voie de détournement de la politique de confiance

Le principal associé peut modifier la politique de confiance d'un rôle IAM pour s'autoriser à assumer ce rôle, en obtenant les autorisations du rôle.

Possède un chemin de données vers un

Le principal associé peut chiffrer ou supprimer des données d'une manière susceptible d'être utilisée pour les rançongiciels, par exemple en chiffrant des objets Amazon S3 à l'aide d'une AWS KMS clé gérée par le client, puis en modifiant la politique relative aux clés.

Dispose d'un chemin de restriction supprimé

Le principal associé peut supprimer les restrictions de sécurité telles que les limites d'autorisation, les politiques de contrôle des services ou les instructions de refus de politiques basées sur les ressources, élargissant ainsi ce que peuvent faire les autres principaux ou la ressource elle-même.

A un rôle de passe pour créer le chemin de l'exécuteur

Le principal associé peut créer une nouvelle ressource de calcul (telle qu'une fonction Lambda ou une instance Amazon EC2) et lui transmettre un rôle privilégié, libérant ainsi ses propres autorisations via la nouvelle ressource.

Dispose d'un rôle d'échange (chemin d'exécuteur existant)

Le principal associé peut modifier le rôle IAM attaché à une ressource de calcul existante, en le remplaçant par un rôle plus privilégié pour augmenter l'accès.

Dispose d'une voie d'escalade en chaîne de rôles

Le principal associé peut assumer une séquence de rôles, chaque rôle de la chaîne bénéficiant d'autorisations progressivement plus larges, pour atteindre finalement un rôle hautement privilégié.

Possède un chemin d'exécution privilégié pour l'injection de code

Le principal associé peut injecter du code dans une ressource de calcul en cours d'exécution dotée d'autorisations élevées, en exécutant des opérations arbitraires sous le rôle privilégié de cette ressource.

A désactivé le chemin de la piste d'audit

Le principal associé peut désactiver les services de journalisation ou de surveillance CloudTrail, tels que la couverture efficace de ses traces pendant ou après une escalade.

A accès au chemin d'exécution existant

Le principal associé peut invoquer ou se connecter à une ressource de calcul existante et utiliser le rôle qui lui est attaché pour effectuer des actions privilégiées.

Dispose d'un parcours de création d'identifiants

Le principal associé peut créer de nouvelles informations d'identification à long terme (telles que des clés d'accès ou des profils de connexion) pour d'autres mandants, en établissant des chemins d'accès persistants qui survivent aux rotations de mots de passe ou aux expirations de session.

Dispose d'un chemin d'accès aux données du rôle de passe

Le principal associé peut créer une ressource de service et lui transmettre un rôle ayant accès à des données sensibles, en obtenant un accès indirect à ces données via la nouvelle ressource.

A un rôle de passe, une tâche, un chemin de détournement

Le principal associé peut transmettre un rôle à une tâche planifiée ou pilotée par un événement (telle qu'une fonction Lambda déclenchée par un événement), ce qui lui permet d'exécuter du code arbitraire avec les autorisations de ce rôle.

Dispose d'un chemin d'accès aux données à saut unique

Le principal associé peut accéder directement à des ressources de données sensibles (telles que des compartiments Amazon S3 ou des tables DynamoDB) via ses autorisations existantes, sans avoir besoin d'étapes d'escalade intermédiaires.

Possède une capacité d'avancement

Le principal associé dispose d'un chemin d'escalade des privilèges qui fait progresser ses capacités globales au-delà de ce que suggèrent ses autorisations directement attribuées. Il s'agit d'une classification générale pour les chemins qui ne correspondent pas à un modèle plus spécifique.

Remédier aux expositions pour AWS Lambda functions

AWS Security Hub peut générer des résultats d'exposition pour les AWS Lambda fonctions.

Sur la console Security Hub, la fonction Lambda impliquée dans la détection d'une exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes

de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration pour les fonctions Lambda
  - La fonction Lambda est déployée en dehors d'un Amazon VPC
  - La fonction Lambda est accessible via API Gateway sans autorisation
- Caractéristiques d'accessibilité pour les fonctions Lambda
  - La fonction Lambda peut être invoquée publiquement
- Caractéristiques de vulnérabilité des fonctions Lambda
  - La fonction Lambda présente des vulnérabilités logicielles exploitables par le réseau
  - La fonction Lambda présente des vulnérabilités logicielles
  - La fonction Lambda contient des progiciels malveillants
  - La fonction Lambda présente des vulnérabilités de code
- Traits d'impact pour les fonctions Lambda
  - Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié
  - A une trajectoire d'escalade politique directe
  - A une voie de détournement de la politique de confiance
  - Possède un chemin de données vers un
  - Dispose d'un chemin de restriction supprimé
  - A un rôle de passe pour créer le chemin de l'exécuteur
  - Dispose d'un rôle d'échange (chemin d'exécuteur existant)
  - Dispose d'une voie d'escalade en chaîne de rôles

- Possède un chemin d'exécution privilégié pour l'injection de code
- A désactivé le chemin de la piste d'audit
- A accès au chemin d'exécution existant
- Dispose d'un parcours de création d'identifiants
- Dispose d'un chemin d'accès aux données du rôle de passe
- A un rôle de passe, une tâche, un chemin de détournement
- Dispose d'un chemin d'accès aux données à saut unique
- Possède une capacité d'avancement

Caractéristiques de mauvaise configuration pour les fonctions Lambda

Voici les caractéristiques de configuration erronée des fonctions Lambda et les étapes de correction suggérées.

La fonction Lambda est déployée en dehors d'un Amazon VPC

Les fonctions Lambda sont déployées par défaut avec un accès à l'Internet public. Cette configuration par défaut permet aux fonctions Lambda d'atteindre les points de terminaison des AWS services et les API externes, mais elle les expose également à des risques de sécurité potentiels. Les fonctions ayant accès à Internet peuvent être utilisées pour exfiltrer des données, communiquer avec des serveurs non autorisés ou devenir des points d'entrée pour des acteurs externes en cas de compromission. Amazon VPC assure l'isolation du réseau en limitant vos fonctions Lambda pour qu'elles ne communiquent qu'avec les ressources de votre réseau privé défini. En suivant les principes de sécurité standard, déployez les fonctions Lambda au sein d'un VPC afin d'améliorer la sécurité grâce à l'isolation du réseau.

Remédiation : attacher la fonction au VPC

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre la fonction Lambda dans la console Lambda. Pour sécuriser votre fonction Lambda en limitant son accès au réseau, attachez-la à un VPC doté des contrôles réseau appropriés.

Avant d'associer votre fonction à un VPC, planifiez tout accès aux AWS services dont elle pourrait avoir besoin, car les fonctions des sous-réseaux privés sans passerelles NAT ni points de terminaison VPC ne peuvent pas atteindre les API de service. AWS Pour plus d'informations sur la manière d'associer une fonction Lambda à un Amazon VPC de votre compte, consultez Associer des fonctions Lambda à un Amazon VPC de votre. Compte AWS Envisagez d'utiliser des points de

terminaison VPC pour la connectivité des services sans accès à Internet si votre fonction nécessite d'accéder à AWS des services depuis un sous-réseau privé. Configurez une passerelle NAT si vous avez besoin d'une connectivité Internet sortante à partir de sous-réseaux privés.

La fonction Lambda est accessible via API Gateway sans autorisation

Les méthodes API Gateway sans autorisation permettent à tout appelant ayant accès à l'API Gateway d'invoquer la fonction Lambda intégrée sans vérification d'identité. Cette configuration présente des risques de sécurité, car les appelants peuvent invoquer la fonction Lambda sans autorisation appropriée, ce qui peut entraîner un abus des capacités de la fonction, une consommation de ressources, un accès à des données sensibles ou des opérations non autorisées. Bien qu'API Gateway puisse disposer de contrôles d'accès au niveau du réseau, l'absence d'autorisation au niveau de la méthode pourrait permettre l'invocation gratuite de la fonction par tout appelant ayant un accès réseau à l'API Gateway. En suivant les meilleures pratiques de sécurité, implémentez des mécanismes d'autorisation appropriés pour les méthodes API Gateway qui s'intègrent aux fonctions Lambda.

Correction : configurer l'authentification API Gateway

Dans l'onglet Ressources de l'exposition, choisissez le lien vers la ressource pour accéder à la méthode API Gateway. Passez en revue la configuration d'autorisation actuelle et implémentez les mécanismes d'authentification appropriés.

API Gateway prend en charge plusieurs options d'authentification, notamment AWS IAM, les groupes d'utilisateurs Amazon Cognito, les autorisations Lambda et les clés d'API. Choisissez la méthode d'authentification qui correspond le mieux à vos exigences de sécurité et à votre cas d'utilisation. Pour obtenir des instructions détaillées sur la configuration de l'authentification, consultez la section Contrôle et gestion de l'accès à une API REST dans API Gateway dans le guide du développeur d'API Gateway.

Caractéristiques d'accessibilité pour les fonctions Lambda

Voici les caractéristiques d'accessibilité des fonctions Lambda et les étapes de correction suggérées.

La fonction Lambda peut être invoquée publiquement

Les politiques Lambda basées sur les ressources déterminent qui peut invoquer vos fonctions. Une fonction dont la politique de ressources inclut « * » comme principal (ou aucun principal) permet à tout AWS utilisateur authentifié de l'invoquer. Cela crée un risque important, en particulier pour les fonctions qui traitent des données sensibles, modifient des ressources ou disposent d'autorisations

élevées. Les utilisateurs non autorisés pourraient exploiter cette configuration pour effectuer des opérations indésirables, susceptibles d'exposer des données, de manipuler des ressources ou d'abuser des fonctionnalités. Conformément aux meilleures pratiques de sécurité, limitez l'accès aux fonctions Lambda aux seuls mandants autorisés.

Correction : modifier la politique basée sur les ressources de la fonction

Dans l'onglet Ressources de l'exposition, ouvrez la ressource à l'aide du lien hypertexte. Cela ouvre la fonction Lambda dans la console Lambda. Limitez l'accès à votre fonction Lambda en spécifiant uniquement les identifiants de AWS compte autorisés ou des principaux IAM spécifiques (utilisateurs, rôles ou services) dans la politique basée sur les ressources. Vous ne pouvez modifier les politiques basées sur les ressources que par programmation.

Caractéristiques de vulnérabilité des fonctions Lambda

Voici les caractéristiques de vulnérabilité des fonctions Lambda et les étapes de correction suggérées.

La fonction Lambda présente des vulnérabilités logicielles exploitables par le réseau

Les packages logiciels utilisés dans le code de fonction Lambda peuvent contenir des vulnérabilités et des expositions courantes (CVE) qui ont de fortes chances d'être exploitées. Les CVE critiques présentent des risques de sécurité importants pour votre AWS environnement. Les attaquants peuvent exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. Les vulnérabilités critiques présentant une forte probabilité d'exploitation constituent des menaces de sécurité immédiates, car le code d'exploitation est peut-être déjà accessible au public et utilisé activement par des attaquants ou des outils d'analyse automatisés. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités pour protéger votre fonction contre les attaques.

Correction : mettre à jour les fonctions concernées

Consultez la section Références de l'onglet Vulnérabilité correspondant à cette caractéristique. La documentation du fournisseur peut inclure des conseils de correction spécifiques. Mettez à jour les bibliothèques vulnérables vers leurs dernières versions sécurisées en suivant les procédures recommandées par le fournisseur.

En général, le flux de travail de correction varie selon que vous avez déployé le package Lambda en chargeant un fichier zip ou en créant une fonction Lambda avec une image de conteneur. Après avoir mis à jour les bibliothèques, mettez à jour le code de la fonction Lambda pour utiliser la version corrigée. Déployez ensuite la version mise à jour.

La fonction Lambda présente des vulnérabilités logicielles

Les fonctions Lambda utilisent souvent des bibliothèques et des dépendances tierces qui peuvent contenir des failles de sécurité d'une gravité ou d'une exploitabilité inférieures à celles des CVE critiques. Bien que ces vulnérabilités non critiques ne soient pas exploitables dans l'immédiat, elles constituent tout de même des failles de sécurité qui pourraient être associées à d'autres vulnérabilités pour compromettre votre fonction. Au fil du temps, de nouvelles techniques d'exploitation pourraient également apparaître, augmentant le risque de ces vulnérabilités. En suivant les principes de sécurité standard, corrigez ces vulnérabilités pour maintenir un environnement sécurisé.

Correction : mettre à jour les fonctions concernées

Consultez la section Références de l'onglet Vulnérabilité correspondant à cette caractéristique. La documentation du fournisseur peut inclure des conseils de correction spécifiques. Mettez à jour les bibliothèques vulnérables vers leurs dernières versions sécurisées en suivant les procédures recommandées par le fournisseur.

En général, le flux de travail de correction varie selon que vous avez déployé le package Lambda en chargeant un fichier zip ou en créant une fonction Lambda avec une image de conteneur. Après avoir mis à jour les bibliothèques, mettez à jour le code de la fonction Lambda pour utiliser la version corrigée. Déployez ensuite la version mise à jour.

La fonction Lambda contient des progiciels malveillants

Les packages malveillants sont des composants logiciels contenant du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les packages malveillants constituent une menace active et critique pour votre fonction Lambda, car les attaquants peuvent exécuter automatiquement du code malveillant sans exploiter de vulnérabilité. En suivant les meilleures pratiques de sécurité, supprimez les packages malveillants pour protéger votre fonction Lambda contre d'éventuelles attaques.

Remédiation : suppression des packages malveillants

Consultez les détails du package malveillant dans la section Références de l'onglet Vulnérabilité du trait pour comprendre la menace. Supprimez les packages malveillants identifiés de votre code de fonction et de vos dépendances. Pour les fonctions utilisant des couches, vérifiez si les packages malveillants sont installés dans l'une des couches et supprimez-les.

Mettez à jour votre package de déploiement ou l'image de votre conteneur pour exclure les packages malveillants, puis déployez la version mise à jour. Pour obtenir des instructions, consultez

Déploiement de fonctions Lambda en tant qu'archives de fichiers .zip pour les archives de fichiers .zip ou Création d'une fonction Lambda à l'aide d'une image de conteneur pour les images de conteneur.

La fonction Lambda présente des vulnérabilités de code

Le code de l'application de la fonction Lambda contient des failles de sécurité susceptibles d'être exploitées par des acteurs malveillants. Les vulnérabilités du code incluent les fuites de données, les failles d'injection, le chiffrement manquant et la cryptographie faible qui sont identifiés par une analyse automatique du code. Ces vulnérabilités présentent des risques de sécurité pour votre AWS environnement, car les attaquants peuvent les exploiter pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. Les vulnérabilités de code représentent des failles de sécurité qui peuvent être associées à d'autres vecteurs d'attaque pour compromettre votre fonction. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités de code afin de protéger votre fonction contre les attaques.

Correction : mettre à jour les fonctions concernées

Consultez la section Références de l'onglet Vulnérabilité du trait. Les résultats d'Amazon Inspector peuvent inclure des conseils de correction spécifiques et des extraits de code indiquant les emplacements de code vulnérables. Résolvez les problèmes de sécurité identifiés dans le code de votre fonction à l'aide des blocs de code prêts à l'emploi fournis ou en mettant en œuvre des pratiques de codage sécurisées.

Passez toujours en revue les suggestions de correction du code avant de les adopter, car vous devrez peut-être les modifier pour vous assurer que votre code fonctionne comme prévu. Après avoir corrigé les vulnérabilités, mettez à jour le code de la fonction Lambda pour utiliser la version corrigée. Pour obtenir des instructions, consultez la section Mise à jour du code de fonction dans le Guide du AWS Lambda développeur.

Déployez ensuite la version mise à jour. Pour obtenir des instructions, consultez Déploiement de fonctions Lambda en tant qu'archives de fichiers .zip pour les archives de fichiers .zip ou Création d'une fonction Lambda à l'aide d'une image de conteneur pour les images de conteneur. Pour plus d'informations sur la numérisation de code Amazon Inspector, consultez la section Analyse de code Lambda d'Amazon Inspector dans le guide de l'utilisateur d'Amazon Inspector.

Traits d'impact pour les fonctions Lambda

Les caractéristiques d'impact décrivent le rayon d'explosion potentiel d'une exposition. Security Hub analyse les autorisations effectives du Gestion des identités et des accès AWS principal associé

à la fonction Lambda afin de déterminer les ressources en aval qu'un attaquant pourrait atteindre si la fonction est compromise. Chaque trait d'impact identifie un modèle d'escalade de privilèges spécifique. Pour réduire votre rayon d'action, passez en revue les chemins d'autorisation décrits dans chaque trait et supprimez tous les privilèges inutiles.

Conformément aux principes de sécurité standard, accordez le moindre privilège en ne fournissant que les autorisations requises pour effectuer une tâche. Remplacez les politiques générales par des politiques restreintes qui n'accordent que les actions et les ressources spécifiques nécessaires. Pour identifier les autorisations non utilisées à supprimer, utilisez IAM Access Analyzer pour générer des recommandations en fonction de l'historique des accès. Pour plus d'informations, consultez les sections Constatations relatives à l'accès externe et inutilisé et Appliquer les autorisations de moindre privilège dans le guide de l'utilisateur IAM.

Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié

Le principal associé peut transmettre un rôle et injecter du code dans une ressource de calcul qui dispose déjà d'autorisations élevées. Cela permet au mandant de prendre le contrôle total de l'exécuteur testamentaire et d'effectuer toutes les actions autorisées par le rôle de l'exécuteur testamentaire.

A une trajectoire d'escalade politique directe

Le principal associé peut modifier directement les politiques IAM pour s'accorder des autorisations supplémentaires, augmentant ainsi ses propres privilèges sans ressources intermédiaires.

A une voie de détournement de la politique de confiance

Le principal associé peut modifier la politique de confiance d'un rôle IAM pour s'autoriser à assumer ce rôle, en obtenant les autorisations du rôle.

Possède un chemin de données vers un

Le principal associé peut chiffrer ou supprimer des données d'une manière susceptible d'être utilisée pour les rançongiciels, par exemple en chiffrant des objets Amazon S3 à l'aide d'une AWS KMS clé gérée par le client, puis en modifiant la politique relative aux clés.

Dispose d'un chemin de restriction supprimé

Le principal associé peut supprimer les restrictions de sécurité telles que les limites d'autorisation, les politiques de contrôle des services ou les instructions de refus de politiques basées sur les ressources, élargissant ainsi ce que peuvent faire les autres principaux ou la ressource elle-même.

A un rôle de passe pour créer le chemin de l'exécuteur

Le principal associé peut créer une nouvelle ressource de calcul (telle qu'une fonction Lambda ou une instance Amazon EC2) et lui transmettre un rôle privilégié, libérant ainsi ses propres autorisations via la nouvelle ressource.

Dispose d'un rôle d'échange (chemin d'exécuteur existant)

Le principal associé peut modifier le rôle IAM attaché à une ressource de calcul existante, en le remplaçant par un rôle plus privilégié pour augmenter l'accès.

Dispose d'une voie d'escalade en chaîne de rôles

Le principal associé peut assumer une séquence de rôles, chaque rôle de la chaîne bénéficiant d'autorisations progressivement plus larges, pour atteindre finalement un rôle hautement privilégié.

Possède un chemin d'exécution privilégié pour l'injection de code

Le principal associé peut injecter du code dans une ressource de calcul en cours d'exécution dotée d'autorisations élevées, en exécutant des opérations arbitraires sous le rôle privilégié de cette ressource.

A désactivé le chemin de la piste d'audit

Le principal associé peut désactiver les services de journalisation ou de surveillance CloudTrail, tels que la couverture efficace de ses traces pendant ou après une escalade.

A accès au chemin d'exécution existant

Le principal associé peut invoquer ou se connecter à une ressource de calcul existante et utiliser le rôle qui lui est attaché pour effectuer des actions privilégiées.

Dispose d'un parcours de création d'identifiants

Le principal associé peut créer de nouvelles informations d'identification à long terme (telles que des clés d'accès ou des profils de connexion) pour d'autres mandants, en établissant des chemins d'accès persistants qui survivent aux rotations de mots de passe ou aux expirations de session.

Dispose d'un chemin d'accès aux données du rôle de passe

Le principal associé peut créer une ressource de service et lui transmettre un rôle ayant accès à des données sensibles, en obtenant un accès indirect à ces données via la nouvelle ressource.

A un rôle de passe, une tâche, un chemin de détournement

Le principal associé peut transmettre un rôle à une tâche planifiée ou pilotée par un événement (telle qu'une fonction Lambda déclenchée par un événement), ce qui lui permet d'exécuter du code arbitraire avec les autorisations de ce rôle.

Dispose d'un chemin d'accès aux données à saut unique

Le principal associé peut accéder directement à des ressources de données sensibles (telles que des compartiments Amazon S3 ou des tables DynamoDB) via ses autorisations existantes, sans avoir besoin d'étapes d'escalade intermédiaires.

Possède une capacité d'avancement

Le principal associé dispose d'un chemin d'escalade des privilèges qui fait progresser ses capacités globales au-delà de ce que suggèrent ses autorisations directement attribuées. Il s'agit d'une classification générale pour les chemins qui ne correspondent pas à un modèle plus spécifique.

Corriger les risques pour les instances et les clusters Amazon RDS

AWS Security Hub peut générer des résultats d'exposition pour les instances et les clusters Amazon RDS.

Sur la console Security Hub, l'instance ou le cluster Amazon RDS impliqué dans une détection d'exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la recherche. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration pour les instances et les clusters Amazon RDS
  - L'instance de base de données Amazon RDS est configurée avec un accès public
  - Le cluster de bases de données Amazon RDS possède un instantané qui est partagé publiquement
  - L'instance de base de données Amazon RDS possède un instantané qui est partagé publiquement
  - L'instance de base de données Amazon RDS possède un instantané qui n'est pas chiffré au repos
  - Le cluster de bases de données Amazon RDS possède un instantané qui n'est pas chiffré au repos
  - L'instance de base de données Amazon RDS possède un groupe de sécurité ouvert
  - L'authentification de base de données IAM est désactivée sur l'instance de base de données Amazon RDS.
  - L'instance de base de données Amazon RDS utilise le nom d'utilisateur administrateur par défaut.
  - Le cluster de bases de données Amazon RDS utilise le nom d'utilisateur administrateur par défaut.
  - Les mises à niveau automatiques des versions mineures de l'instance de base de données Amazon RDS sont désactivées
  - Les sauvegardes automatiques de l'instance de base de données Amazon RDS sont désactivées.
  - La protection contre la suppression de l'instance de base de données Amazon RDS est désactivée
  - La protection contre la suppression est désactivée sur le cluster de bases de données Amazon RDS
  - L'instance de base de données Amazon RDS utilise le port par défaut pour le moteur de base de données

  - L'instance de base de données Amazon RDS n'est pas couverte par un plan de sauvegarde
- Caractéristiques de données sensibles pour les instances de bases de données Amazon RDS
  - L'instance de base de données Amazon RDS contient des données sensibles

Caractéristiques de mauvaise configuration pour les instances et les clusters Amazon RDS

Ce qui suit décrit les caractéristiques de mauvaise configuration et les étapes de correction pour les instances et les clusters Amazon RDS.

L'instance de base de données Amazon RDS est configurée avec un accès public

Les instances Amazon RDS dotées d'un accès public sont potentiellement accessibles via Internet via leurs points de terminaison. Bien que l'accès public soit parfois nécessaire pour les fonctionnalités de l'instance, cette configuration peut être utilisée comme vecteur d'attaque potentiel pour les utilisateurs non autorisés qui tentent d'accéder à votre base de données. Les bases de données accessibles au public peuvent être exposées à des scans de ports, à des attaques par force brute et à des tentatives d'exploitation. Conformément aux principes de sécurité standard, limitez l'exposition publique des ressources de votre base de données.

Remédiation : modifier les paramètres d'accès public

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS. Déterminez si l'instance de base de données nécessite une accessibilité publique en fonction de l'architecture de votre application. Pour plus d'informations, consultez Configuration de l'accès public ou privé dans Amazon RDS.

Le cluster de bases de données Amazon RDS possède un instantané qui est partagé publiquement

Les instantanés publics sont accessibles à tous Compte AWS, ce qui peut exposer des données sensibles à des utilisateurs non autorisés. Any Compte AWS est autorisé à copier ces instantanés publics et à créer des instances de base de données à partir de ceux-ci, ce qui pourrait entraîner des violations de données ou un accès non autorisé aux données. Conformément aux meilleures pratiques de sécurité, limitez l'accès à vos instantanés Amazon RDS aux seules organisations Comptes AWS et organisations de confiance.

Solution : configurer un instantané Amazon RDS pour un accès privé

Dans la recherche d'exposition, ouvrez la ressource via le lien hypertexte. Pour plus d'informations sur la modification des paramètres de partage d'instantanés, consultez la section Partage d'un

instantané dans le guide de l'utilisateur d'Amazon Aurora. Pour plus d'informations sur la manière d'arrêter de partager des instantanés, consultez la section Arrêter le partage de clichés dans le guide de l'utilisateur d'Amazon Aurora. .

L'instance de base de données Amazon RDS possède un instantané qui est partagé publiquement

Les instantanés publics sont accessibles à tous Compte AWS, ce qui peut exposer des données sensibles à des utilisateurs non autorisés. Any Compte AWS est autorisé à copier ces instantanés publics et à créer des instances de base de données à partir de ceux-ci, ce qui pourrait entraîner des violations de données ou un accès non autorisé aux données. Conformément aux meilleures pratiques de sécurité, limitez l'accès à vos instantanés Amazon RDS aux seules organisations Comptes AWS et organisations de confiance.

Solution : configurer un instantané Amazon RDS pour un accès privé

Dans la recherche d'exposition, ouvrez la ressource via le lien hypertexte. Pour plus d'informations sur la façon de modifier les paramètres de partage d'instantanés, consultez la section Partager un instantané de base de données dans le guide de l'utilisateur Amazon RDS. Pour plus d'informations sur la manière d'arrêter de partager des instantanés, consultez la section Arrêter de partager un instantané de base de données dans le guide de l'utilisateur Amazon RDS. .

L'instance de base de données Amazon RDS possède un instantané qui n'est pas chiffré au repos

Les instantanés d'instance de base de données Amazon RDS non chiffrés peuvent exposer des données sensibles si un accès non autorisé à la couche de stockage est obtenu. Sans chiffrement, les données contenues dans les instantanés pourraient être exposées par un accès non autorisé. Cela crée un risque de violations de données et de violations de conformité. En suivant les meilleures pratiques de sécurité, chiffrez toutes les ressources de base de données et leurs sauvegardes afin de préserver la confidentialité des données.

Remédiation : mettre à jour les ressources concernées

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instantané concerné dans la console Amazon RDS. Vous ne pouvez pas chiffrer directement un instantané non chiffré existant.

Créez plutôt une copie cryptée de l'instantané non chiffré. Pour obtenir des instructions détaillées, consultez la section Copie d'instantanés de clusters de bases de données et chiffrement des ressources Amazon RDS dans le guide de l'utilisateur Amazon Aurora.

Le cluster de bases de données Amazon RDS possède un instantané qui n'est pas chiffré au repos

Les instantanés de clusters de bases de données Amazon RDS non chiffrés peuvent exposer des données sensibles si un accès non autorisé à la couche de stockage est obtenu. Sans chiffrement, les données contenues dans les instantanés pourraient être exposées par un accès non autorisé. Cela crée un risque de violations de données et de violations de conformité. En suivant les meilleures pratiques de sécurité, chiffrez toutes les ressources de base de données et leurs sauvegardes afin de préserver la confidentialité des données.

Correction : créer une copie cryptée de l'instantané

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instantané concerné dans la console Amazon RDS. Vous ne pouvez pas chiffrer directement un instantané non chiffré existant.

Créez plutôt une copie cryptée de l'instantané non chiffré. Pour obtenir des instructions détaillées, consultez la section Copie d'instantanés de clusters de bases de données et chiffrement des ressources Amazon RDS dans le guide de l'utilisateur Amazon Aurora.

L'instance de base de données Amazon RDS possède un groupe de sécurité ouvert

Les groupes de sécurité agissent comme des pare-feux virtuels pour vos instances Amazon RDS afin de contrôler le trafic entrant et sortant. Les groupes de sécurité ouverts, qui permettent un accès illimité à partir de n'importe quelle adresse IP, peuvent exposer les instances de votre base de données à un accès non autorisé et à des attaques potentielles. Conformément aux principes de sécurité standard, limitez l'accès des groupes de sécurité à des adresses IP et à des ports spécifiques afin de respecter le principe du moindre privilège.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Passez en revue les règles des groupes de sécurité et évaluez la configuration actuelle

Dans la recherche d'exposition, ouvrez la ressource pour le groupe de sécurité de l'instance de base de données. Évaluez quels ports sont ouverts et accessibles à partir de larges plages d'adresses IP, telles que`(0.0.0.0/0 or ::/0)`. Pour plus d'informations sur l'affichage des détails des groupes de sécurité, consultez DescribeSecurityGroups le manuel Amazon Elastic Compute Cloud API Reference.

Modifier les règles des groupes de sécurité

Modifiez les règles de votre groupe de sécurité pour restreindre l'accès à des adresses IP ou à des plages d'adresses IP fiables spécifiques. Lorsque vous mettez à jour les règles de votre groupe de sécurité, pensez à séparer les exigences d'accès pour les différents segments du réseau en créant des règles pour chaque plage d'adresses IP source requise ou en limitant l'accès à des ports spécifiques. Pour modifier les règles des groupes de sécurité, consultez la section Configurer les règles des groupes de sécurité dans le guide de l'utilisateur Amazon EC2. Pour modifier le port par défaut d'une instance de base de données Amazon RDS existante, consultez la section Modification du cluster de bases de données à l'aide de la console, de l'interface de ligne de commande et de l'API dans le guide de l'utilisateur Amazon Aurora.

L'authentification de base de données IAM est désactivée sur l'instance de base de données Amazon RDS.

L'authentification de base de données IAM vous permet de vous authentifier auprès de votre base de données Amazon RDS à l'aide d'informations d'identification IAM plutôt que de mots de passe de base de données. Cela offre plusieurs avantages en matière de sécurité, tels que la gestion centralisée des accès, des informations d'identification temporaires et l'élimination du stockage des mots de passe de base de données dans le code de l'application. L'authentification de base de données IAM permet de s'authentifier auprès des instances de base de données à l'aide d'un jeton d'authentification au lieu d'un mot de passe. Par conséquent, le trafic réseau en provenance et à destination de l'instance de base de données est chiffré à l'aide du protocole SSL. Sans authentification IAM, les bases de données reposent généralement sur une authentification par mot de passe, ce qui peut entraîner une réutilisation des mots de passe et des mots de passe faibles. En suivant les meilleures pratiques de sécurité, activez l'authentification de la base de données IAM.

Correction : activer l'authentification de la base de données IAM

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS. Vous pouvez activer l'authentification de base de données IAM dans les options de base de données.

Pour plus d'informations, consultez Activation et désactivation de l'authentification de base de données IAM dans le guide de l'utilisateur Amazon RDS. Après avoir activé l'authentification IAM, mettez à jour vos instances de base de données pour utiliser l'authentification IAM au lieu de l'authentification par mot de passe.

L'instance de base de données Amazon RDS utilise le nom d'utilisateur administrateur par défaut.

L'utilisation de noms d'utilisateur par défaut (par exemple, « admin », « root ») pour les instances de base de données augmente les risques de sécurité, car ceux-ci sont largement connus et

souvent ciblés par des attaques par force brute. Les noms d'utilisateur par défaut sont prévisibles et permettent aux utilisateurs non autorisés d'accéder plus facilement à votre base de données. Avec les noms d'utilisateur par défaut, les attaquants n'ont besoin que de mots de passe, et non des deux, pour accéder à votre base de données. Conformément aux meilleures pratiques de sécurité, utilisez des noms d'utilisateur d'administrateur uniques pour votre instance de base de données afin de renforcer la sécurité grâce à l'obscurité et de réduire le risque de tentatives d'accès non autorisées.

Solution : configurer un nom d'utilisateur administrateur unique

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS. Vous ne pouvez pas modifier le nom d'utilisateur administrateur d'une instance de base de données Amazon RDS existante. Pour créer un nom d'administrateur unique, vous devez créer une nouvelle instance de base de données avec un nom d'utilisateur personnalisé et migrer vos données.

Le cluster de bases de données Amazon RDS utilise le nom d'utilisateur administrateur par défaut.

L'utilisation de noms d'utilisateur par défaut (par exemple, « admin », « root ») pour les instances de base de données augmente les risques de sécurité, car ceux-ci sont largement connus et souvent ciblés par des attaques par force brute. Les noms d'utilisateur par défaut sont prévisibles et permettent aux utilisateurs non autorisés d'accéder plus facilement à votre base de données. Avec les noms d'utilisateur par défaut, les attaquants n'ont besoin que de mots de passe, et non des deux, pour accéder à votre base de données. Conformément aux meilleures pratiques de sécurité, utilisez des noms d'utilisateur d'administrateur uniques pour votre instance de base de données afin de renforcer la sécurité grâce à l'obscurité et de réduire le risque de tentatives d'accès non autorisées.

Solution : configurer un nom d'utilisateur administrateur unique

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS. Vous ne pouvez pas modifier le nom d'utilisateur administrateur d'une instance de base de données Amazon RDS existante. Pour créer un nom d'administrateur unique, vous devez créer une nouvelle instance de base de données avec un nom d'utilisateur personnalisé et migrer vos données.

Les mises à niveau automatiques des versions mineures de l'instance de base de données Amazon RDS sont désactivées

Les mises à niveau automatiques des versions mineures garantissent que vos instances Amazon RDS reçoivent automatiquement des mises à niveau mineures des versions du moteur lorsqu'elles sont disponibles. Ces mises à niveau incluent souvent des correctifs de sécurité importants et des

corrections de bogues qui contribuent à maintenir la sécurité et la stabilité de votre base de données. Votre base de données risque de présenter des failles de sécurité connues qui ont été corrigées dans les nouvelles versions mineures. Sans mises à jour automatiques, les instances de base de données peuvent accumuler des failles de sécurité à mesure que de nouveaux CVE sont découverts. Conformément aux meilleures pratiques de sécurité, activez les mises à niveau automatiques des versions mineures pour toutes les instances Amazon RDS.

Correction : activer les mises à niveau automatiques des versions mineures

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS. Vous pouvez consulter les paramètres de mise à niveau mineure automatique dans l'onglet Maintenance et sauvegardes.

Pour plus d'informations, consultez Mises à niveau automatiques des versions mineures d'Amazon RDS pour MySQL. Vous pouvez également configurer votre fenêtre de maintenance pour qu'elle se produise pendant les périodes de faible activité de la base de données.

Les sauvegardes automatiques de l'instance de base de données Amazon RDS sont désactivées.

Les sauvegardes automatisées assurent la restauration instantanée de vos instances Amazon RDS, ce qui vous permet de restaurer votre base de données à tout moment au cours de votre période de rétention. Lorsque les sauvegardes automatiques sont désactivées, vous risquez de perdre des données en cas de suppression malveillante, de corruption des données ou d'autres scénarios de perte de données. En cas d'activité malveillante, telle qu'une attaque par rançongiciel, la suppression de tables de base de données ou une corruption, la possibilité de restaurer une base de données à un moment antérieur à l'incident réduit le temps nécessaire à la restauration après un incident. En suivant les meilleures pratiques de sécurité, activez les sauvegardes automatisées avec une période de conservation appropriée pour toutes les bases de données de production.

La protection contre la suppression de l'instance de base de données Amazon RDS est désactivée

La protection contre la suppression des bases de données est une fonctionnalité qui permet d'empêcher la suppression de vos instances de base de données. Lorsque la protection contre la suppression est désactivée, votre base de données peut être supprimée par n'importe quel utilisateur disposant des autorisations suffisantes, ce qui peut entraîner une perte de données ou une interruption de l'application. Les attaquants peuvent supprimer votre base de données, ce qui entraîne des interruptions de service, des pertes de données et une augmentation du temps de restauration. En suivant les meilleures pratiques de sécurité, activez la protection contre la suppression pour vos instances de bases de données RDS afin d'empêcher toute suppression malveillante.

Solution : activez la protection contre la suppression pour votre cluster de bases de données Amazon RDS

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre le cluster de bases de données concerné.

La protection contre la suppression est désactivée sur le cluster de bases de données Amazon RDS

La protection contre la suppression des bases de données est une fonctionnalité qui permet d'empêcher la suppression de vos instances de base de données. Lorsque la protection contre la suppression est désactivée, votre base de données peut être supprimée par n'importe quel utilisateur disposant des autorisations suffisantes, ce qui peut entraîner une perte de données ou une interruption de l'application. Les attaquants peuvent supprimer votre base de données, ce qui entraîne des interruptions de service, des pertes de données et une augmentation du temps de restauration. En suivant les meilleures pratiques de sécurité, activez la protection contre la suppression pour vos clusters de bases de données RDS afin d'empêcher toute suppression malveillante.

Solution : activez la protection contre la suppression pour votre cluster de bases de données Amazon RDS

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre le cluster de bases de données concerné.

L'instance de base de données Amazon RDS utilise le port par défaut pour le moteur de base de données

Les instances Amazon RDS qui utilisent des ports par défaut pour les moteurs de base de données peuvent être confrontées à des risques de sécurité accrus, car ces ports par défaut sont largement connus et sont souvent ciblés par des outils d'analyse automatisés. La modification de votre instance de base de données pour utiliser des ports autres que ceux par défaut ajoute un niveau de sécurité supplémentaire grâce à l'obscurité, ce qui rend plus difficile pour les utilisateurs non autorisés d'effectuer des attaques automatisées ou ciblées sur votre base de données. Les ports par défaut sont généralement scannés par des personnes non autorisées et peuvent entraîner le ciblage de votre instance de base de données. Conformément aux meilleures pratiques de sécurité, remplacez le port par défaut par un port personnalisé afin de réduire le risque d'attaques automatisées ou ciblées.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Mettre à jour les ressources concernées

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS.

Mettre à jour les chaînes de connexion des applications

Après avoir modifié le port, mettez à jour toutes les applications et tous les services qui se connectent à votre instance Amazon RDS pour utiliser le nouveau numéro de port.

L'instance de base de données Amazon RDS n'est pas couverte par un plan de sauvegarde

AWS Backup est un service de sauvegarde entièrement géré qui centralise et automatise la sauvegarde des données entre. Services AWS Si votre instance de base de données n'est pas couverte par un plan de sauvegarde, vous risquez de perdre des données en cas de suppression malveillante, de corruption de données ou d'autres scénarios de perte de données. En cas d'activité malveillante, telle qu'une attaque par rançongiciel, la suppression de tables de base de données ou une corruption, la possibilité de restaurer une base de données à un moment antérieur à l'incident réduit le temps nécessaire à la restauration après un incident. Conformément aux meilleures pratiques de sécurité, incluez vos instances Amazon RDS dans un plan de sauvegarde afin de garantir la protection des données.

Correction : créez et attribuez un plan de sauvegarde pour votre instance de base de données

Dans la recherche d'exposition, choisissez le lien vers la ressource. Cela ouvre l'instance de base de données concernée dans la console Amazon RDS. Déterminez la fréquence de sauvegarde, la période de conservation et les règles de cycle de vie les mieux adaptées à vos applications.

Caractéristiques de données sensibles pour les instances de bases de données Amazon RDS

Voici les caractéristiques des données sensibles pour les instances de bases de données Amazon RDS et les étapes de correction suggérées.

L'instance de base de données Amazon RDS contient des données sensibles

Une analyse de sécurité des données a confirmé la présence d'enregistrements sensibles sur l'instance de base de données Amazon RDS. Un produit de sécurité des données intégré définit cette caractéristique lorsqu'il inspecte le contenu de l'instance de base de données et identifie les enregistrements nécessitant une protection.

La présence de données sensibles augmente l'impact de toutes les autres faiblesses sur la même instance de base de données. Un chemin réseau ou une configuration d'accès permissif qui exposerait autrement les données de l'application expose plutôt des enregistrements réglementés ou confidentiels. Un acteur malveillant qui accède à l'instance de base de données peut interroger et copier ces enregistrements en masse et les conserver en dehors de votre environnement. L'auteur de la menace peut également utiliser toutes les informations d'identification récupérées pour s'authentifier auprès d'autres systèmes. Conformément aux meilleures pratiques de sécurité, nous vous recommandons de restreindre l'accès au réseau et à l'identité aux instances de base de données Amazon RDS qui stockent des enregistrements sensibles, et de chiffrer ces enregistrements au repos et en transit.

Les données sensibles peuvent inclure :

- Informations d'identification, telles que les mots de passe, les clés d'accès et les chaînes de connexion
- Informations personnelles identifiables
- Informations financières, telles que les numéros de compte et les données des cartes de paiement
- Contenu confidentiel nécessitant une protection

La suppression des enregistrements sensibles est le seul moyen de supprimer cette caractéristique. Si votre charge de travail nécessite que l'instance de base de données stocke des données sensibles, les meilleures pratiques de sécurité suivantes réduisent le risque d'exposition.

Vérifiez les données sensibles de l'instance de base de données

Dans la recherche d'exposition, ouvrez la ressource à l'aide du lien hypertexte. Cela ouvre l'instance de base de données concernée. Notez l'identifiant de l'instance de base de données et enregistrez les groupes de sécurité VPC répertoriés sous Connectivité et sécurité. Passez en revue le résultat de sécurité des données qui a signalé les enregistrements sensibles afin de déterminer quelles bases de données, quels schémas et quelles tables les contiennent.

En fonction du type de données sensibles découvert, mettez en œuvre les contrôles de sécurité appropriés :

- Restreindre l'accès réseau entrant — Dans la console Amazon RDS, choisissez Bases de données, sélectionnez l'instance de base de données, puis choisissez Connectivité et sécurité. Ouvrez chaque groupe de sécurité VPC rattaché et passez en revue ses règles entrantes. Remplacez toute règle qui autorise le port de base de données depuis `0.0.0.0/0` ou `::/0` par

les plages CIDR ou les ID de groupe de sécurité spécifiques utilisés par vos applications. Pour plus d'informations, consultez Contrôle d'accès par groupe de sécurité dans le Guide de l'utilisateur Amazon RDS.

- Supprimer l'accessibilité publique : dans la console Amazon RDS, sélectionnez l'instance de base de données, choisissez Modifier et, sous Connectivité, définissez Accès public sur Non accessible au public. Placez l'instance de base de données dans des sous-réseaux privés qui n'ont aucune route vers une passerelle Internet. Vous pouvez y accéder depuis vos applications via le VPC, AWS Direct Connect ou une connexion VPN. Pour plus d'informations sur les réseaux VPC, veuillez consulter la rubrique Working with a DB instance in a VPC (Utilisation d'une instance de base de données dans un VPC) dans le Guide de l'utilisateur Amazon RDS.
- Limiter le nombre de personnes pouvant s'authentifier auprès de la base de données : accordez à chaque application et à chaque utilisateur uniquement les privilèges de base de données nécessaires à son fonctionnement. Révoquez l'accès en lecture aux tables contenant des enregistrements sensibles à tout utilisateur de base de données qui n'en a pas besoin. Utilisez l'authentification de base de données IAM afin que les identités IAM et les jetons éphémères contrôlent l'accès plutôt que des mots de passe de base de données de longue durée. Pour plus d'informations, consultez la section Authentification de la base de données IAM dans le guide de l'utilisateur Amazon RDS.
- Chiffrez les enregistrements sensibles au repos — Dans la console Amazon RDS, sélectionnez l'instance de base de données et choisissez l'onglet Configuration pour voir si l'instance de base de données utilise le chiffrement. Vous ne pouvez pas activer le chiffrement au repos sur une instance de base de données non chiffrée existante. Pour chiffrer ses données, créez un instantané de l'instance de base de données. Copiez le cliché et sélectionnez une clé AWS KMS pour la copie, puis restaurez la copie chiffrée du cliché sur une nouvelle instance de base de données. Redirigez vos applications vers le nouveau point de terminaison et supprimez l'instance de base de données non chiffrée et ses instantanés. Pour plus d'informations, consultez la section Chiffrement des ressources Amazon RDS dans le Guide de l'utilisateur Amazon RDS.
- Exiger le chiffrement en transit : configurez les clients de votre base de données auxquels vous connecter à SSL/TLS l'aide du bundle de certificats Amazon RDS. Appliquez des connexions chiffrées à l'instance de base de données via le paramètre fourni à cette fin par votre moteur de base de données. Pour plus d'informations, consultez la section Utilisation SSL/TLS pour chiffrer une connexion à une instance de base de données ou à un cluster dans le Guide de l'utilisateur Amazon RDS.
- Surveillez l'accès à l'instance de base de données : publiez les journaux du moteur de base de données sur Amazon CloudWatch Logs et vérifiez-les pour détecter les connexions provenant

de sources inattendues et les requêtes portant sur les tables contenant des enregistrements sensibles. Pour plus d'informations, consultez la section Surveillance des fichiers journaux Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Remédier aux expositions pour les compartiments Amazon S3

AWS Security Hub peut générer des résultats d'exposition pour les compartiments Amazon Simple Storage Service (Amazon S3).

Sur la console Security Hub, le compartiment Amazon S3 impliqué dans une détection d'exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la recherche. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de mauvaise configuration pour les compartiments Amazon S3
  - La gestion des versions du compartiment Amazon S3 est désactivée
  - Object Lock est désactivé sur le compartiment Amazon S3
  - Le compartiment Amazon S3 n'est pas chiffré au repos avec AWS KMS clés

  - Multi-factor la suppression par authentification (MFA) est désactivée sur un compartiment Amazon S3 versionné
  - Le compartiment Amazon S3 autorise les principaux d'autres AWS comptes pour modifier les autorisations des compartiments
- Caractéristiques d'accessibilité pour les compartiments Amazon S3
  - Le compartiment Amazon S3 dispose d'un accès public en lecture
  - Le compartiment Amazon S3 dispose d'un accès public en écriture
- Caractéristiques des données sensibles pour les compartiments Amazon S3
  - Le compartiment Amazon S3 contient des données sensibles

Caractéristiques de mauvaise configuration pour les compartiments Amazon S3

Voici les caractéristiques de configuration erronées des compartiments Amazon S3 et les étapes à suivre pour y remédier.

La gestion des versions du compartiment Amazon S3 est désactivée

La gestion des versions d'Amazon S3 vous permet de conserver plusieurs variantes d'un objet dans le même compartiment. Lorsque la gestion des versions est désactivée, Amazon S3 ne stocke que la version la plus récente de chaque objet, ce qui signifie que si des objets sont supprimés ou remplacés accidentellement ou par malveillance, ils ne peuvent pas être récupérés. Versioning-enabled les buckets offrent une protection contre les suppressions accidentelles, les défaillances d'applications et les incidents de sécurité tels que les attaques de rançongiciels, qui peuvent entraîner une modification ou une suppression non autorisée des données. En suivant les meilleures pratiques de sécurité, activez la gestion des versions pour les compartiments contenant des données importantes qu'il serait difficile, voire impossible, de recréer en cas de perte.

Correction : activer la gestion des versions

Pour activer la gestion des versions d'Amazon S3 sur un compartiment, consultez la section Activation de la gestion des versions sur les compartiments dans le guide de l'utilisateur Amazon S3. Lorsque vous activez le versionnage, envisagez de mettre en œuvre des règles de cycle de vie pour gérer le stockage, car le versionnage permet de conserver plusieurs copies des objets.

Object Lock est désactivé sur le compartiment Amazon S3

Amazon S3 Object Lock fournit un modèle WORM (write-once-read-many) pour les objets Amazon S3, empêchant leur suppression ou leur remplacement pendant une période déterminée ou

indéfiniment. Lorsque le verrouillage des objets est désactivé, vos objets peuvent être vulnérables à une suppression, à une modification ou à un chiffrement accidentels ou malveillants par un rançongiciel. Object Lock est particulièrement important pour la conformité aux exigences réglementaires qui exigent un stockage immuable des données et pour la protection contre les menaces sophistiquées telles que les rançongiciels qui peuvent tenter de chiffrer vos données. En activant Object Lock, vous pouvez appliquer des politiques de conservation en tant que couche supplémentaire de protection des données et créer une stratégie de sauvegarde immuable pour vos données critiques. En suivant les meilleures pratiques de sécurité, activez Object Lock pour empêcher toute modification malveillante de vos objets.

Correction : configurer le verrouillage des objets S3

Notez que le verrouillage des objets ne peut être activé que lors de la création d'un nouveau compartiment. Vous devrez donc créer un nouveau compartiment avec le verrouillage des objets activé. Pour les migrations de grande envergure, pensez à utiliser les opérations par lots pour copier des objets dans le nouveau compartiment. Avant de verrouiller des objets, vous devez également activer la gestion des versions d'Amazon S3 et le verrouillage des objets sur un bucket. Étant donné que le verrouillage des objets ne peut être activé que sur les nouveaux compartiments, vous devez migrer les données existantes vers un nouveau compartiment avec Object Lock activé. Pour plus d'informations sur la façon de configurer Object Lock sur un bucket, consultez la section Configuration d'Amazon S3 Object Lock dans le guide de l'utilisateur Amazon S3. Après avoir configuré Object Lock, choisissez un mode de rétention adapté à votre environnement.

Le compartiment Amazon S3 n'est pas chiffré au repos avec AWS KMS clés

Amazon S3 applique le chiffrement côté serveur avec des clés gérées par Amazon S3 comme niveau de cryptage par défaut pour tous les nouveaux compartiments. Bien que les clés gérées par Amazon S3 fournissent une protection de chiffrement robuste, elles n'offrent pas le même niveau de contrôle d'accès et de fonctionnalités d'audit que AWS Key Management Service les clés. Lorsque vous utilisez des clés KMS, l'accès aux objets nécessite des autorisations à la fois sur le compartiment Amazon S3 et sur la clé KMS qui a chiffré l'objet. Cela est particulièrement important pour les données sensibles pour lesquelles vous avez besoin d'un contrôle précis sur les personnes autorisées à accéder aux objets chiffrés et d'un enregistrement d'audit complet de l'utilisation des clés de chiffrement. Conformément aux meilleures pratiques de sécurité, utilisez des clés KMS pour chiffrer des compartiments contenant des données sensibles ou pour des environnements soumis à des exigences de conformité strictes.

Correction : configurer la clé de compartiment S3

Pour configurer un compartiment afin d'utiliser une clé de compartiment Amazon S3 pour les nouveaux objets, consultez Configuration de votre compartiment pour utiliser une clé de compartiment Amazon S3 SSE-KMS pour les nouveaux objets dans le Guide de l'utilisateur Amazon S3. Pour plus d'informations sur le chiffrement d'un objet existant, consultez la section Chiffrement d'objets avec Amazon S3 Batch Operations sur le blog AWS Storage.

Lors de la mise en œuvre du AWS KMS chiffrement, tenez compte des points suivants :

- Gestion des clés : décidez si vous souhaitez utiliser une clé AWS gérée ou une clé gérée par le client (CMK). Les CMK offrent aux clients un contrôle total sur le cycle de vie et l'utilisation de leurs clés. Pour plus d'informations sur la différence entre ces deux types de clés, consultez la section Clés AWS KMS dans le Guide du AWS Key Management Service développeur.
- Rotation des touches : pour des mesures de sécurité supplémentaires, activez la rotation automatique des touches pour vos clés KMS. Pour plus d'informations, consultez la section Activer la rotation automatique des touches dans le Guide du AWS Key Management Service développeur.

Multi-factor la suppression par authentification (MFA) est désactivée sur un compartiment Amazon S3 versionné

Multi-factor la suppression par authentification (MFA) fournit un niveau de sécurité supplémentaire pour votre compartiment Amazon S3. Elle nécessite une authentification multifactorielle pour les opérations destructrices d'Amazon S3. Lorsque la suppression MFA est désactivée, les utilisateurs disposant des autorisations appropriées peuvent supprimer définitivement les versions des objets ou suspendre la gestion des versions sur votre bucket sans problèmes d'authentification supplémentaires. L'activation de la suppression MFA permet de vous protéger contre la suppression non autorisée ou accidentelle de vos données, en offrant une protection renforcée contre les attaques de rançongiciels, les menaces internes et les erreurs opérationnelles. La suppression MFA est particulièrement utile pour les compartiments contenant des données critiques ou sensibles à la conformité qui doivent être protégées contre toute suppression non autorisée. En suivant les meilleures pratiques de sécurité, activez l'authentification multifacteur pour vos compartiments Amazon S3.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Passez en revue les types de MFA

AWS prend en charge les types de MFA suivants. Bien que l'authentification à l'aide d'un appareil physique fournisse généralement une protection de sécurité plus stricte, l'utilisation de tout type d'authentification multifacteur est plus sûre que la désactivation de l'authentification multifacteur.

Appliquez le MFA au niveau de la politique en matière de ressources

Utilisez la clé de `aws:MultiFactorAuthAge` condition dans une politique de compartiment pour exiger le MFA pour les opérations sensibles. Pour plus d'informations, consultez la section Exiger l'authentification multifacteur dans le guide de l'utilisateur d'Amazon S3.

Activer MFA

Pour activer la suppression de l'authentification multifacteur, assurez-vous d'abord que le contrôle de version est activé sur votre compartiment Amazon S3. La suppression MFA n'est prise en charge que sur les buckets pour lesquels le contrôle de version est activé. Pour plus d'informations sur l'activation de la gestion des versions d'Amazon S3, consultez la section Activation de la gestion des versions sur les buckets dans le guide de l'utilisateur Amazon S3. La suppression du MFA ne peut pas être activée via la console Amazon S3. Vous devez utiliser l'API Amazon S3 ou le AWS CLI. Pour plus d'informations, consultez la section Configuration de la suppression de MFA dans le guide de l'utilisateur Amazon S3.

Le compartiment Amazon S3 autorise les principaux d'autres AWS comptes pour modifier les autorisations des compartiments

Les politiques relatives aux compartiments Amazon S3 contrôlent l'accès aux compartiments et aux objets. Lorsque les politiques de compartiment autorisent les principaux d'autres AWS comptes à modifier les autorisations du compartiment, les utilisateurs non autorisés peuvent reconfigurer votre compartiment. Si les informations d'identification principales externes sont compromises, des utilisateurs non autorisés peuvent prendre le contrôle de votre compartiment, ce qui peut entraîner des violations de données ou des interruptions de service. Conformément aux principes de sécurité standard, limitez les actions de gestion des autorisations aux seuls mandants approuvés.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Examiner et identifier les politiques relatives aux compartiments

Dans l'exposition, identifiez le compartiment Amazon S3 dans le champ ARN. Dans la console Amazon S3, sélectionnez le compartiment et accédez à l'onglet Autorisations pour

consulter la politique du compartiment. Passez en revue la politique d'autorisations associée au bucket. Recherchez les déclarations de politique qui autorisent des actions, comme `s3:PutBucketPolicy, s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:*` les déclarations de politique qui autorisent l'accès aux principaux en dehors de votre compte, comme indiqué dans la déclaration principale.

Modifier la politique en matière de bucket

Modifiez la politique du bucket pour supprimer ou restreindre les actions accordées à d'autres AWS comptes :

- Supprimez les déclarations de politique qui accordent des actions de gestion des autorisations aux comptes externes.
- Si un accès entre comptes est requis, remplacez les autorisations générales par `(s3:*)` des actions spécifiques qui n'incluent pas la gestion des autorisations des compartiments.

Pour plus d'informations sur la modification d'une politique de compartiment, consultez la section Ajouter une politique de compartiment à l'aide de la console Amazon S3 dans le guide de l'utilisateur Amazon S3.

Caractéristiques d'accessibilité pour les compartiments Amazon S3

Voici les caractéristiques d'accessibilité des compartiments Amazon S3 et les étapes de correction suggérées.

Le compartiment Amazon S3 dispose d'un accès public en lecture

Les compartiments Amazon S3 avec accès public en lecture permettent à toute personne sur Internet de consulter le contenu de votre compartiment. Bien que cela puisse être nécessaire pour les sites Web accessibles au public ou les ressources partagées, cela peut créer des risques de sécurité si le compartiment contient des données sensibles. L'accès public en lecture peut entraîner une visualisation et un téléchargement non autorisés, ce qui peut entraîner des violations de données si des données sensibles sont stockées dans ces compartiments. Conformément aux principes de sécurité standard, limitez l'accès aux compartiments Amazon S3 aux utilisateurs et aux systèmes nécessaires.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Bloquer l'accès du public au niveau du compartiment

Amazon S3 fournit des paramètres de blocage de l'accès public qui peuvent être configurés à la fois au niveau du compartiment et au niveau du compte pour empêcher l'accès public, quelles que soient les politiques de compartiment ou les ACL. Pour plus d'informations, consultez la section Bloquer l'accès public à votre stockage Amazon S3 dans le guide de l'utilisateur Amazon S3. Après avoir bloqué l'accès public, vérifiez la configuration du contrôle d'accès de votre bucket pour vous assurer qu'elle correspond à vos exigences d'accès. Passez ensuite en revue la politique de votre compartiment Amazon S3 pour définir explicitement qui peut accéder à votre compartiment. Pour des exemples de politiques de compartiment, consultez Exemples de politiques de compartiment Amazon S3 dans le guide de l'utilisateur Amazon S3.

Autres méthodes d'accès

Si un accès public en lecture est requis, envisagez ces alternatives plus sécurisées :

- Amazon CloudFront — À utiliser CloudFront avec un Origin Access Identity (OAI) ou un Origin Access Control (OAC) pour autoriser l'accès en lecture depuis un compartiment Amazon S3 privé. Cette alternative limite l'accès direct à votre compartiment Amazon S3 tout en permettant au contenu d'être accessible au public via CloudFront. Pour plus d'informations, consultez la section Restreindre l'accès à une origine Amazon S3 dans l'Amazon CloudFront Developer Guide.
- URL présignées : utilisez des URL présignées pour accéder temporairement à des objets spécifiques. Pour plus d'informations, consultez la section Partage d'objets avec des URL présignées dans le guide de l'utilisateur Amazon S3.

Le compartiment Amazon S3 dispose d'un accès public en écriture

Les compartiments Amazon S3 dotés d'un accès public en écriture permettent à toute personne sur Internet de télécharger, modifier ou supprimer des objets de votre compartiment. Cela crée des risques de sécurité importants, notamment la possibilité que quelqu'un télécharge des fichiers malveillants, modifie des fichiers existants et supprime des données. L'accès public en écriture crée des failles de sécurité qui peuvent être exploitées par des attaquants. Conformément aux principes de sécurité standard, limitez l'accès en écriture à vos compartiments Amazon S3 aux seuls utilisateurs et systèmes nécessaires.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Bloquer l'accès public au niveau du compte et du bucket

Amazon S3 fournit des paramètres d'accès public par blocs qui peuvent être configurés à la fois au niveau du compartiment et au niveau du compte pour empêcher l'accès public, quelles que soient les politiques de compartiment ou les ACL. Pour plus d'informations, consultez la section Bloquer l'accès public à votre stockage Amazon S3 dans le guide de l'utilisateur Amazon S3.

Modifier les politiques relatives aux compartiments

Pour une approche plus précise de la suppression de l'accès public à l'écriture, consultez la politique en matière de bucket. Vous pouvez rechercher `s3:PutObject`s`3:DeleteObject`, ou`s3:*`. Pour plus d'informations sur la gestion des politiques de compartiment, consultez la section Politiques de compartiment pour Amazon S3 dans le guide de l'utilisateur Amazon S3.

Autres méthodes d'accès

Si un accès public en écriture est requis, envisagez ces alternatives plus sécurisées :

- URL présignées : utilisez des URL présignées pour accéder temporairement à des objets spécifiques. Pour plus d'informations, consultez la section Partage d'objets avec des URL présignées dans le guide de l'utilisateur Amazon S3.
- Proxy Amazon API Gateway : utilisez un intermédiaire tel qu'API Gateway AWS Lambda pour valider et autoriser les demandes avant d'écrire dans votre compartiment Amazon S3. Cette approche garantit que les clients n'écrivent jamais directement dans le bucket. Pour plus d'informations, consultez Tutoriel : Création d'une API REST en tant que proxy Amazon S3 dans le Guide du développeur d'API Gateway.
- Amazon CloudFront — À utiliser CloudFront avec un contrôle d'accès à l'origine (OAC) configuré pour toujours signer les demandes. Activez les méthodes PUT et POST pour autoriser les écritures authentifiées sans exposer directement votre compartiment Amazon S3. Configurez votre politique en matière de bucket pour limiter `s3:DeleteObject` les autorisations aux administrateurs autorisés uniquement, afin que les utilisateurs non autorisés ne puissent pas supprimer les objets que vous souhaitez conserver. Pour plus d'informations, consultez la section Restreindre l'accès à une origine Amazon S3 dans l'Amazon CloudFront Developer Guide.

Caractéristiques des données sensibles pour les compartiments Amazon S3

Voici les caractéristiques des données sensibles pour les compartiments Amazon S3 et les étapes de correction suggérées.

Le compartiment Amazon S3 contient des données sensibles

Une analyse de sécurité des données a confirmé la présence de données sensibles dans le compartiment Amazon S3. Un produit de sécurité des données intégré définit cette caractéristique lorsqu'il inspecte les objets du bucket et identifie le contenu qui nécessite une protection. Security Hub signale la caractéristique de la même manière, quel que soit le produit inspecté.

Les données sensibles peuvent inclure :

- Informations d'identification
- Informations personnelles identifiables
- Informations financières
- Contenu confidentiel nécessitant une protection

Si des données sensibles sont exposées à la suite d'une mauvaise configuration ou d'un accès non autorisé, cela peut entraîner des violations de conformité, des violations de données, une usurpation d'identité ou des pertes financières. En suivant les meilleures pratiques de sécurité, assurez-vous d'une classification correcte des données et d'une surveillance continue des données sensibles dans vos compartiments Amazon S3.

Correction

Pour supprimer cette caractéristique, supprimez les données sensibles du compartiment. Si votre charge de travail nécessite que le compartiment stocke des données sensibles, implémentez les contrôles de sécurité suivants afin de réduire le risque d'exposition.

Passez en revue les données sensibles du bucket

Dans la recherche d'exposition, choisissez Open resource. Passez en revue le résultat de sécurité des données qui a signalé les données sensibles afin de déterminer quels objets ou préfixes les contiennent. Si la détection provient de Macie, le type de découverte décrit la catégorie de données sensibles. Pour plus d'informations, consultez la section Types de résultats obtenus par Macie dans le guide de l'utilisateur Amazon Macie.

En fonction du type de données sensibles découvert, mettez en œuvre les contrôles de sécurité appropriés :

- Restreindre l'accès au compartiment — Passez en revue les autorisations du compartiment pour vous assurer qu'elles respectent le principe du moindre privilège. Utilisez les politiques IAM, les

politiques de bucket et les ACL pour restreindre l'accès. Pour plus d'informations, consultez la section Gestion des identités et des accès pour Amazon S3 dans le guide de l'utilisateur Amazon S3.

- Activer le chiffrement côté serveur — Activez le chiffrement côté serveur avec des clés KMS pour une protection supplémentaire. Pour plus d'informations, consultez la section Utilisation du chiffrement côté serveur avec des clés AWS KMS (SSE-KMS) dans le guide de l'utilisateur Amazon S3.
- Rédigez ou transformez les données sensibles — Si les objets n'ont pas besoin de conserver de valeurs sensibles, utilisez-les AWS Glue DataBrew pour préparer les données. Appliquez les transformations de masquage, de remplacement ou de hachage qui suppriment ces valeurs avant que les systèmes en aval ne consomment les données. Écrivez la sortie préparée dans un compartiment distinct doté de ses propres contrôles d'accès. Pour plus d'informations, veuillez consulter la rubrique Présentation de AWS Glue DataBrew dans le Guide du développeur AWS Glue DataBrew .

Corriger les risques liés aux instances d'Amazon Notebook SageMaker

AWS Security Hub peut générer des résultats d'exposition pour les instances Amazon SageMaker Notebook.

Sur la console Security Hub, l'instance de bloc-notes impliquée dans une détection d'exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de remédiation fournis dans cette rubrique peuvent nécessiter des consultations supplémentaires dans d'autres AWS ressources.

Table des matières

- Caractéristiques de configuration erronées pour les instances Amazon SageMaker Notebook
  - L'accès direct à Internet est activé pour l'instance Amazon SageMaker Notebook
  - L'accès root est activé sur l'instance Amazon SageMaker Notebook
- Caractéristiques des données sensibles pour les instances Amazon SageMaker Notebook
  - L'instance Amazon SageMaker Notebook contient des données sensibles
- Caractéristiques d'impact pour les instances Amazon SageMaker Notebook
  - Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié
  - A une trajectoire d'escalade politique directe
  - A une voie de détournement de la politique de confiance
  - Possède un chemin de données vers un
  - Dispose d'un chemin de restriction supprimé
  - A un rôle de passe pour créer le chemin de l'exécuteur
  - Dispose d'un rôle d'échange (chemin d'exécuteur existant)
  - Dispose d'une voie d'escalade en chaîne de rôles
  - Possède un chemin d'exécution privilégié pour l'injection de code
  - A désactivé le chemin de la piste d'audit
  - A accès au chemin d'exécution existant
  - Dispose d'un parcours de création d'identifiants
  - Dispose d'un chemin d'accès aux données du rôle de passe
  - A un rôle de passe, une tâche, un chemin de détournement
  - Dispose d'un chemin d'accès aux données à saut unique
  - Possède une capacité d'avancement

Caractéristiques de configuration erronées pour les instances Amazon SageMaker Notebook

Voici les caractéristiques de configuration erronées des instances Amazon SageMaker Notebook et les étapes à suivre pour y remédier.

L'accès direct à Internet est activé pour l'instance Amazon SageMaker Notebook

Lorsque cette option `DirectInternetAccess` est activée sur une instance de SageMaker bloc-notes Amazon, le trafic sortant est acheminé via une passerelle de traduction d'adresses SageMaker-managed réseau (NAT) vers Internet. Cela fournit un chemin de sortie qui peut être utilisé pour l'exfiltration de données ou comme canal de commande et de contrôle si l'ordinateur portable est compromis. En suivant les meilleures pratiques de sécurité, désactivez l'accès direct à Internet et placez les instances de bloc-notes dans un VPC avec des points de terminaison VPC pour les services requis. AWS

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Désactivation de l'accès Internet direct

Le `DirectInternetAccess` paramètre ne peut pas être modifié après la création d'une instance de bloc-notes. Pour la désactiver, créez une nouvelle instance de bloc-notes avec `DirectInternetAccess` définie sur `Disabled` dans un sous-réseau privé au sein d'un VPC, puis migrez vos blocs-notes et vos données depuis l'instance existante. Pour obtenir des instructions, consultez Connecter une instance de bloc-notes dans un VPC à des ressources externes dans l'Amazon SageMaker Developer Guide.

Configuration des points de terminaison de VPC

Lorsque l'accès direct à Internet est désactivé, l'instance de bloc-notes nécessite des points de terminaison VPC pour accéder à AWS des services tels qu'Amazon S3 et l'API Amazon SageMaker . Créez des points de terminaison VPC d'interface pour les services dont votre ordinateur portable a besoin. Pour plus d'informations sur les points de terminaison VPC, consultez Qu'est-ce que c'est ? AWS PrivateLink dans le AWS PrivateLink Guide.

L'accès root est activé sur l'instance Amazon SageMaker Notebook

Lorsque cette option `RootAccess` est activée sur une instance de SageMaker bloc-notes Amazon, les utilisateurs disposent de tous les privilèges OS-level root. L'accès root permet des modifications arbitraires du système, des portes dérobées persistantes et l'installation illimitée de packages.

Conformément aux meilleures pratiques de sécurité, désactivez l'accès root pour les instances de bloc-notes, sauf si cela est explicitement requis pour votre flux de travail.

Remédiation : désactivez l'accès root

Vous ne pouvez pas modifier le `RootAccess` paramètre sur une instance de bloc-notes en cours d'exécution. Pour le désactiver, arrêtez l'instance, puis mettez à jour la configuration de l'instance pour qu'elle soit définie `RootAccess` sur`Disabled`. La plupart des flux de travail des ordinateurs portables, y compris l'installation de packages avec `pip` et l'exécution de configurations de cycle de vie, continuent de fonctionner sans accès root. Pour obtenir des instructions, consultez la section Contrôler l'accès root à une instance de SageMaker bloc-notes Amazon dans l'Amazon SageMaker Developer Guide.

Considérations supplémentaires

Si un accès root est requis pour des tâches spécifiques, envisagez plutôt d'utiliser des blocs-notes Amazon SageMaker Studio, qui fournissent des environnements isolés basés sur des conteneurs avec des contrôles d'accès plus précis. Vous pouvez également utiliser des configurations de cycle de vie pour préinstaller les packages requis au moment de la création de l'instance, réduisant ainsi le besoin d'accès root lors d'une utilisation normale.

Caractéristiques des données sensibles pour les instances Amazon SageMaker Notebook

Voici les caractéristiques des données sensibles des instances Amazon SageMaker Notebook et les étapes de correction suggérées.

L'instance Amazon SageMaker Notebook contient des données sensibles

Une analyse de sécurité des données a confirmé la présence de données sensibles sur l'instance Amazon SageMaker Notebook. Un produit de sécurité des données intégré définit cette caractéristique. Le produit inspecte les fichiers du bloc-notes, les sorties et les périphériques de stockage associés, et identifie le contenu qui nécessite une protection. Nous signalons cette caractéristique de manière cohérente dans Security Hub, quel que soit le produit intégré qui a effectué l'inspection.

Les données sensibles augmentent l'impact de toutes les autres faiblesses sur la même instance de bloc-notes. Un rôle d'exécution permissif, une voie de sortie directe d'Internet ou un accès trop large exposent un contenu réglementé ou confidentiel. Un acteur malveillant qui accède au bloc-notes peut lire et copier ces enregistrements à partir des fichiers du bloc-notes, des cellules de sortie et des points de contrôle enregistrés. L'auteur de la menace peut ensuite conserver ces enregistrements en

dehors de votre environnement. Ils peuvent également utiliser toutes les informations d'identification présentes dans le bloc-notes pour s'authentifier auprès d'autres systèmes.

Conformément aux meilleures pratiques de sécurité, nous vous recommandons de restreindre l'accès aux instances de bloc-notes contenant des données sensibles et de chiffrer le stockage attaché au repos.

Les données sensibles peuvent inclure :

- Informations d'identification, telles que les mots de passe, les clés d'accès et les chaînes de connexion
- Informations personnelles identifiables
- Informations financières, telles que les numéros de compte et les données des cartes de paiement
- Contenu confidentiel nécessitant une protection

La suppression des données sensibles du bloc-notes est le seul moyen de supprimer cette caractéristique. Si le bloc-notes doit faire référence à des données sensibles, les meilleures pratiques de sécurité suivantes réduisent le risque d'exposition.

Vérifiez les données sensibles de l'instance de bloc-notes

Dans la recherche d'exposition, ouvrez la ressource à l'aide du lien hypertexte. Cela ouvre l'instance de bloc-notes concernée. Notez le nom de l'instance du bloc-notes, le AWS compte et la AWS région. Passez en revue le résultat de sécurité des données qui a signalé les données sensibles pour déterminer quels fichiers de bloc-notes, cellules de sortie ou points de contrôle les contiennent.

En fonction du type de données sensibles découvert, mettez en œuvre les contrôles de sécurité appropriés :

- Supprimer les valeurs sensibles du bloc-notes — Supprimez les valeurs sensibles du code du bloc-notes et effacez les cellules de sortie qui les contiennent. Supprimez tous les points de contrôle enregistrés et les copies exportées qui conservent les valeurs. Lorsqu'une valeur doit rester référencée, remplacez-la par un espace réservé symbolisé ou masqué. Pour plus d'informations, consultez la section Utiliser les instances Amazon SageMaker Notebook dans le Guide du SageMaker développeur Amazon.
- Effectuez une rotation de toutes les informations d'identification exposées : si le bloc-notes contenait des informations d'identification, considérez-les comme compromises. Désactivez et alternez les informations d'identification, puis consultez les journaux d'audit du système

concerné pour utiliser les valeurs exposées. Récupérez les secrets au moment de l'exécution AWS Secrets Manager à l'aide d'un rôle d'exécution restreint au lieu de les intégrer au contenu du bloc-notes. Pour plus d'informations, consultez la section Rotation AWS Secrets Manager des secrets dans le Guide de AWS Secrets Manager l'utilisateur.

- Restreindre les personnes autorisées à ouvrir l'instance de bloc-notes : accordez l'accès uniquement aux identités IAM qui en ont besoin. Étendez le rôle d'exécution aux actions et ressources spécifiques utilisées par le bloc-notes. Contrôlez qui peut ouvrir le bloc-notes en limitant les `sagemaker:CreatePresignedNotebookInstanceUrl` autorisations. Pour plus d'informations, consultez des exemples de politiques SageMaker basées sur l'identité Amazon dans l'Amazon SageMaker Developer Guide.
- Chiffrez la mémoire du bloc-notes au repos : associez une AWS KMS clé à l'instance du bloc-notes afin que le volume de stockage contenant les fichiers et les points de contrôle du bloc-notes soit chiffré au repos. Utilisez une clé gérée par le client afin de contrôler la politique des clés. N'`kms:Decrypt`accordez cette clé qu'aux identités qui ont besoin de lire le bloc-notes. Pour plus d'informations, consultez la section Protéger les données au repos à l'aide du chiffrement dans l'Amazon SageMaker Developer Guide.
- Surveillez l'accès à l'instance du bloc-notes : vérifiez AWS CloudTrail s'il y a des `sagemaker:CreatePresignedNotebookInstanceUrl` appels et des accès provenant d'identités ou de sources inattendues. Pour plus d'informations, consultez la section Consigner les appels d' SageMaker API Amazon AWS CloudTrail dans le Guide du SageMaker développeur Amazon.

Caractéristiques d'impact pour les instances Amazon SageMaker Notebook

Les caractéristiques d'impact décrivent le rayon d'explosion potentiel d'une exposition. Security Hub analyse les autorisations effectives du Gestion des identités et des accès AWS principal associé à l'instance de SageMaker bloc-notes afin de déterminer les ressources en aval qu'un attaquant pourrait atteindre si l'instance de bloc-notes est compromise. Chaque trait d'impact identifie un modèle d'escalade de privilèges spécifique. Pour réduire votre rayon d'action, passez en revue les chemins d'autorisation décrits dans chaque trait et supprimez tous les privilèges inutiles.

Conformément aux principes de sécurité standard, accordez le moindre privilège en ne fournissant que les autorisations requises pour effectuer une tâche. Remplacez les politiques générales par des politiques restreintes qui n'accordent que les actions et les ressources spécifiques nécessaires. Pour identifier les autorisations non utilisées à supprimer, utilisez IAM Access Analyzer pour générer des recommandations en fonction de l'historique des accès. Pour plus d'informations, consultez

les sections Constatations relatives à l'accès externe et inutilisé et Appliquer les autorisations de moindre privilège dans le guide de l'utilisateur IAM.

Dispose d'un contrôle total sur le chemin de l'exécuteur privilégié

Le principal associé peut transmettre un rôle et injecter du code dans une ressource de calcul qui dispose déjà d'autorisations élevées. Cela permet au mandant de prendre le contrôle total de l'exécuteur testamentaire et d'effectuer toutes les actions autorisées par le rôle de l'exécuteur testamentaire.

A une trajectoire d'escalade politique directe

Le principal associé peut modifier directement les politiques IAM pour s'accorder des autorisations supplémentaires, augmentant ainsi ses propres privilèges sans ressources intermédiaires.

A une voie de détournement de la politique de confiance

Le principal associé peut modifier la politique de confiance d'un rôle IAM pour s'autoriser à assumer ce rôle, en obtenant les autorisations du rôle.

Possède un chemin de données vers un

Le principal associé peut chiffrer ou supprimer des données d'une manière susceptible d'être utilisée pour les rançongiciels, par exemple en chiffrant des objets Amazon S3 à l'aide d'une AWS KMS clé gérée par le client, puis en modifiant la politique relative aux clés.

Dispose d'un chemin de restriction supprimé

Le principal associé peut supprimer les restrictions de sécurité telles que les limites d'autorisation, les politiques de contrôle des services ou les instructions de refus de politiques basées sur les ressources, élargissant ainsi ce que peuvent faire les autres principaux ou la ressource elle-même.

A un rôle de passe pour créer le chemin de l'exécuteur

Le principal associé peut créer une nouvelle ressource de calcul (telle qu'une fonction Lambda ou une instance Amazon EC2) et lui transmettre un rôle privilégié, blanchissant ainsi ses propres autorisations via la nouvelle ressource.

Dispose d'un rôle d'échange (chemin d'exécuteur existant)

Le principal associé peut modifier le rôle IAM attaché à une ressource de calcul existante, en le remplaçant par un rôle plus privilégié pour augmenter l'accès.

Dispose d'une voie d'escalade en chaîne de rôles

Le principal associé peut assumer une séquence de rôles, chaque rôle de la chaîne bénéficiant d'autorisations progressivement plus larges, pour atteindre finalement un rôle hautement privilégié.

Possède un chemin d'exécution privilégié pour l'injection de code

Le principal associé peut injecter du code dans une ressource de calcul en cours d'exécution dotée d'autorisations élevées, en exécutant des opérations arbitraires sous le rôle privilégié de cette ressource.

A désactivé le chemin de la piste d'audit

Le principal associé peut désactiver les services de journalisation ou de surveillance CloudTrail, tels que la couverture efficace de ses traces pendant ou après une escalade.

A accès au chemin d'exécution existant

Le principal associé peut invoquer ou se connecter à une ressource de calcul existante et utiliser le rôle qui lui est attaché pour effectuer des actions privilégiées.

Dispose d'un parcours de création d'identifiants

Le principal associé peut créer de nouvelles informations d'identification à long terme (telles que des clés d'accès ou des profils de connexion) pour d'autres mandants, en établissant des chemins d'accès persistants qui survivent aux rotations de mots de passe ou aux expirations de session.

Dispose d'un chemin d'accès aux données du rôle de passe

Le principal associé peut créer une ressource de service et lui transmettre un rôle ayant accès à des données sensibles, en obtenant un accès indirect à ces données via la nouvelle ressource.

A un rôle de passe, une tâche, un chemin de détournement

Le principal associé peut transmettre un rôle à une tâche planifiée ou pilotée par un événement (telle qu'une fonction Lambda déclenchée par un événement), ce qui lui permet d'exécuter du code arbitraire avec les autorisations de ce rôle.

Dispose d'un chemin d'accès aux données à saut unique

Le principal associé peut accéder directement à des ressources de données sensibles (telles que des compartiments Amazon S3 ou des tables DynamoDB) via ses autorisations existantes, sans avoir besoin d'étapes d'escalade intermédiaires.

Possède une capacité d'avancement

Le principal associé dispose d'un chemin d'escalade des privilèges qui fait progresser ses capacités globales au-delà de ce que suggèrent ses autorisations directement attribuées. Il s'agit d'une classification générale pour les chemins qui ne correspondent pas à un modèle plus spécifique.

Corriger les risques pour les machines virtuelles Azure

AWS Security Hub peut générer des résultats d'exposition pour les machines virtuelles Azure.

Sur la console Security Hub, la machine virtuelle Azure impliquée dans une détection d'exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la recherche. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les machines virtuelles Azure
  - La machine virtuelle Azure possède un groupe de sécurité réseau ouvert
  - La machine virtuelle Azure possède une règle de sécurité qui autorise l'accès SSH ou RDP
  - Le rôle associé à la machine virtuelle Azure est associé à une attribution de rôle d'accès administratif.

- La machine virtuelle Azure possède un système d'exploitation en fin de vie
- Caractéristiques d'accessibilité pour les machines virtuelles Azure
  - La machine virtuelle Azure est accessible via Internet
- Caractéristiques de vulnérabilité des machines virtuelles Azure
  - La machine virtuelle Azure présente des vulnérabilités logicielles exploitables par le réseau avec une forte probabilité d'exploitation
  - La machine virtuelle Azure présente des vulnérabilités logicielles
  - La machine virtuelle Azure contient des packages logiciels malveillants

Caractéristiques de mauvaise configuration pour les machines virtuelles Azure

Voici les caractéristiques de configuration erronée des machines virtuelles Azure et les étapes à suivre pour y remédier.

La machine virtuelle Azure possède un groupe de sécurité réseau ouvert

Un groupe de sécurité réseau (NSG) agit comme un pare-feu virtuel pour votre machine virtuelle Azure, filtrant le trafic entrant et sortant à l'aide d'un ensemble de règles de sécurité hiérarchisées. Un groupe de sécurité réseau ouvert contient des règles qui autorisent un accès illimité depuis n'importe quelle source (par exemple, une source de `Any` ou`0.0.0.0/0`). Ces règles peuvent exposer votre machine virtuelle à un accès non autorisé depuis Internet. Conformément aux principes de sécurité standard, limitez les règles des groupes de sécurité réseau aux seules adresses IP, ports et protocoles spécifiques requis par votre charge de travail.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Passez en revue les règles des groupes de sécurité réseau et évaluez la configuration actuelle

Identifiez le groupe de sécurité réseau associé à l'interface réseau ou au sous-réseau de la machine virtuelle et passez en revue ses règles de sécurité entrantes. Évaluez quels ports autorisent le trafic provenant d'un large éventail de sources, telles que `Any` ou`0.0.0.0/0`. Les règles sont traitées par ordre de priorité. Vérifiez donc qu'une règle permissive ne l'emporte pas sur une règle plus restrictive. Pour plus d'informations, consultez la section Groupes de sécurité réseau dans la documentation Microsoft Azure.

Restreindre les règles des groupes de sécurité réseau

Modifiez ou supprimez les règles qui autorisent un accès illimité. Remplacez une source étendue, par exemple par `Any` des adresses IP fiables, des plages d'adresses CIDR, des balises de service ou des groupes de sécurité d'applications spécifiques nécessitant un accès. Limitez la plage de ports de destination aux seuls ports utilisés par votre charge de travail. Pour plus d'informations, consultez la section Gérer les groupes de sécurité réseau dans la documentation Microsoft Azure.

La machine virtuelle Azure possède une règle de sécurité qui autorise l'accès SSH ou RDP

Les protocoles de gestion à distance tels que SSH (port 22) et RDP (port 3389) permettent aux utilisateurs de se connecter à des machines virtuelles Azure et de les gérer à distance. Lorsqu'une règle de groupe de sécurité réseau autorise ces ports depuis Internet (une source de `Any` ou`0.0.0.0/0`), la surface d'attaque de votre machine virtuelle augmente considérablement et celle-ci est exposée à des attaques par force brute et basées sur des informations d'identification. Conformément aux principes de sécurité standard, limitez l'accès à distance à des adresses IP spécifiques et fiables, ou supprimez complètement l'accès Internet direct à ces ports.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Restreindre la règle du groupe de sécurité réseau

Limitez l'accès SSH et RDP à des adresses IP fiables ou à des plages d'adresses CIDR spécifiques à la place`Any`, ou supprimez la règle entrante si l'accès à distance depuis Internet n'est pas requis. Pour plus d'informations, consultez la section Gérer les groupes de sécurité réseau dans la documentation Microsoft Azure.

Utilisez Azure Bastion pour une connectivité sécurisée

Au lieu d'exposer les ports SSH ou RDP à Internet, utilisez Azure Bastion pour vous connecter à votre machine virtuelle via TLS sans adresse IP publique ni ports entrants ouverts. Pour plus d'informations, consultez Azure Bastion dans la documentation Microsoft Azure.

Utilisez l'accès juste à temps aux machines virtuelles

Activez l'accès juste à temps (JIT) aux machines virtuelles dans Microsoft Defender pour Cloud afin que les ports de gestion tels que SSH et RDP restent fermés par défaut et ouverts uniquement pour les demandes approuvées et limitées dans le temps provenant d'une adresse IP source spécifiée. Pour plus d'informations, consultez la section Activer l'accès juste à temps dans la documentation Microsoft Azure.

Le rôle associé à la machine virtuelle Azure est associé à une attribution de rôle d'accès administratif.

Vous pouvez attribuer une identité gérée à une machine virtuelle Azure et lui attribuer des rôles de contrôle d'accès basé sur les rôles Azure (Azure RBAC) pour accéder à d'autres ressources Azure. Lorsque l'identité associée est affectée à un rôle administratif (tel que `Owner` ou`Contributor`) de grande envergure, elle accorde généralement des autorisations bien supérieures à celles requises par la charge de travail. Si la machine virtuelle est compromise, un attaquant peut utiliser ces autorisations excessives pour se déplacer latéralement dans votre environnement, accéder à des données ou manipuler des ressources. Conformément aux principes de sécurité standard, accordez le moindre privilège en n'attribuant que les autorisations dont la charge de travail a besoin.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Examiner et identifier les attributions de rôles administratifs

Dans le portail Azure, passez en revue les attributions de rôles pour l'identité associée à la machine virtuelle. Recherchez les rôles d'administrateur privilégiés tels que `Owner`, ou`Contributor`, ou`User Access Administrator`, et les rôles personnalisés qui utilisent un caractère générique (`*`) dans leur`Actions`. Pour plus d'informations, consultez la section Répertorier les attributions de rôles Azure dans la documentation Microsoft Azure.

Implémentation d'un accès sur la base du moindre privilège

Remplacez les attributions de rôles administratifs par le rôle intégré le moins privilégié qui accorde uniquement les autorisations requises par la charge de travail. Attribuez-le au périmètre le plus restreint (ressource ou groupe de ressources) qui répond à vos besoins. Lorsque vous créez des rôles personnalisés, spécifiez `Actions` et `DataActions` explicitement au lieu d'utiliser un caractère générique. Pour plus d'informations, consultez la section Meilleures pratiques pour Azure RBAC dans la documentation Microsoft Azure.

La machine virtuelle Azure possède un système d'exploitation en fin de vie

La machine virtuelle Azure exécute un système d'exploitation en fin de vie qui n'est plus pris en charge ou maintenu par son fournisseur. Lorsqu'un système d'exploitation arrive en fin de vie, le fournisseur cesse de publier des mises à jour de sécurité et des avis, ce qui laisse les vulnérabilités connues irrémédiablement intactes et expose la machine virtuelle à des attaques. En suivant les meilleures pratiques de sécurité, passez à une version du système d'exploitation prise en charge.

Correction : mise à niveau vers une version du système d'exploitation prise en charge

Planifiez une mise à niveau sur place ou migrez la charge de travail vers une machine virtuelle exécutant une version du système d'exploitation prise en charge. Avant la mise à niveau, vérifiez la compatibilité des applications et effectuez une sauvegarde ou un instantané afin de pouvoir revenir en arrière si nécessaire. Pour Windows, suivez les instructions de mise à niveau sur place ; pour Linux, suivez les instructions de mise à niveau de votre fournisseur de distribution. Pour plus d'informations, consultez la section Effectuer une mise à niveau sur place d'une machine virtuelle Windows Server dans la documentation Microsoft Azure.

Caractéristiques d'accessibilité pour les machines virtuelles Azure

Voici les caractéristiques d'accessibilité des machines virtuelles Azure et les étapes de correction suggérées.

La machine virtuelle Azure est accessible via Internet

Une machine virtuelle Azure dont les ports sont accessibles depuis Internet peut être exposée à une attaque. Une machine virtuelle devient accessible lorsqu'elle possède une adresse IP publique. Il peut également devenir accessible lorsqu'un équilibreur de charge, une passerelle d'application ou un autre chemin réseau autorise le trafic entrant depuis Internet. Conformément aux principes de sécurité standard, mettez en œuvre des contrôles d'accès réseau au moindre privilège en limitant le trafic entrant aux seules sources et ports nécessaires.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Restreindre ou supprimer l'exposition à Internet

Vérifiez si la machine virtuelle nécessite une adresse IP publique. Si ce n'est pas le cas, dissociez l'adresse IP publique de l'interface réseau et utilisez plutôt une adresse IP privée. Si la connectivité Internet sortante est toujours requise, utilisez une passerelle NAT.

Si un accès entrant est requis, placez la machine virtuelle derrière un équilibreur de charge, un pare-feu Azure ou une passerelle d'applications plutôt que de l'exposer directement. Pour plus d'informations, consultez la section Adresses IP publiques dans la documentation Microsoft Azure.

Renforcer les règles des groupes de sécurité du réseau entrant

Modifiez ou supprimez les règles des groupes de sécurité du réseau entrant qui autorisent un accès illimité (Anyou`0.0.0.0/0`), et limitez l'accès aux plages de sources, aux ports et aux protocoles spécifiques dont votre charge de travail a besoin. Pour plus d'informations, consultez la section Groupes de sécurité réseau dans la documentation Microsoft Azure.

Utiliser Azure Bastion pour l'accès à la gestion

Pour la connectivité de gestion, utilisez Azure Bastion pour accéder à la machine virtuelle via TLS sans adresse IP publique ni SSH/RDP ports ouverts. Pour plus d'informations, consultez Azure Bastion dans la documentation Microsoft Azure.

Caractéristiques de vulnérabilité des machines virtuelles Azure

Voici les caractéristiques de vulnérabilité des machines virtuelles Azure et les étapes à suivre pour y remédier.

La machine virtuelle Azure présente des vulnérabilités logicielles exploitables par le réseau avec une forte probabilité d'exploitation

Les vulnérabilités et expositions courantes (CVE) peuvent affecter les packages logiciels installés sur les machines virtuelles Azure. Une vulnérabilité hautement prioritaire est exploitable par le réseau et présente une forte probabilité d'exploitation. Cela représente une menace de sécurité immédiate, car le code d'exploitation est peut-être déjà accessible au public et utilisé activement par des attaquants ou des outils d'analyse automatisés. Corrigez rapidement ces vulnérabilités pour protéger votre machine virtuelle.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Réviser le résultat et y remédier

Utilisez l'évaluation des vulnérabilités de Microsoft Defender for Cloud pour examiner les CVE concernés et les étapes de correction pour la machine virtuelle. Le volet de détails de chaque découverte inclut les CVE pertinents et les mesures correctives recommandées. Pour plus d'informations, consultez la section Corriger les vulnérabilités des machines dans la documentation Microsoft Azure.

Appliquer les mises à jour

Utilisez Azure Update Manager pour évaluer et déployer des mises à jour du système d'exploitation et des logiciels sur vos machines virtuelles selon un calendrier. Si aucune mise à jour n'est disponible, envisagez de supprimer ou de désactiver le logiciel vulnérable, ou de restreindre l'accès au réseau jusqu'à la publication d'un correctif. Pour plus d'informations, consultez Azure Update Manager dans la documentation Microsoft Azure.

Considérations futures

Pour éviter que cela ne se reproduise, autorisez Microsoft Defender pour serveurs à analyser en permanence vos machines virtuelles à la recherche de vulnérabilités, et établissez un calendrier de mise à jour régulier avec Azure Update Manager. Pour plus d'informations, consultez Microsoft Defender pour serveurs dans la documentation Microsoft Azure.

La machine virtuelle Azure présente des vulnérabilités logicielles

Les vulnérabilités et expositions courantes (CVE) peuvent affecter les packages logiciels installés sur les machines virtuelles Azure. Les vulnérabilités non critiques représentent des failles de sécurité dont la gravité ou l'exploitabilité sont inférieures à celles des vulnérabilités hautement prioritaires. Bien qu'ils présentent un risque immédiat moindre, les attaquants peuvent toujours exploiter des vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités pour protéger votre machine virtuelle contre les attaques.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Réviser le résultat et y remédier

Utilisez l'évaluation des vulnérabilités de Microsoft Defender for Cloud pour examiner les CVE concernés et suivez les étapes de correction décrites dans le volet des informations de recherche. Pour plus d'informations, consultez la section Corriger les vulnérabilités des machines dans la documentation Microsoft Azure.

Appliquer les mises à jour

Utilisez Azure Update Manager pour évaluer et déployer des mises à jour du système d'exploitation et des logiciels sur vos machines virtuelles. Pour gérer les mises à jour de manière cohérente à grande échelle, configurez l'application de correctifs planifiée. Pour plus d'informations, consultez Azure Update Manager dans la documentation Microsoft Azure.

La machine virtuelle Azure contient des packages logiciels malveillants

Les packages malveillants sont des composants logiciels contenant du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les packages malveillants constituent une menace active et critique pour votre machine virtuelle, car les attaquants peuvent exécuter le code malveillant automatiquement sans exploiter de vulnérabilité distincte. En suivant les meilleures pratiques de sécurité, supprimez les packages malveillants pour protéger votre machine virtuelle contre d'éventuelles attaques.

Remédiation : examinez et supprimez les packages malveillants

Passez en revue les détails de la découverte pour comprendre la menace et identifier les packages concernés, puis supprimez les packages identifiés à l'aide du gestionnaire de packages approprié au système d'exploitation. Après la suppression, lancez une analyse pour confirmer qu'il ne reste aucun composant malveillant associé. Pour plus d'informations, consultez Microsoft Defender pour serveurs dans la documentation Microsoft Azure.

Remédier aux expositions pour les conteneurs blob Azure Storage

AWS Security Hub peut générer des résultats d'exposition pour les conteneurs blob Azure Storage.

Sur la console Security Hub, le conteneur blob Azure Storage impliqué dans une détection d'exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la recherche. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques d'accessibilité pour les conteneurs blob Azure Storage
  - Le compte de stockage permet un accès anonyme aux blobs
- Caractéristiques de configuration erronées pour les conteneurs blob Azure Storage
  - Le compte de stockage ne nécessite pas le protocole HTTPS pour les opérations de transfert

- Le compte de stockage n'est pas chiffré avec des clés gérées par le client
- Le compte de stockage permet l'accès entre locataires
- La suppression logicielle de blob est désactivée sur le compte de stockage
- Le compte de stockage permet la suppression permanente des blobs supprimés
- La gestion des versions des blobs est désactivée sur le conteneur blob Azure Storage
- Le conteneur de stockage n'a pas de politique d'immuabilité

Caractéristiques d'accessibilité pour les conteneurs blob Azure Storage

Voici les caractéristiques d'accessibilité des conteneurs blob Azure Storage et les étapes de correction suggérées.

Le compte de stockage permet un accès anonyme aux blobs

Lorsque l'accès anonyme en lecture est activé, les clients non authentifiés peuvent lire les données blob sans autorisation. Lorsque le compte de stockage autorise l'accès anonyme (public) à un blob et que le niveau d'accès d'un conteneur le permet, n'importe qui sur l'Internet public peut lire les données contenues dans ce conteneur. Conformément aux principes de sécurité standard, interdisez l'accès anonyme au niveau du compte et exigez que chaque demande soit autorisée, à moins que votre scénario ne dépende explicitement d'un accès public en lecture.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Interdire l'accès anonyme au compte de stockage

Définissez la `AllowBlobPublicAccess` propriété du compte de stockage sur`false`. L'interdiction de l'accès anonyme au niveau du compte annule les paramètres d'accès de tous les conteneurs du compte et bloque les futures demandes anonymes. Pour plus d'informations, consultez la section Empêcher l'accès anonyme en lecture dans la documentation Microsoft Azure.

Définissez le niveau d'accès au conteneur sur privé

Si des conteneurs individuels ont été configurés pour un accès public, définissez le niveau d'accès anonyme de chaque conteneur de `Private` manière à ce que toutes les demandes nécessitent une autorisation. Avant de modifier le paramètre, examinez toutes les applications clientes susceptibles de dépendre d'un accès anonyme. Pour plus d'informations, consultez la section Configurer l'accès anonyme en lecture dans la documentation Microsoft Azure.

Caractéristiques de configuration erronées pour les conteneurs blob Azure Storage

Voici les caractéristiques de configuration erronées des conteneurs blob Azure Storage et les étapes à suivre pour y remédier.

Le compte de stockage ne nécessite pas le protocole HTTPS pour les opérations de transfert

Lorsqu'un compte de stockage ne nécessite pas de transfert sécurisé, il accepte les demandes via HTTP non chiffré. Les données et informations d'identification envoyées via HTTP peuvent être interceptées ou modifiées en transit par un attaquant sur le chemin réseau. Conformément aux principes de sécurité standard, exigez un transfert sécurisé afin que le compte n'accepte que les demandes via HTTPS.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Exiger un transfert sécurisé

Activez la propriété Transfert sécurisé requis sur le compte de stockage (la `enableHttpsTrafficOnly` propriété). Lorsqu'un transfert sécurisé est requis, toute demande effectuée via HTTP est rejetée. Pour plus d'informations, voir Exiger un transfert sécurisé dans la documentation Microsoft Azure.

Appliquer une version minimale de TLS

Définissez la version TLS minimale du compte de stockage sur 1.2 (la `minimumTlsVersion` propriété) afin que les demandes utilisant des versions de protocole plus anciennes et moins sécurisées soient rejetées. Vérifiez que vos clients prennent en charge le protocole TLS 1.2 avant d'appliquer ce paramètre. Pour plus d'informations, voir Configurer la version TLS minimale pour un compte de stockage dans la documentation Microsoft Azure.

Le compte de stockage n'est pas chiffré avec des clés gérées par le client

Par défaut, Azure Storage chiffre les données au repos à l'aide de Microsoft-managed clés. Customer-managed les clés (CMK) vous permettent de contrôler la clé qui protège vos données, y compris la possibilité de modifier, de révoquer et d'auditer l'accès à la clé. Si les exigences de conformité de votre organisation nécessitent le contrôle des clés de chiffrement, l'absence de clés gérées par le client constitue une lacune. Conformément aux meilleures pratiques de protection des données, configurez le compte de stockage pour utiliser les clés gérées par le client stockées dans Azure Key Vault ou un HSM géré.

Correction : configurer les clés gérées par le client

Stockez une clé dans Azure Key Vault ou Azure Key Vault Managed HSM, avec la protection contre la suppression logicielle et la purge activée. Accordez les `unwrapkey` autorisations `getwrapkey`, et à une identité gérée, puis configurez le compte de stockage pour utiliser cette clé pour le chiffrement. Vous pouvez passer de la gestion par le client à la gestion des Microsoft-managed clés à tout moment. Pour plus d'informations, consultez la section Customer-managed Clés de chiffrement du stockage dans la documentation Microsoft Azure.

Le compte de stockage permet l'accès entre locataires

Cross-tenant les paramètres d'accès, tels que la réplication d'objets entre locataires ou la délégation de signature d'accès partagé (SAS) entre locataires, peuvent entraîner la sortie des données du locataire Microsoft Entra propriétaire du compte de stockage. Si votre charge de travail ne nécessite pas le partage de données entre locataires, le fait de laisser ces paramètres activés augmente le risque que les données quittent les limites de vos locataires. Conformément aux principes de sécurité standard, désactivez l'accès croisé sauf si cela est explicitement requis.

Correction : désactivez les paramètres d'accès entre locataires

Sur le compte de stockage, désactivez la réplication d'objets entre locataires (définie `allowCrossTenantReplication` sur`false`) et, lorsque cela est possible, limitez la délégation SAS entre locataires. Vérifiez vos exigences en matière de réplication et de partage avant de procéder à la modification. Pour plus d'informations, consultez la section Présentation du compte Azure Storage dans la documentation Microsoft Azure.

La suppression logicielle de blob est désactivée sur le compte de stockage

Blob soft delete protège les blobs, les instantanés et les versions individuels contre les suppressions et remplacements accidentels ou malveillants. Il conserve les données supprimées pendant une période de conservation configurable, au cours de laquelle vous pouvez les restaurer. Lorsque la suppression logicielle est désactivée, les données blob supprimées ou remplacées ne peuvent pas être récupérées, ce qui expose votre compte à une perte de données permanente. Conformément aux meilleures pratiques en matière de protection des données, activez la suppression logicielle des blobs avec une période de conservation appropriée.

Correction : activer la suppression logicielle des blobs

Activez la suppression logicielle des blobs sur le compte de stockage et définissez une période de conservation (1 à 365 jours) qui répond à vos exigences en matière de restauration. Pour une protection plus complète, activez également la suppression logicielle des conteneurs et la gestion

des versions des blobs. Pour plus d'informations, consultez la section Suppression logicielle pour les blobs dans la documentation Microsoft Azure.

Le compte de stockage permet la suppression permanente des blobs supprimés

Lorsque la suppression définitive est autorisée (la `allowPermanentDelete` propriété l'est`true`), les blobs et les instantanés supprimés peuvent être supprimés avant l'expiration de la période de rétention de la suppression logicielle. Cela compromet la protection fournie par la suppression logicielle, car un utilisateur ou un mandant compromis peut détruire définitivement les données récupérables avant l'expiration de la période de conservation. Conformément aux meilleures pratiques en matière de protection des données, n'autorisez pas la suppression définitive des blobs supprimés de manière logicielle, sauf si vous avez une exigence spécifique et bien comprise.

Remédiation : désactiver la suppression définitive

Définissez la `allowPermanentDelete` propriété du compte de stockage de `false` manière à ce que les blobs et les instantanés supprimés puissent être restaurés pendant toute la durée de conservation. Pour plus d'informations, consultez la section Suppression logicielle pour les blobs dans la documentation Microsoft Azure.

La gestion des versions des blobs est désactivée sur le conteneur blob Azure Storage

La gestion des versions d'un blob conserve automatiquement les versions précédentes d'un blob. Lorsqu'un blob est modifié ou supprimé, son état antérieur est conservé en tant que version précédente que vous pouvez restaurer. Lorsque le contrôle de version est désactivé, les remplacements et les suppressions ne peuvent pas être annulés à un état antérieur, ce qui augmente le risque de perte ou de corruption irrécupérables des données. Conformément aux meilleures pratiques en matière de protection des données, activez la gestion des versions des blobs, ainsi que la suppression logicielle, pour une protection optimale des données.

Correction : activer la gestion des versions des blobs

Activez la gestion des versions sur le service blob du compte de stockage. Pour contrôler le coût de conservation de nombreuses versions, utilisez une politique de gestion du cycle de vie pour supprimer automatiquement les anciennes versions. Pour plus d'informations, consultez la section Gestion des versions des blobs dans la documentation Microsoft Azure.

Le conteneur de stockage n'a pas de politique d'immuabilité

Une politique d'immuabilité stocke les données blob dans un état WORM (Write Once, Read Many). Dans cet état, les données ne peuvent pas être modifiées ou supprimées pendant un intervalle

spécifié (politique de conservation basée sur le temps) ou tant qu'une suspension légale n'est pas levée. Sans politique d'immuabilité, les données critiques ou relatives à la conformité contenues dans le conteneur peuvent être remplacées ou supprimées, y compris par des utilisateurs privilégiés. Lorsque des exigences réglementaires ou d'intégrité des données s'appliquent, configurez une politique d'immuabilité pour le conteneur.

Remédiation : configurer une politique d'immuabilité

Configurez une politique de rétention basée sur le temps ou une suspension légale du conteneur. Verrouillez la politique basée sur le temps une fois les tests terminés afin que les données soient entièrement protégées dans un état WORM. Activez la suppression logicielle avant d'appliquer des politiques d'immuabilité pour une protection supplémentaire. Pour plus d'informations, consultez la section Stockage immuable des données blob dans la documentation Microsoft Azure.

Corriger les risques pour les bases de données Azure SQL

AWS Security Hub peut générer des résultats d'exposition pour les bases de données Azure SQL.

Sur la console Security Hub, la base de données Azure SQL impliquée dans la détection d'une exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les bases de données Azure SQL
  - L'accès au réseau public est activé pour la base de données Azure SQL
  - La base de données Azure SQL n'applique pas AD-only l'authentification Azure
  - La base de données Azure SQL utilise un nom d'utilisateur d'administrateur par défaut ou commun
  - La sauvegarde géo-redondante est désactivée dans la base de données Azure SQL

Caractéristiques de mauvaise configuration pour les bases de données Azure SQL

Voici les caractéristiques de configuration erronée des bases de données Azure SQL et les étapes de correction suggérées.

L'accès au réseau public est activé pour la base de données Azure SQL

Lorsque l'accès au réseau public est activé sur le serveur logique, la base de données est accessible via un point de terminaison public et peut accepter des connexions depuis l'Internet public (sous réserve des règles de pare-feu). Un terminal public augmente la surface d'attaque de votre base de données et l'expose à des tentatives de connexion non autorisées. Conformément aux principes de sécurité standard, désactivez l'accès au réseau public et connectez-vous à la base de données en privé, ou limitez strictement les règles de pare-feu du serveur.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Désactivez l'accès au réseau public et utilisez Private Link

Définissez l'accès du serveur logique au réseau public `Disabled` et connectez-vous à la base de données via un point de terminaison privé (Azure Private Link) au sein de votre réseau virtuel. Cela permet de conserver le trafic de base de données sur le backbone Azure et hors de l'Internet public. Pour plus d'informations, consultez la section Contrôles d'accès réseau pour Azure SQL Database dans la documentation Microsoft Azure.

Restreindre les règles de pare-feu si un accès public est requis

Si vous devez maintenir l'accès public activé, supprimez toute règle autorisant l'accès Internet complet et désactivez Autoriser les services et ressources Azure à accéder à ce serveur lorsqu'il

n'est pas nécessaire. Limitez les règles de pare-feu au niveau du serveur aux adresses IP fiables spécifiques dont votre charge de travail a besoin. Pour plus d'informations, consultez la section Contrôles d'accès réseau pour Azure SQL Database dans la documentation Microsoft Azure.

Appliquer une version minimale de TLS

Définissez la version TLS minimale du serveur logique sur 1.2 afin que les connexions utilisant des versions de protocole plus anciennes et moins sécurisées soient rejetées. Vérifiez que vos clients prennent en charge le protocole TLS 1.2 avant d'appliquer ce paramètre. Pour plus d'informations, consultez la section Paramètres de connectivité pour Azure SQL Database dans la documentation Microsoft Azure.

La base de données Azure SQL n'applique pas AD-only l'authentification Azure

Lorsque Entra-only l'authentification Microsoft (anciennement AD-only authentification Azure) n'est pas appliquée, le serveur logique accepte également l'authentification SQL, qui repose sur des mots de passe stockés et gérés dans la base de données. L'authentification SQL est plus vulnérable au vol d'informations d'identification et aux attaques par force brute et ne bénéficie pas des contrôles centralisés de Microsoft Entra tels que l'accès conditionnel et l'authentification multifactorielle. Conformément aux principes de sécurité standard, appliquez Entra-only l'authentification Microsoft afin que seules les identités Microsoft Entra puissent se connecter.

Solution : appliquer l'authentification Microsoft Entra-only

Définissez un administrateur Microsoft Entra pour le serveur logique, puis activez Entra-only l'authentification Microsoft. Cela désactive l'authentification SQL afin que seules les identités Microsoft Entra puissent se connecter au serveur et à ses bases de données. Vérifiez que vos applications prennent en charge l'authentification Microsoft Entra avant d'appliquer ce paramètre. Pour plus d'informations, consultez la section Entra-only Authentification Microsoft dans la documentation Microsoft Azure.

La base de données Azure SQL utilise un nom d'utilisateur d'administrateur par défaut ou commun

La connexion administrateur du serveur logique utilise un nom d'utilisateur connu ou courant, tel que `sqladminadmin`, ou`sa`. Les noms d'utilisateur d'administrateur courants sont prévisibles, ce qui fait du serveur une cible plus facile pour les attaques par force brute et par bourrage d'informations d'identification, car un attaquant n'a besoin que de deviner le mot de passe. Conformément aux principes de sécurité standard, évitez les noms d'utilisateur d'administrateur par défaut ou courants et centralisez l'accès administratif via Microsoft Entra ID.

Solution : utilisez un administrateur autre que celui par défaut et utilisez l'authentification Microsoft Entra

Évitez les noms de connexion d'administrateur prévisibles. Dans la mesure du possible, appliquez Entra-only l'authentification Microsoft et gérez l'accès administratif via les identités et les groupes Microsoft Entra plutôt que par le biais d'un identifiant d'administrateur SQL. Suivez les meilleures pratiques de sécurité Azure SQL pour gérer les connexions et l'accès avec le moindre privilège. Pour plus d'informations, consultez les meilleures pratiques de sécurité de la base de données Azure SQL dans la documentation Microsoft Azure.

La sauvegarde géo-redondante est désactivée dans la base de données Azure SQL

Azure SQL Database stocke les sauvegardes automatisées dans un stockage géo-redondant par défaut, qui réplique les sauvegardes vers une région jumelée et permet la restauration géographique en cas de panne régionale. Lorsque la redondance du stockage de sauvegarde est définie sur un stockage localement redondant ou sur un stockage redondant par zone, la géo-restauration n'est pas disponible. Vous ne pouvez pas restaurer la base de données dans une autre région si la région principale devient indisponible. Conformément aux meilleures pratiques en matière de protection des données, utilisez un stockage de sauvegarde géo-redondant pour les bases de données qui nécessitent une résilience aux pannes régionales.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Configuration du stockage de sauvegarde géo-redondant

Définissez la redondance du stockage de sauvegarde de la base de données sur un stockage géo-redondant (GRS) ou un stockage redondant par zone géographique (GZRS) afin que la géo-restauration soit disponible. Les modifications s'appliquent aux sauvegardes futures et peuvent prendre jusqu'à 48 heures pour être prises en compte. Pour plus d'informations, consultez la section Sauvegardes automatisées dans la base de données Azure SQL dans la documentation Microsoft Azure.

Configurer la rétention à long terme

Pour les bases de données soumises à des exigences de conformité ou de restauration à long terme, configurez une politique de rétention à long terme (LTR). LTR conserve les sauvegardes complètes pendant une durée maximale de 10 ans, en plus de la conservation à court terme par défaut. Pour

plus d'informations, consultez Long-term la section Conservation dans Azure SQL Database dans la documentation Microsoft Azure.

Corriger les risques pour les comptes Azure Cosmos DB

AWS Security Hub peut générer des résultats d'exposition pour les comptes Azure Cosmos DB.

Sur la console Security Hub, le compte Azure Cosmos DB impliqué dans une détection d'exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les comptes Azure Cosmos DB
  - L'accès au réseau public est activé sur le compte Azure Cosmos DB
  - Le compte Azure Cosmos DB n'utilise pas la sauvegarde continue

Caractéristiques de mauvaise configuration pour les comptes Azure Cosmos DB

Voici les caractéristiques de configuration erronée des comptes Azure Cosmos DB et les étapes de correction suggérées.

L'accès au réseau public est activé sur le compte Azure Cosmos DB

Lorsque l'accès au réseau public est activé, le compte Azure Cosmos DB est accessible via un point de terminaison public. Il peut accepter des connexions depuis l'Internet public, sous réserve des règles de pare-feu et de réseau virtuel. Un terminal public augmente la surface d'attaque de votre compte et l'expose à des tentatives de connexion non autorisées et à une éventuelle exfiltration de données. Conformément aux principes de sécurité standard, désactivez l'accès au réseau public et connectez-vous au compte en privé, ou limitez strictement les règles de pare-feu du compte.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Désactivez l'accès au réseau public et utilisez Private Link

Définissez la `publicNetworkAccess` propriété du compte `Disabled` et connectez-vous via un point de terminaison privé (Azure Private Link) au sein de votre réseau virtuel. Associés à des politiques de groupe de sécurité réseau restrictives, les terminaux privés contribuent à réduire le risque d'exfiltration de données. Pour plus d'informations, consultez la section Configurer Azure Private Link dans la documentation Microsoft Azure.

Restreindre les règles de pare-feu si un accès public est requis

Si vous devez maintenir l'accès public activé, configurez les règles de pare-feu IP et les règles de réseau virtuel pour n'autoriser que les sources fiables spécifiques dont votre charge de travail a besoin, au lieu d'autoriser tous les réseaux. Pour plus d'informations, consultez la section Configurer le pare-feu IP dans la documentation Microsoft Azure.

Le compte Azure Cosmos DB n'utilise pas la sauvegarde continue

Avec le mode de sauvegarde continue, vous pouvez utiliser la restauration instantanée pour effectuer une restauration après une écriture ou une suppression accidentelle. Vous pouvez également restaurer n'importe quel horodatage d'une base de données ou d'un conteneur supprimé pendant la période de conservation. Lorsque le compte utilise le mode de sauvegarde périodique au lieu d'une sauvegarde continue, vous ne pouvez pas effectuer de restauration instantanée en libre-service. Cette limitation augmente le temps de restauration et le risque de perte de données suite à une modification accidentelle ou malveillante. Conformément aux meilleures pratiques en matière de protection des données, activez le mode de sauvegarde continue là où votre charge de travail le permet.

Correction : activer le mode de sauvegarde continue

Configurez le compte pour utiliser le mode de sauvegarde continue (niveau 7 jours ou 30 jours) afin que la restauration instantanée soit disponible. Passez en revue les limites actuelles et les API prises en charge avant de passer de la sauvegarde périodique à la sauvegarde continue. Pour plus d'informations, consultez la section Sauvegarde continue avec restauration instantanée dans la documentation Microsoft Azure.

Remédier aux expositions pour les applications Azure Function

AWS Security Hub peut générer des résultats d'exposition pour les applications Azure Function.

Sur la console Security Hub, l'application Azure Function impliquée dans la détection d'une exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les applications Azure Function
  - L'application Azure Function est déployée en dehors d'un réseau virtuel
  - Le rôle associé à l'application Azure Function est associé à une attribution de rôle d'accès administratif.
- Caractéristiques d'accessibilité pour les applications Azure Function

  - L'application Azure Function permet l'appel anonyme d'un déclencheur HTTP
- Caractéristiques de vulnérabilité des applications Azure Function
  - L'application Azure Function présente des vulnérabilités logicielles exploitables par le réseau avec une forte probabilité d'exploitation
  - L'application Azure Function présente des vulnérabilités logicielles
  - L'application Azure Function contient des packages logiciels malveillants

Caractéristiques de mauvaise configuration pour les applications Azure Function

Voici les caractéristiques de configuration erronées des applications Azure Function et les étapes de correction suggérées.

L'application Azure Function est déployée en dehors d'un réseau virtuel

Lorsqu'une application Function n'est pas intégrée à un réseau virtuel, ses points de terminaison et le trafic sortant traversent le réseau public plutôt que les limites de votre réseau privé. Lorsque l'application Function n'est pas intégrée à un réseau virtuel, vous ne pouvez pas appliquer de contrôles au niveau du réseau tels que des points de terminaison privés, des groupes de sécurité réseau et un accès sortant restreint. Cet écart augmente la visibilité de l'application. En suivant les principes de sécurité standard, intégrez l'application Function à un réseau virtuel et utilisez des points de terminaison privés sur lesquels votre plan d'hébergement le prend en charge.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Intégrez l'application Function à un réseau virtuel

Activez l'intégration du réseau virtuel pour l'application Function. Lorsque votre plan d'hébergement le permet (Flex Consumption, Elastic Premium ou Dedicated), utilisez des points de terminaison privés afin que l'application soit accessible uniquement depuis votre réseau. Pour plus d'informations, consultez les options réseau d'Azure Functions dans la documentation Microsoft Azure.

Restreindre l'accès entrant

Sur les forfaits d'hébergement qui ne prennent pas en charge les terminaux privés, utilisez des restrictions d'accès pour autoriser le trafic entrant uniquement à partir de plages d'adresses IP fiables, et désactivez l'accès au réseau public lorsqu'il n'est pas nécessaire. Pour plus d'informations, consultez la section Configuration des restrictions d'accès dans la documentation Microsoft Azure.

Le rôle associé à l'application Azure Function est associé à une attribution de rôle d'accès administratif.

Vous pouvez attribuer une identité gérée à une application Azure Function et lui attribuer des rôles de contrôle d'accès basé sur les rôles Azure (Azure RBAC) pour accéder à d'autres ressources Azure. Lorsque l'identité associée est affectée à un rôle administratif (tel que `Owner` ou`Contributor`) à grande échelle, elle accorde généralement des autorisations bien supérieures à celles requises par l'application. Si l'application Function est compromise, un attaquant peut utiliser ces autorisations excessives pour se déplacer latéralement dans votre environnement, accéder à des données ou manipuler des ressources. Conformément aux principes de sécurité standard, accordez le minimum de privilèges en n'attribuant que les autorisations dont l'application a besoin.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Examiner et identifier les attributions de rôles administratifs

Dans le portail Azure, passez en revue les attributions de rôles pour l'identité associée à l'application Function. Recherchez les rôles d'administrateur privilégiés tels que `Owner`Contributor, ou`User Access Administrator`, et les rôles personnalisés qui utilisent un caractère générique (`*`) dans leur`Actions`. Pour plus d'informations, consultez la section Répertorier les attributions de rôles Azure dans la documentation Microsoft Azure.

Implémentation d'un accès sur la base du moindre privilège

Remplacez les attributions de rôles administratifs par le rôle intégré le moins privilégié qui accorde uniquement les autorisations requises par l'application, et attribuez-le de la manière la plus étroite qui répond à vos besoins. Utilisez une identité gérée au lieu de secrets stockés pour les connexions à d'autres services Azure. Pour plus d'informations, consultez la section Meilleures pratiques pour Azure RBAC dans la documentation Microsoft Azure.

Caractéristiques d'accessibilité pour les applications Azure Function

Voici les caractéristiques d'accessibilité des applications Azure Function et les étapes de correction suggérées.

L'application Azure Function permet l'appel anonyme d'un déclencheur HTTP

Une HTTP-triggered fonction dont le niveau d'autorisation est défini sur `anonymous` peut être invoquée sur Internet sans clé d'accès ni authentification. Les déclencheurs HTTP anonymes

exposent la logique de votre fonction à des appelants non authentifiés, ce qui peut entraîner des abus, une exposition des données ou un déni de portefeuille par le biais d'une invocation incontrôlée. Conformément aux principes de sécurité standard, exigez des clés d'authentification ou d'accès pour HTTP-triggered les fonctions, sauf si un accès anonyme est explicitement requis.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Exiger une autorisation pour les déclencheurs HTTP

Augmentez le niveau d'autorisation du déclencheur HTTP de `anonymous` à `function` ou de `admin` telle sorte que les demandes doivent inclure une clé d'accès valide et nécessitent le protocole HTTPS. Pour renforcer la protection, activez App Service Authentication/Authorization ou utilisez Azure API Management pour lancer l'application. Pour plus d'informations, consultez la section Sécurisation d'Azure Functions dans la documentation Microsoft Azure.

Exiger une authentification auprès d'un fournisseur d'identité géré

Les clés d'accès étant un contrôle d'autorisation plutôt qu'une authentification, activez l'authentification App Service (Easy Auth) avec Microsoft Entra ID afin que les appelants présentent une identité valide. Désactivez également les points de terminaison administratifs (les `/admin` itinéraires) lorsqu'ils ne sont pas nécessaires. Pour plus d'informations, consultez la section Sécurisation d'Azure Functions dans la documentation Microsoft Azure.

Caractéristiques de vulnérabilité des applications Azure Function

Voici les caractéristiques de vulnérabilité des applications Azure Function et les étapes de correction suggérées.

L'application Azure Function présente des vulnérabilités logicielles exploitables par le réseau avec une forte probabilité d'exploitation

Les vulnérabilités et expositions courantes (CVE) peuvent affecter les packages logiciels et les dépendances de votre application Function. Une vulnérabilité hautement prioritaire est exploitable par le réseau et présente une forte probabilité d'exploitation, ce qui représente une menace de sécurité immédiate, car le code d'exploitation est peut-être déjà accessible au public et activement utilisé par les attaquants. Corrigez rapidement ces vulnérabilités pour protéger votre application Function.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Mettre à jour les dépendances concernées

Passez en revue les CVE concernés dans la découverte, puis mettez à jour les packages vulnérables et les dépendances vers leurs dernières versions sécurisées et redéployez l'application. Maintenez l'application Function sur un environnement d'exécution compatible afin que les mises à jour de sécurité de la plate-forme continuent de s'appliquer. Pour plus d'informations, consultez Microsoft Defender pour App Service dans la documentation Microsoft Azure.

Considérations futures

Pour éviter que cela ne se reproduise, intégrez l'analyse des dépendances et des vulnérabilités à votre pipeline de création et de déploiement, et utilisez Microsoft Defender for Cloud pour surveiller la configuration de votre application et détecter les vulnérabilités. Pour plus d'informations, consultez Microsoft Defender pour App Service dans la documentation Microsoft Azure.

L'application Azure Function présente des vulnérabilités logicielles

Les vulnérabilités et expositions courantes (CVE) peuvent affecter les packages logiciels et les dépendances de votre application Function. Les vulnérabilités non critiques représentent des failles de sécurité dont la gravité ou l'exploitabilité sont inférieures à celles des vulnérabilités hautement prioritaires. Bien qu'ils présentent un risque immédiat moindre, les attaquants peuvent toujours exploiter des vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. En suivant les meilleures pratiques de sécurité, corrigez ces vulnérabilités pour protéger votre application Function.

Correction : mettre à jour les dépendances concernées

Mettez à jour les packages vulnérables et les dépendances vers leurs dernières versions sécurisées et redéployez l'application. Si aucune mise à jour n'est disponible, envisagez de supprimer ou de désactiver le composant vulnérable jusqu'à la publication d'un correctif. Pour plus d'informations, consultez Microsoft Defender pour App Service dans la documentation Microsoft Azure.

L'application Azure Function contient des packages logiciels malveillants

Les packages malveillants sont des composants logiciels contenant du code dangereux conçu pour compromettre la confidentialité, l'intégrité et la disponibilité de vos systèmes et de vos données. Les packages malveillants constituent une menace active et critique pour votre application Function, car les attaquants peuvent exécuter le code malveillant automatiquement sans exploiter de vulnérabilité

distincte. En suivant les meilleures pratiques de sécurité, supprimez les packages malveillants pour protéger votre application Function contre d'éventuelles attaques.

Remédiation : examinez et supprimez les packages malveillants

Consultez les détails de la recherche pour identifier les packages concernés, les supprimer des dépendances de votre projet, effectuer une reconstruction à partir d'une source fiable et redéployer l'application. Après la correction, auditez votre chaîne d'approvisionnement en dépendances pour vous assurer qu'il ne reste aucun composant malveillant associé. Pour plus d'informations, consultez Microsoft Defender pour App Service dans la documentation Microsoft Azure.

Corriger les risques pour les applications Azure Container

AWS Security Hub peut générer des résultats d'exposition pour les applications Azure Container.

Sur la console Security Hub, l'application Azure Container impliquée dans la détection d'une exposition et ses informations d'identification sont répertoriées dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les applications Azure Container

  - L'application Azure Container possède des informations d'identification en texte clair dans les variables d'environnement
  - L'application Azure Container possède un groupe de sécurité réseau ouvert
  - L'application Azure Container possède une identité gérée qui ne respecte pas le principe du moindre privilège
  - Le rôle associé à l'application Azure Container est associé à une attribution de rôle d'accès administratif.
- Caractéristiques d'accessibilité pour les applications Azure Container
  - L'application Azure Container est accessible via Internet

Caractéristiques de mauvaise configuration pour les applications Azure Container

Voici les caractéristiques de configuration erronées des applications Azure Container et les étapes de correction suggérées.

L'application Azure Container possède des informations d'identification en texte clair dans les variables d'environnement

L'application Container transmet des données secrètes, telles que des chaînes de connexion, des clés d'API ou des mots de passe, au conteneur sous forme de variables d'environnement en texte brut. La configuration, les journaux ou un conteneur compromis peuvent exposer des informations d'identification en texte clair dans les variables d'environnement, ce qui permet à un attaquant de les réutiliser pour accéder à d'autres systèmes. Conformément aux principes de sécurité standard, stockez les valeurs sensibles sous forme de secrets et référencez-les plutôt que de les intégrer dans du texte en clair.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Transférer les informations d'identification vers des secrets

Remplacez les valeurs des variables d'environnement en texte brut par des secrets d'application Container ou des secrets de référence stockés dans Azure Key Vault. Mettez à jour le conteneur pour lire les valeurs de ces références secrètes. Faites pivoter toutes les informations d'identification qui étaient précédemment exposées en texte brut. Pour plus d'informations, consultez la section Gérer les secrets dans Azure Container Apps dans la documentation Microsoft Azure.

Utilisez une identité gérée dans la mesure du possible

Pour les connexions aux services Azure qui la prennent en charge, utilisez l'identité gérée de l'application Container au lieu de stocker un secret. Pour plus d'informations, consultez la section Identités gérées dans Azure Container Apps dans la documentation Microsoft Azure.

L'application Azure Container possède un groupe de sécurité réseau ouvert

Le groupe de sécurité réseau protégeant l'environnement de l'application Container contient des règles qui autorisent un accès illimité depuis n'importe quelle source (par exemple, une source de `Any` ou`0.0.0.0/0`). Un groupe de sécurité réseau ouvert expose l'environnement de l'application Container à un accès non autorisé depuis Internet. Conformément aux principes de sécurité standard, limitez les règles des groupes de sécurité réseau aux seules adresses IP, ports et protocoles spécifiques requis par votre charge de travail.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Restreindre les règles des groupes de sécurité réseau

Vérifiez le groupe de sécurité réseau associé au sous-réseau de l'environnement de l'application Container et modifiez ou supprimez les règles qui autorisent un accès illimité. Remplacez une source étendue, par exemple `Any` par les plages de confiance spécifiques dont votre charge de travail a besoin. Pour plus d'informations, consultez la section Mise en réseau dans Azure Container Apps dans la documentation Microsoft Azure.

Définissez des restrictions d'entrée IP

Outre les règles de groupe de sécurité réseau sur le sous-réseau d'environnement, configurez les restrictions d'entrée IP sur l'application conteneur elle-même afin d'autoriser ou de refuser le trafic entrant par plage d'adresses IP. Pour plus d'informations, consultez la section Configuration des restrictions d'entrée IP dans Azure Container Apps dans la documentation Microsoft Azure.

L'application Azure Container possède une identité gérée qui ne respecte pas le principe du moindre privilège

L'application Container possède une identité gérée qui bénéficie d'un accès supérieur à celui requis par la charge de travail. Une identité gérée trop privilégiée élargit le rayon d'action si l'application Container est compromise, car un attaquant peut agir avec toutes les autorisations de l'identité.

Conformément aux principes de sécurité standard, accordez à l'identité uniquement les autorisations dont la charge de travail a besoin, dans la limite la plus étroite.

Remédiation : définissez l'étendue de l'identité gérée au niveau de privilège minimal

Passez en revue les attributions de rôles accordées à l'identité gérée de l'application Container et supprimez celles qui ne sont pas obligatoires. Attribuez le rôle intégré le moins privilégié au périmètre le plus restreint (ressource ou groupe de ressources) qui répond à vos besoins. Pour plus d'informations, consultez la section Meilleures pratiques pour Azure RBAC dans la documentation Microsoft Azure.

Le rôle associé à l'application Azure Container est associé à une attribution de rôle d'accès administratif.

L'identité gérée associée à l'application Container est assignée à un rôle administratif (tel que `Owner` ou`Contributor`) dans une large mesure. Cette affectation accorde généralement des autorisations bien supérieures à celles requises par la charge de travail. Si l'application Container est compromise, un attaquant peut utiliser ces autorisations excessives pour se déplacer latéralement dans votre environnement, accéder à des données ou manipuler des ressources. Conformément aux principes de sécurité standard, accordez le moindre privilège en n'attribuant que les autorisations dont l'application a besoin.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Examiner et identifier les attributions de rôles administratifs

Dans le portail Azure, passez en revue les attributions de rôles pour l'identité associée à l'application Container. Recherchez les rôles d'administrateur privilégiés tels que `Owner`, ou`Contributor`, ou`User Access Administrator`, et les rôles personnalisés qui utilisent un caractère générique (`*`) dans leur`Actions`. Pour plus d'informations, consultez la section Répertorier les attributions de rôles Azure dans la documentation Microsoft Azure.

Implémentation d'un accès sur la base du moindre privilège

Remplacez les attributions de rôles administratifs par le rôle intégré le moins privilégié qui accorde uniquement les autorisations requises par l'application, et attribuez-le de la manière la plus étroite qui répond à vos besoins. Pour plus d'informations, consultez la section Meilleures pratiques pour Azure RBAC dans la documentation Microsoft Azure.

Caractéristiques d'accessibilité pour les applications Azure Container

Voici les caractéristiques d'accessibilité des applications Azure Container et les étapes de correction suggérées.

L'application Azure Container est accessible via Internet

L'application Container est accessible depuis l'Internet public, soit parce que l'entrée externe est activée (`ingress.external`définie sur`true`), soit parce que son environnement possède une adresse IP publique. L'accessibilité publique augmente la surface d'attaque de l'application Container et l'expose à des demandes non autorisées. Conformément aux principes de sécurité standard, désactivez l'entrée externe lorsqu'elle n'est pas requise, utilisez un environnement interne ou placez l'application derrière un point d'entrée contrôlé et authentifié.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Restreindre ou supprimer les entrées externes

Définissez l'entrée sur interne si l'application ne doit être accessible que depuis votre réseau virtuel ou votre environnement. Si un accès public est requis, limitez-le à l'aide de restrictions IP d'entrée. Accédez à l'application à l'aide d'une passerelle telle qu'Azure Application Gateway ou Azure Front Door.

Ces passerelles fournissent une authentification et un pare-feu pour les applications Web. Pour plus d'informations, consultez la section Ingress in Azure Container Apps dans la documentation Microsoft Azure.

Utiliser un environnement interne

Pour éviter d'attribuer une adresse IP publique, déployez l'application Container dans un environnement interne (intégré au réseau virtuel) qui utilise une adresse IP privée et n'exposez que les points de terminaison qui doivent être publics via un point d'entrée contrôlé. Pour plus d'informations, consultez la section Mise en réseau dans Azure Container Apps dans la documentation Microsoft Azure.

Exiger le protocole HTTPS et l'authentification pour les entrées publiques

Lorsque l'entrée doit rester publique, désactivez les connexions non sécurisées (définies sur`false`) `allowInsecure` afin que le trafic ne soit diffusé que via HTTPS. Activez la fonction d'authentification

intégrée avec Microsoft Entra ID afin que les demandes non authentifiées soient rejetées. Pour plus d'informations, consultez la section Authentification et autorisation dans Azure Container Apps dans la documentation Microsoft Azure.

Corriger les risques pour les clusters Azure Kubernetes Service

AWS Security Hub peut générer des résultats d'exposition pour les clusters Azure Kubernetes Service (AKS).

Sur la console Security Hub, le cluster AKS impliqué dans la détection d'une exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la découverte. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les clusters Azure Kubernetes Service
  - Le cluster Azure Kubernetes Service exécute une version de Kubernetes non prise en charge
  - Le cluster Azure Kubernetes Service contient des secrets Kubernetes non chiffrés
- Caractéristiques d'accessibilité pour les clusters Azure Kubernetes Service
  - Le cluster Azure Kubernetes Service autorise l'accès public

Caractéristiques de mauvaise configuration pour les clusters Azure Kubernetes Service

Voici les caractéristiques de mauvaise configuration des clusters Azure Kubernetes Service et les étapes de correction suggérées.

Le cluster Azure Kubernetes Service exécute une version de Kubernetes non prise en charge

Le cluster AKS exécute une version de Kubernetes qui n'est plus prise en charge par Microsoft. Les versions de Kubernetes non prises en charge cessent de recevoir des correctifs de sécurité et des corrections de bogues, ce qui laisse sans réponse les vulnérabilités connues dans les composants du plan de contrôle et des nœuds et expose le cluster à des attaques. En suivant les meilleures pratiques de sécurité, conservez le cluster sur une version de Kubernetes prise en charge.

Correction : mise à niveau vers une version de Kubernetes prise en charge

Mettez à niveau le plan de contrôle du cluster et les pools de nœuds vers une version de Kubernetes prise en charge. Les versions mineures ne pouvant pas être ignorées, effectuez une mise à niveau séquentielle via chaque version mineure et appliquez le dernier correctif. Passez en revue les principales modifications apportées à chaque version avant de procéder à la mise à niveau.

Envisagez d'activer les mises à niveau automatiques pour rester à jour. Pour plus d'informations, consultez la section Versions de Kubernetes prises en charge dans AKS dans la documentation Microsoft Azure.

Le cluster Azure Kubernetes Service contient des secrets Kubernetes non chiffrés

Par défaut, le cluster stocke les secrets Kubernetes dans le magasin de données etcd sans être chiffrés par une clé contrôlée par le client. Sans chiffrement au repos à l'aide d'un service de gestion de clés, toute personne ayant accès aux données etcd sous-jacentes peut lire des valeurs secrètes sensibles telles que les informations d'identification et les jetons. En suivant les meilleures pratiques de protection des données, activez le chiffrement KMS etcd afin que les secrets Kubernetes soient chiffrés au repos avec une clé dans Azure Key Vault.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Activer le cryptage KMS etcd

Configurez le cluster pour utiliser le chiffrement etcd du service de gestion des clés (KMS) avec une clé stockée dans Azure Key Vault. Accordez à l'identité du cluster des autorisations de chiffrement et

de déchiffrement sur la clé. Re-encrypt secrets existants après avoir activé la fonctionnalité. Activez la protection contre la suppression logicielle et la purge dans le coffre de clés afin que la clé ne soit pas perdue. Pour plus d'informations, consultez la section Chiffrement KMS etcd dans AKS dans la documentation Microsoft Azure.

Activez la protection contre la suppression logicielle et la purge dans le coffre de clés afin que la clé ne soit pas perdue. Pour plus d'informations, consultez la section Chiffrement KMS etcd dans AKS dans la documentation Microsoft Azure.

Stockez des secrets dans Azure Key Vault

Pour éviter de stocker des valeurs sensibles sous forme de secrets Kubernetes dans etcd, utilisez le fournisseur Azure Key Vault pour le pilote CSI Secrets Store afin de monter les secrets, les clés et les certificats d'Azure Key Vault dans des pods lors de l'exécution. Pour plus d'informations, consultez le fournisseur Azure Key Vault pour le pilote CSI Secrets Store dans la documentation Microsoft Azure.

Caractéristiques d'accessibilité pour les clusters Azure Kubernetes Service

Voici les caractéristiques d'accessibilité des clusters Azure Kubernetes Service et les étapes de correction suggérées.

Le cluster Azure Kubernetes Service autorise l'accès public

Le serveur API est le point de terminaison que vous utilisez pour communiquer avec le plan de contrôle Kubernetes de votre cluster. Le cluster est accessible depuis Internet lorsque le point de terminaison du serveur d'API est public ou lorsque les charges de travail sont exposées via un équilibreur de charge public ou une entrée. Les terminaux publics augmentent votre surface d'attaque et augmentent le risque d'accès non autorisé à votre serveur API Kubernetes. Les attaquants peuvent potentiellement accéder aux ressources du cluster ou les modifier et lire des données sensibles. Conformément aux meilleures pratiques de sécurité, limitez l'accès au serveur d'API et aux charges de travail de votre cluster aux seules plages d'adresses IP nécessaires.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Restreindre l'accès au serveur API

Utilisez un cluster privé pour que le serveur d'API soit accessible uniquement depuis votre réseau virtuel, ou configurez des plages d'adresses IP autorisées pour limiter les adresses sources qui

peuvent atteindre le point de terminaison du serveur d'API public. Pour plus d'informations, consultez la section Clusters privés Azure Kubernetes Service dans la documentation Microsoft Azure.

Limiter l'exposition du public aux charges de travail

Passez en revue les services exposés par le biais d'équilibreurs de charge publics ou d'entrées, et limitez ou supprimez l'exposition du public lorsque cela n'est pas nécessaire. Utilisez des équilibreurs de charge internes, des règles de groupe de sécurité réseau et un pare-feu d'applications Web sur un point d'entrée contrôlé pour les charges de travail qui doivent être atteintes depuis Internet. Pour plus d'informations, consultez la section Concepts de mise en réseau pour AKS dans la documentation Microsoft Azure.

Corriger les risques pour les utilisateurs d'Azure Graph

AWS Security Hub peut générer des résultats d'exposition pour les utilisateurs d'Azure Graph.

Sur la console Security Hub, l'utilisateur Azure Graph impliqué dans une détection d'exposition et ses informations d'identification sont répertoriés dans la section Ressources des détails de la recherche. Par programmation, vous pouvez récupérer les détails des ressources à l'aide de l'GetFindingsV2API Security Hub CSPM.

Après avoir identifié la ressource impliquée dans une recherche d'exposition, vous pouvez supprimer la ressource si vous n'en avez pas besoin. La suppression d'une ressource non essentielle peut réduire votre profil d'exposition et vos AWS coûts. Si la ressource est essentielle, suivez les étapes de remédiation recommandées pour atténuer les risques. Les sujets de remédiation sont divisés en fonction du type de trait.

Un seul résultat d'exposition contient des problèmes identifiés dans plusieurs sujets de remédiation. À l'inverse, vous pouvez résoudre un problème d'exposition et réduire son niveau de gravité en abordant un seul sujet de remédiation. Votre approche en matière de remédiation des risques dépend des exigences et des charges de travail de votre organisation.

> **Note**
>
> Les conseils de correction fournis dans cette rubrique peuvent nécessiter une consultation supplémentaire dans d'autres ressources Microsoft Azure.

Table des matières

- Caractéristiques de mauvaise configuration pour les utilisateurs d'Azure Graph
  - Le rôle associé à l'utilisateur Azure Graph est associé à une attribution de rôle d'accès administratif
  - L'authentification multifacteur n'est pas activée pour l'utilisateur Azure Graph

Caractéristiques de mauvaise configuration pour les utilisateurs d'Azure Graph

Voici les caractéristiques des erreurs de configuration pour les utilisateurs d'Azure Graph et les étapes de correction suggérées.

Le rôle associé à l'utilisateur Azure Graph est associé à une attribution de rôle d'accès administratif

L'utilisateur Azure Graph dispose d'une attribution de rôle administratif de contrôle d'accès basé sur les rôles Azure (Azure RBAC), tel que`Owner`, `Contributor` ou. `User Access Administrator` La mission a souvent une portée étendue, comme un abonnement ou un groupe de gestion. Les attributions de rôles administratifs accordent des autorisations étendues, de sorte qu'un attaquant peut utiliser un compte utilisateur compromis pour se déplacer latéralement, accéder à des données ou manipuler des ressources dans votre environnement. Conformément aux principes de sécurité standard, accordez le minimum de privilèges et limitez les attributions de rôles d'administrateur privilégiés.

Correction

Prenez une ou plusieurs des mesures suivantes pour remédier à cette exposition :

Examiner et identifier les attributions de rôles administratifs

Dans le portail Azure, passez en revue les attributions de rôles de l'utilisateur. Recherchez les rôles d'administrateur privilégiés tels que `Owner`Contributor, ou`User Access Administrator`, et les rôles personnalisés qui utilisent un caractère générique (`*`) dans leur`Actions`. Pour plus d'informations, consultez la section Répertorier les attributions de rôles Azure dans la documentation Microsoft Azure.

Implémentation d'un accès sur la base du moindre privilège

Supprimez les attributions de rôles privilégiés inutiles et remplacez-les par le rôle intégré le moins privilégié, attribué de la manière la plus étroite. Préférez les rôles liés à la fonction aux rôles d'administrateur privilégiés. Limitez le nombre de titulaires d'abonnements au minimum : Microsoft recommande de ne pas en dépasser trois.

Attribuez des rôles à des groupes plutôt qu'à des utilisateurs individuels. Utilisez Microsoft Entra Privileged Identity Management pour rendre les rôles privilégiés éligibles à une activation juste à temps et limitée dans le temps au lieu d'accorder un accès permanent. Pour plus d'informations, consultez la section Meilleures pratiques pour Azure RBAC dans la documentation Microsoft Azure.

L'authentification multifacteur n'est pas activée pour l'utilisateur Azure Graph

L'utilisateur d'Azure Graph peut se connecter de manière interactive sans authentification multifactorielle (MFA). Sans MFA, un compte n'est protégé que par un mot de passe, ce qui le rend vulnérable aux attaques de phishing, de pulvérisation de mots de passe et de bourrage d'informations d'identification. Un seul mot de passe compromis suffit pour qu'un attaquant puisse se connecter. Conformément aux principes de sécurité standard, exigez l'authentification multifacteur pour tous les utilisateurs dotés d'une connexion interactive.

Solution : Exiger une authentification multifactorielle

Exiger l'authentification multifacteur pour l'utilisateur par le biais d'une politique d'accès conditionnel Microsoft Entra. Pour une couverture étendue, activez les paramètres de sécurité par défaut ou une politique d'accès conditionnel qui exige l'authentification multifacteur pour tous les utilisateurs. Priorisez une politique dédiée pour les administrateurs.

Dans la mesure du possible, exigez des méthodes résistantes au phishing, telles que des clés de sécurité FIDO2, des clés d'accès ou Windows Hello for Business, grâce à une authentification à accès conditionnel renforcée. Évitez d'autoriser les méthodes de hameçonnage telles que les SMS ou la voix. Pour plus d'informations, consultez Planifier un déploiement d'authentification multifactorielle dans la documentation Microsoft Azure.

Comprendre les résultats des accès non utilisés dans Security Hub

Security Hub utilise IAM Access Analyzer pour identifier les autorisations, les rôles, les clés d'accès et les mots de passe IAM non utilisés sur votre compte. Ces résultats vous aident à mettre en œuvre les meilleures pratiques de sécurité en matière d'accès au moindre privilège en mettant en évidence les principes et les autorisations IAM qui ne sont pas utilisés activement. Cette fonctionnalité est fournie à tous les clients de Security Hub sans frais supplémentaires.

Comment fonctionne l'analyse des accès non utilisés

Lorsque vous activez Security Hub, le service crée automatiquement un analyseur d'accès IAM lié au service dans votre compte. Cet analyseur évalue tous les principaux IAM (rôles et utilisateurs) par rapport aux données d' AWS CloudTrail activité afin de déterminer quels principaux et quelles

autorisations n'ont pas été utilisés au cours d'une période rétrospective de 90 jours. La période rétrospective n'est pas configurable.

IAM Access Analyzer réévalue tous les résultats actifs toutes les 24 heures. Lorsqu'un principal ou une autorisation précédemment inutilisé devient actif, le résultat correspondant est automatiquement résolu.

L'analyseur d'accès non utilisé fonctionne dans l'est des États-Unis (Virginie du Nord) car IAM est un service mondial. Security Hub reproduit les résultats dans toutes les régions où vous avez activé Security Hub. Il n'est pas nécessaire d'activer Security Hub dans l'est des États-Unis (Virginie du Nord) pour que l'analyseur fonctionne.

Types de recherche d'accès non utilisés

Security Hub génère quatre types de résultats d'accès non utilisés :

Type de résultat	Description	Ressource évaluée
Rôle DIAM inutilisé	Un rôle IAM qui n'a pas été assumé au cours de la période rétrospective de 90 jours.	Rôle IAM
UnusedIAM UserAccessKey	Clé d'accès utilisateur IAM qui n'a pas été utilisée pour signer des demandes d'API au cours de la période rétrospective de 90 jours.	Utilisateur IAM
UnusedIAM UserPassword	Mot de passe utilisateur IAM qui n'a pas été utilisé pour la connexion à la console au cours de la période rétrospective de 90 jours.	Utilisateur IAM
UnusedPermission	Actions IAM spécifiques accordées à un rôle ou à un utilisateur mais qui n'ont pas été invoquées au cours de la période rétrospective de 90 jours.	Rôle IAM ou utilisateur IAM

Service-linked analyseur

L'analyseur d'accès IAM créé par Security Hub est un analyseur lié à un service. Vous pouvez l'afficher dans la console IAM Access Analyzer, mais vous ne pouvez ni le modifier ni le supprimer tant que Security Hub est activé.

Lorsque vous désactivez Security Hub dans toutes les régions, l'analyseur lié aux services est automatiquement supprimé. Si la suppression automatique échoue, vous pouvez supprimer l'analyseur en appelant l'opération d'API IAM Access Analyzer`DeleteServiceLinkedAnalyzer`. Cette opération ne réussit que lorsque Security Hub est complètement désactivé pour votre compte.

L'analyseur lié aux services est distinct de tous les analyseurs gérés par le client que vous avez créés indépendamment dans IAM Access Analyzer. La création ou la suppression d'analyseurs gérés par le client n'affecte pas l'analyseur lié aux services, et vice versa.

Affichage des résultats d'accès non utilisés

Les résultats d'accès non utilisés apparaissent dans la console Security Hub à côté des autres résultats de Security Hub. Vous pouvez filtrer les résultats par type pour n'afficher que les résultats d'accès non utilisés. Les résultats d'accès non utilisés sont formatés dans l'Open Cybersecurity Schema Framework (OCSF), le même format que celui utilisé pour tous les résultats de Security Hub.

Pour les UnusedPermission résultats, si vous supprimez certaines autorisations inutilisées de la politique trop permissive, mais pas toutes, Security Hub ferme la recherche existante et en crée une nouvelle pour la politique révisée si elle est toujours trop permissive.

Les résultats d'accès non utilisés sont également accessibles depuis la console IAM Access Analyzer. Les résultats d'accès non utilisés dans la console IAM Access Analyzer sont en lecture seule et ne sont visibles que dans la région USA Est (Virginie du Nord).

Accès non utilisé aux résultats d'exposition

Les informations d'accès non utilisées peuvent apparaître sous forme de caractéristiques contextuelles dans les résultats d'exposition de Security Hub. Lorsqu'un rôle IAM attaché à une ressource possède des autorisations non utilisées, le résultat d'exposition inclut cela comme contexte supplémentaire. Cela vous permet de comprendre le rayon d'action potentiel d'une vulnérabilité : une ressource dotée d'un rôle IAM privilégié présente un risque plus élevé qu'une ressource dotée des autorisations les plus restreintes.

Les types de ressources suivants peuvent afficher des caractéristiques contextuelles d'accès non utilisées dans leurs résultats d'exposition :

- Instances Amazon Elastic Compute Cloud
- AWS Lambda fonctions
- Services Amazon Elastic Container Service

- Clusters Amazon Elastic Kubernetes Service
- Utilisateurs IAM (directement)

Pour plus d'informations sur les résultats d'exposition, voirRésultats d'exposition dans Security Hub.

Recommandations de politique pour les autorisations non utilisées

À des fins UnusedPermission de recherche, Security Hub peut générer des recommandations en matière de politique de moindre privilège. Ces recommandations vous présentent une politique de remplacement limitée qui ne conserve que les autorisations réellement utilisées par votre principal. Pour de plus amples informations, veuillez consulter Génération de recommandations de politique pour les résultats d'accès non utilisés.

Tarification

L'analyseur d'accès IAM lié à un service est fourni à tous les clients de Security Hub sans frais supplémentaires. L'analyseur ou les résultats d'accès non utilisés ne vous sont pas facturés séparément.

Génération de recommandations de politique pour les résultats d'accès non utilisés

En cas de détection d'autorisations non utilisées, Security Hub peut générer des recommandations de politique de moindre privilège qui vous indiquent une politique de remplacement limitée. La recommandation évalue chaque politique associée au principal IAM et génère une stratégie de remplacement qui ne conserve que les autorisations que le principal a réellement utilisées. Cette fonctionnalité est fournie à tous les clients de Security Hub sans frais supplémentaires.

Comment fonctionnent les recommandations politiques

La génération de recommandations de politiques est une opération asynchrone. Pour générer et récupérer une recommandation :

1. Récupérez les autorisations inutilisées trouvées depuis Security Hub à l'aide de l'opération `GetFindingsV2` API. Notez le `metadata.uid` champ de la découverte.
2. Appelez `GenerateRecommendedPolicyV2` le responsable de la découverte`metadata.uid`. Cela lance la génération de recommandations, qui se termine généralement en 20 secondes.

3. Sondage `GetRecommendedPolicyV2` avec le même résultat `metadata.uid` jusqu'à ce que le `status` champ revienne`SUCCEEDED`.
4. La réponse contient une ou plusieurs étapes de recommandation. Chaque étape spécifie `recommendedAction` l'une des options suivantes `CREATE_POLICY` (créer et joindre une politique de remplacement limitée) ou `DETACH_POLICY` (détacher la politique d'origine trop privilégiée). Pour `CREATE_POLICY` les étapes, la réponse inclut à la fois le `existingPolicy` JSON et le `recommendedPolicy` JSON afin que vous puissiez les comparer.

Vous devez appeler `GenerateRecommendedPolicyV2` avant d'appeler `GetRecommendedPolicyV2` si aucune recommandation n'a été générée précédemment pour cette découverte.

Qui peut générer des recommandations

Le propriétaire du compte et les administrateurs délégués peuvent appeler les opérations d'API suivantes :

- Les titulaires de comptes peuvent générer et consulter des recommandations concernant les autorisations non utilisées trouvées dans leur propre compte.
- Les administrateurs délégués peuvent générer et consulter des recommandations pour les informations relatives aux autorisations non utilisées de tout compte membre au sein de leur organisation.

Si vous n'êtes pas un administrateur délégué et que le résultat appartient à un autre compte, l'opération d'API renvoie une `AccessDeniedException` erreur.

Cycle de vie des recommandations

- Les recommandations sont mises en cache pendant 90 jours et restent disponibles tant que le résultat est actif (pas fermé). Cependant, appeler `GenerateRecommendedPolicyV2` plusieurs fois invalide le cache et démarre une nouvelle tâche qui remplace la politique mise en cache. `GenerateRecommendedPolicyV2`N'appelez qu'une seule fois par découverte.
- La recommandation suit un modèle de détachement et d'attachement. Elle ne modifie pas vos politiques IAM existantes. Vous passez en revue la politique recommandée et vous l'appliquez manuellement dans la console IAM ou via l'API IAM.

- Si le problème est résolu (par exemple, parce que les autorisations précédemment inutilisées sont désormais utilisées), la recommandation n'est plus disponible.

Cas d'erreur

Les opérations de l'API renvoient des erreurs dans les situations suivantes :

- Le résultat a été résolu — `InvalidInputException` (HTTP 400).
- La découverte n'est pas une recherche d'autorisations inutilisées — `InvalidInputException` (HTTP 400).
- Le principal IAM a été créé via le jeu d'autorisations IAM Identity Center. Les politiques relatives aux principaux ensembles d'autorisations ne peuvent pas être modifiées directement. La recommandation renvoie un `FAILED` statut avec une explication.
- L'appelant n'est pas un administrateur délégué et le résultat appartient à un autre compte `AccessDeniedException` (HTTP 403).
- Aucune recommandation n'a encore été générée et vous appelez `GetRecommendedPolicyV2` sans avoir d'abord appelé `GenerateRecommendedPolicyV2` — `ResourceNotFoundException` (HTTP 404).

Utilisation de la console

Dans la console Security Hub, vous pouvez générer une recommandation de politique en consultant les autorisations non utilisées et en choisissant l'onglet Remédiation. La console affiche un spinner de chargement pendant la création de la recommandation. Lorsque la recommandation est prête, vous pouvez sélectionner Aperçu pour voir une comparaison côte à côte de votre politique actuelle et du remplacement du moindre privilège recommandé. Vous pouvez copier la politique recommandée au format JSON.

Référence des API

- GenerateRecommendedPolicyV2— Lance la génération asynchrone d'une recommandation de politique de moindre privilège pour la détection d'autorisations non utilisées. Prend les résultats `metadata.uid` comme entrée. Renvoie HTTP 200 avec un corps vide en cas de succès.
- GetRecommendedPolicyV2— Récupère la recommandation de politique générée. Prend les résultats `metadata.uid` comme entrée. Supporte la pagination avec `maxResults` (1 à 100) et

des `nextToken` paramètres. Renvoie l'état de la recommandation (`IN_PROGRESSSUCCEEDED`, ou`FAILED`), les étapes de recommandation, l'ARN de la ressource et les éventuelles erreurs.

Pour une documentation détaillée sur l'API, consultez le document de référence de l'API Security Hub.

Numérisation réseau dans Security Hub

L'analyse du réseau est une fonctionnalité optionnelle de Security Hub qui effectue des tests actifs d'accessibilité réseau sur vos ressources cloud. Control-plane l'analyse évalue les groupes de sécurité, les listes de contrôle d'accès réseau (NACL) et les tables de routage afin de déterminer ce qui pourrait être accessible. L'analyse du réseau va plus loin en détectant ce qui est réellement accessible. Il sonde vos ressources depuis l'extérieur de vos comptes pour identifier les ports ouverts et les services en cours d'exécution.

Toutes les analyses proviennent d'adresses IP AWS détenues et répondent à deux questions : cette ressource est-elle accessible depuis Internet ? Si accessible, qu'est-ce qui fonctionne ? Network Scanning publie les résultats sous forme de résultats OCSF autonomes dans Security Hub avec des preuves d'analyse.

Types de ressources pris en charge

La numérisation réseau prend en charge les types de ressources suivants.

Fournisseur de cloud	Type de ressource
AWS	Instance EC2 (avec adresse IP publique)
AWS	IP élastique (EIP)
AWS	Équilibreur de charge réseau (NLB)
AWS	Équilibreur de charge des applications (ALB)
AWS	Équilibreur de charge classique (CLB)
Azure	Adresse IP publique

> **Note**
>
> L'analyse réseau analyse chaque type de ressource indépendamment. Pour les équilibreurs de charge, Network Scanning résout et analyse le nom DNS. L'analyse réseau analyse uniquement les instances EC2 individuelles derrière un équilibreur de charge si elles possèdent leur propre adresse IP publique ou EIP.

Activer la numérisation réseau

Pour activer la numérisation réseau, Security Hub doit être activé sur votre compte. Vous pouvez activer la numérisation réseau par le biais d'une politique de configuration ou pour des comptes individuels.

Comptes d'organisation (recommandé) — Activez l'analyse réseau sur les comptes et les régions de votre organisation en créant ou en modifiant une politique de configuration. Pour plus d'informations sur la modification d'une politique de configuration, consultez la section Modification d'une stratégie de configuration. Lorsque la numérisation réseau est activée par le biais d'une politique de configuration, les comptes membres ne peuvent pas désactiver cette fonctionnalité.

Comptes individuels : pour les comptes qui ne sont pas gérés par une politique de configuration, vous pouvez activer l'analyse réseau à l'aide de l'une des méthodes suivantes.

> **Note**
>
> En activant l'analyse réseau, vous autorisez Security Hub à effectuer une analyse réseau active des ressources de vos AWS environnements et des environnements Azure. Cela inclut les tentatives de connexion au port TCP, l'identification des applications et des protocoles, ainsi que la collecte de bannières de service, d'en-têtes HTTP et de métadonnées de certificats TLS.

Security Hub console

Pour activer la numérisation réseau

1. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Paramètres généraux.

3. Localisez la section Numérisation réseau.
4. Sélectionnez Activer.
5. Confirmez l'autorisation pour poursuivre l'analyse active du réseau.

Security Hub API

Appelez l'`EnableSecurityHubFeatureV2`API avec le nom `NETWORK_SCANNING` de la fonctionnalité.

> **Note**
>
> L'appel de cette API alors que la numérisation réseau est déjà activée renvoie une réponse 200. Le service conserve l'`UpdatedAt`horodatage de l'activation initiale.

AWS CLI

Exécutez la commande suivante pour activer la numérisation réseau :

```
aws securityhub enable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Comment fonctionne la numérisation réseau

Une fois que vous avez activé la numérisation réseau, les événements suivants se produisent :

- La numérisation réseau analyse les ressources existantes dans les 24 heures environ suivant l'activation de la fonctionnalité.
- L'analyse du réseau analyse les nouvelles ressources peu de temps après que Security Hub a reçu la notification de la ressource créée.
- L'analyse réseau réanalyse les ressources lorsque certaines modifications du plan de contrôle éligibles sont apportées à une ressource éligible au scan.
- L'analyse du réseau réanalyse les ressources actives toutes les 12 heures environ pour détecter les changements d'accessibilité.

Les ressources éphémères ou de courte durée peuvent ne pas être analysées avant d'être supprimées.

Résultats de l'analyse réseau

Network Scanning publie les résultats au format Open Cybersecurity Schema Framework (OCSF), à l'aide de l'extension AWS OCSF, et ils apparaissent aux côtés des autres résultats de Security Hub. L'analyse du réseau permet de déterminer si une ressource possède des ports accessibles ou non. Si aucun résultat n'existe pour un type de ressource pris en charge, l'analyse réseau n'a pas encore analysé la ressource.

Résultats concernant les ports accessibles

Chaque résultat représente un port accessible unique sur une combinaison de ressources et d'adresses spécifique. La `port_scan_result_list` section d'une découverte de l'OCSF contient les résultats de l'analyse. Les exemples suivants montrent les informations renvoyées pour une ressource accessible :

```
"port_scan_result_list": [
    {
      "port_info": {
        "port": 6379,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1,
      "svc_name": "redis"
    }
],
```

```
"port_scan_result_list": [
    {
      "http_response": {
        "code": 200,
        "content_type": "text/html; charset=UTF-8",
        "http_headers": [
          {
            "name": "Server",
            "value": "Apache/2.4.68 (Amazon Linux)"
          },
```

```
          {
            "name": "Content-Type",
            "value": "text/html; charset=UTF-8"
          }
        ],
        "latency": 124
      },
      "port_info": {
        "port": 8080,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1
    }
  ],
```


Résultats informatifs concernant l'absence de ports ouverts

L'analyse réseau crée une détection lorsqu'elle ne détecte aucun port ouvert sur une ressource. Cette constatation est d'une gravité de `Informational` et ne nécessite aucune action. Cela confirme que la numérisation réseau a scanné la ressource.

Le résultat informationnel reste ouvert dans Security Hub jusqu'à ce que vous supprimiez la ressource ou que l'analyse réseau détecte des ports ouverts sur la ressource. Lorsque l'analyse réseau identifie des ports ouverts sur une ressource à l'aide d'un résultat informationnel, il ferme le résultat informationnel. Il crée ensuite une recherche pour chaque port ouvert.

Les informations relatives à l'absence de port ouvert concernent les ports actuellement pris en charge par la numérisation réseau. Pour obtenir la liste des ports pris en charge, consultezthe section called "Ports pris en charge".

Identifier les événements du cycle de vie

Le tableau suivant décrit le cycle de vie d'une découverte d'analyse réseau.

Événement	Qu'est-ce qui se passe
Aucun port ouvert n'a été détecté	L'analyse réseau crée une `Informational` détection qui ne nécessite aucune action

Événement	Qu'est-ce qui se passe
Ports ouverts détectés sur la ressource avec recherche d'informations	L'analyse réseau ferme la recherche d'informations et crée une recherche pour chaque port ouvert
Port détecté pour la première fois comme étant accessible	Network Scanning crée et publie une nouvelle découverte
Port toujours accessible lors de la nouvelle analyse (aucun changement)	L'analyse réseau actualise régulièrement les résultats
Le port est toujours accessible mais les preuves ont changé	Network Scanning republie les résultats avec des preuves actualisées
Le port n'est plus accessible	La recherche reste ouverte jusqu'à ce que la prochaine analyse confirme que le port est inaccessible
Ressource arrêtée ou supprimée	L'analyse réseau ferme tous les résultats de la ressource en définissant l'`activity_name` attribut sur `Close`
Adresse IP supprimée de la ressource	L'analyse réseau ferme les résultats pour cette adresse IP spécifique
Numérisation réseau désactivée	L'analyse du réseau ne produit aucun nouveau résultat ; les résultats existants restent inchangés jusqu'à ce qu'ils vieillissent
Security Hub désactivé	Vous n'avez plus accès aux résultats

Si un port est accessible par intermittence, l'analyse réseau base ses résultats sur des preuves positives au moment du scan. Une fois que vous avez résolu un problème (par exemple, en fermant une règle de pare-feu ou en arrêtant un service), l'analyse réseau ferme la détection lors de l'analyse suivante.

La désactivation de la numérisation réseau ne ferme pas immédiatement les résultats. Les résultats existants restent visibles jusqu'à leur expiration au cours du cycle de vie normal des recherches de Security Hub.

> **Note**
>
> Lorsque vous associez une adresse IP élastique (EIP) à une instance Amazon EC2, Network Scanning produit des résultats sur la ressource EIP. L'EIP est la ressource IP de premier niveau propriétaire de l'adresse. Pour les ressources du Network Load Balancer (NLB), le nom DNS et les EIP associées sont des points d'entrée réseau distincts, de sorte que l'analyse du réseau produit des résultats distincts pour chacun.

Scannez les preuves

Lorsque l'analyse réseau détecte qu'un port est accessible, la découverte inclut des preuves concernant le service accessible. Les types de preuves suivants peuvent être collectés :

Bannière TCP

: Octets initiaux envoyés par le service lors de la connexion, tels qu'une chaîne de version SSH.

Métadonnées HTTP

: En-têtes de réponse et code d'état HTTP.

Certificat TLS

: Nom commun (CN), émetteur, date d'expiration et statut autosigné.

Détection de service

: Application ou protocole identifié s'exécutant sur le port.

Exclusion de ressources de la numérisation

Pour exclure une ressource de l'analyse réseau, ajoutez la clé de balise `SecurityHubNetworkScanExclusion` à la ressource. La valeur de la balise peut être n'importe quelle valeur ou être vide.

Vous devez appliquer la balise à la ressource réelle dont l'adresse IP publique peut être scannée :

- Pour un EIP attaché à une instance EC2, marquez l'EIP, pas l'instance EC2.
- Pour une instance EC2 avec uniquement une adresse IP publique (pas d'EIP), étiquetez l'instance EC2.

- Pour un équilibreur de charge, identifiez l'équilibreur de charge et toutes les cibles avec des adresses IP publiques individuelles.

Lorsque vous ajoutez la balise d'exclusion, l'analyse réseau arrête les analyses futures et ferme les résultats actifs pour cette ressource. La suppression de la balise permet de réactiver la numérisation de la ressource.

Ports pris en charge

L'analyse réseau analyse les ports TCP connus suivants sur les ressources éligibles.

```
21, 22, 23, 25, 53, 80, 110, 143, 443, 445, 1433, 3306, 3389, 5432,
5900, 6379, 8080, 8443, 9200, 27017
```

Multi-cloud soutien

L'analyse réseau prend en charge les adresses IP publiques Azure. Pour analyser les ressources Azure, créez un connecteur Security Hub dans votre environnement Azure. Pour plus d'informations sur l'intégration à Microsoft Azure, consultez la section Intégration de Security Hub à Microsoft Azure.

Le comportement d'analyse, les preuves et les résultats des ressources Azure sont identiques aux AWS ressources. Les résultats apparaissent à côté des AWS résultats avec les métadonnées appropriées du fournisseur de cloud et de la région.

Disponibilité dans les Régions

La numérisation réseau est disponible dans AWS les régions commerciales où Security Hub est disponible.

Désactiver la numérisation réseau

Si votre organisation utilise des politiques de configuration, l'administrateur délégué peut désactiver l'analyse réseau sur des comptes et des régions spécifiques en modifiant la politique de configuration. Pour plus d'informations sur la modification d'une politique de configuration, consultez la section Modification d'une stratégie de configuration. Lorsque vous modifiez la politique, sélectionnez la fonctionnalité d'analyse réseau, choisissez Désactiver, puis spécifiez les comptes et les régions dans lesquels vous souhaitez désactiver la numérisation.

Pour les comptes qui ne sont pas gérés par une politique de configuration, vous pouvez désactiver l'analyse réseau à l'aide de l'une des méthodes suivantes.

Security Hub console

Pour désactiver la numérisation réseau

1. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Paramètres généraux.
3. Localisez la section Numérisation réseau.
4. Choisissez Désactiver.
5. Confirmez que vous souhaitez désactiver la numérisation réseau.

Security Hub API

Appelez l'`DisableSecurityHubFeatureV2`API avec le nom `NETWORK_SCANNING` de la fonctionnalité.

AWS CLI

Exécutez la commande suivante pour désactiver l'analyse réseau :

```
aws securityhub disable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Lorsque vous désactivez la numérisation réseau :

- L'analyse réseau ne déclenche pas de nouvelles analyses.
- Les résultats existants restent visibles jusqu'à leur expiration au cours du cycle de vie normal des recherches de Security Hub.
- L'analyse réseau complète toutes les analyses déjà en cours.

Automatisations dans Security Hub

Security Hub inclut des fonctionnalités qui modifient automatiquement les résultats et prennent des mesures en fonction de vos spécifications.

Security Hub prend actuellement en charge les types d'automatisations suivants :

- Règles d'automatisation : mettez à jour et supprimez automatiquement les résultats, et envoyez les résultats aux outils de billetterie, en temps quasi réel, en fonction de critères définis.
- Réponse et correction automatisées : créez des EventBridge règles Amazon personnalisées qui définissent les actions automatiques à prendre en fonction de résultats et d'informations spécifiques.

Les règles d'automatisation sont utiles lorsque vous souhaitez mettre à jour automatiquement les champs de recherche dans l'Open Cybersecurity Schema Framework (OCSF). Par exemple, vous pouvez utiliser une règle d'automatisation pour mettre à jour le niveau de gravité des résultats pour les ressources dotées d'une étiquette spécifique. L'utilisation de la règle d'automatisation élimine le besoin de mettre à jour manuellement le niveau de gravité de chaque résultat associé à une balise spécifique. Vous pouvez configurer des règles d'automatisation pour créer des tickets dans des outils tels que Jira Cloud et ServiceNow lorsque les résultats correspondent à des attributs spécifiques. Les tickets sont créés à partir des résultats dès leur arrivée dans Security Hub.

EventBridge les règles sont utiles lorsque vous souhaitez prendre des mesures en dehors de Security Hub pour obtenir des résultats spécifiques ou envoyer des résultats spécifiques à des outils tiers à des fins de correction ou d'enquête supplémentaire. Les règles peuvent être utilisées pour déclencher des actions prises en charge, telles que l'appel d'une AWS Lambda fonction ou la notification d'un résultat spécifique à une rubrique Amazon Simple Notification Service (Amazon SNS).

Les règles d'automatisation entrent en vigueur avant EventBridge leur application. En d'autres termes, les règles d'automatisation sont déclenchées et mettent à jour un résultat avant de le EventBridge recevoir. EventBridge les règles s'appliquent ensuite à la découverte mise à jour.

Règles d'automatisation dans Security Hub

Avec Security Hub, vous pouvez automatiser des tâches telles que la mise à jour, la recherche de détails et la création de tickets pour des intégrations tierces.

Règles d'automatisation et Régions AWS

Les règles d'automatisation peuvent être créées en une seule, Région AWS puis appliquées à toutes les configurations Régions AWS. Lorsque vous utilisez l'agrégation de régions, vous ne pouvez créer des règles que dans la région d'origine. Lorsque vous créez des règles dans la région d'origine, toutes les règles que vous définissez sont appliquées à toutes les régions liées, sauf si vos critères de règles excluent une région liée spécifique. Vous devez créer une règle d'automatisation pour toute région qui n'est pas une région liée.

Actions et critères relatifs aux règles

Les règles d'automatisation de Security Hub utilisent des critères pour référencer les attributs OCSF dans les résultats de Security Hub. Par exemple, les filtres pris en charge pour le `Criteria` paramètre dans CreateAutomationRuleV2 correspondent aux filtres pris en charge pour le `Filters` paramètre dans GetFindings V2. Cela signifie que les filtres utilisés dans les règles d'automatisation peuvent être utilisés pour obtenir des résultats. Security Hub prend en charge les champs OCSF suivants pour les critères des règles d'automatisation.

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
`activity_id`	`Activity ID`	`Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)`	`Number`
`activity_name`	`Provider status`	`EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`
`class_name`	`Finding class name`	`EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`
`cloud.account.name`	`Finding account name`	`EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`
`cloud.account.uid`	`Account ID`	`EQUALS, PREFIX, CONTAINS,`	`String`

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
		NOT_EQUALS, PREFIX_NOT_EQUALS	
cloud.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.region	Region	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.category	Assessment category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean
compliance.assessments.name	Assessment name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
compliance.control	Security control ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control_parameters	Control parameter name	EQUALS	Map
compliance.standards	Applicable standards	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.status	Compliance status	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
confidence_score	Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
finding_info.created_time_dt	Created at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.desc	Finding description	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.first_seen_time_dt	First observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.last_seen_time_dt	Last observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.modified_time_dt	Updated at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.related_events.product.uid	Related findings product ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
finding_info.related_events.title	Related findings title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.traits.category	Traits category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.uid	Related findings ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events_count	Related findings count	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.src_url	Source URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.tags	Finding info tags	EQUALS	Map

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
finding_info.title	Finding title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.types	Finding type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.uid	Provider finding ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.feature.uid	Generator ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.name	Product name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
metadata.product.uid	Product ARN	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.vendor_name	Company name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.desc	Recommendation text	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.references	Recommendation URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.cloud_partition	Resource partition	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.modified_time_dt	Resource last modified time	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
resources.name	Resource name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.name	Account name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.uid	Account	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.org.uid	Organization	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
resources .region	Resource region	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
resources.tags	Resource tags	EQUALS	Map
resources.type	Resource type	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
resources.uid	Resource ID	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
vendor_at tributes. severity	Provider severity	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
vendor_at tributes. severity_id	Provider severity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
vulnerabilities.affected_code.file.path	Affected code file path	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.affected_packages.name	Affected package name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.cvss.base_score	CVE CVSS base score	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
vulnerabilities.cve.epss.score	Epss score	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.uid	Vulnerability ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Champ OCSF	Valeur du filtre de console	Opérateurs de filtre	Type de champ
vulnerabilities.fix_coverage	Software vulnerabilities coverage	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.is_exploit_available	Software vulnerabilities with exploit available	True, False	Boolean
vulnerabilities.is_fix_available	Software vulnerabilities with fix available	True, False	Boolean
vulnerabilities.related_vulnerabilities	Related vulnerabilities	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Pour les critères étiquetés comme des champs de chaîne, l'utilisation de différents opérateurs de filtre sur le même champ affecte la logique d'évaluation. Pour plus d'informations, consultez le StringFilter document de référence de l'API Security Hub.

Chaque critère prend en charge un nombre maximum de valeurs pouvant être utilisées pour filtrer les résultats correspondants. Pour connaître les limites de chaque critère, consultez OcsfFindingFilters la référence de l'API Security Hub

Champs OCSF pouvant être mis à jour

Les champs OCSF qui peuvent être mis à jour à l'aide de règles d'automatisation sont les suivants.

- `Comment`

- `SeverityId`
- `StatusId`

Comment les règles d'automatisation évaluent les résultats

Une règle d'automatisation évalue les résultats nouveaux et mis à jour que Security Hub génère ou ingère une fois que vous avez créé la règle.

Les règles d'automatisation évaluent les résultats originaux fournis par le fournisseur. Les fournisseurs peuvent fournir de nouveaux résultats et mettre à jour les résultats existants grâce à leur intégration à Security Hub. Les règles ne sont pas déclenchées lorsque vous mettez à jour les champs de recherche après leur création par le biais de l'`BatchUpdateFindingsV2`opération. Si vous créez une règle d'automatisation et effectuez une `BatchUpdateFindingsV2` mise à jour qui affecte le même champ de recherche, la dernière mise à jour définit la valeur de ce champ. Prenons l'exemple suivant :

Vous utilisez `BatchUpdateFindingsV2` pour mettre à jour le `Status` champ d'un résultat de `New` à`In Process`. Si vous appelez`GetFindingsV2`, le `Status` champ a désormais une valeur de`In Process`. Vous créez une règle d'automatisation qui change le `Status` champ de la découverte de `New` à `Suppressed` (n'oubliez pas que les règles ignorent les mises à jour effectuées avec`BatchUpdateFindingsV2`). Le fournisseur de recherche met à jour le résultat et remplace le `Status` champ par`New`. Si vous appelez`GetFindingsV2`, la valeur du `Status` champ est désormais la suivante `Suppressed` : la règle d'automatisation a été appliquée et cette règle a été la dernière action entreprise suite à la découverte.

Lorsque vous créez ou modifiez une règle sur la console Security Hub, celle-ci affiche un aperçu des résultats qui correspondent aux critères de la règle. Alors que les règles d'automatisation évaluent les résultats originaux envoyés par le fournisseur de la recherche, l'aperçu de la console reflète les résultats dans leur état final, tels qu'ils seraient affichés dans une réponse à l'opération de l'`GetFindingsV2`API (c'est-à-dire après l'application d'actions de règles ou d'autres mises à jour à la découverte).

Comment les règles d'automatisation sont ordonnées

Un ordre de règles est attribué à chaque règle d'automatisation. Cela détermine l'ordre dans lequel Security Hub applique vos règles d'automatisation et devient important lorsque plusieurs règles concernent le même champ de recherche ou de recherche.

Lorsque plusieurs actions de règle concernent la même recherche ou le même champ de recherche, la règle dont la valeur numérique est la plus élevée pour l'ordre des règles s'applique en dernier et a l'effet ultime.

Lorsque vous créez une règle dans la console Security Hub, Security Hub attribue automatiquement l'ordre des règles en fonction de l'ordre de création des règles. La première règle que vous créez aura un ordre de règle de 1. Lorsqu'il existe plusieurs règles, chaque règle créée par la suite aura la valeur numérique disponible la plus élevée suivante pour l'ordre des règles.

Lorsque vous créez une règle via CreateAutomationRuleV2 l'API ou AWS CLI, Security Hub applique la règle dont la valeur numérique est la plus faible en `RuleOrder` premier. Il applique ensuite les règles suivantes dans l'ordre croissant. Si plusieurs résultats sont identiques`RuleOrder`, Security Hub applique d'abord une règle avec une valeur antérieure pour le `UpdatedAt` champ (c'est-à-dire que la règle modifiée la plus récente s'applique en dernier).

Vous pouvez modifier l'ordre des règles à tout moment.

Exemple d'ordre des règles :

Règle A (l'ordre des règles est**1**) :

- Critères de la règle A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` est `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` est `NEW`
  - `Workflow.Status` = `ACTIVE`
- Actions relevant de la Règle A
  - Mettre à jour `Confidence` vers `95`
  - Mettre à jour `Severity` vers `CRITICAL`
  - Mettre à jour `Comment` vers `This needs attention`

Règle B (l'ordre des règles est**2**) :

- Critères de la règle B
  - `AwsAccountId` = `123456789012`
- Actions relevant de la Règle B

- Mettre à jour `Severity` vers `INFORMATIONAL`

Tout d'abord, les actions de la Règle A s'appliquent aux résultats de Security Hub qui correspondent aux critères de la Règle A. Les actions de la Règle B s'appliquent ensuite aux résultats de Security Hub avec l'ID de compte spécifié. Dans cet exemple, étant donné que la règle B s'applique `Severity` en dernier, la valeur finale des résultats provenant de l'ID de compte spécifié est`INFORMATIONAL`. Sur la base de l'action de la Règle A, la valeur `Confidence` finale des résultats correspondants est95.

Third-party intégrations

Vous pouvez utiliser des règles d'automatisation pour créer des tickets pour les intégrations avec Jira Cloud etServiceNow ITSM. Pour plus d'informations, consultez la section Création d'une règle pour une intégration tierce.

Scénarios dans lesquels les règles d'automatisation ne fonctionnent pas

Voici les scénarios dans lesquels les règles d'automatisation ne fonctionnent pas.

- Le compte autonome devient membre d'une organisation dotée d'un administrateur délégué
- Le compte de gestion de l'organisation supprime l'administrateur délégué et définit un nouvel administrateur délégué
- La configuration de l'agrégateur pour l'administrateur délégué ou le compte autonome change lorsqu'une région non liée devient une région liée

Dans ces scénarios, un membre d'une organisation peut gérer les règles d'automatisation en effectuant des opérations de liste, d'obtention et de suppression dans les API AWS CLI ou.

Lorsqu'une région non liée devient une région liée, l'administrateur délégué ou le compte autonome peut gérer les ressources d'une région liée en effectuant des opérations de liste, d'obtention et de suppression.

Création de règles d'automatisation dans Security Hub

Cette rubrique explique comment créer des règles d'automatisation. Vous pouvez utiliser des règles d'automatisation pour mettre à jour les détails d'une découverte ou créer un ticket pour une intégration tierce. Vous devez créer des règles d'automatisation individuellement et à l' Région AWS endroit où vous souhaitez les appliquer. Toutefois, si vous créez une règle d'automatisation dans

une région d'agrégation, elle est appliquée dans toutes les régions. Sinon, si vous créez une règle d'automatisation dans une région non liée, elle est appliquée uniquement dans cette région.

Création d'une règle qui met à jour les informations de recherche

La procédure suivante explique comment créer une règle qui met à jour les détails de recherche.

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations.
3. Choisissez Créer une règle.
4. Dans Détails, entrez le nom de votre règle d'automatisation.
   - (Facultatif) Entrez une description pour votre règle d'automatisation.
5. Sous Actions, choisissez Mettre à jour les détails des résultats. Vous pouvez rechercher des critères et ajouter des critères dans la barre de recherche. Pour vérifier si certains résultats correspondent à vos critères, choisissez Aperçu des résultats correspondants.
6. Sous Mettre à jour les informations de recherche, choisissez au moins un détail de recherche à mettre à jour lorsqu'une recherche correspond à vos critères. Vous pouvez choisir Sévérité, État ou Commentaire.
7. Dans Paramètres des règles, sélectionnez Activé ou Désactivé. Si vous sélectionnez Activé, la règle d'automatisation est activée et traite les nouveaux résultats. Si vous sélectionnez Désactivé, la règle d'automatisation est désactivée et ne traite aucun résultat.
8. (Facultatif) Sous Balises, choisissez Ajouter une nouvelle étiquette pour saisir une paire clé-valeur à appliquer à votre règle d'automatisation.
9. Choisissez Créer une règle.

Création d'une règle pour une intégration tierce

La procédure suivante décrit comment créer une règle qui crée un ticket pour une intégration tierce. Pour plus d'informations sur les intégrations prises en charge par Security Hub CSPM, consultez la section Third-party Intégrations pour Security Hub CSPM.

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations.

3. Choisissez Créer une règle.
4. Dans Détails, entrez le nom de votre règle d'automatisation.
   - (Facultatif) Entrez une description pour votre règle d'automatisation.
5. Sous Actions, choisissez Créer un ticket. Vous pouvez rechercher des critères et ajouter des critères dans la barre de recherche. Pour vérifier si certains résultats correspondent à vos critères, choisissez Aperçu des résultats correspondants.
6. Sous Créer un ticket, choisissez une intégration de billetterie informatique dans la liste déroulante, puis choisissez Ajouter une intégration.
7. Dans Paramètres des règles, sélectionnez Activé ou Désactivé. Si vous sélectionnez Activé, la règle d'automatisation est activée et traite les nouveaux résultats. Si vous sélectionnez Désactivé, la règle d'automatisation est désactivée et ne traite aucun résultat.
8. (Facultatif) Sous Balises, choisissez Ajouter une nouvelle étiquette pour saisir une paire clé-valeur à appliquer à votre règle d'automatisation.
9. Choisissez Créer une règle.

Affichage des détails des règles d'automatisation dans Security Hub

Cette rubrique explique comment afficher les détails des règles d'automatisation. Vous pouvez consulter les informations suivantes concernant une règle d'automatisation :

- Nom et description
- Actions et critères
- État des règles et résultats existants
- Étiquettes

Pour afficher les détails d'une règle d'automatisation

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations. Cet écran affiche toutes les règles d'automatisation que vous avez créées.
3. Sélectionnez la règle d'automatisation que vous souhaitez consulter. Sélectionnez Afficher les détails. Vous pouvez également choisir le nom de la règle d'automatisation que vous souhaitez afficher.

Mise à jour de l'ordre des règles dans Security Hub

Cette rubrique explique comment mettre à jour l'ordre des règles d'automatisation dans la console. Si vous souhaitez modifier les critères d'une règle d'automatisation, consultez la section Modification des règles d'automatisation dans Security Hub.

Vous ne pouvez pas mettre à jour l'ordre des règles pour une règle d'automatisation sans mettre à jour l'ordre des règles pour chaque règle d'automatisation. Par exemple, vous disposez de quatre règles d'automatisation : Règle A (1), Règle B (2), Règle C (3) et Règle D (4). Vous voulez que la Règle D soit appliquée en premier. Pour ce faire, vous modifiez son numéro de 4 à 1. Par conséquent, la règle A obtient 2, la règle B 3 et la règle C 4.

Pour mettre à jour l'ordre des règles pour vos règles d'automatisation

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations.
3. Sélectionnez la règle d'automatisation que vous souhaitez modifier. Sous Commande, cliquez sur l'icône en forme de crayon à côté du numéro de commande. Utilisez les flèches pour déterminer le nouveau numéro de commande. Cliquez sur l'icône ✓ pour confirmer. Cliquez sur l'icône X pour annuler. Vous pouvez également choisir Changer l'ordre pour déplacer la règle d'automatisation vers le bas, vers le haut ou vers le haut de la liste.

Désactivation des règles d'automatisation dans Security Hub

Cette rubrique explique comment désactiver les règles d'automatisation. Lorsque vous désactivez les règles d'automatisation, Security Hub cesse de les appliquer. Vous pouvez désactiver les règles d'automatisation à tout moment et à l' Région AWS endroit où vous les avez créées.

Pour désactiver une règle

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations.
3. Sélectionnez la règle d'automatisation que vous souhaitez désactiver. Sous État, choisissez l'icône en forme de crayon à côté de Activé. Choisissez la liste déroulante, puis sélectionnez Désactivé. Cliquez sur l'icône ✓ pour confirmer. Cliquez sur l'icône X pour annuler. Vous pouvez également choisir Désactiver dans la liste déroulante Actions.

Activation d'une règle d'automatisation dans Security Hub

Cette rubrique explique comment activer les règles d'automatisation. Lorsque vous activez les règles d'automatisation, Security Hub recommence à les appliquer. Vous pouvez activer les règles d'automatisation à tout moment et à l' Région AWS endroit où vous les avez créées.

Pour activer une règle

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations.
3. Sélectionnez la règle d'automatisation que vous souhaitez activer. Sous État, choisissez l'icône en forme de crayon à côté de Désactivé. Choisissez la liste déroulante, puis sélectionnez Activé. Cliquez sur l'icône ✓ pour confirmer. Cliquez sur l'icône X pour annuler. Vous pouvez également choisir Activer dans la liste déroulante Actions.

Duplication des règles d'automatisation dans Security Hub

Cette rubrique explique comment dupliquer des règles d'automatisation. La duplication des règles d'automatisation peut vous permettre de gagner du temps si vous voulez éviter de les créer de toutes pièces. Lorsque vous dupliquez des règles d'automatisation, vous pouvez mettre à jour les détails, les actions, les paramètres des règles et les balises. Vous pouvez modifier les règles d'automatisation Région AWS là où vous les avez créées.

Pour dupliquer une règle

1. Connectez-vous à votre AWS compte et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis choisissez Automatisations.
3. Sélectionnez la règle d'automatisation que vous souhaitez dupliquer. Choisissez ensuite Actions, puis Dupliquer.
4. Apportez et révisez vos modifications, puis choisissez Créer une règle.

Modifier les règles d'automatisation dans Security Hub

Cette rubrique explique comment modifier les règles d'automatisation. Vous pouvez modifier les règles d'automatisation Région AWS là où vous les avez créées.

Vous pouvez modifier les règles d'automatisation suivantes :

- Nom et description
- Actions
- Rule settings

Vous ne pouvez pas modifier les balises des règles d'automatisation.

Pour modifier une règle

1. Connectez-vous à votre AWS compte. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, sous Gestion, choisissez Automatisations.
3. Sélectionnez la règle d'automatisation que vous souhaitez modifier. Sélectionnez Actions, puis Edit (Modifier).
4. Apportez et révisez vos modifications.
5. Sélectionnez Enregistrer les modifications.

Supprimer des règles d'automatisation dans Security Hub

Cette rubrique explique comment supprimer des règles d'automatisation. Vous pouvez supprimer les règles d'automatisation Région AWS là où vous les avez créées.

Pour supprimer une règle

1. Connectez-vous à votre AWS compte et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis Automatisations.
3. Sélectionnez la règle d'automatisation que vous souhaitez supprimer. Choisissez Actions, puis Supprimer.
4. Sélectionnez Supprimer.

Règles d'automatisation dans EventBridge

Vous pouvez utiliser les règles d'automatisation d'Amazon EventBridge pour répondre aux résultats de Security Hub. Security Hub envoie les résultats EventBridge sous forme d'événements en

temps quasi réel. Vous pouvez rédiger des règles de base qui indiquent les actions automatisées à effectuer lorsqu'un événement correspond à une règle. Les actions qui peuvent être déclenchées automatiquement sont les suivantes :

- Configuration d'une destination d'API dans EventBridge.
- Invocation des commandes d'exécution d'Amazon EC2
- Invocation de fonctions Lambda
- Invoquer des machines à états Step Functions
- Notification d'une rubrique Amazon SNS ou d'une file d'attente Amazon SQS
- Transmettre des événements à Kinesis Data Streams
- Envoi d'un résultat à un service de billetterie tiers, de conversation instantané, de gestion des informations et des événements de sécurité (SIEM) ou à un outil de réponse aux incidents et de gestion des incidents
- Envoyer un événement à un EventBridge bus depuis un autre AWS compte

Security Hub envoie les nouvelles découvertes et les mises à jour EventBridge sous forme d'événements. Vous configurez ensuite EventBridge des règles pour répondre à chaque événement Security Hub. Pour plus d'informations, voir Qu'est-ce que c'est EventBridge ? dans le Guide de EventBridge l'utilisateur.

> **Note**
>
> Si vous avez défini EventBridge des règles pour les résultats dans Security Hub CSPM, elles peuvent se chevaucher avec les règles définies pour Security Hub. Pour éviter d'envoyer des résultats dupliqués, évaluez les règles que vous avez définies pour Security Hub CSPM afin de déterminer si elles chevauchent les règles que vous avez définies pour Security Hub. Le cas échéant, désactivez toutes les règles CSPM de Security Hub remplacées par des règles de Security Hub.

> **Note**
>
> Il est recommandé de s'assurer que les utilisateurs autorisés à accéder EventBridge utilisent Gestion des identités et des accès AWS des politiques qui accordent les autorisations

minimales requises. Pour plus d'informations, consultez EventBridge et Gestion des identités et des accès AWS dans le Guide de EventBridge l'utilisateur.

EventBridge types d'événements

Security Hub utilise les types d' EventBridge événements Amazon suivants pour s'intégrer EventBridge.

Sur le EventBridge tableau de bord de Security Hub, All Events inclut tous ces types d'événements.

Résultats importés dans la version V2

Security Hub envoie automatiquement tous les nouveaux résultats et toutes les mises à jour des résultats existants EventBridge sous forme d'Findings Imported V2événements. Chaque Findings Imported V2 événement contient une seule découverte.

Chaque résultat importé et chaque résultat mis à jour par le biais d'une `BatchUpdateFindingsV2` demande déclenche un Findings Imported V2 événement.

Pour les comptes administrateurs, le flux d'événements EventBridge inclut des événements contenant des résultats provenant à la fois de leur compte et de leurs comptes membres.

Dans une région d'agrégation, le flux d'événements inclut des événements pour les résultats de la région d'agrégation et des régions liées. Cross-Region les résultats sont inclus dans le flux d'événements en temps quasi réel.

Vous pouvez définir des règles EventBridge qui acheminent automatiquement les résultats vers un flux de travail de correction, un outil tiers ou une autre EventBridge cible prise en charge. Les règles peuvent inclure des filtres qui n'appliquent la règle que si la découverte comporte des valeurs d'attribut spécifiques.

Vous utilisez cette méthode pour envoyer automatiquement tous les résultats, ou tous les résultats présentant des caractéristiques spécifiques, à un flux de travail de réponse ou de correction.

> **Note**
>
> Security Hub et Security Hub CSPM envoient tous deux leurs résultats à la EventBridge source de. `aws.securityhub` Assurez-vous que vos EventBridge règles utilisent le type de

détail spécifique à Security Hub afin d'éviter les notifications dupliquées liées aux résultats du Security Hub CSPM.

EventBridge formats d'événements

Le type d'Findings Imported V2événement utilise le format d'événement suivant.

Exemple

Ce format est utilisé lorsque Security Hub envoie un événement à EventBridge.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Findings Imported V2",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "e51603d1054aad9d9f498d82d6e81acf4cf6bc88140e8ad2273123c73b81084"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

Chaque événement envoie un résultat unique. *<finding content>*est le contenu en JSON du résultat envoyé par l'événement.

Pour une liste complète des attributs de recherche, consultez les résultats de l'OCSF dans Security Hub CSPM.

Configuration des règles pour EventBridge

Vous pouvez créer une règle dans Amazon EventBridge qui définit une action à effectuer lorsqu'un Findings Imported V2 événement est reçu. Findings Imported V2les événements sont déclenchés par des mises à jour via `BatchUpdateFindingsV2`.

Chaque règle contient un modèle d'événement qui identifie les événements qui déclenchent la règle. Le modèle d'événement contient toujours la source de l'événement (`aws.securityhub`) et le type d'événement (Findings Imported V2). Le modèle d'événement peut également spécifier des filtres pour identifier les résultats auxquels la règle s'applique.

La règle d'événement identifie ensuite les cibles de la règle. Les cibles sont les actions à effectuer lorsque vous recevez EventBridge un événement Findings Imported V2 et que le résultat correspond aux filtres.

Les instructions fournies ici utilisent la EventBridge console. Lorsque vous utilisez la console, crée EventBridge automatiquement la politique basée sur les ressources requise qui permet d' EventBridge écrire dans Amazon CloudWatch Logs.

Vous pouvez également utiliser le `PutRule` fonctionnement de l' EventBridge API. Toutefois, si vous utilisez l' EventBridge API, vous devez créer la politique basée sur les ressources. Pour plus d'informations sur la politique requise, consultez la section CloudWatch Consigne les autorisations dans le guide de EventBridge l'utilisateur Amazon.

Format du modèle d'événement

Le format du modèle d'événement pour les événements Findings Imported V2 est le suivant :

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`identifie Security Hub comme étant le service qui génère l'événement.
- `detail-type`identifie le type d'événement.
- `detail`est facultatif et fournit les valeurs de filtre pour le modèle d'événement. Si le modèle d'événement ne contient aucun `detail` champ, tous les résultats déclenchent la règle.

Vous pouvez filtrer les résultats en fonction de n'importe quel attribut de recherche. Pour chaque attribut, vous fournissez un tableau d'une ou de plusieurs valeurs séparées par des virgules.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Si vous fournissez plusieurs valeurs pour un attribut, ces valeurs sont jointes par`OR`. Un résultat correspond au filtre d'un attribut individuel si le résultat possède l'une des valeurs répertoriées. Par exemple, si vous fournissez les deux valeurs `INFORMATIONAL` et `LOW` comme valeurs pour`Severity.Label`, le résultat correspond s'il possède une étiquette de gravité égale à `INFORMATIONAL` ou`LOW`.

Les attributs sont joints par`AND`. Un résultat correspond s'il correspond aux critères de filtre pour tous les attributs fournis.

Lorsque vous fournissez une valeur d'attribut, elle doit refléter l'emplacement de cet attribut dans la structure OCSF (AWS Open Cybersecurity Schema Framework).

Dans l'exemple suivant, le modèle d'événement fournit des valeurs de filtre pour `ProductArn` et. Ainsi`Severity.Label`, une recherche correspond si elle est générée par Amazon Inspector et si elle possède une étiquette de gravité égale à `INFORMATIONAL` ou`LOW`.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Création d'une règle d'événement

Vous pouvez utiliser un modèle d'événement prédéfini ou un modèle d'événement personnalisé pour créer une règle dans EventBridge. Si vous sélectionnez un motif prédéfini, renseignez EventBridge automatiquement `source` et`detail-type`. EventBridge fournit également des champs permettant de spécifier des valeurs de filtre pour les attributs de recherche suivants :

- `cloud.account.uid`
- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

Pour créer une EventBridge règle (console)

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. À l'aide des valeurs suivantes, créez une EventBridge règle qui surveille la recherche d'événements :
   - Pour Type de règle, choisissez Règle avec un modèle d'événement.
   - Choisissez comment créer le modèle d'événement.

Pour créer le modèle d'événement avec...	Faites ceci...	
Un modèle	Dans la section Modèle d'événement, choisissez les options suivantes : • Pour Source d'événement, choisissez Services AWS . • Pour le AWS service, choisissez Security Hub.	

Pour créer le modèle d'événement avec...	Faites ceci...	
	• Pour Type d'événement, choisissez Findings Imported V2. • (Facultatif) Pour rendre la règle plus précise, ajoutez des valeurs de filtre. Par exemple, pour limiter la règle aux résultats dont les états d'enregistrement sont actifs, pour les états d'enregistrement spécifiques, choisissez Actif.	

Pour créer le modèle d'événement avec...	Faites ceci...
Un modèle d'événement personnalisé (Utilisez un modèle personnalisé si vous souhaitez filtrer les résultats en fonction d'attributs qui n'apparaissent pas dans la EventBridge console.)	• Dans la section Modèle d'événement, choisissez Modèles personnalisés (éditeur JSON), puis collez le modèle d'événement suivant dans la zone de texte : `{ "source": [ "aws.securityhub" ], "detail-type": [ "Findings Imported V2" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>"] } } }` • Mettez à jour le modèle d'événement pour inclure l'attribut et les valeurs d'attribut que vous souhaitez utiliser comme filtre. Par exemple, pour appliquer la règle à des résultats dont la gravité

Pour créer le modèle d'événement avec...	Faites ceci...	
	est de`Critical`, utilisez l'exemple de modèle suivant : `{ "source": ["aws.securityhub" ], "detail-type": ["Findings Imported V2"], "detail":{ "findings": { "Severity": ["Critical"] } } }`	

- Pour Types de cibles, choisissez un AWS service, et pour Sélectionner une cible, choisissez une cible telle qu'une rubrique ou une AWS Lambda fonction Amazon SNS. La cible est déclenchée lorsqu'un événement correspond au modèle d'événement défini dans la règle est reçu.

Pour plus d'informations sur la création de règles, consultez la section Création de EventBridge règles Amazon qui réagissent à des événements dans le Guide de EventBridge l'utilisateur Amazon.

> **Note**
>
> Si vous avez défini EventBridge des règles pour les résultats dans Security Hub CSPM, elles peuvent se chevaucher avec les règles définies pour Security Hub. Pour éviter d'envoyer des résultats dupliqués, évaluez les règles que vous avez définies pour Security Hub CSPM afin de déterminer si elles chevauchent les règles que vous avez définies pour Security Hub. Le

cas échéant, désactivez toutes les règles CSPM de Security Hub remplacées par des règles de Security Hub.

Third-party intégrations pour Security Hub

Vous pouvez améliorer votre niveau de sécurité grâce à des intégrations tierces pour AWS Security Hub. Grâce à cette fonctionnalité, vous pouvez activer des intégrations qui utilisent les résultats de Security Hub, ce qui vous permet d'intégrer vos outils opérationnels, d'investigation et de réponse à Security Hub. Security Hub prend actuellement en charge l'intégration avec Jira Cloud etServiceNow.

Rubriques

- Intégrations pour AWS Hub de sécurité Jira Cloud
- Intégrations pour ServiceNow
- Principales politiques de KMS pour les intégrations de billetterie de Security Hub
- Tester les intégrations de billetterie configurées

Intégrations pour AWS Hub de sécurité Jira Cloud

Cette rubrique décrit comment intégrer Security Hub àJira Cloud. Avant d'effectuer l'une des procédures décrites dans cette rubrique, vous devez acheter un plan Jira Cloud d'abonnement. Pour plus d'informations sur les plans d'abonnement, consultez la section Tarification sur le Atlassian site Web.

Cette intégration vous permet d'envoyer les résultats de Security Hub à Jira Cloud, manuellement ou automatiquement, afin que vous puissiez les gérer dans le cadre de vos flux de travail opérationnels. Par exemple, vous pouvez attribuer la propriété à des problèmes nécessitant une investigation et une résolution.

Pour les comptes d'une organisation, seul l'administrateur délégué peut configurer une intégration. L'administrateur délégué peut utiliser manuellement la fonction de création de ticket pour les résultats de tout compte de membre. En outre, l'administrateur délégué peut utiliser des règles d'automatisation pour créer automatiquement des tickets pour tous les résultats associés aux comptes des membres. Lors de la définition d'une règle d'automatisation, l'administrateur délégué peut définir des critères, qui peuvent inclure tous les comptes membres ou des comptes de membres spécifiques. Pour plus d'informations sur la configuration d'un administrateur délégué, consultez la section Configuration d'un compte d'administrateur délégué dans Security Hub.

Pour les comptes n'appartenant pas à une organisation, tous les aspects de cette fonctionnalité sont disponibles.

Conditions préalables

Avant de connecter Security Hub à votre Jira Cloud environnement, vous devez vous assurer que les étapes de configuration suivantes sont effectuées dans votre environnement Jira.

- Installez l'application cloud AWS Security Hub pour Jira.
- Avoir au moins un projet de développement logiciel géré par l'entreprise.
- Attribuez l' AWS application aux projets de développement logiciel pour lesquels vous souhaitez recevoir des résultats de Security Hub.

Les étapes correspondant à chacune de ces conditions préalables sont répertoriées ci-dessous.

1. Installer la AWS Hub de sécurité pour Jira Cloud app

Security Hub dispose d'une application pour faciliter son intégration à Jira. Cette application installe des champs personnalisés et un type de problème personnalisé. Security Hub les utilise pour renseigner des attributs spécifiques relatifs aux résultats.

1. Connectez-vous à votre Atlassian site en tant qu'administrateur.
2. Choisissez Paramètres, puis Applications.
3. Si vous êtes redirigé vers la page de la place de marché, choisissez Rechercher de nouvelles applications. Si vous êtes dirigé vers la page des applications, choisissez Explorer les applications, puis recherchez AWS Security Hub pour Jira Cloud. Choisissez ensuite Get it now.

2. Créer un projet ou vérifier des projets existants

Cette étape est obligatoire si vous n'avez pas créé de projet. Pour plus d'informations sur la création d'un projet, voir Créer un nouveau projet dans la Jira Cloud Support documentation.

Exigences relatives à la création d'un projet

Assurez-vous de suivre les étapes suivantes lors de la création d'un nouveau projet.

- Choisissez Développement logiciel pour le modèle de projet.
- Choisissez Company-managed le type de projet.

Exigences relatives aux projets existants

Tous les projets existants de votre environnement Jira qui sont intégrés à Security Hub doivent être du type de Company-managed projet.

3. Ajoutez vos projets au AWS Hub de sécurité pour Jira Cloud app

Pour que Security Hub puisse envoyer correctement les résultats à votre environnement Jira, chaque projet que vous souhaitez utiliser avec Security Hub doit être associé au AWS Security Hub pour Jira Cloud l'application. L'association d'un projet Jira à l'application garantit que les champs personnalisés nécessaires pour Security Hub sont associés au projet et peuvent être renseignés lorsque Security Hub envoie des résultats au projet.

1. Connectez-vous à votre Atlassian site en tant qu'administrateur.
2. Choisissez Paramètres, puis Applications.
3. Dans la liste des applications, choisissez AWS Security Hub pour Jira Cloud.
4. Choisissez l'onglet Paramètres du connecteur.
5. Sous Projets activés, choisissez Ajouter un projet Jira.
    a. Dans la liste déroulante, choisissez Tout ajouter ou sélectionnez un projet. Répétez cette partie de l'étape si vous souhaitez ajouter plusieurs projets, mais pas tous les projets.
    b. Choisissez Enregistrer.

Vous pouvez vérifier quels projets ont été correctement installés depuis l'onglet Installation Manager. Vous pouvez également vérifier les configurations des champs, des écrans, des états et des flux de travail à partir de l'onglet Installation Manager.

Pour plus d'informations à ce sujetJira Cloud, consultez Jira Cloud les ressources du Atlassian site Web.

Recommandations

Création d'un compte système dédié pour votre environnement Jira

L'intégration de Security Hub Jira Cloud utilise une connexion OAuth associée à un utilisateur spécifique au sein de votre instance Jira. La création d'un compte système dédié à utiliser pour votre connexion Security Hub OAuth est recommandée pour votre connexion pour les raisons suivantes :

- Un utilisateur système dédié garantit que la connexion n'est pas associée à un employé dont les autorisations d'accès à l'environnement Jira pourraient changer au fil du temps, ce qui aurait un impact sur la capacité de Security Hub à s'intégrer à votre environnement Jira.
- Chaque problème créé par Security Hub dans Jira affiche un champ Créé par contenant le nom d'utilisateur utilisé pour créer la connexion OAuth. L'utilisation d'un compte système pour la connexion OAuth permet à ce compte système d'apparaître en tant que créateur du ticket, ce qui permet de savoir que le résultat a été créé via l'intégration de Security Hub et non manuellement par un autre utilisateur de Jira.

Configurer une intégration entre Security Hub et Jira Cloud

La procédure suivante doit être effectuée pour chacun de vos Jira Cloud projets auxquels vous souhaitez envoyer les résultats de Security Hub.

> **Note**
>
> Lorsque vous créez un Jira Cloud connecteur, vous êtes redirigé depuis le connecteur actuel Région AWS vers`"https://3rdp.oauth.console.api.aws"`, afin que vous puissiez terminer l'enregistrement du connecteur. Ensuite, vous revenez à l' Région AWS endroit où le connecteur est créé.

Pour configurer une intégration pour Jira Cloud

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home ?region=us-est-1.
2. Dans le volet de navigation, choisissez Gestion, puis Intégrations.
3. Choisissez AjouterJira Cloud.
4. Pour plus de détails, entrez un nom descriptif unique pour votre intégration et déterminez si vous souhaitez saisir une description facultative pour votre intégration.
5. Pour les chiffrements, choisissez la manière dont vous souhaitez crypter vos informations d'intégration dans Security Hub.
   - Utiliser la clé AWS détenue : avec cette option, une clé de service appartenant à Security Hub est utilisée pour crypter vos données d'identification d'intégration dans Security Hub.

- Choisissez une autre clé KMS (avancée) - Avec cette option, vous choisissez AWS KMS key celle que vous avez créée et que vous souhaitez utiliser pour chiffrer vos données d'identification d'intégration dans Security Hub. Pour plus d'informations sur la création d'une AWS KMS clé, voir Créer une AWS KMS clé dans le Guide du AWS Key Management Service développeur. Si vous choisissez d'utiliser votre propre clé, vous devez ajouter des déclarations de politique à la clé KMS qui autorisent Security Hub à accéder à la clé. Consultez les politiques AWS KMS clés relatives aux intégrations de billetterie de Security Hub pour plus de détails sur les politiques nécessaires.

> **Note**
>
> Vous ne pouvez pas modifier ces paramètres une fois cette configuration terminée. Toutefois, si vous choisissez Clé personnalisée, vous pouvez modifier votre politique de clé personnalisée à tout moment.

6. (Facultatif) Pour les balises, créez et ajoutez-en une à votre intégration. Vous pouvez ajouter jusqu'à 50 balises.
7. Pour Autorisations, choisissez Créer un connecteur et autorisez. Une fenêtre contextuelle apparaît dans laquelle vous choisissez Autoriser pour terminer l'autorisation. Une fois l'autorisation terminée, une case à cocher apparaît pour vous informer que l'autorisation a été validée.
8. Pour les configurations, entrez l'ID Jira Cloud du projet.
9. Choisissez Configuration complète. Une fois la configuration terminée, vous pouvez consulter vos intégrations configurées dans l'onglet Intégrations configurées.

Après avoir configuré votre intégration avec Jira, vous pouvez tester la connexion pour vérifier que tout est correctement configuré dans votre environnement Jira et dans Security Hub. Pour plus d'informations, consultez la section Tester les intégrations de billetterie configurées.

Informations supplémentaires sur l'intégration de Jira

Considérations relatives aux limites de débit

Jira applique des limites de débit d'API pour maintenir la stabilité du service et garantir une utilisation équitable sur l'ensemble de sa plateforme. Lorsque vous utilisez l'intégration AWS de Security Hub à Jira, ces limites de débit peuvent avoir un impact sur le traitement des résultats de Security

Hub, en particulier dans les environnements générant de grands volumes de résultats. Cela peut retarder la création des tickets et, dans les scénarios où le volume de recherches est extrêmement élevé, certains résultats peuvent ne pas être traités du tout dans les tickets Jira. Pour optimiser votre intégration, envisagez d'implémenter des filtres sur les règles d'automatisation dans Security Hub afin de hiérarchiser la gestion des tickets en fonction des résultats les plus importants, de surveiller l'utilisation de votre API Jira via leur console d'administration et de planifier votre flux de travail en fonction des limites de débit spécifiques de votre niveau de licence Jira. Pour les implémentations critiques pour l'entreprise, contactez votre administrateur Jira pour vérifier vos allocations de limites de débit.

Pour plus d'informations sur les limites de débit de l'API Jira, consultez la documentation sur les limites de débit sur le site Web de l'Atlassian Developers Guide.

Authentification et sécurité

L'authentification par API Jira nécessite une configuration OAuth 2.0 appropriée pour un accès sécurisé. Assurez-vous que votre application respecte les meilleures pratiques de sécurité d'Atlassian pour l'intégration des API.

Ressources :

- API Jira REST v3 : documentation de l'API Jira REST v3 sur le site Web d'Atlassian
- Implémentation d'OAuth 2.0 (3LO) : guide de mise en œuvre d'OAuth 2.0 (3LO) sur le site Web d'Atlassian
- Administrer les applications Jira Cloud : ressources d'administration de Jira Cloud sur le site Web d'Atlassian
- Gérer les autorisations Jira : gérez les autorisations des projets sur le site Web d'Atlassian

Création d'un ticket pour Jira Cloud intégration

Après avoir créé une intégration avecJira Cloud, vous pouvez créer un ticket pour une découverte.

> **Note**
>
> Une découverte sera toujours associée à un seul ticket tout au long de son cycle de vie. Security Hub envoie toutes les mises à jour ultérieures d'un résultat au même ticket après sa création initiale. Si un connecteur associé à une règle d'automatisation est modifié, le

connecteur mis à jour est utilisé uniquement pour les résultats nouveaux et entrants qui correspondent aux critères de la règle.

Pour créer un ticket pour une découverte

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home ?region=us-est-1.
2. Dans le volet de navigation, sous Inventaire, choisissez Résultats.
3. Choisissez une découverte. Dans la recherche, choisissez Créer un ticket.
4. Pour l'intégration, ouvrez le menu déroulant et choisissez une intégration. Cette intégration est celle que vous avez créée précédemment lors de la configuration du Jira Cloud projet. Choisissez l'intégration à laquelle vous souhaitez envoyer les résultats.
5. Choisissez Créer.

Consulter un billet pour un Jira Cloud intégration

Après avoir créé un ticket pour une découverte, vous pouvez l'ouvrir sur votre Jira Cloud instance.

Pour consulter les résultats de votre Jira Cloud instance

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home ?region=us-est-1.
2. Dans le volet de navigation, sous Inventaire, choisissez Résultats.
3. Choisissez la recherche dans laquelle vous avez créé le ticket.
4. Dans la recherche, choisissez l'ID du ticket pour afficher le ticket sur votre Jira Cloud instance ou Afficher le JSON.

Intégrations pour ServiceNow

Cette rubrique explique comment accéder à la console Security Hub pour configurer une intégration pourServiceNow ITSM. Avant d'effectuer l'une des procédures décrites dans cette rubrique, vous devez être abonné pour ServiceNow ITSM pouvoir ajouter cette intégration. Pour plus d'informations, consultez la page de tarification sur le ServiceNow site Web.

Pour les comptes d'une organisation, seul l'administrateur délégué peut configurer une intégration. L'administrateur délégué peut utiliser manuellement la fonction de création de ticket pour les résultats de tout compte de membre. En outre, l'administrateur délégué peut utiliser des règles d'automatisation pour créer automatiquement des tickets pour tous les résultats associés aux comptes des membres. Lors de la définition d'une règle d'automatisation, l'administrateur délégué peut définir des critères, qui peuvent inclure tous les comptes membres ou des comptes de membres spécifiques. Pour plus d'informations sur la configuration d'un administrateur délégué, consultez la section Configuration d'un compte d'administrateur délégué dans Security Hub.

Pour les comptes n'appartenant pas à une organisation, tous les aspects de cette fonctionnalité sont disponibles.

Prérequis : configuration ServiceNow de l'environnement

Vous devez remplir les conditions préalables suivantes avant de configurer une intégration pourServiceNow ITSM. Dans le cas contraire, votre intégration entre ServiceNow ITSM et Security Hub ne fonctionnera pas.

1. Installation de l'intégration de Security Hubfindings pour la gestion des services informatiques (ITSM)

La procédure suivante décrit comment installer le plug-in Security Hub.

1. Connectez-vous à votre ServiceNow ITSM instance, puis ouvrez le navigateur de l'application.
2. Accédez à la ServiceNow boutique.
3. Recherchez l'intégration des résultats de Security Hub pour la gestion des services informatiques (ITSM), puis choisissez Obtenir pour installer l'application.

> **Note**
>
> Dans les paramètres de l'application Security Hub, choisissez l'action à effectuer lorsque de nouveaux résultats de Security Hub sont envoyés à votre ServiceNow ITSM environnement. Vous pouvez choisir Ne rien faire, Créer un incident, Créer un problème ou Créer les deux (incident/problem).

2. Configurer le type d'autorisation des informations d'identification du client pour les demandes OAuth entrantes

Vous devez configurer ce type d'autorisation pour les demandes OAuth entrantes. Pour plus d'informations, consultez la section Le type d'autorisation des informations d'identification du client pour l'OAuth entrant est pris en charge sur la ServiceNow page Web d'assistance.

3. Création d'une application OAuth

Si vous avez déjà créé une application OAuth, vous pouvez ignorer cette condition préalable. Pour plus d'informations sur la création d'une application OAuth, consultez la section Configuration d'OAuth sur le site Web. ServiceNow

Prérequis - configurer AWS Secrets Manager

Pour utiliser l'intégration de Security Hub avec ServiceNow, les informations d'identification de votre application ServiceNow OAuth doivent être stockées dans Secrets Manager. Le stockage de vos informations d'identification dans Secrets Manager vous permet de contrôler et de visualiser leur utilisation, tout en permettant à Security Hub d'utiliser les informations d'identification pour s'intégrer à votre ServiceNow instance. Pour stocker vos informations d'identification dans Secrets Manager, vous devez utiliser une AWS KMS clé gérée par le client afin de protéger les secrets. Cette AWS KMS clé vous permet de protéger les secrets lorsqu'ils sont stockés au repos et permet également d'associer une politique à la clé qui autorise Security Hub à accéder à la clé qui protège le secret.

Suivez les étapes ci-dessous pour configurer Secrets Manager pour vos ServiceNow informations d'identification.

Étape 1 : Joignez une politique à votre AWS KMS clé

Pour configurer correctement votre ServiceNow intégration, vous devez d'abord autoriser Security Hub à utiliser la AWS KMS clé associée à vos ServiceNow informations d'identification dans Secrets Manager.

Pour modifier le AWS KMS politique clé permettant à Security Hub d'accéder à vos ServiceNow informations d'identification

1. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
2. Pour modifier la AWS région, utilisez le sélecteur de région en haut à droite de la page.
3. Sélectionnez une AWS KMS clé existante ou suivez les étapes pour créer une nouvelle clé dans le Guide du AWS KMS développeur.

4. Dans la section Key policy (Politique de clé), choisissez Edit (Modifier).
5. Si l'option Passer en mode stratégie s'affiche, choisissez-la pour afficher la politique clé, puis choisissez Modifier.
6. Copiez le bloc de politique suivant dans votre politique de AWS KMS clé, pour autoriser Security Hub à utiliser votre clé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::your-account-id:root"
        },
        "Action": "kms:*",
        "Resource": "*"
        },
        {
        "Sid": "Allow Security Hub connector service to decrypt secrets",
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "kms:Decrypt",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
            "kms:ViaService": "secretsmanager.your-region.amazonaws.com"
            },
            "StringLike": {
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:your-
region:your-account-id:secret:ServiceNow*"
            }
        }
        }
    ]
    }
```

7. Modifiez la politique en remplaçant les valeurs suivantes dans l'exemple de stratégie :

   - *your-account-id*Remplacez-le par votre identifiant de AWS compte.

- Remplacez *your-region* par votre AWS région (par exemple,`us-east-1`).

8. Si vous avez ajouté la déclaration de politique avant la déclaration finale, ajoutez une virgule avant d'ajouter cette déclaration. Assurez-vous que la syntaxe JSON de votre politique AWS KMS clé est valide.
9. Choisissez Enregistrer.
10. (Facultatif) Copiez l'ARN de la clé dans un bloc-notes pour l'utiliser ultérieurement.

Étape 2 : Création du secret dans Secrets Manager

Créez un secret dans Secrets Manager qui stockera vos ServiceNow informations d'identification. Security Hub accède à ce secret lors de l'interaction avec votre ServiceNow environnement.

Suivez les étapes pour créer un secret dans le Guide de AWS Secrets Manager l'utilisateur. Après avoir créé votre secret, copiez l'ARN secret car vous en aurez besoin lors de la création de votre connecteur Security Hub.

Lors de la création du secret, assurez-vous de configurer les éléments suivants :

Type de secret

Other type of secret (Autre type de secret)

Key/value paires (format texte brut)

```
{
    "ClientId": "your-servicenow-client-id",
    "ClientSecret": "your-servicenow-client-secret"
    }
```

> **Note**
>
> Les noms des champs doivent être exacts `ClientId` et `ClientSecret` (distinction majuscules/minuscules). Security Hub a besoin de ces noms exacts pour récupérer les informations d'identification.

Clé de chiffrement

Utilisez la AWS KMS clé que vous avez configurée à l'étape 1

Politique en matière de ressources

Utilisez la stratégie de ressource suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "secretsmanager:GetSecretValue",
        "Resource": "arn:aws:secretsmanager:your-region:your-account-
id:secret:ServiceNow*",
        "Condition": {
            "StringEquals": {
            "aws:SourceAccount": "your-account-id",
            "aws:SourceArn": "arn:aws:securityhub:your-region:your-account-id:*"
            }
        }
        }
    ]
    }
```

Maintenant que votre secret est configuré, vous pouvez créer un connecteur Security Hub à l'aide de l'API ou de la AWS console CreateConnector V2. Vous devrez fournir :

- InstanceName: URL de votre ServiceNow instance (par exemple,`your-instance.service-now.com`)
- SecretArn: l'ARN du secret que vous avez créé dans cette procédure

Configurer une intégration pour ServiceNow ITSM

Security Hub peut créer automatiquement des incidents ou des problèmes dansServiceNow ITSM.

Pour configurer une intégration pour ServiceNow ARTICLE

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home ?region=us-est-1.
2. Dans le volet de navigation, choisissez Gestion, puis Intégrations.
3. Sous ServiceNow ITSM, choisissez Ajouter une intégration.
4. Pour plus de détails, entrez un nom pour votre intégration et déterminez si vous souhaitez saisir une description facultative pour votre intégration.
5. Pour les chiffrements, choisissez la manière dont vous souhaitez crypter vos informations d'intégration dans Security Hub.

   - Utiliser la clé AWS détenue : avec cette option, une clé de service appartenant à Security Hub est utilisée pour crypter vos données d'identification d'intégration dans Security Hub.
   - Choisissez une autre clé KMS (avancée) - Avec cette option, vous choisissez AWS KMS key celle que vous avez créée et que vous souhaitez utiliser pour chiffrer vos données d'identification d'intégration dans Security Hub. Pour plus d'informations sur la création d'une AWS KMS clé, voir Créer une AWS KMS clé dans le Guide du AWS Key Management Service développeur. Si vous choisissez d'utiliser votre propre clé, vous devez ajouter des déclarations de politique à la clé KMS qui autorisent Security Hub à accéder à la clé. Consultez les politiques AWS KMS clés relatives aux intégrations de billetterie de Security Hub pour plus de détails sur les politiques nécessaires.

   > **Note**
   >
   > Vous ne pouvez pas modifier ces paramètres une fois cette configuration terminée. Toutefois, si vous choisissez Clé personnalisée, vous pouvez modifier votre politique de clé personnalisée à tout moment.

6. Pour les informations d'identification, entrez votre ServiceNow ITSM URL et l'ARN de votre AWS Secrets Manager secret qui a été généré dans la section des prérequis.
7. Pour les balises, déterminez si vous souhaitez créer et ajouter une balise facultative à votre intégration.
8. Choisissez Ajouter une intégration. Une fois la configuration terminée, vous pouvez consulter vos intégrations configurées dans l'onglet Intégrations configurées.

Après avoir configuré votre intégration avec ServiceNow, vous pouvez tester la connexion pour vérifier que tout est correctement configuré dans votre ServiceNow environnement et dans Security Hub. Pour plus d'informations, consultez la section Tester les intégrations de billetterie configurées.

Création d'un ticket pour ServiceNow ARTICLE intégration

Après avoir créé une intégration avecServiceNow ITSM, vous pouvez créer un ticket pour une découverte.

> **Note**
>
> Une découverte sera toujours associée à un seul ticket tout au long de son cycle de vie. Security Hub envoie toutes les mises à jour ultérieures d'un résultat au même ticket après sa création initiale. Si un connecteur associé à une règle d'automatisation est modifié, le connecteur mis à jour est utilisé uniquement pour les résultats nouveaux et entrants qui correspondent aux critères de la règle.

Pour créer un ticket pour une découverte

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home ?region=us-est-1.
2. Dans le volet de navigation, sous Inventaire, choisissez Résultats.
3. Choisissez une découverte. Dans la recherche, choisissez Créer un ticket.
4. Pour l'intégration, ouvrez le menu déroulant et choisissez une intégration.
5. Choisissez Créer.

Consulter un billet pour ServiceNow ARTICLE intégration

Après avoir créé un ticket pour une découverte, vous pouvez l'ouvrir sur votre ServiceNow ITSM instance.

Pour consulter les résultats de votre ServiceNow ARTICLE instance

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home ?region=us-est-1.

2. Dans le volet de navigation, sous Inventaire, choisissez Résultats.
3. Choisissez la recherche dans laquelle vous avez créé le ticket.
4. Dans la recherche, choisissez l'ID du ticket pour afficher le ticket sur votre ServiceNow ITSM instance ou Afficher le JSON.

Principales politiques de KMS pour les intégrations de billetterie de Security Hub

Lorsque vous utilisez des clés KMS gérées par le client avec les intégrations de billetterie de Security Hub, des politiques supplémentaires doivent être ajoutées à la clé KMS pour permettre à Security Hub d'interagir avec la clé. En outre, des politiques doivent être ajoutées pour autoriser le principal qui ajoute la clé au connecteur Security Hub à accéder à la clé.

Politique d'autorisations de Security Hub

La politique suivante décrit les autorisations dont Security Hub a besoin pour accéder à la clé KMS associée à votre Jira et à vos ServiceNow connecteurs et les utiliser. Cette politique doit être ajoutée à chaque clé KMS associée à un connecteur Security Hub.

La politique contient les autorisations suivantes :

- Permet à Security Hub de protéger, d'accéder temporairement ou d'actualiser les jetons utilisés pour communiquer avec vos intégrations de billetterie, à l'aide de la clé. Les autorisations sont limitées aux opérations liées à des connecteurs Security Hub spécifiques via le bloc de conditions qui vérifie l'ARN source et le contexte de chiffrement.
- Permet à Security Hub de lire les métadonnées relatives à la clé KMS en autorisant l'`DescribeKey`opération. Cette autorisation est nécessaire pour que Security Hub puisse vérifier l'état et la configuration de la clé. L'accès est limité à des connecteurs Security Hub spécifiques via la condition ARN source.

```
{
    "Sid": "Allow Security Hub access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
```

```
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
 "arn:aws:securityhub:Region:AccountId:connectorv2/*",
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        }
    }
}
```

Modifiez la politique en remplaçant les valeurs suivantes dans l'exemple de stratégie :

- Remplacer *CloudProviderName* par `JIRA_CLOUD` ou `SERVICENOW`
- *AccountId*Remplacez-le par l'ID de compte sur lequel vous créez le connecteur Security Hub.
- Remplacez *Region* par votre AWS région (par exemple,`us-east-1`).

Accès principal IAM pour les opérations du Security Hub

Tout responsable qui attribue des clés KMS gérées par le client à un connecteur Security Hub doit être autorisé à effectuer des opérations clés (décrire, générer, déchiffrer, rechiffrer et répertorier les alias) pour la clé ajoutée au connecteur. Cela s'applique aux API CreateConnector V2 et CreateTicket V2. La déclaration de politique suivante doit être incluse dans la politique pour tout mandant interagissant avec ces API.

```
{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        }
    }
}
```

Modifiez la politique en remplaçant les valeurs suivantes dans l'exemple de stratégie :

- *RoleName*Remplacez-le par le nom du rôle IAM qui effectue des appels vers Security Hub.
- Remplacez *CloudProviderName* par `JIRA_CLOUD` ou `SERVICENOW`.
- *AccountId*Remplacez-le par l'ID de compte sur lequel vous créez le connecteur Security Hub.
- Remplacez *Region* par votre AWS région (par exemple,`us-east-1`).

Tester les intégrations de billetterie configurées

Pour Jira configuré et ServiceNow les intégrations, vous pouvez tester la connexion pour vous assurer que toute la configuration dans Security Hub et dans votre ServiceNow environnement Jira est terminée.

La fonction de ticket de test crée un ticket dont le titre est`TESTING Test CreateTicketV2 Finding`. Le ticket de test est rempli d'exemples de données telles que l'ID de compte et la région du compte sur lequel le test est effectué, des exemples de détails sur les ressources et un exemple de AWS Finding JSON.

Tester les intégrations à l'aide de la console

Pour tester votre intégration, procédez comme suit :

1. Dans le panneau de navigation de Security Hub, choisissez Intégrations.
2. Dans l'onglet Intégrations configurées, choisissez l'intégration que vous souhaitez tester.
3. Sur la page de présentation de votre intégration, choisissez Créer un ticket de test.
4. Security Hub affiche un message de réussite et un lien vers le ticket de test en cas de réussite du test. Si le test échoue, Security Hub affiche un message d'erreur. En fonction du message d'erreur, résolvez les problèmes de configuration dans Security Hub ou dans votre Jira ServiceNow environnement.

> **Note**
>
> La fonction de ticket de test est destinée à aider à vérifier la fonctionnalité de bout en bout lors de la configuration d'une nouvelle connexion ou lorsque vous apportez des modifications à une connexion existante. Cette fonctionnalité crée un nouveau ticket dans votre ServiceNow environnement Jira ou dans votre environnement à chaque fois qu'il est utilisé et n'est pas destinée à une vérification régulière de votre connexion.

Tests réalisés avec AWS CLI

Pour tester votre intégration à l'aide de AWS CLI, utilisez la `create-ticket-v2` commande avec le `--mode DRYRUN` paramètre :

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

Exemple

L'exemple suivant montre comment tester une intégration :

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

Réponse réussie

Une réponse réussie renvoie les informations suivantes :

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

`TicketSrcUrl`Dans la réponse, vous trouverez un lien direct pour consulter le ticket de test dans votre environnement Jira ou dans votre ServiceNow environnement.

Si le test échoue, un message d'erreur s'affiche indiquant le problème de configuration à résoudre.

Résolution des erreurs d'intégration au cloud Jira

Lorsque vous testez votre intégration Jira Cloud depuis Security Hub, les messages d'erreur suivants peuvent être renvoyés. Ces messages d'erreur peuvent fournir des informations sur l'origine du problème de configuration avec le connecteur et sur la manière de le résoudre.

Messages d'erreur d'intégration à Jira Cloud

Erreur	Message d'erreur	Cause probable et résolution
ConflictException	Impossible de trouver le projet Jira	Cause probable : le projet sur le connecteur est incorrect ou un credentials/permissions problème nous empêche d'accéder au projet. Solution probable : ajoutez le projet approprié au connecteur ou authentifiez-vous à nouveau auprès de Jira avec les informations d'identification appropriées.
ConflictException	Type de problème de Security Hub introuvable	Cause probable : le problème ou le type de problème lié à l'installation de l'application n'est pas associé au projet. Solution probable : effectuez l'étape préalable pour installer l'application

Erreur	Message d'erreur	Cause probable et résolution
		Jira dans votre environnement Jira et associer l'application au projet.

Application MCP (version préliminaire)

Security Hub offre une expérience agentique grâce à une application MCP (Model Context Protocol). Grâce à cette application, votre agent IA peut étudier les résultats d'exposition. Il peut également diagnostiquer un connecteur Azure existant ou évaluer les prérequis du connecteur Azure avant sa création.

Chaque appel à l'outil de résultats renvoie un résumé textuel pour que l'agent raisonne. Lorsqu'il est disponible, il renvoie également une visualisation interactive que vous pouvez vérifier au cours de la même conversation. Connector Diagnostics renvoie un texte structuré qui sépare les résultats confirmés des contrôles qui n'ont pas pu être vérifiés.

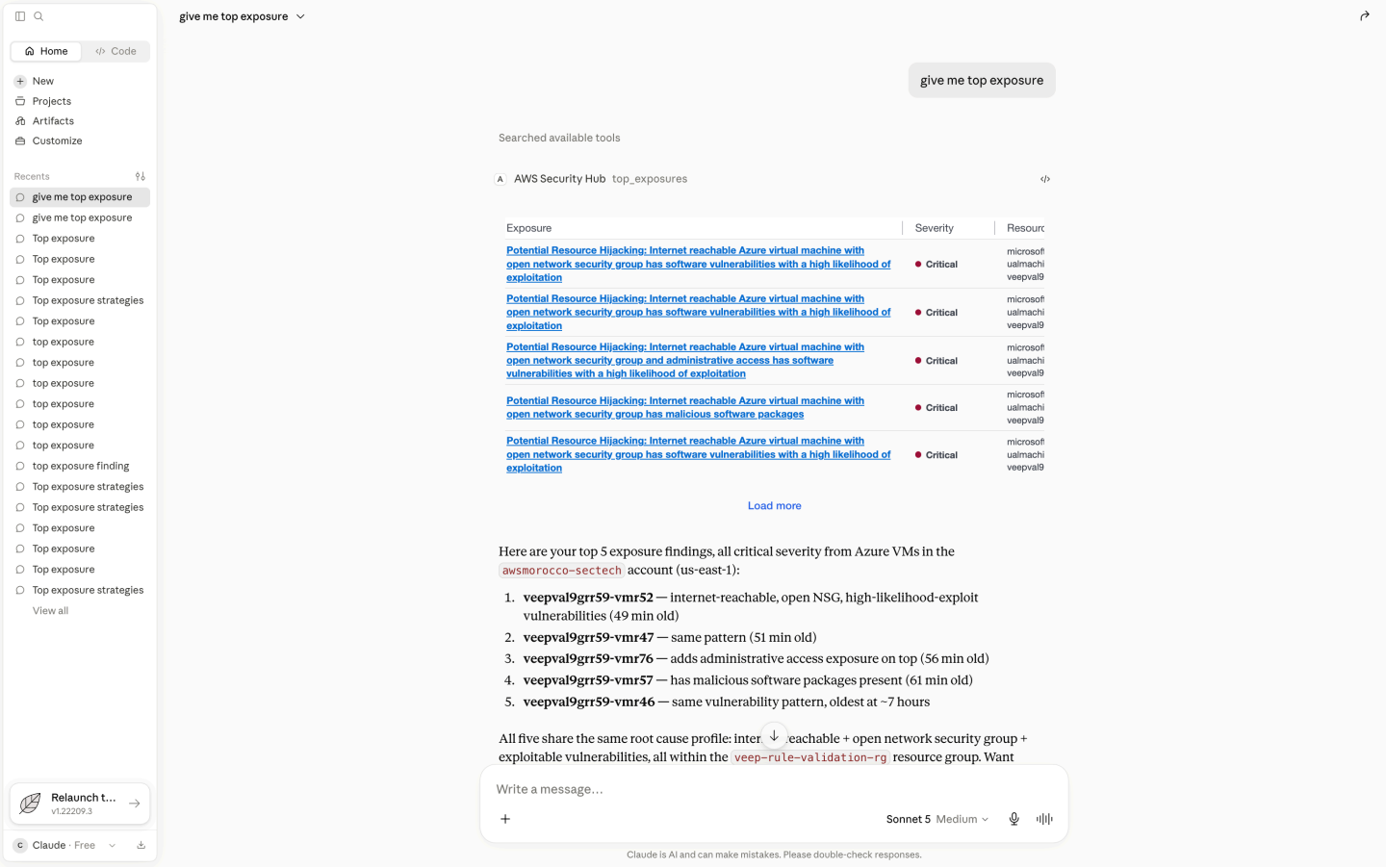
L'application MCP est un serveur MCP local qui s'exécute sur votre machine et appelle les API Security Hub directement à l'aide de vos informations d'identification existantes AWS . Connector Diagnostics peut également exécuter des requêtes Azure CLI limitées en lecture seule à l'aide de votre session Azure CLI existante. Chaque outil est en lecture seule et ne modifie pas votre posture de sécurité ni les ressources de votre connecteur. L'application MCP est disponible dans toutes les régions AWS commerciales où Security Hub est disponible.

> **Important**
>
> L'application Security Hub MCP est en avant-première publique.

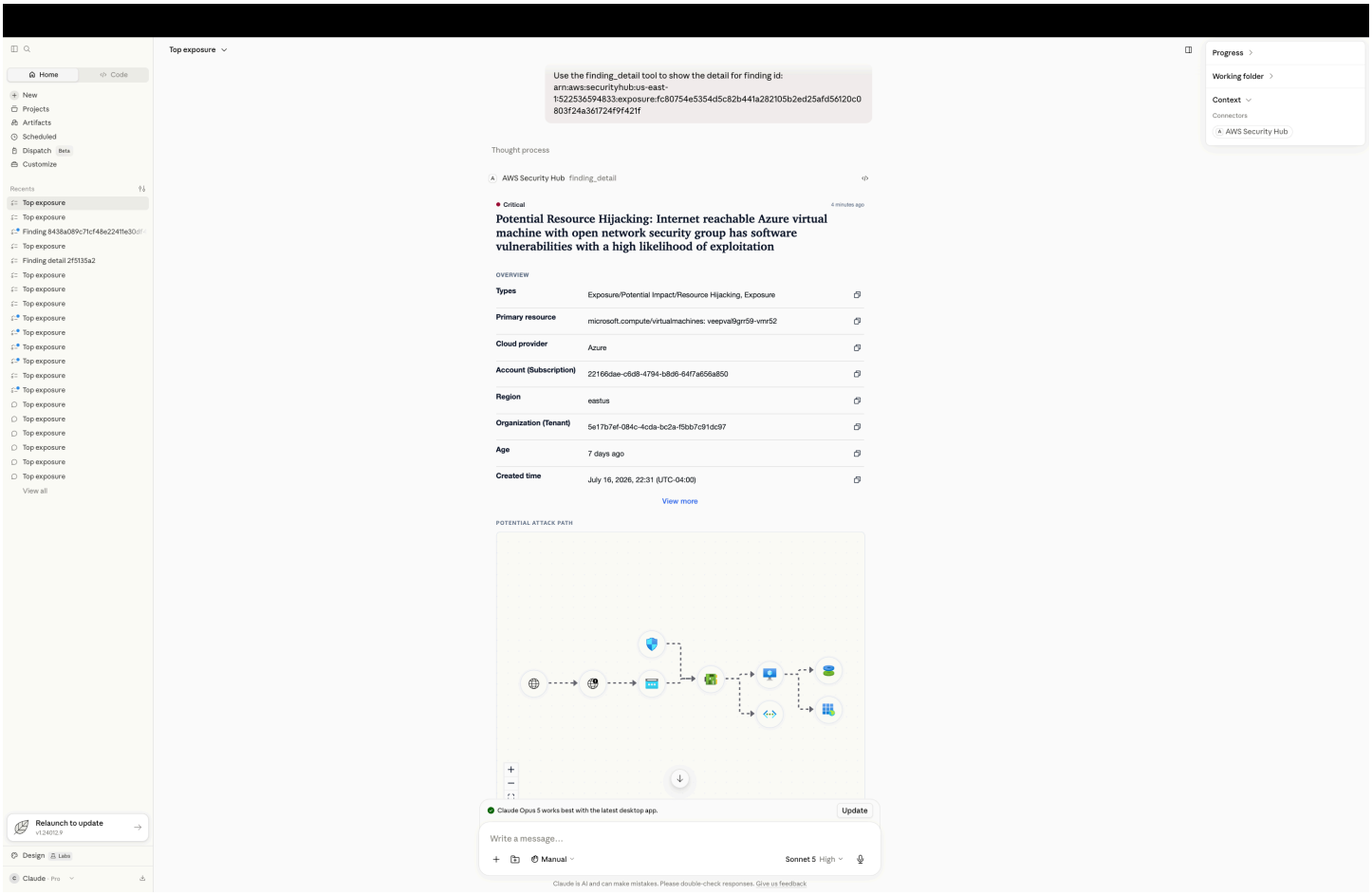
Exemples d'applications MCP

Les exemples suivants montrent comment l'application MCP affiche des visualisations interactives dans Claude Desktop pendant que vous étudiez vos expositions.

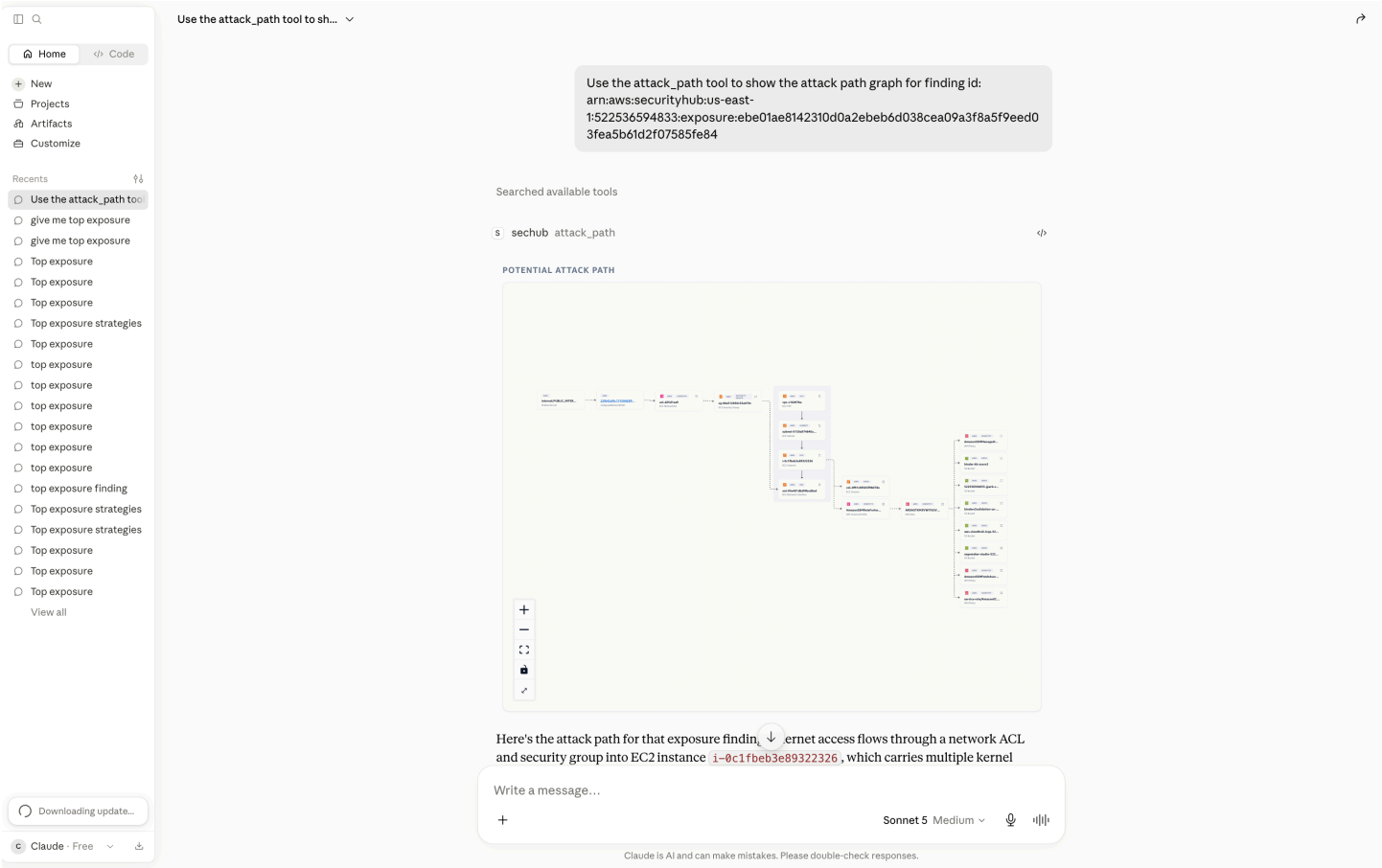
Principales expositions — Répertorie vos résultats d'exposition les plus critiques, dans un tableau interactif. L'image suivante montre le tableau des expositions les plus élevées.



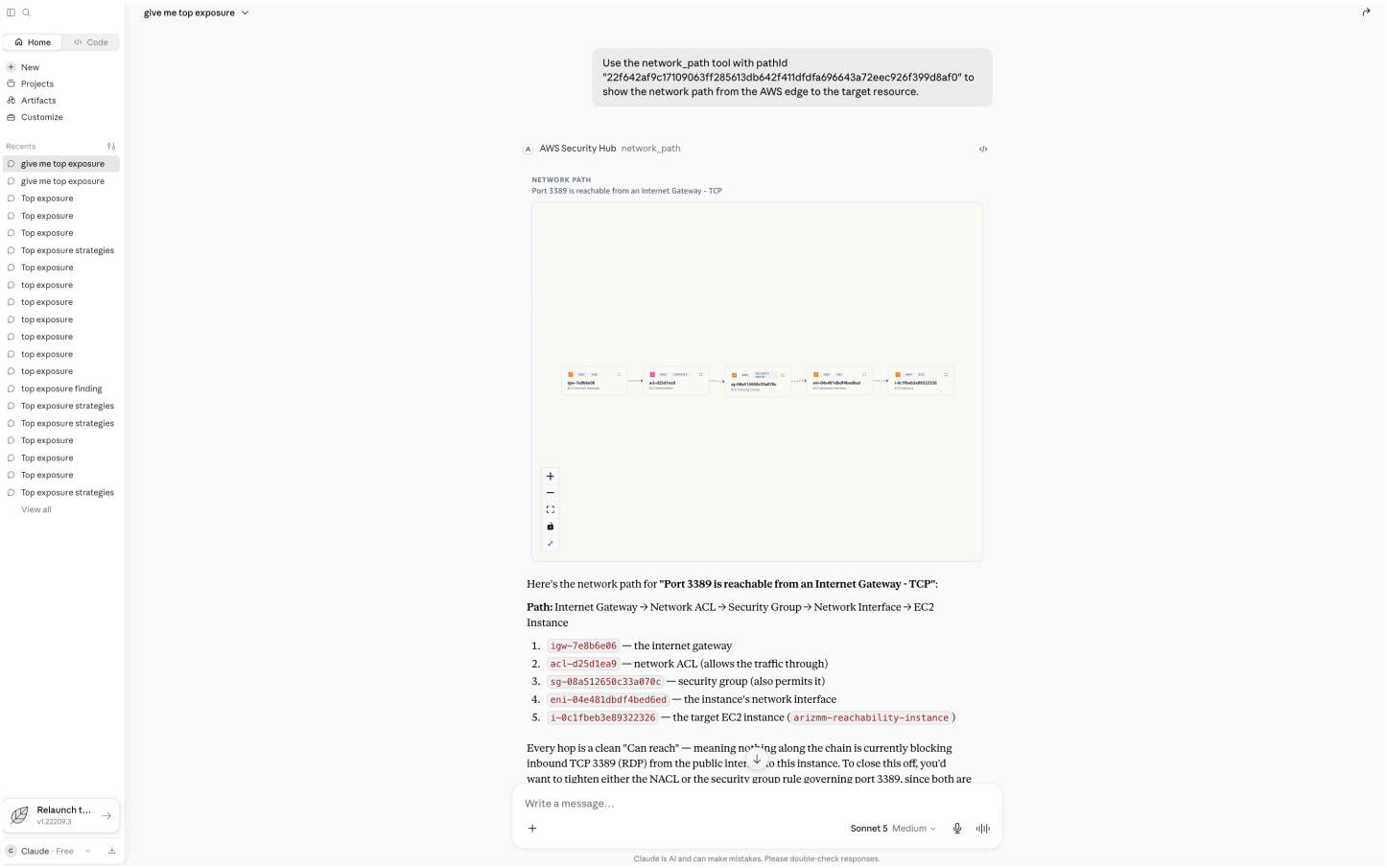
Détails de la découverte : passez en revue la vue d'ensemble d'un résultat d'exposition unique, ainsi que le résumé des caractéristiques corrélées, la trajectoire d'attaque et les conseils de remédiation. L'image suivante montre la vue détaillée de la recherche.



Trajectoire d'attaque : visualisez la manière dont une exposition est accessible sous forme de graphique interactif. Les nœuds représentent les ressources, les identités et les services. Les arêtes représentent les relations entre elles. L'image suivante montre le graphique de la trajectoire d'attaque.



Chemin réseau : explorez les sauts réseau ordonnés entre la AWS périphérie et la ressource cible (par exemple, Internet Gateway to NACL to Security Group to ENI to Instance). L'image suivante montre le chemin réseau.



Diagnostic du connecteur : demandez pourquoi un connecteur Azure existant est dégradé ou a échoué. L'agent identifie les problèmes confirmés, distingue les contrôles qui n'ont pas pu être vérifiés et recommande la moindre réparation sans modifier votre environnement.

Préparation du connecteur : vérifiez les prérequis d'Azure avant de créer un connecteur. L'agent indique quelles conditions préalables ont été satisfaites, ont échoué ou n'ont pas pu être vérifiées.

Concepts clés

Détection de l'exposition : découverte qui met en corrélation plusieurs signaux, tels que les vulnérabilités, les erreurs de configuration, l'accessibilité du réseau et les données sensibles, dans une vue unique d'une ressource exposée au risque.

Diagnostics des connecteurs : trois outils en lecture seule pour les connecteurs Azure. Les outils diagnostiquent un connecteur existant, évaluent une configuration proposée et extraient des extraits exacts du script de configuration Azure pris en charge. L'agent sélectionne les outils et traduit leurs résultats structurés en une explication.

Serveur MCP local : programme qui s'exécute sur votre ordinateur et agit comme une passerelle bidirectionnelle sécurisée entre Claude Desktop et Security Hub. Le serveur contient les outils utilisés par votre agent IA, y compris les outils qui rendent l'interface utilisateur dans Claude Desktop. Il utilise la chaîne AWS d'informations d'identification de votre machine et ne possède aucune information d'identification propre.

Application MCP — Une application interactive qui s'affiche dans Claude Desktop. Chaque vue de l'application MCP effectue une tâche unique, telle que l'affichage du tableau des expositions les plus importantes ou un graphique de la trajectoire d'attaque.

Double réponse : un seul appel à l'outil de résultats renvoie deux résultats : un résumé textuel compact que votre agent raisonne, et une visualisation interactive affichée au cours de la même conversation que vous pouvez consulter.

Conditions préalables

- Un AWS compte sur lequel Security Hub est activé. Les résultats d'exposition ne sont requis que pour les résultats et les outils d'exposition.
- Claude Desktop est installé. Pour le programme d'installation, voir le téléchargement de Claude Desktop sur le site Web de Claude.
- AWS informations d'identification configurées dans votre chaîne d'informations d'identification AWS SDK standard.
- Pour les diagnostics Azure-side du connecteur, installez l'interface de ligne de commande Azure. Authentifiez-vous auprès du locataire du connecteur en exécutant `az login --tenant`*`tenant-id`*, où se *`tenant-id`* trouve l'ID du locataire Azure qui contient le connecteur. L'application MCP utilise la session Azure CLI locale qui en résulte. N'ajoutez pas d'informations d'identification Azure à la configuration MCP.

> **Note**
>
> Vous pouvez exécuter Connector Diagnostics sans session Azure CLI authentifiée. Le résultat inclut l'évaluation disponible AWS et marque les Azure-dependent contrôles comme non vérifiés. Il ne considère jamais les preuves Azure non disponibles comme étant saines.

Configuration du serveur MCP

L'application MCP s'installe dans Claude Desktop à partir d'un fichier groupé. Avant de procéder à l'installation, vérifiez `aws sts get-caller-identity` que cela fonctionne et qu'une région est `aws configure get region` renvoyée dans votre terminal, afin que le serveur puisse lire vos AWS informations d'identification et votre région.

1. Téléchargez le bundle d'applications Security Hub MCP.
2. Ouvrez le `.mcpb` fichier téléchargé. Claude Desktop lance un flux de configuration. Suivez les instructions pour installer le serveur.
3. Pour vérifier la connexion, saisissez une question dans Claude Desktop, telle que « Quelles sont mes principales failles de sécurité ? » ou « Mon connecteur Azure dans us-west-2 est dégradé. Pouvez-vous déterminer ce qui ne va pas ? » Si vous recevez un message d'erreur, consultez les instructions figurant dans le message d'erreur et confirmez vos informations d'identification et votre région.

Utilisation de Connector Diagnostics

Décrivez le problème du connecteur ou la configuration proposée en langage naturel. L'agent sélectionne l'outil en lecture seule approprié, interprète son résultat structuré et vous indique quelles vérifications ont été confirmées et quelles vérifications ne l'ont pas été.

Diagnostiquer un connecteur existant

1. Identifiez le connecteur à l'aide de son identifiant ou de son nom exact. Indiquez également le AWS compte et la région qui contiennent le connecteur si l'agent ne peut pas les déterminer à partir de votre demande.
2. Posez une question telle que « Mon connecteur Azure dans us-west-2 est dégradé. Pouvez-vous déterminer ce qui ne va pas et me dire ce que je dois corriger en premier ? »
3. Passez en revue les résultats confirmés séparément des contrôles qui n'ont pas été vérifiés. Lorsque l'authentification Azure n'est pas disponible, l'agent limite ses conclusions aux preuves AWS secondaires.

Évaluer un connecteur proposé

1. Indiquez le AWS compte, AWS la région et l'ID du locataire Azure. Fournissez également 1 à 10 ID d'abonnement Azure que le connecteur proposé couvrira. Indiquez à l'agent les prérequis de service à évaluer : gestion de la posture de sécurité dans le cloud (CSPM), analyse des machines virtuelles Inspector ou détection des menaces. Ces sélections portent sur les contrôles de préparation. Il ne s'agit pas de paramètres de création de connecteurs.
2. Posez une question telle que « Avant de créer mon connecteur Azure, vérifiez si les prérequis sont prêts pour ces abonnements ».
3. Passez en revue les contrôles réussis, ceux qui ont échoué et ceux qui n'ont pas été vérifiés. Un résultat de préparation sain signifie que les prérequis vérifiés ont été remplis. Cela ne signifie pas qu'un connecteur existe, qu'il est en cours d'exécution ou qu'il a été restauré.

Récupérez les instructions de configuration

Si un résultat fait référence à une étape d'intégration, demandez à l'agent de montrer cette étape. Par exemple, demandez « Montrez-moi l'étape 6 du script de configuration du connecteur Azure pris en charge ». Pour le script complet, consultez la section Configuration de Microsoft Azure pour l'intégrer à Security Hub. L'outil renvoie un extrait exact mais ne l'exécute pas. Exécutez l'intégralité du script pris en charge car ses étapes partagent les mêmes fonctions de configuration et d'assistance.

> **Note**
>
> Connector Diagnostics ne répare ni ne modifie jamais les ressources. La correction est un guide pour une action distincte que vous contrôlez. Le diagnostic indique la restauration uniquement lorsque de nouvelles preuves d'exécution le prouvent.

Outils disponibles

`top_exposures`— Répertorie vos résultats d'exposition les plus urgents sous forme de tableau interactif. Appelez d'abord cet outil car les outils de recherche préalable nécessitent un identifiant de recherche figurant dans cette liste.

`finding_detail`— Renvoie la vue d'ensemble d'un résultat, y compris le résumé de ses caractéristiques de recherche corrélées.

`finding_overview`— Renvoie un résumé textuel d'une découverte en identifiant la recherche.

`correlated_finding_detail`— Répertorie les résultats corrélés à une exposition pour un seul trait, tel que la vulnérabilité, la mauvaise configuration ou l'accessibilité.

`attack_path`— Construit le graphique de la trajectoire d'attaque pour une découverte.

`network_path`— Étend le chemin réseau d'une découverte en sauts ordonnés entre la AWS périphérie et la ressource cible.

`recommendation`— Renvoie des conseils de correction pour un résultat, y compris des liens vers la documentation.

`resource_detail`— Renvoie la configuration d'une AWS ressource par ID abrégé (par exemple`i-1234`) ou ARN.

`diagnose_connector`— Diagnostique un connecteur Azure existant à l'aide de l'état de Security Hub et des preuves limitées de la CLI Azure lorsqu'elles sont disponibles. Il renvoie les résultats confirmés, l'étendue affectée, les conseils de correction et l'actualité des données. Il répertorie également toutes les vérifications qui n'ont pas pu être vérifiées.

`assess_connector_readiness`— Évalue le AWS côté secondaire et les Azure-side prérequis d'un connecteur Azure proposé avant sa création. Il ne crée pas de connecteur.

`get_connector_setup_instructions`— Renvoie des extraits exacts du script d'intégration Azure fourni et pris en charge. Il n'exécute pas le script.

Surveillance de l'utilisation et des coûts dans Security Hub

La page Utilisation vous aide à comprendre et à gérer les coûts liés au fonctionnement de Security Hub au sein de votre organisation. Sur cette page, vous pouvez consulter vos coûts actuels, consulter les coûts mensuels prévus, explorer l'utilisation par fonctionnalité ou par compte et trouver des stratégies pour optimiser vos dépenses.

Qui peut accéder à la page d'utilisation

La page Utilisation est disponible depuis n'importe quel compte sur lequel Security Hub est activé. Pour y accéder, ouvrez la console Security Hub et choisissez Utilisation sous Paramètres dans le volet de navigation.

> **Important**
>
> Si votre compte est un compte de membre d'une AWS organisation et qu'aucun administrateur délégué de Security Hub n'a été désigné, les données d'utilisation ne sont pas disponibles. Pour consulter les données d'utilisation, le compte de gestion de votre organisation doit désigner un administrateur délégué. Pour de plus amples informations, veuillez consulter the section called "Désignation d'un administrateur délégué".

L'expérience varie en fonction de votre type de compte :

- Compte administrateur délégué ou compte de gestion : vous pouvez consulter la page d'utilisation complète avec un récapitulatif des coûts de l'organisation, l'utilisation par fonctionnalité, l'utilisation par compte et les stratégies d'optimisation des coûts.
- Compte de membre ou compte autonome : un récapitulatif des coûts du compte s'affiche, indiquant l'utilisation par fonctionnalité, pour votre compte uniquement. L'onglet Par compte n'est pas disponible car vous consultez un seul compte.

Synthèse des coûts liés à l'organisation et au compte

> **Note**
>
> La section récapitulative des coûts de l'organisation n'est visible que depuis le compte administrateur délégué ou le compte de gestion. Les comptes membres et les comptes autonomes voient plutôt un récapitulatif des coûts du compte.

Lorsque vous ouvrez la page Utilisation à partir d'un compte administrateur délégué ou d'un compte de gestion, la section Récapitulatif des coûts de l'organisation affiche un aperçu général des coûts du Security Hub de votre organisation pour le cycle de facturation en cours. Cette section inclut les éléments suivants :

- Dernière actualisation des données : date à laquelle Security Hub a actualisé pour la dernière fois les données d'utilisation de votre organisation. Security Hub actualise ces données régulièrement. Si les données datent de plus de 24 heures lorsque vous visitez la page d'utilisation, Security Hub déclenche automatiquement une actualisation. L'actualisation s'effectue en quelques heures, selon

la taille de votre organisation. Pendant l'actualisation des données, une alerte apparaît avec un message indiquant que les données seront bientôt disponibles.

- Coûts actuels : montant total que votre organisation a engagé pour utiliser Security Hub entre le début du cycle de facturation en cours et la date de dernière actualisation des données.
- Coûts mensuels prévus (30 jours) : coût mensuel estimé basé sur les 7 derniers jours d'utilisation, extrapolé à un cycle de facturation complet de 30 jours. Cette projection inclut à la fois l'utilisation des versions d'essai payantes et gratuites afin de vous donner une estimation réaliste de vos coûts mensuels. Les coûts prévus ne tiennent pas compte des remises (EDP) avec AWS lesquelles vous avez négocié. Si vos coûts prévus semblent inférieurs à vos coûts actuels, cela signifie que votre utilisation a diminué et, sur la base des 7 derniers jours d'utilisation, la facture de 30 jours sera inférieure à votre facture du cycle de facturation en cours.

Vue Capacités

La vue Capability montre vos coûts et votre utilisation dans l'ensemble de l'organisation, organisés par capacité de sécurité. Les fonctionnalités sont organisées en trois groupes extensibles. Vous pouvez développer ou réduire chaque groupe pour voir les différents types d'utilisation qu'il contient. Chaque type d'utilisation correspond directement à un type d'utilisation correspondant dans AWS Cost Explorer.

Plan Security Hub Essentials : surveille vos instances EC2, vos images de conteneurs ECR, vos fonctions Lambda, vos utilisateurs IAM et vos rôles IAM. Couvre l'analyse des risques et de l'exposition, la gestion des vulnérabilités (optimisée par Amazon Inspector), la gestion de la posture de sécurité (optimisée par Security Hub CSPM) et les réponses en matière de sécurité. Toutes ces fonctionnalités sont incluses dans le forfait Essentials à un prix unique par ressource. Vous n'avez pas besoin d'activer ou de payer séparément Amazon Inspector ou AWS Security Hub CSPM, et vous n'êtes pas facturé deux fois pour l'utilisation du service sous-jacent.

Analyse des menaces : inclut les événements CloudTrail de gestion et les événements liés aux données, l'activité du réseau et d'autres journaux. Ces fonctionnalités couvrent la détection des menaces fournie par Amazon GuardDuty.

Fonctionnalités supplémentaires : inclut le scan de code des fonctions Lambda. Il s'agit d'une amélioration optionnelle fournie par Amazon Inspector pour analyser le code de l'application de la fonction Lambda à la recherche de failles de sécurité.

Pour plus d'informations sur la tarification de chaque fonctionnalité, consultez la rubrique Tarification de Security Hub.

Le tableau de cette vue inclut les colonnes suivantes pour chaque type d'utilisation :

- Utilisation actuelle : volume d'utilisation total pour ce type d'utilisation depuis le début du cycle de facturation jusqu'à la date de dernière actualisation des données, pour tous les comptes et toutes les régions.
- Utilisation gratuite : volume d'utilisation total pour ce type d'utilisation sur les comptes actuellement en période d'essai gratuit. Les valeurs d'utilisation gratuite apparaissent en vert.
- Coûts actuels : coût total pour ce type d'utilisation depuis le début du cycle de facturation jusqu'à la date de dernière actualisation des données, pour tous les comptes et toutes les régions.
- Valeur de l'essai gratuit : coût que vous auriez dû payer pour ce type d'utilisation si les comptes actuellement en période d'essai gratuit ne l'étaient pas. Cela vous permet de comprendre la valeur de l'essai gratuit.
- Coûts mensuels prévus (30 jours) : coût mensuel estimé pour ce type d'utilisation, extrapolé à partir des 7 derniers jours d'utilisation pour tous les comptes et toutes les régions. Cela inclut l'utilisation des versions d'essai payantes et gratuites pour fournir une estimation du coût mensuel.

Vue Compte

> **Note**
>
> L'affichage du compte est disponible uniquement à partir du compte administrateur délégué ou du compte de gestion.

Choisissez l'affichage des comptes pour afficher vos coûts organisés par compte de membre individuel dans toutes les régions. Cette vue vous permet d'identifier les comptes qui génèrent les coûts les plus élevés.

Le tableau répertorie chaque compte avec les colonnes suivantes :

- Compte : Compte AWS identifiant, affiché sous forme de lien cliquable. Le choix d'un compte ouvre un panneau de répartition détaillé.
- Coûts courants : coût total de ce compte depuis le début du cycle de facturation jusqu'à la date de dernière actualisation des données, dans toutes les régions.
- Valeur de l'essai gratuit — Le coût que ce compte aurait encouru s'il n'avait pas été inclus dans l'essai gratuit.

- Coûts mensuels prévus (30 jours) : coût mensuel estimé pour ce compte, extrapolé à partir des 7 derniers jours d'utilisation dans toutes les régions jusqu'à un cycle de facturation complet de 30 jours. La projection inclut à la fois l'utilisation des versions d'essai payantes et gratuites afin de fournir une estimation représentative de vos coûts mensuels. Les coûts prévus ne tiennent pas compte des remises que vous avez négociées avec AWS (EDP).

  Si Security Hub a été activé sur ce compte au cours des 7 derniers jours, la projection est basée sur le nombre de jours écoulés depuis l'activation. Après 7 jours, la projection utilise la totalité des 7 derniers jours d'utilisation. La page Utilisation ne détecte actuellement pas si Security Hub a été désactivé sur un compte. Si Security Hub a récemment été désactivé sur un ou plusieurs comptes, ces comptes continuent d'apparaître dans la projection jusqu'à ce que leur utilisation soit terminée. Après avoir effectué ces modifications, attendez 7 jours pour que la projection reflète l'état actualisé de votre organisation.

Affichage des détails du compte

Lorsque vous choisissez un compte dans la liste, un panneau de détails s'ouvre sur le côté droit de la page. Ce panneau affiche la même répartition des niveaux de fonctionnalités que la vue Capability, mais filtré en fonction de ce compte spécifique. Vous pouvez consulter l'utilisation actuelle, l'utilisation gratuite, les coûts actuels, la valeur de l'essai gratuit et les coûts mensuels prévus pour chaque type d'utilisation de ce compte, dans toutes les régions.

Stratégies d'optimisation des coûts

Choisissez des stratégies d'optimisation des coûts sur la page Utilisation pour accéder à une page dédiée proposant des moyens pratiques de gérer vos coûts tout en maintenant votre couverture de sécurité.

Chaque stratégie est présentée comme une option indépendante que vous pouvez évaluer et appliquer en fonction des besoins de votre organisation. Les options sans compromis en matière de sécurité sont répertoriées en premier. Après l'application d'une stratégie, les modifications prennent généralement 24 à 48 heures pour être prises en compte dans votre facturation.

Ressources connexes

- Tarification de Security Hub
- AWS Guide de l'utilisateur de Cost Explorer

Désactivation de Security Hub

Désactivation de Security Hub pour un seul compte

Si votre compte ne fait pas partie d'une organisation, vous pouvez désactiver Security Hub dans la console Security Hub à tout moment ou utiliser l'DisableSecurityHubV2 API. Lorsque vous désactivez Security Hub, il cesse d'ingérer les résultats des moteurs de détection et vous perdez également l'accès aux résultats, intégrations et configurations existants.

Lorsque vous désactivez Security Hub pour votre compte dans toutes les régions, Security Hub supprime également l'analyseur d'accès IAM lié au service qui a été créé lorsque vous avez activé le service. Si la suppression automatique échoue, vous pouvez supprimer l'analyseur en appelant l'opération d'API IAM Access Analyzer`DeleteServiceLinkedAnalyzer`. Cette opération ne réussit que lorsque Security Hub est complètement désactivé pour votre compte. Si vous désactivez Security Hub dans une seule région mais que vous restez activé dans d'autres régions, l'analyseur d'accès non utilisé continue de fonctionner et les résultats continuent d'être répliqués dans les régions activées restantes.

Pour désactiver Security Hub

1. Connectez-vous à votre AWS compte à l'aide de vos informations d'identification et ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Général.
3. Dans Security Hub, choisissez Désactiver. Dans la fenêtre contextuelle, entrez**`Disable`**, puis choisissez Désactiver.

Désactivation de Security Hub au sein d'une organisation

Si vous êtes l'administrateur délégué d'une AWS organisation, deux options s'offrent à vous pour désactiver Security Hub sur les comptes des membres.

Option 1 : désactivation de Security Hub à l'aide de moteurs de détection

Vous pouvez tirer parti du déploiement et de la politique de Security Hub (fonctionnalités essentielles et supplémentaires) figurant dans le catalogue des politiques de votre compte d'administrateur délégué pour désactiver Security Hub ainsi qu'Amazon Inspector pour des unités organisationnelles, des comptes ou des régions spécifiques.

Pour désactiver Security Hub et Amazon Inspector sur les comptes des membres à l'aide d'une politique

1. Connectez-vous à l'aide de votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis sélectionnez Configurations.
3. Choisissez Security Hub (fonctionnalités essentielles et supplémentaires) dans le catalogue de configuration.
4. Sur la page Configurer Security Hub de la section Détails, entrez le nom et la description de la politique (par exemple, « Politique de désactivation de Security Hub »).
5. Dans la section Sélection du compte, sélectionnez l'une des options suivantes. Choisissez Toutes les unités organisationnelles et tous les comptes si vous souhaitez appliquer la désactivation à tous les comptes et unités organisationnelles. Choisissez Unités organisationnelles et comptes spécifiques si vous souhaitez appliquer la désactivation à des unités organisationnelles et à des comptes spécifiques. Si vous choisissez cette option, utilisez la barre de recherche ou l'arborescence de la structure organisationnelle pour spécifier les unités organisationnelles et les comptes cibles.
6. Dans la section Régions, choisissez Désactiver toutes les régions pour désactiver Security Hub dans toutes les régions. Choisissez éventuellement de désactiver automatiquement les nouvelles régions. Choisissez Spécifier les régions pour choisir les régions spécifiques que vous souhaitez désactiver.
7. (Facultatif) Pour les paramètres avancés, reportez-vous aux instructions du AWS Organizations.
8. (Facultatif) Pour les balises de ressources, ajoutez des balises sous forme de paires clé-valeur pour vous aider à identifier facilement la configuration.
9. Choisissez Suivant.
10. Vérifiez vos modifications, puis choisissez Appliquer. Vos comptes cibles sont configurés en fonction de cette politique. L'état de configuration de votre politique s'affiche en haut de la page Politiques.

Désactivation d'Amazon GuardDuty et AWS Hub de sécurité CSPM

Pour les fonctionnalités CSPM GuardDuty et Security Hub, vous devez désactiver manuellement les fonctionnalités des comptes d'administrateur délégué respectifs. GuardDuty et Security Hub CSPM

utilisent des déploiements (actions ponctuelles) plutôt que des politiques. La désactivation doit donc être effectuée manuellement depuis leurs consoles respectives.

Option 2 : désactivation de Security Hub uniquement

Si vous disposez d'une politique Security Hub existante et que vous souhaitez désactiver Security Hub uniquement, sans affecter Amazon Inspector ou Security Hub CSPM, procédez comme suit. GuardDuty

Pour désactiver Security Hub uniquement sur les comptes membres

1. Connectez-vous à l'aide de votre AWS compte à l'aide de vos informations d'identification d'administrateur délégué. Ouvrez la console Security Hub à l'adresse https://console.aws.amazon.com/securityhub/v2/home.
2. Dans le volet de navigation, choisissez Gestion, puis sélectionnez Configurations.
3. Choisissez l'une de vos politiques Security Hub dans les politiques configurées.
4. Choisissez Modifier la politique et, dans la section Sélection du compte, sélectionnez l'une des options suivantes. Choisissez Toutes les unités organisationnelles et tous les comptes si vous souhaitez appliquer la désactivation à tous les comptes et unités organisationnelles. Choisissez Unités organisationnelles et comptes spécifiques si vous souhaitez appliquer la désactivation à des unités organisationnelles et à des comptes spécifiques. Si vous choisissez cette option, utilisez la barre de recherche ou l'arborescence de la structure organisationnelle pour spécifier les unités organisationnelles et les comptes cibles.
5. Dans la section Régions, choisissez Désactiver toutes les régions pour désactiver Security Hub dans toutes les régions. Choisissez éventuellement de désactiver automatiquement les nouvelles régions. Choisissez Spécifier les régions pour choisir les régions spécifiques que vous souhaitez désactiver.
6. (Facultatif) Pour les paramètres avancés, reportez-vous aux instructions des AWS organisations.
7. (Facultatif) Pour les balises de ressources, ajoutez des balises sous forme de paires clé-valeur pour vous aider à identifier facilement la configuration.
8. Choisissez Suivant.
9. Vérifiez vos modifications, puis choisissez Appliquer. Vos comptes cibles sont configurés en fonction de cette politique. L'état de configuration de votre politique s'affiche en haut de la page Configurations.

Impact sur les autres services de sécurité

La désactivation de Security Hub par le biais d'une politique Security Hub n'a aucun impact sur les configurations de Security Hub GuardDuty, CSPM et Amazon Inspector.

Si vous devez désactiver Amazon Inspector uniquement pour les comptes membres, vous pouvez utiliser la politique de gestion des vulnérabilités du catalogue de configuration de Security Hub. Accédez à la page de configuration de Security Hub, choisissez Gestion des vulnérabilités dans Amazon Inspector et créez une politique de désactivation en suivant des étapes similaires à la procédure de désactivation de Security Hub ci-dessus.

Sécurité dansAWSSecurity Hub

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWSvous fournit également des services que vous pouvez utiliser en toute sécurité. Third-partyles auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Security Hub, consultez la section AWSServices concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Security Hub. Les rubriques suivantes expliquent comment configurer Security Hub pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre Security Hub.

Rubriques

- Protection des données dansAWSSecurity Hub

- AWS Gestion des identités et des accès pour Security Hub
- Validation de conformité pour AWS Hub de sécurité
- Résilience dans AWS Hub de sécurité
- Sécurité de l'infrastructure dans AWS Hub de sécurité
- AWS Hub de sécurité et interface, points de terminaison VPC (AWS PrivateLink)

Protection des données dansAWSSecurity Hub

Le modèle de responsabilité AWS partagée (modèle de) s'applique à la protection des données dans AWS Security Hub. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous lesAWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avecAWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennentServices AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Security Hub ou un autre outil Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Security Hub est une offre de services multi-locataires. Pour protéger vos données, Security Hub chiffre les données au repos et les données en transit entre les services des composants.

Refus d'utiliser vos données pour améliorer le service

> **Note**
>
> Cette page de documentation s'applique uniquement au AWS Security Hub amélioré lancé le 2 décembre 2025. Si vous êtes client du Security Hub d'origine (désormais AWS AWS Security Hub CSPM), l'utilisation des données décrite ci-dessous ne s'appliquera qu'après avoir activé le AWS Security Hub amélioré.

Vous pouvez choisir de refuser que vos données (définies comme « contenu du Security Hub » dans les conditions du service Security Hub) soient utilisées pour développer et améliorer AWS Security Hub et d'autres AWS services de sécurité en utilisant la politique de désinscription de l' AWS organisation. Vous pouvez choisir de vous désinscrire même si Security Hub ne collecte actuellement aucun contenu de ce type. Pour plus d'informations sur la procédure de désactivation, veuillez consulter Politiques de désactivation des services IA dans le Guide de l'utilisateur AWS Organizations .

> **Note**
>
> Pour que vous puissiez utiliser la politique de désinscription, vos AWS comptes doivent être gérés de manière centralisée par AWS les organisations. Si vous n'avez pas encore

créé d'organisation pour vos AWS comptes, consultez la section Création et gestion d'une organisation dans le Guide de AWS Organizations l'utilisateur.

Les effets de la désactivation sont les suivants :

- Security Hub supprimera le contenu qu'il a collecté et stocké à des fins d'amélioration du service avant votre désinscription (le cas échéant).
- Après votre désinscription, Security Hub ne collectera ni ne stockera plus ce contenu à des fins d'amélioration du service.

La section suivante explique comment Security Hub gérera votre contenu afin d'améliorer le service.

AWS Utilisation des données du Security Hub

À l'heure actuelle, AWS Security Hub ne collecte ni ne stocke aucun contenu de Security Hub à des fins d'amélioration du service. Toutefois, à l'avenir, Security Hub peut collecter et utiliser les résultats de sécurité de tiers que vous regroupez dans Security Hub et d'autres formes de contenu Security Hub (que Security Hub reçoit de votre part ou des services en amont dans le but de fournir les fonctionnalités de Security Hub) afin d'améliorer Security Hub et d'autres fonctionnalités des services de AWS sécurité.

Votre confiance, votre confidentialité et la sécurité de votre contenu sont notre priorité absolue. Si Security Hub commence à collecter du contenu Security Hub à des fins d'amélioration des services à l'avenir, cette page sera mise à jour pour refléter ces modifications et fournir des détails sur les données collectées et la manière dont elles sont utilisées. Vous pouvez vous désinscrire de cette collection de contenus de Security Hub à tout moment en utilisant la politique de désinscription de l' AWS organisation décrite ci-dessus. Pour plus d'informations sur les pratiques en matière de confidentialité des AWS données, consultez la FAQ sur la confidentialité des données.

Références

Pour des procédures de désinscription similaires dans d'autres services AWS de sécurité, voir :

- Désinscription de l'utilisation de vos données à des fins d'amélioration du service dans le Guide de GuardDuty l'utilisateur Amazon.
- Désinscription de l'utilisation de vos données à des fins d'amélioration du service dans le guide de l'utilisateur d'Amazon Security Lake.

AWS Gestion des identités et des accès pour Security Hub

Gestion des identités et des accès AWS (IAM) permet à un Service AWS administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (possède des autorisations) à utiliser les ressources de Security Hub. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment Security Hub fonctionne avec IAM
- Identity-based exemples de politiques pour AWS Security Hub CSPM
- Service-linked rôles pour AWS Hub de sécurité
- AWSpolitiques gérées pour Security Hub
- Résolution des problèmes AWS Identité et accès au Security Hub

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Identité et accès au Security Hub)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Security Hub fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based exemples de politiques pour AWS Security Hub CSPM)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identité. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), de l'authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une interface de ligne de commande pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à l' Services AWS aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de votre annuaire d'entreprise, de votre fournisseur d'identité Web ou Directory Service qui accède à l' Services AWS aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, utilisez AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Il est recommandé d'utiliser des informations d'identification temporaires plutôt que des utilisateurs IAM dotés d'informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le Guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous associez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques en ligne (intégrées directement dans une identité unique) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser

une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Security Hub fonctionne avec IAM

Avant d'utiliser Gestion des identités et des accès AWS (IAM) pour gérer l'accès à AWS Security Hub, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Security Hub.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Hub de sécurité

Fonctionnalité IAM	Support de Security Hub
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Non
Clés de condition de politique	Oui
Listes de contrôle d'accès (ACL)	Non
Attribute-based contrôle d'accès (ABAC) — balises dans les politiques	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Rôles du service	Non
Service-linked rôles	Oui

Pour une vue d'ensemble de la façon dont Security Hub et d'autres fonctionnalités Services AWS fonctionnent avec la plupart des fonctionnalités IAM, consultez Services AWS le Guide de l'utilisateur IAM consacré à l'utilisation d'IAM.

Identity-based politiques relatives à Security Hub

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous pouvez joindre à une identité, telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Security Hub prend en charge les politiques basées sur l'identité. Pour de plus amples informations, veuillez consulter Identity-based exemples de politiques pour AWS Security Hub CSPM.

Resource-based politiques relatives à Security Hub

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Security Hub ne prend pas en charge les politiques basées sur les ressources. Vous ne pouvez pas associer une politique IAM directement à une ressource Security Hub.

Actions politiques pour Security Hub

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de stratégie dans Security Hub utilisent le préfixe suivant avant l'action :

```
securityhub:
```

Par exemple, pour accorder à un utilisateur l'autorisation d'activer Security Hub, qui est une action correspondant au `EnableSecurityHubV2` fonctionnement de l'API Security Hub, incluez l'`securityhub:EnableSecurityHubV2`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Security Hub définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

```
"Action": "securityhub:EnableSecurityHubV2"
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple :

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

Vous pouvez également spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Get`, incluez l'action suivante :

```
"Action": "securityhub:Get*"
```

Cependant, une bonne pratique consiste à créer des stratégies qui suivent le principe du moindre privilège. En d'autres termes, vous devez créer des stratégies qui incluent uniquement les autorisations requises pour effectuer une tâche spécifique.

Pour obtenir la liste des actions de Security Hub, consultez la section Actions définies par AWS Security Hub dans la référence d'autorisation de service. Pour des exemples de politiques qui

spécifient les actions de Security Hub, consultezIdentity-based exemples de politiques pour AWS Security Hub CSPM.

Ressources politiques pour Security Hub

Prend en charge les ressources de politique : non

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Security Hub définit les types de ressources suivants :

- Hub
- Produit (langue française non garantie)
- Agrégateur de recherche, également appelé agrégateur interrégional
- Règle d'automatisation

Vous pouvez spécifier ces types de ressources dans les politiques à l'aide des ARN.

Pour obtenir la liste des types de ressources Security Hub et la syntaxe ARN de chacun d'entre eux, consultez la section Ressources définies par AWS Security Hub dans la référence d'autorisation de service. Pour savoir quelles actions vous pouvez spécifier pour chaque type de ressource, consultez la section Actions définies par AWS Security Hub dans la référence d'autorisation des services. Pour des exemples de politiques qui spécifient des ressources, consultezIdentity-based exemples de politiques pour AWS Security Hub CSPM.

Clés de condition de politique pour Security Hub

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, consultez les clés contextuelles de conditions AWS globales dans le guide de l'utilisateur IAM.

Pour obtenir la liste des clés de condition de Security Hub, consultez la section Clés de condition pour AWS Security Hub dans la référence d'autorisation de service. Pour savoir quelles actions et quelles ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Security Hub. Pour des exemples de politiques utilisant des clés de condition, consultezIdentity-based exemples de politiques pour AWS Security Hub CSPM.

Listes de contrôle d'accès (ACL) dans Security Hub

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Security Hub ne prend pas en charge les ACL, ce qui signifie que vous ne pouvez pas associer une ACL à une ressource Security Hub.

Attribute-based contrôle d'accès (ABAC) avec Security Hub

Prise en charge d'ABAC (balises dans les politiques) : Oui

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à celle de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Vous pouvez associer des balises aux ressources de Security Hub. Vous pouvez également contrôler l'accès aux ressources en fournissant des informations de balise dans l'`Condition`élément d'une politique.

Pour plus d'informations sur le balisage des ressources de Security Hub, consultezBalisage des ressources du Security Hub. Pour un exemple de politique basée sur l'identité qui contrôle l'accès à une ressource en fonction de balises, consultez. Identity-based exemples de politiques pour AWS Security Hub CSPM

Utilisation d'informations d'identification temporaires avec Security Hub

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès de courte durée aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous pouvez obtenir des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRole ou GetFederationToken.

Security Hub prend en charge l'utilisation d'informations d'identification temporaires.

Sessions d'accès direct pour Security Hub

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Par exemple, Security Hub envoie des demandes FAS en aval Services AWS lorsque vous intégrez Security Hub à AWS Organizations et lorsque vous désignez le compte administrateur délégué de Security Hub pour une organisation dans Organisations.

Pour les autres tâches, Security Hub utilise un rôle lié à un service pour effectuer des actions en votre nom. Pour plus de détails sur ce rôle, consultezService-linked rôles pour AWS Hub de sécurité.

Rôles de service pour Security Hub

Security Hub n'assume ni n'utilise de rôles de service. Pour effectuer des actions en votre nom, Security Hub utilise un rôle lié à un service. Pour plus de détails sur ce rôle, consultezService-linked rôles pour AWS Hub de sécurité.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut entraîner des problèmes opérationnels lors de votre utilisation de Security Hub. Modifiez les rôles de service uniquement lorsque Security Hub vous fournit des instructions à cet effet.

Service-linked rôles pour Security Hub

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre compte Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Security Hub utilise un rôle lié à un service pour effectuer des actions en votre nom. Pour plus de détails sur ce rôle, consultezService-linked rôles pour AWS Hub de sécurité.

Identity-based exemples de politiques pour AWS Security Hub CSPM

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources CSPM de Security Hub. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API Console de

gestion AWS AWS CLI, ou de AWS l'API. Un administrateur doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes ayant besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Security Hub CSPM
- Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations
- Exemple : autoriser les utilisateurs à consulter les résultats
- Exemple : autoriser les utilisateurs à créer et à gérer des règles d'automatisation

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer des ressources Security Hub sur votre compte, y accéder ou les supprimer. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations avec le moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par le AWS client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un outil spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger une authentification multifacteur (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root Compte AWS, activez l'authentification multifacteur pour renforcer la sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Security Hub CSPM

Pour accéder à la AWS Security Hub CSPM console, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des détails sur les ressources CSPM de Security Hub dans votre. Compte AWS Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) soumises à cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour vous assurer que ces utilisateurs et rôles peuvent utiliser la console Security Hub CSPM, associez également la politique AWS gérée suivante à l'entité. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut des autorisations pour effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
```

```
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : autoriser les utilisateurs à consulter les résultats

Cet exemple montre comment créer une politique IAM permettant à un utilisateur de consulter les résultats du Security Hub CSPM.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : autoriser les utilisateurs à créer et à gérer des règles d'automatisation

Cet exemple montre comment créer une politique IAM permettant à un utilisateur de créer, d'afficher, de mettre à jour et de supprimer des règles d'automatisation CSPM de Security Hub. Pour que cette politique IAM fonctionne, l'utilisateur doit être un administrateur CSPM de Security Hub. Pour limiter les autorisations, par exemple pour permettre à un utilisateur de consulter uniquement les règles d'automatisation, vous pouvez supprimer les autorisations de création, de mise à jour et de suppression.

```
{
            "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRuleV2",
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:ListAutomationRulesV2",
                "securityhub:GetAutomationRuleV2"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteAutomationRuleV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked rôles pour AWS Hub de sécurité

AWS Security Hub utilise un rôle lié à un service Gestion des identités et des accès AWS (IAM) nommé. `AWSServiceRoleForSecurityHubV2` Ce rôle lié à un service est un rôle IAM directement lié à Security Hub. Il est prédéfini par Security Hub et inclut toutes les autorisations dont Security Hub a besoin pour appeler d'autres ressources Services AWS et surveiller AWS des ressources en votre nom. Security Hub utilise ce rôle lié à un service partout Régions AWS où Security Hub est disponible.

Un rôle lié à un service facilite la configuration de Security Hub car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Security Hub définit les autorisations de son rôle lié à un service et, sauf indication contraire, seul Security Hub peut assumer ce rôle. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et vous ne pouvez pas associer cette politique d'autorisations à aucune autre entité IAM.

Pour consulter les détails du rôle lié à un service, vous pouvez utiliser la console Security Hub. Dans le volet de navigation, choisissez Général sous Paramètres. Ensuite, dans la section Autorisations de service, choisissez Afficher les autorisations de service.

Vous ne pouvez supprimer le rôle lié au service Security Hub qu'après avoir désactivé Security Hub dans toutes les régions où il est activé. Cela protège les ressources de votre Security Hub car vous ne pouvez pas supprimer par inadvertance les autorisations d'accès à celles-ci.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM et recherchez les services dont la valeur est Oui dans la colonne des rôles. Service-linked Choisissez Oui avec un lien pour consulter la documentation sur les rôles liés à un service pour ce service.

Rubriques

- Service-linked autorisations de rôle pour Security Hub
- Création d'un rôle lié à un service pour Security Hub
- Modification d'un rôle lié à un service pour Security Hub
- Supprimer un rôle lié à un service pour Security Hub

Service-linked autorisations de rôle pour Security Hub

Security Hub utilise le rôle lié à un service nommé. `AWSServiceRoleForSecurityHubV2` Il s'agit d'un rôle lié à un service requis pour que AWS Security Hub puisse accéder à vos ressources. Ce

rôle lié à un service permet à Security Hub d'effectuer des tâches telles que la réception des résultats d'autres utilisateurs Services AWS et la configuration de l' AWS Config infrastructure requise pour effectuer des contrôles de sécurité. Le rôle lié à un service `AWSServiceRoleForSecurityHubV2` fait confiance au service `securityhub.amazonaws.com` pour endosser le rôle.

Le rôle lié à un service `AWSServiceRoleForSecurityHubV2` utilise la stratégie gérée par `AWSSecurityHubV2ServiceRolePolicy`.

Vous devez accorder des autorisations pour permettre à une identité IAM (telle qu'un rôle, un groupe ou un utilisateur) de créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForSecurityHubV2` lié à un service soit créé avec succès, l'identité IAM que vous utilisez pour accéder à Security Hub doit disposer des autorisations requises. Pour accorder les autorisations requises, associez la stratégie suivante à l'identité IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Création d'un rôle lié à un service pour Security Hub

Le rôle `AWSServiceRoleForSecurityHubV2` lié à un service est créé automatiquement lorsque vous activez Security Hub pour la première fois ou lorsque vous activez Security Hub dans une région où vous ne l'aviez pas activé auparavant. Vous pouvez également créer le rôle `AWSServiceRoleForSecurityHubV2` lié à un service manuellement à l'aide de la console IAM, de l'interface de ligne de commande IAM ou de l'API IAM. Pour de plus amples informations sur la création manuelle d'un rôle, veuillez consulter Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

> **Important**
>
> Le rôle lié à un service qui est créé pour un compte administrateur de Security Hub ne s'applique pas aux comptes de membres de Security Hub associés.

Modification d'un rôle lié à un service pour Security Hub

Security Hub ne vous permet pas de modifier le rôle `AWSServiceRoleForSecurityHubV2` lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Security Hub

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, supprimez le rôle. Ainsi, vous n'avez pas d'entité inutilisée qui n'est pas activement surveillée ou maintenue.

Lorsque vous désactivez Security Hub, Security Hub ne supprime pas automatiquement le rôle `AWSServiceRoleForSecurityHubV2` lié au service pour vous. Si vous réactivez Security Hub, le service peut alors recommencer à utiliser le rôle lié au service existant. Si vous n'avez plus besoin d'utiliser Security Hub, vous pouvez supprimer manuellement le rôle lié au service.

> **Important**
>
> Avant de supprimer le rôle `AWSServiceRoleForSecurityHubV2` lié à un service, vous devez d'abord désactiver Security Hub dans toutes les régions où il est activé. Pour de plus amples informations, veuillez consulter Désactivation de Security Hub. Si Security Hub

n'est pas désactivé lorsque vous tentez de supprimer le rôle lié à un service, la suppression échoue.

Pour supprimer le rôle `AWSServiceRoleForSecurityHubV2` lié à un service, vous pouvez utiliser la console IAM, l'interface de ligne de commande IAM ou l'API IAM. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

AWSpolitiques gérées pour Security Hub

Une politique AWS gérée est une politique autonome créée et administrée parAWS. AWSles politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWSest le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWSpolitique gérée : AWSSecurityHubFullAccess

Vous pouvez associer la politique `AWSSecurityHubFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet principal à toutes les actions du Security Hub. Cette politique doit être attachée à un mandant avant qu'il n'active Security Hub manuellement pour son compte. Par exemple, les responsables disposant de ces autorisations peuvent à la fois consulter et mettre à jour l'état des résultats. Ils peuvent également configurer des informations personnalisées, activer les intégrations et activer et désactiver les normes et les contrôles. Les titulaires d'un compte administrateur peuvent également gérer les comptes des membres.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `securityhub`— Permet aux principaux un accès complet à toutes les actions du Security Hub.
- `guardduty`— Permet aux principaux d'obtenir des informations sur l'état du compte sur Amazon GuardDuty.
- `iam`— Permet aux principaux de créer un rôle lié à un service pour Security Hub.
- `inspector`— Permet aux principaux d'obtenir des informations sur l'état du compte dans Amazon Inspector.
- `pricing`— Permet aux donneurs d'ordre d'obtenir une liste de prix Services AWS et de produits.

Pour consulter les autorisations associées à cette politique, consultez AWSSecurityHubFullAccessle Guide de référence des politiques AWS gérées.

AWSpolitique gérée : AWSSecurityHubReadOnlyAccess

Vous pouvez associer la politique `AWSSecurityHubReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations dans Security Hub. Les responsables auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour dans Security Hub. Par exemple, les directeurs disposant de ces autorisations peuvent consulter la liste des résultats associés à leur compte, mais ne peuvent pas modifier le statut d'un résultat. Ils peuvent consulter les résultats des informations, mais ne peuvent pas créer ou configurer des informations personnalisées. Ils ne peuvent pas configurer les contrôles ou les intégrations de produits.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `securityhub`— Permet aux utilisateurs d'effectuer des actions qui renvoient une liste d'éléments ou des détails sur un élément. Cela inclut les opérations d'API qui commencent par `GetList`, ou`Describe`.

Pour consulter les autorisations associées à cette politique, consultez AWSSecurityHubReadOnlyAccessle Guide de référence des politiques AWS gérées.

AWSpolitique gérée : AWSSecurityHubOrganizationsAccess

Vous pouvez associer la politique `AWSSecurityHubOrganizationsAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives pour activer et gérer Security Hub pour une organisation dansAWS Organizations. Les autorisations associées à cette politique permettent au compte de gestion de l'organisation de désigner le compte d'administrateur délégué pour Security Hub. Ils permettent également au compte administrateur délégué d'activer les comptes de l'organisation en tant que comptes de membres.

Cette politique fournit uniquement des autorisations pourAWS Organizations. Le compte de gestion de l'organisation et le compte d'administrateur délégué nécessitent également des autorisations pour les actions associées. Ces autorisations peuvent être accordées à l'aide de la politique `AWSSecurityHubFullAccess` gérée.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `organizations:ListAccounts`— Permet aux principaux de récupérer la liste des comptes faisant partie d'une organisation.
- `organizations:DescribeOrganization`— Permet aux directeurs de récupérer des informations sur l'organisation.
- `organizations:ListRoots`— Permet aux directeurs de répertorier la racine d'une organisation.
- `organizations:ListDelegatedAdministrators`— Permet aux principaux de répertorier l'administrateur délégué d'une organisation.
- `organizations:ListAWSServiceAccessForOrganization`— Permet aux directeurs de répertorier les informations Services AWS utilisées par une organisation.
- `organizations:ListOrganizationalUnitsForParent`— Permet aux directeurs de répertorier les unités organisationnelles (UO) enfants d'une UO parent.
- `organizations:ListAccountsForParent`— Permet aux directeurs de répertorier les comptes enfants d'une unité d'organisation parent.
- `organizations:ListParents`— Répertorie la racine ou les unités organisationnelles (UO) qui servent de parent immédiat à l'unité d'organisation ou au compte enfant spécifié.
- `organizations:DescribeAccount` : autorise les principaux à extraire des informations sur un compte dans l'organisation.

- `organizations:DescribeOrganizationalUnit`— Permet aux directeurs de récupérer des informations sur une unité organisationnelle de l'organisation.
- `organizations:ListPolicies`— Récupère la liste de toutes les politiques d'une organisation d'un type spécifique.
- `organizations:ListPoliciesForTarget`— Répertorie les politiques directement associées à la racine, à l'unité organisationnelle (UO) ou au compte cible spécifié.
- `organizations:ListTargetsForPolicy`— Répertorie toutes les racines, unités organisationnelles (UO) et comptes auxquels la politique spécifiée est attachée.
- `organizations:EnableAWSServiceAccess`— Permet aux directeurs d'activer l'intégration avec les Organizations.
- `organizations:RegisterDelegatedAdministrator`— Permet aux principaux de désigner le compte d'administrateur délégué.
- `organizations:DeregisterDelegatedAdministrator`— Permet aux principaux de supprimer le compte d'administrateur délégué.
- `organizations:DescribePolicy`— Récupère les informations relatives à une politique.
- `organizations:DescribeEffectivePolicy`— Renvoie le contenu de la politique effective pour le type de politique et le compte spécifiés.
- `organizations:CreatePolicy`— Crée une politique d'un type spécifique que vous pouvez associer à une racine, à une unité organisationnelle (UO) ou à un AWS compte individuel.
- `organizations:UpdatePolicy`— Met à jour une politique existante avec un nouveau nom, une nouvelle description ou un nouveau contenu.
- `organizations:DeletePolicy`— Supprime la politique spécifiée de votre organisation.
- `organizations:AttachPolicy`— Attache une politique à une racine, à une unité organisationnelle (UO) ou à un compte individuel.
- `organizations:DetachPolicy`— Détache une politique d'une racine, d'une unité organisationnelle (UO) ou d'un compte cible.
- `organizations:EnablePolicyType`— Active un type de politique dans une racine.
- `organizations:DisablePolicyType`— Désactive un type de politique organisationnelle dans une racine.
- `organizations:TagResource`— Ajoute une ou plusieurs balises à une ressource spécifiée.
- `organizations:UntagResource`— Supprime toutes les balises contenant les clés spécifiées d'une ressource spécifiée.

- `organizations:ListTagsForResource`— Répertorie les balises associées à une ressource spécifiée.

Pour consulter les autorisations associées à cette politique, consultez AWSSecurityHubOrganizationsAccesslle Guide de référence des politiques AWS gérées.

AWSpolitique gérée : AWSSecurityHubV2ServiceRolePolicy

Cette politique permet à Security Hub de gérer les AWS Config règles et les ressources du Security Hub pour votre organisation et en votre nom. Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos identités IAM. Pour de plus amples informations, veuillez consulter the section called "Service-linked rôles".

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `access-analyzer`— Créez et supprimez des analyseurs d'accès IAM liés à un service lorsque les clients activent ou désactivent Security Hub, listez les analyseurs pour vérifier que l'état de l'analyseur correspond à l'état d'activation, et générez et récupérez des recommandations de politique pour les résultats d'accès non utilisés.
- `cloudwatch`— Récupérez les données de métriques pour prendre en charge les fonctionnalités de mesure des ressources du Security Hub et les indicateurs de santé du connecteur.
- `config`— Gérez les enregistreurs de configuration liés à un service et les enregistreurs de configuration tiers liés à un service pour les ressources du Security Hub, y compris la prise en charge des enregistreurs de configuration globaux. Répertoriez les enregistreurs de configuration et obtenez des informations sur les connecteurs pour prendre en charge les intégrations cloud tierces.
- `ecr`— Récupérez des informations sur les images et les référentiels Amazon Elastic Container Registry pour prendre en charge les fonctionnalités de mesure.
- `iam`— Créez les rôles liés aux services suivants : AWS Config IAM Access Analyzer dans le compte client et Amazon Inspector pour les analyses par des tiers. Récupérez les informations de compte pour prendre en charge les fonctionnalités de mesure. Récupérez les politiques IAM existantes afin que les clients puissent consulter une comparaison entre leur politique actuelle et le remplacement recommandé selon le principe du moindre privilège.

- `inspector2`— Créez, mettez à jour, supprimez et répertoriez les connecteurs Amazon Inspector et les configurations de scan des connecteurs pour prendre en charge les intégrations cloud tierces.
- `lambda`— Récupérez les informations relatives aux AWS Lambda fonctions pour renforcer les capacités de mesure.
- `organizations`— Récupérez les informations relatives au compte et à l'unité organisationnelle (UO) d'une organisation.
- `securityhub`— Gérez la configuration du Security Hub. Créez, mettez à jour et supprimez des connecteurs Security Hub pour prendre en charge les intégrations cloud tierces.
- `sts`— Obtenez des jetons d'identité Web pour la fédération des identités sortantes afin de prendre en charge les intégrations cloud tierces.
- `tag`— Récupère des informations sur les balises de ressources.

Pour consulter les autorisations associées à cette politique, consultez AWSSecurityHubV2ServiceRolePolicyle Guide de référence des politiques AWS gérées.

Mises à jour de Security Hub pourAWSstratégies gérées

Le tableau suivant fournit des informations détaillées sur les mises à jour apportées aux politiques AWS gérées pour AWS Security Hub depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les mises à jour des politiques, abonnez-vous au flux RSS sur la page d'historique des documents du Security Hub.

Modifier	Description	Date
AWSSecurityHubV2ServiceRolePolicy— Politique mise à jour	Security Hub a mis à jour la politique pour prendre en charge les intégrations tierces. La mise à jour ajoute les autorisations suivantes : gérer les enregistreurs de configuration tiers, créer et gérer les connecteurs Security Hub et Amazon Inspector, récupérer	30 juin 2026

Modifier	Description	Date
	les indicateurs de santé des connecteurs CloudWatch, créer le rôle lié au service Amazon Inspector pour le scan par des tiers et obtenir des jetons d'identité Web pour la fédération.	
AWSSecurityHubV2ServiceRolePolicy— Politique mise à jour	Security Hub a mis à jour la politique pour ajouter des autorisations IAM Access Analyzer. La mise à jour permet à Security Hub de créer et de gérer des analyseurs gérés par des services, de répertorier les analyseurs pour vérifier que la configuration de l'analyseur est conforme à l'état d'activation, de générer et de récupérer des recommandations de politique pour les résultats d'accès non utilisés, et de récupérer les politiques IAM pour l'affichage des recommandations.	10 mai 2026

Modifier	Description	Date
AWSSecurityHubOrganizationsAccess— Politique mise à jour	Security Hub a mis à jour la politique afin d'ajouter des autorisations permettant de décrire les politiques de ressources destinées à prendre en charge les fonctionnalités de Security Hub. Security Hub est en version préliminaire et peut faire l'objet de modifications.	12 novembre 2025
AWSSecurityHubFullAccess— Politique mise à jour	Security Hub a mis à jour la politique afin d'ajouter des fonctionnalités relatives à la gestion GuardDuty, à Amazon Inspector et à la gestion des comptes afin de prendre en charge les fonctionnalités de Security Hub. Security Hub est en version préliminaire et peut faire l'objet de modifications.	17 novembre 2025

Modifier	Description	Date
AWSSecurityHubV2ServiceRolePolicy— Politique mise à jour	Security Hub a mis à jour la politique afin d'ajouter des fonctionnalités de mesure pour Amazon Elastic Container RegistryAWS Lambda, Amazon CloudWatch, et Gestion des identités et des accès AWS pour prendre en charge les fonctionnalités de Security Hub. La mise à jour a également ajouté la prise en charge des AWS Config enregistreurs mondiaux. Security Hub est en version préliminaire et peut faire l'objet de modifications.	5 novembre 2025
AWSSecurityHubOrganizationsAccess : mise à jour d'une politique existante	Security Hub a ajouté de nouvelles autorisations à la politique. Les autorisations permettent à la direction de l'organisation d'activer et de gérer Security Hub et Security Hub CSPM pour une organisation.	17 juin 2025
AWSSecurityHubFullAccess : mise à jour d'une politique existante	Security Hub CSPM a ajouté de nouvelles autorisations qui permettent aux principaux de créer un rôle lié à un service pour Security Hub.	17 juin 2025

Modifier	Description	Date
AWSSecurityHubV2ServiceRolePolicy : nouvelle politique	Security Hub a ajouté une nouvelle politique permettant à Security Hub de gérer les AWS Config règles et les ressources du Security Hub pour l'organisation d'un client et pour le compte du client. Security Hub est en version préliminaire et peut faire l'objet de modifications.	17 juin 2025
AWSSecurityHubFullAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour la politique afin d'obtenir des informations sur les prix Services AWS et les produits.	24 avril 2024
AWSSecurityHubReadOnlyAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour cette politique gérée en ajoutant un `Sid` champ.	22 février 2024
AWSSecurityHubFullAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour la politique afin de déterminer si Amazon GuardDuty et Amazon Inspector sont activés dans un compte. Cela permet aux clients de rassembler des informations relatives à la sécurité provenant de plusieurs sources. Services AWS	16 novembre 2023

Modifier	Description	Date
AWSSecurityHubOrganizationsAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour la politique afin d'accorder des autorisations supplémentaires afin de permettre un accès en lecture seule aux AWS Organizations fonctionnalités d'administrateur délégué. Cela inclut des détails tels que la racine, les unités organisationnelles (UO), les comptes, la structure organisationnelle et l'accès aux services.	16 novembre 2023
AWSSecurityHubOrganizationsAccess— Nouvelle politique	Security Hub CSPM a ajouté une nouvelle politique qui accorde les autorisations nécessaires à l'intégration du Security Hub CSPM aux Organizations.	15 mars 2021
Security Hub CSPM a commencé à suivre les modifications	Security Hub CSPM a commencé à suivre les modifications apportées à ses politiques AWS gérées.	15 mars 2021

Résolution des problèmes AWS Identité et accès au Security Hub

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Security Hub et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Security Hub
- Je ne suis pas autorisé à effectuer iam : PassRole

- Je souhaite accéder par programmation à Security Hub
- Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à Security Hub
- Je veux autoriser des personnes extérieures à mon Compte AWS pour accéder aux ressources de mon Security Hub

Je ne suis pas autorisé à effectuer une action dans Security Hub

Si cela vous Console de gestion AWS indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` essaie d'utiliser la console pour afficher les détails d'un *`widget`* mais n'y est pas `securityhub:`*`GetWidget`* autorisé.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `securityhub:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Security Hub.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Security Hub. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite accéder par programmation à Security Hub

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la section Connexion pour le développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.
Identité de la main-d'œuvre	Utilisez des informations d'identification temporaires pour signer les demandes	Suivez les instructions de l'interface que vous souhaitez utiliser.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
(Utilisateurs gérés dans IAM Identity Center)	programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	• Pour cela AWS CLI, reportez-vous AWS CLI à la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à Security Hub

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Je veux autoriser des personnes extérieures à mon Compte AWS pour accéder aux ressources de mon Security Hub

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Security Hub prend en charge ces fonctionnalités, consultezComment Security Hub fonctionne avec IAM.
- Pour savoir comment donner accès à vos ressources par l'intermédiaire de celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS qui vous appartient dans le Guide de l'utilisateur IAM.
- Pour savoir comment donner accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Validation de conformité pour AWS Hub de sécurité

Notre nouvelle expérience AWS d'inscription n'est pas conçue pour les charges de travail réglementées. Si vous utilisez notre nouvelle interface d' AWS inscription, mais que vous souhaitez l'utiliser AWS pour des charges de travail réglementées, vous pouvez vous inscrire à des fonctionnalités AWS (avancées) ou activer des fonctionnalités avancées pour votre AWS environnement.

Pour savoir si un s' Service AWS inscrit dans le cadre de programmes de conformité spécifiques, consultez Services AWS la section Étendue par programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Résilience dans AWS Hub de sécurité

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur Régions AWS les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans AWS Hub de sécurité

En tant que service géré, AWS Security Hub est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et la manière de AWS protéger l'infrastructure, consultez AWS Cloud Security. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans Security Pillar AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder à Security Hub via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Suites de chiffrement avec une confidentialité directe parfaite (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

AWS Hub de sécurité et interface, points de terminaison VPC (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre VPC et AWS Security Hub en créant une interface VPC endpoint. Les points de terminaison de l'interface sont alimentés par AWS PrivateLink une technologie qui vous permet d'accéder en privé aux API de Security Hub sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API Security Hub. Le trafic entre votre VPC et Security Hub ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux. Pour plus d'informations, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC avec interface dans le guide Amazon Virtual Private Cloud.

Considérations relatives aux points de terminaison VPC Security Hub

Avant de configurer un point de terminaison VPC d'interface pour Security Hub, assurez-vous de consulter les prérequis et les autres informations figurant dans le guide Amazon Virtual Private Cloud.

Security Hub prend en charge les appels vers toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison VPC d'interface pour Security Hub

Vous pouvez créer un point de terminaison VPC pour le service Security Hub à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez la section Créer un point de terminaison VPC dans le guide Amazon Virtual Private Cloud.

Créez un point de terminaison VPC pour Security Hub en utilisant le nom de service suivant :

`com.amazonaws.region.securityhub`

Où se *region* trouve le code de la région applicable Région AWS.

Si vous activez le DNS privé pour le terminal, vous pouvez envoyer des requêtes d'API à Security Hub en utilisant son nom DNS par défaut pour la région, par exemple `securityhub.us-east-1.amazonaws.com` pour la région USA Est (Virginie du Nord).

Création d'une politique de point de terminaison VPC pour Security Hub

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à Security Hub. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez la section Contrôler l'accès aux terminaux VPC à l'aide de politiques relatives aux terminaux dans le guide Amazon Virtual Private Cloud.

Exemple : politique de point de terminaison VPC pour les actions de Security Hub

Voici un exemple de politique relative aux terminaux pour Security Hub. Lorsqu'elle est connectée à un terminal, cette politique donne accès aux actions Security Hub répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
```

```
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Sous-réseaux partagés

Vous ne pouvez pas créer, décrire, modifier ou supprimer de points de terminaison de VPC dans des sous-réseaux qui sont partagés avec vous. Toutefois, vous pouvez utiliser les points de terminaison d'un VPC dans les sous-réseaux qui sont partagés avec vous. Pour plus d'informations sur le partage de VPC, consultez la section Partager vos sous-réseaux VPC avec d'autres comptes dans le guide Amazon Virtual Private Cloud.

Journalisation des appels d'API Security Hub avec CloudTrail

est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Security Hub. CloudTrail capture les appels d'API pour Security Hub sous forme d'événements. Les appels capturés incluent les appels depuis la console Security Hub et les appels de code vers les opérations de l'API Security Hub. Si vous créez un historique, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Security Hub. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents sur la CloudTrail console dans l'historique des événements. À l'aide des informations CloudTrail collectées, vous pouvez déterminer la demande qui a été faite à Security Hub, l'adresse IP à partir de laquelle la demande a été faite, qui l'a faite, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, notamment sur la manière de le configurer et de l'activer, consultez le Guide de AWS CloudTrail l'utilisateur.

Informations sur le Security Hub dans CloudTrail

CloudTrail est activé Compte AWS lors de la création de votre compte. Lorsqu'une activité liée à un événement pris en charge se produit dans Security Hub, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements.

Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte . Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement permanent des événements survenus sur votre compte, y compris les événements relatifs à Security Hub, créez un historique. Un journal permet CloudTrail de transmettre des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et y donner suite. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Security Hub prend en charge l'enregistrement de toutes les actions de l'API Security Hub en tant qu'événements dans CloudTrail les journaux. Pour consulter la liste des opérations de Security Hub, consultez la référence de l'API Security Hub.

Lorsque l'activité relative aux actions suivantes est enregistrée CloudTrail, la valeur de `responseElements` est définie sur`null`. Cela garantit que les informations sensibles ne sont pas incluses dans CloudTrail les journaux.

- `GetFindingsV2`

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec des informations d'identification root ou utilisateur Gestion des identités et des accès AWS (IAM)
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Exemple : entrées du fichier journal de Security Hub

Un journal est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une pile ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateAutomationRuleV2`action. Dans cet exemple, une règle d'automatisation appelée `TestAutomationRule` est créée. Les `Account ID` attributs `Severity` et sont spécifiés en tant que critères. Lorsque la règle correspond, elle `Severity` est mise à jour sur Élevé. Pour plus d'informations sur les règles d'automatisation, consultezRègles d'automatisation dans Security Hub.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:Admin",
        "arn": "arn:aws:sts::555555555555:assumed-role/Admin",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "aarn:aws:iam::555555555555:role/Admin",
                "accountId": "555555555555",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2025-11-15T18:49:13Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-11-15T18:51:17Z",
    "eventSource": "securityhub.amazonaws.com",
```

```
    "eventName": "CreateAutomationRuleV2",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.50",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Description": "Test Automation Rule",
        "Actions": [
            {
                "Type": "FINDING_FIELDS_UPDATE",
                "FindingFieldsUpdate": {
                    "SeverityId": 4
                }
            }
        ],
        "RuleStatus": "ENABLED",
        "Criteria": {
            "OcsfFindingCriteria": {
                "CompositeFilters": [
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "severity",
                                "Filter": {
                                    "Value": "Medium",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    },
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "cloud.account.uid",
                                "Filter": {
                                    "Value": "111122223333",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    }
                ],
                "CompositeOperator": "AND"
```

```
            }
        },
        "ClientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
        "RuleOrder": 61,
        "RuleName": "TestAutomationRule",
        "Tags": {}
    },
    "responseElements": {
        "RuleArn": "arn:aws:securityhub:us-west-2:555555555555:automation-rulev2/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "RuleId": "c8bc6f90-29e9-4eb7-919f-b145e44eb8ec"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management"
}
```

Présentation de AWS Hub de sécurité CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) vous fournit une vue complète de votre état de sécurité et vous aide à évaluer votre AWS environnement par rapport aux normes AWS et aux meilleures pratiques du secteur de la sécurité.

AWS Security Hub CSPM collecte des données de sécurité provenant de produits tiers pris en charge et vous aide à analyser vos tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires. Comptes AWS Services AWS

Pour vous aider à gérer l'état de sécurité de votre organisation, Security Hub CSPM prend en charge plusieurs normes de sécurité. Il s'agit notamment de la norme FSBP (AWS Foundational Security Best Practices) développée par AWS et de cadres de conformité externes tels que le Center for Internet Security (CIS), le Payment Card Industry Data Security Standard (PCI DSS) et le National Institute of Standards and Technology (NIST). Chaque norme comprend plusieurs contrôles de sécurité, chacun représentant une bonne pratique en matière de sécurité. Security Hub CSPM effectue des vérifications par rapport aux contrôles de sécurité et génère des résultats de contrôle pour vous aider à évaluer votre conformité par rapport aux meilleures pratiques de sécurité.

En plus de générer des résultats de contrôle, Security Hub CSPM reçoit également des résultats d'autres produits, Services AWS tels qu'Amazon GuardDuty, Amazon Inspector et Amazon Macie, et de produits tiers pris en charge. Cela vous donne un aperçu unique de toute une série de problèmes liés à la sécurité. Vous pouvez également envoyer les résultats CSPM de Security Hub à d'autres produits tiers pris Services AWS en charge.

Security Hub CSPM propose des fonctionnalités d'automatisation qui vous aident à trier et à résoudre les problèmes de sécurité. Par exemple, vous pouvez utiliser des règles d'automatisation pour mettre à jour automatiquement les résultats critiques en cas d'échec d'un contrôle de sécurité. Vous pouvez également tirer parti de l'intégration avec Amazon EventBridge pour déclencher des réponses automatiques à des résultats spécifiques.

Rubriques

- Avantages du Security Hub CSPM
- Accès à Security Hub CSPM
- Services connexes
- Essai gratuit et tarifs de Security Hub CSPM

- Concepts et terminologie dans Security Hub CSPM
- Activation de Security Hub CSPM
- Gestion des comptes d'administrateur et de membre dans Security Hub CSPM
- Comprendre l'agrégation entre régions dans Security Hub CSPM
- Comprendre les normes de sécurité dans Security Hub CSPM
- Comprendre les contrôles de sécurité dans Security Hub CSPM
- Comprendre les intégrations dans Security Hub CSPM
- Intégration du Security Hub CSPM à Microsoft Azure
- Création et mise à jour des résultats dans Security Hub CSPM
- Afficher des informations dans Security Hub CSPM
- Modification automatique des résultats et prise en compte des résultats dans Security Hub CSPM
- Utilisation du tableau de bord dans Security Hub CSPM
- Limites régionales pour Security Hub CSPM
- Création de ressources Security Hub CSPM avec CloudFormation
- Abonnement aux annonces CSPM de Security Hub avec Amazon SNS
- Désactivation du Security Hub CSPM
- Sécurité dans AWS Security Hub CSPM
- Journalisation des appels de l'API Security Hub avec CloudTrail

Avantages du Security Hub CSPM

Voici quelques-unes des principales manières dont Security Hub CSPM vous aide à surveiller votre conformité et votre niveau de sécurité dans votre AWS environnement.

Effort réduit pour collecter et hiérarchiser les conclusions

> Security Hub CSPM réduit les efforts de collecte et de hiérarchisation des résultats de sécurité sur les comptes issus de produits intégrés Services AWS et AWS partenaires. Security Hub CSPM traite les données de recherche à l'aide du format ASFF (AWS Security Finding Format), un format de recherche standard. Il n'est donc plus nécessaire de gérer les résultats provenant d'une myriade de sources dans de multiples formats. Security Hub CSPM met également en corrélation les résultats des différents fournisseurs pour vous aider à hiérarchiser les plus importants.

Contrôles automatiques de sécurité selon les bonnes pratiques et les normes

Security Hub CSPM exécute automatiquement une configuration et des contrôles de sécurité continus au niveau du compte, conformément aux AWS meilleures pratiques et aux normes du secteur. Security Hub CSPM utilise les résultats de ces contrôles pour calculer les scores de sécurité et identifier les comptes et les ressources spécifiques qui nécessitent une attention particulière.

Vue consolidée des conclusions dans les comptes et les fournisseurs

Security Hub CSPM consolide vos résultats de sécurité sur l'ensemble des comptes et des produits des fournisseurs et affiche les résultats sur la console Security Hub CSPM. Vous pouvez également récupérer les résultats via l'API CSPM de Security Hub ou les kits de développement logiciel (AWS CLI SDK). Grâce à une vision globale de votre état de sécurité actuel, vous pouvez identifier les tendances, identifier les problèmes potentiels et prendre les mesures correctives nécessaires.

Possibilité d'automatiser la recherche, les mises à jour et les mesures correctives

Vous pouvez créer des règles d'automatisation qui modifient ou suppriment les résultats en fonction de vos critères définis. Security Hub CSPM prend également en charge une intégration avec Amazon. EventBridge Pour automatiser la correction de résultats spécifiques, vous pouvez définir des actions personnalisées à prendre lorsqu'un résultat est généré. Vous pouvez, par exemple, configurer des actions personnalisées, pour envoyer des conclusions à un système de tickets ou à un système de correction automatique.

Accès à Security Hub CSPM

Security Hub CSPM est disponible dans la plupart des cas. Régions AWS Pour obtenir la liste des régions dans lesquelles Security Hub CSPM est actuellement disponible, voir Points de terminaison et AWS quotas Security Hub CSPM dans le. Références générales AWS Pour plus d'informations sur la gestion Régions AWS de votre compte Compte AWS, consultez la section Spécifier les éléments que Régions AWS votre compte peut utiliser dans le Guide de Gestion de compte AWS référence.

Dans chaque région, vous pouvez accéder à Security Hub CSPM et l'utiliser de l'une des manières suivantes :

Console Security Hub CSPM

Console de gestion AWS Il s'agit d'une interface basée sur un navigateur que vous pouvez utiliser pour créer et gérer AWS des ressources. Dans le cadre de cette console, la console Security Hub CSPM permet d'accéder à votre compte, à vos données et à vos ressources Security Hub CSPM. Vous pouvez effectuer des tâches CSPM Security Hub à l'aide de la console Security Hub CSPM : consulter les résultats, créer des règles d'automatisation, créer une région d'agrégation, etc.

API CSPM Security Hub

L'API Security Hub CSPM vous donne un accès programmatique à votre compte, à vos données et à vos ressources Security Hub CSPM. Grâce à l'API, vous pouvez envoyer des requêtes HTTPS directement à Security Hub CSPM. Pour plus d'informations sur l'API, consultez la référence de AWS Security Hub l'API .

AWS CLI

Avec le AWS CLI, vous pouvez exécuter des commandes sur la ligne de commande de votre système pour exécuter les tâches CSPM de Security Hub. Dans certains cas, l'utilisation de la ligne de commande peut s'avérer plus rapide et plus pratique que l'utilisation de la console. La ligne de commande est également utile si vous souhaitez créer des scripts qui exécutent des tâches. Pour plus d'informations sur l'installation et l'utilisation de AWS CLI, consultez le Guide de AWS Command Line Interface l'utilisateur.

AWS SDK

AWS fournit des kits SDK composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes, par exemple Java, Go, Python, C++ et .NET. Les SDK fournissent un accès programmatique pratique à Security Hub CSPM et à d'autres outils Services AWS dans la langue de votre choix. Ils gèrent également des tâches telles que la signature cryptographique des demandes, la gestion des erreurs et la relance automatique des demandes. Pour plus d'informations sur l'installation et l'utilisation des AWS kits SDK, consultez la section Outils sur AWS lesquels s'appuyer.

Important

Security Hub CSPM détecte et consolide uniquement les résultats générés une fois que vous avez activé Security Hub CSPM. Il ne détecte ni ne consolide de manière rétroactive les résultats de sécurité générés avant que vous n'activiez Security Hub CSPM.

Security Hub CSPM reçoit et traite les résultats uniquement dans la région où vous avez activé Security Hub CSPM sur votre compte.
Pour une conformité totale avec les contrôles de sécurité de CIS AWS Foundations Benchmark, vous devez activer Security Hub CSPM dans toutes les régions prises en charge AWS .

Services connexes

Pour sécuriser davantage votre AWS environnement, pensez à en utiliser d'autres Services AWS en combinaison avec Security Hub CSPM. Certains Services AWS envoient leurs résultats à Security Hub CSPM, et Security Hub CSPM normalise les résultats dans un format standard. Certains Services AWS peuvent également recevoir les résultats du Security Hub CSPM.

Pour obtenir la liste des autres personnes Services AWS qui envoient ou reçoivent les résultats CSPM de Security Hub, consultez. Service AWS intégrations avec Security Hub CSPM

Security Hub CSPM utilise des règles liées à des services AWS Config pour exécuter des contrôles de sécurité pour la plupart des contrôles. Les contrôles font référence à des AWS ressources Services AWS et à des ressources spécifiques. Pour obtenir la liste des contrôles CSPM de Security Hub, consultez. Référence de contrôle pour Security Hub CSPM Vous devez activer AWS Config et enregistrer les ressources dans Security Hub CSPM AWS Config pour générer la plupart des résultats de contrôle. Pour de plus amples informations, veuillez consulter Considérations avant l'activation et la configuration AWS Config.

Essai gratuit et tarifs de Security Hub CSPM

Lorsque vous activez Security Hub CSPM Compte AWS pour la première fois, ce compte est automatiquement inscrit à un essai gratuit de 30 jours de Security Hub CSPM.

Lorsque vous utilisez Security Hub CSPM pendant la période d'essai gratuite, l'utilisation d'autres services avec lesquels Security Hub CSPM interagit vous est facturée, tels que les objets. AWS Config Les AWS Config règles activées uniquement selon les normes de sécurité CSPM de Security Hub ne vous sont pas facturées.

L'utilisation de Security Hub CSPM ne vous est pas facturée avant la fin de votre essai gratuit.

Affichage des détails d'utilisation

Security Hub CSPM fournit des informations d'utilisation, notamment le nombre de contrôles de sécurité et de résultats traités par votre compte. Les détails d'utilisation incluent également la durée restante de l'essai gratuit. Ces informations peuvent vous aider à comprendre votre utilisation du Security Hub CSPM après la fin de la période d'essai gratuite. Les informations d'utilisation sont également disponibles après la fin de l'essai gratuit.

Pour afficher les informations d'utilisation (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Utilisation sous Paramètres.

Les informations d'utilisation concernent uniquement le compte courant et la région en cours. Dans une région d'agrégation, les informations d'utilisation n'incluent pas les régions liées. Pour plus d'informations sur les régions liées, consultezthe section called "Types de données agrégées".

Pour consulter le détail des coûts de votre compte, utilisez la console AWS de facturation.

Informations de tarification

Pour plus d'informations sur la manière dont Security Hub CSPM facture les résultats ingérés et les contrôles de sécurité, consultez la rubrique Tarification de Security Hub CSPM.

Concepts et terminologie dans Security Hub CSPM

Dans AWS Security Hub CSPM, nous nous appuyons sur des AWS concepts et une terminologie communs et utilisons ces termes supplémentaires.

Compte

Un compte Amazon Web Services (AWS) standard qui contient vos AWS ressources. Vous pouvez vous connecter AWS avec votre compte et activer Security Hub CSPM.

Un compte peut inviter d'autres comptes à activer Security Hub CSPM et à s'associer à ce compte dans Security Hub CSPM. L'acceptation d'une invitation d'adhésion est facultative. Si les invitations sont acceptées, le compte devient un compte administrateur et les comptes ajoutés

sont des comptes de membres. Les comptes administrateurs peuvent consulter les résultats dans leurs comptes membres.

Si vous êtes inscrit AWS Organizations, votre organisation désigne un compte administrateur CSPM Security Hub pour l'organisation. Le compte administrateur CSPM de Security Hub peut activer d'autres comptes d'organisation en tant que comptes de membres.

Un compte ne peut pas être à la fois un compte administrateur et un compte membre. Un compte ne peut avoir qu'un seul compte administrateur.

Pour de plus amples informations, veuillez consulter Gestion des comptes d'administrateur et de membre dans Security Hub CSPM.

Compte administrateur

Un compte dans Security Hub CSPM qui est autorisé à consulter les résultats des comptes membres associés.

Un compte devient un compte administrateur de l'une des manières suivantes :

- Le compte invite d'autres comptes à s'y associer dans Security Hub CSPM. Lorsque ces comptes acceptent l'invitation, ils deviennent des comptes membres et le compte qui les invite devient leur compte administrateur.
- Le compte est désigné par un compte de gestion de l'organisation en tant que compte administrateur CSPM de Security Hub. Le compte administrateur CSPM de Security Hub peut activer n'importe quel compte d'organisation en tant que compte membre et peut également inviter d'autres comptes à devenir des comptes membres.

Un compte ne peut avoir qu'un seul compte administrateur. Un compte ne peut pas être à la fois un compte administrateur et un compte membre.

Région d'agrégation

La définition d'une région d'agrégation vous permet de visualiser les résultats de sécurité de plusieurs sources Régions AWS dans une seule fenêtre.

La région d'agrégation est la région à partir de laquelle vous visualisez et gérez les résultats. Les résultats sont agrégés à la région d'agrégation à partir des régions liées. Les mises à jour des résultats sont reproduites dans toutes les régions.

Dans la région d'agrégation, les pages Normes de sécurité , Insights et Findings incluent des données provenant de toutes les régions liées.

Pour de plus amples informations, veuillez consulter the section called "Agrégation des données entre les régions".

Résultat archivé

Une découverte dont l'état d'enregistrement est (`RecordState`)`ARCHIVED`. L'archivage d'un résultat indique que le fournisseur du résultat estime que celui-ci n'est plus pertinent. L'état de l'enregistrement est différent de l'état du flux de travail, qui permet de suivre l'état de l'enquête sur une découverte.

Les fournisseurs de recherche peuvent utiliser le BatchImportFindings fonctionnement de l'API CSPM Security Hub pour archiver les résultats qu'ils ont créés. Security Hub CSPM archive automatiquement les résultats des contrôles qui répondent à certains critères. Pour de plus amples informations, veuillez consulter Génération, mise à jour et archivage des résultats des contrôles.

Sur la console Security Hub CSPM, les paramètres de filtre par défaut excluent les résultats archivés des listes et des tableaux de recherche. Vous pouvez mettre à jour les paramètres pour inclure les résultats archivés. Si vous récupérez les résultats à l'aide de l'GetFindingsAPI CSPM de Security Hub, l'opération extrait à la fois les résultats archivés et les résultats actifs. Pour exclure les résultats archivés, vous pouvez filtrer les résultats. Par exemple :

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS Format de recherche de sécurité (ASFF)

Format normalisé pour le contenu des résultats que Security Hub CSPM regroupe ou génère. Le format AWS Security Finding vous permet d'utiliser Security Hub CSPM pour afficher et analyser les résultats générés par les services de sécurité, des solutions tierces ou AWS Security Hub CSPM lui-même à partir de l'exécution de contrôles de sécurité. Pour de plus amples informations, veuillez consulter AWS Format de recherche de sécurité (ASFF).

Contrôle

Protection ou contre-mesure prescrite pour un système d'information ou une organisation visant à protéger la confidentialité, l'intégrité et la disponibilité de ses informations, ainsi qu'à satisfaire à

un ensemble d'exigences de sécurité définies. Une norme de sécurité est associée à un ensemble de contrôles.

Le terme contrôle de sécurité fait référence aux contrôles qui ont un identifiant et un titre de contrôle uniques pour toutes les normes. Le terme contrôle standard fait référence aux contrôles qui ont des identifiants et des titres de contrôle spécifiques à la norme. Actuellement, Security Hub CSPM prend en charge les contrôles standard uniquement dans les régions chinoises et. AWS GovCloud (US) Regions Les contrôles de sécurité sont pris en charge dans toutes les autres régions.

Action personnalisée

Un mécanisme CSPM Security Hub pour envoyer les résultats sélectionnés à. EventBridge Une action personnalisée est créée dans Security Hub CSPM. Il est ensuite lié à une EventBridge règle. La règle définit une action spécifique à effectuer lorsqu'un résultat reçu est associé à l'ID de l'action personnalisée. Des actions personnalisées peuvent être utilisées, par exemple pour envoyer un résultat spécifique, ou un petit ensemble de résultats, vers un flux de travail de réponse ou de correction. Pour de plus amples informations, veuillez consulter the section called "Création d'une action personnalisée".

Compte administrateur délégué (organisations)

Dans AWS Organizations, le compte administrateur délégué d'un service est capable de gérer l'utilisation d'un service pour l'organisation.

Dans Security Hub CSPM, le compte administrateur Security Hub CSPM est également le compte administrateur délégué pour Security Hub CSPM. Lorsque le compte de gestion de l'organisation désigne pour la première fois un compte administrateur Security Hub CSPM, Security Hub CSPM appelle les organisations pour faire de ce compte le compte administrateur délégué.

Le compte de gestion de l'organisation doit ensuite choisir le compte d'administrateur délégué comme compte d'administrateur CSPM de Security Hub dans toutes les régions.

Résultat

Enregistrement observable d'une vérification de sécurité ou d'une détection liée à la sécurité. Security Hub CSPM génère et met à jour les résultats après avoir effectué les contrôles de sécurité. C'est ce que l'on appelle les résultats de contrôle. Les résultats peuvent également provenir d'intégrations avec d'autres produits Services AWS et des produits tiers.

Pour de plus amples informations, veuillez consulter the section called "Résultats".

Cross-Region agrégation

L'agrégation des résultats, des informations, des états de conformité des contrôles et des scores de sécurité des régions liées à une région d'agrégation. Vous pouvez ensuite consulter toutes vos données de la région d'agrégation et mettre à jour les résultats et les informations de la région d'agrégation.

Pour de plus amples informations, veuillez consulter the section called "Agrégation des données entre les régions".

Détecter l'ingestion

L'importation de résultats dans Security Hub CSPM à partir d'autres AWS services et de fournisseurs partenaires tiers.

La détection d'événements d'ingestion inclut à la fois de nouvelles découvertes et des mises à jour des résultats existants.

Informations

Ensemble de conclusions connexes définies par une déclaration d'agrégation et des filtres facultatifs. Un aperçu permet d'identifier une zone de sécurité qui nécessite une attention et une intervention. Security Hub CSPM propose plusieurs informations gérées (par défaut) que vous ne pouvez pas modifier. Vous pouvez également créer des informations CSPM personnalisées sur Security Hub pour suivre les problèmes de sécurité propres à votre AWS environnement et à votre utilisation. Pour de plus amples informations, veuillez consulter the section called "Informations".

Région liée

Lorsque vous activez l'agrégation interrégionale, une région liée est une région qui regroupe les résultats, les informations, contrôle les états de conformité et les scores de sécurité dans la région d'agrégation.

Dans une région liée, les pages Résultats et informations contiennent uniquement les résultats de cette région.

Pour de plus amples informations, veuillez consulter the section called "Agrégation des données entre les régions".

Compte membre

Compte qui a autorisé un compte administrateur à consulter ses résultats et à y donner suite.

Un compte devient un compte membre de l'une des manières suivantes :

- Le compte accepte une invitation provenant d'un autre compte.
- Pour un compte d'organisation, le compte administrateur CSPM de Security Hub active le compte en tant que compte de membre.

Exigences connexes

Ensemble d'exigences sectorielles ou réglementaires qui sont mappées à un contrôle.

Règle

Ensemble de critères automatisés utilisés pour évaluer si un contrôle est respecté. Lorsqu'une règle est évaluée, elle peut aboutir ou échouer. Si l'évaluation ne parvient pas à déterminer si la règle réussit ou échoue, la règle est alors dans un état d'avertissement. Si la règle ne peut pas être évaluée, son état est Non disponible.

Vérification de sécurité

Évaluation ponctuelle spécifique d'une règle par rapport à une ressource unique, aboutissant à un état `PASSED` `FAILED``WARNING`, ou`NOT_AVAILABLE`. L'exécution d'une vérification de sécurité génère un résultat.

Compte administrateur CSPM de Security Hub

Compte d'organisation qui gère l'adhésion à Security Hub CSPM pour une organisation.

Le compte de gestion de l'organisation désigne le compte administrateur CSPM de Security Hub dans chaque région. Le compte de gestion de l'organisation doit choisir le même compte administrateur Security Hub CSPM dans toutes les régions.

Le compte administrateur Security Hub CSPM est également le compte administrateur délégué pour Security Hub CSPM dans les organisations.

Le compte administrateur CSPM de Security Hub peut activer n'importe quel compte d'organisation en tant que compte de membre. Le compte administrateur du Security Hub CSPM peut également inviter d'autres comptes à devenir des comptes membres.

Norme de sécurité

Déclaration publiée sur un sujet et qui spécifie les caractéristiques, généralement mesurables et sous la forme de contrôles, qui doivent être satisfaites ou atteintes pour la conformité. Les normes de sécurité peuvent être basées sur des cadres réglementaires, des bonnes pratiques ou des

politiques internes de l'entreprise. Un contrôle peut être associé à une ou plusieurs normes prises en charge dans Security Hub CSPM. Pour en savoir plus sur les normes de sécurité dans Security Hub CSPM, consultez. Comprendre les normes de sécurité dans Security Hub CSPM

Sévérité

La sévérité attribuée à un contrôle CSPM Security Hub permet d'identifier l'importance de ce contrôle. La sévérité d'un contrôle peut être critique, élevée , moyenne, faible ou informative. La sévérité attribuée aux résultats du contrôle est égale à la gravité du contrôle lui-même. Pour en savoir plus sur la manière dont Security Hub CSPM attribue la gravité à un contrôle, consultez. Niveaux de gravité des résultats de contrôle

État du flux de travail

État d'avancement d'une enquête sur un résultat. Ceci est suivi à l'aide de l'`Workflow.Status`attribut.

L'état du flux de travail est initialement `NEW`. Si vous avez demandé au propriétaire de la ressource d'agir sur le résultat, vous pouvez définir l'état du flux de travail sur `NOTIFIED`. Si le résultat ne pose pas de problème et ne nécessite aucune action, définissez l'état du flux de travail sur `SUPPRESSED`. Après avoir examiné et corrigé un résultat, définissez l'état du flux de travail sur `RESOLVED`.

Par défaut, la plupart des listes de recherche incluent uniquement les résultats dont le statut de flux de travail est `NEW` ou `NOTIFIED`. Les listes de constatations pour les contrôles comprennent également les résultats `RESOLVED`.

Pour l'opération GetFindings, vous pouvez inclure un filtre sur l'état du flux de travail.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

La console Security Hub CSPM fournit une option permettant de définir l'état du flux de travail pour les résultats. Les clients (ou les outils SIEM, billetterie, gestion des incidents ou SOAR travaillant pour le compte d'un client pour mettre à jour les résultats des fournisseurs de recherche) peuvent également utiliser BatchUpdateFindings pour mettre à jour l'état du flux de travail.

Activation de Security Hub CSPM

Il existe deux manières d'activer AWS Security Hub CSPM : en l'intégrant AWS Organizations ou manuellement.

Nous vous recommandons vivement de procéder à l'intégration à Organizations pour les environnements multi-comptes et multi-régions. Si vous possédez un compte autonome, il est nécessaire de configurer Security Hub CSPM manuellement.

Vérification des autorisations nécessaires

Après vous être inscrit à Amazon Web Services (AWS), vous devez permettre à Security Hub CSPM d'utiliser ses capacités et fonctionnalités. Pour activer Security Hub CSPM, vous devez d'abord configurer des autorisations vous permettant d'accéder à la console Security Hub CSPM et aux opérations de l'API. Pour ce faire, vous ou votre AWS administrateur pouvez utiliser Gestion des identités et des accès AWS (IAM) pour associer la politique AWS gérée appelée `AWSSecurityHubFullAccess` à votre identité IAM.

Pour activer et gérer Security Hub CSPM via l'intégration des organisations, vous devez également joindre la politique AWS gérée appelée. `AWSSecurityHubOrganizationsAccess`

Pour de plus amples informations, veuillez consulter AWS politiques gérées pour Security Hub.

Activation de Security Hub CSPM avec l'intégration des organisations

Pour commencer à utiliser Security Hub CSPM avec AWS Organizations, le compte de AWS Organizations gestion de l'organisation désigne un compte en tant que compte administrateur CSPM Security Hub délégué pour l'organisation. Security Hub CSPM est automatiquement activé dans le compte administrateur délégué de la région actuelle.

Choisissez votre méthode préférée et suivez les étapes pour désigner l'administrateur délégué.

Security Hub CSPM console

Pour désigner l'administrateur CSPM délégué de Security Hub lors de l'intégration

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Accéder à Security Hub CSPM. Vous êtes invité à vous connecter au compte de gestion de l'organisation.

3. Sur la page Désigner un administrateur délégué, dans la section Compte administrateur délégué, spécifiez le compte administrateur délégué. Nous vous recommandons de choisir le même administrateur délégué que celui que vous avez défini pour les autres services AWS de sécurité et de conformité.
4. Choisissez Définir un administrateur délégué.

Security Hub CSPM API

Appelez l'`EnableOrganizationAdminAccount`API depuis le compte de gestion des organisations. Indiquez l' Compte AWS ID du compte administrateur délégué CSPM de Security Hub.

AWS CLI

Exécutez la `enable-organization-admin-account` commande depuis le compte de gestion des organisations. Indiquez l' Compte AWS ID du compte administrateur délégué CSPM de Security Hub.

Exemple de commande :

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Pour plus d'informations sur l'intégration avec les organisations, consultezIntégration de Security Hub CSPM àAWS Organizations.

Configuration centralisée

Lorsque vous intégrez Security Hub CSPM à des organisations, vous avez la possibilité d'utiliser une fonctionnalité appelée configuration centrale pour configurer et gérer Security Hub CSPM pour votre organisation. Nous vous recommandons vivement d'utiliser la configuration centralisée car elle permet à l'administrateur de personnaliser la couverture de sécurité pour l'organisation. Le cas échéant, l'administrateur délégué peut autoriser un compte membre à configurer ses propres paramètres de couverture de sécurité.

La configuration centralisée permet à l'administrateur délégué de configurer Security Hub CSPM entre les comptes, les unités d'organisation et. Régions AWS L'administrateur délégué configure Security Hub CSPM en créant des politiques de configuration. Dans le cadre d'une politique de configuration, vous pouvez spécifier les paramètres suivants :

- Si Security Hub CSPM est activé ou désactivé
- Quelles normes de sécurité sont activées et désactivées
- Quels contrôles de sécurité sont activés et désactivés
- S'il faut personnaliser les paramètres de certaines commandes

En tant qu'administrateur délégué, vous pouvez créer une politique de configuration unique pour l'ensemble de votre organisation ou différentes politiques de configuration pour vos différents comptes et unités d'organisation. Par exemple, les comptes de test et les comptes de production peuvent utiliser différentes politiques de configuration.

Les comptes membres et les unités d'organisation qui utilisent une politique de configuration sont gérés de manière centralisée et ne peuvent être configurés que par l'administrateur délégué. L'administrateur délégué peut désigner des comptes de membres et des unités d'organisation spécifiques comme étant autogérés afin de permettre au membre de configurer ses propres paramètres sur une Region-by-Region base.

Si vous n'utilisez pas la configuration centralisée, vous devez configurer Security Hub CSPM séparément pour chaque compte et chaque région. C'est ce que l'on appelle la configuration locale. Dans le cadre de la configuration locale, l'administrateur délégué peut activer automatiquement Security Hub CSPM et un ensemble limité de normes de sécurité dans les nouveaux comptes d'organisation de la région actuelle. La configuration locale ne s'applique pas aux comptes d'organisation existants ni aux régions autres que la région actuelle. La configuration locale ne prend pas non plus en charge l'utilisation de politiques de configuration.

Activation manuelle de Security Hub CSPM

Vous devez activer Security Hub CSPM manuellement si vous possédez un compte autonome ou si vous ne l'intégrez pas. AWS Organizations Les comptes autonomes ne peuvent pas être intégrés AWS Organizations et doivent utiliser l'activation manuelle.

Lorsque vous activez Security Hub CSPM manuellement, vous désignez un compte administrateur Security Hub CSPM et vous invitez d'autres comptes à devenir des comptes membres. La relation administrateur-membre est établie lorsqu'un compte de membre potentiel accepte l'invitation.

Choisissez votre méthode préférée et suivez les étapes pour activer Security Hub CSPM. Lorsque vous activez Security Hub CSPM depuis la console, vous avez également la possibilité d'activer les normes de sécurité prises en charge.

Security Hub CSPM console

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Lorsque vous ouvrez la console Security Hub CSPM pour la première fois, choisissez Accéder à Security Hub CSPM.
3. Sur la page d'accueil, la section Normes de sécurité répertorie les normes de sécurité prises en charge par Security Hub CSPM.

   Cochez la case correspondant à une norme pour l'activer, puis désactivez-la pour la désactiver.

   Vous pouvez activer ou désactiver une norme ou ses contrôles individuels à tout moment. Pour plus d'informations sur la gestion des normes de sécurité, consultezComprendre les normes de sécurité dans Security Hub CSPM.
4. Choisissez Enable Security Hub (Activer le hub de sécurité).

Security Hub CSPM API

Invoquez l'`EnableSecurityHub`API. Lorsque vous activez Security Hub CSPM depuis l'API, les normes de sécurité par défaut suivantes sont automatiquement activées :

- AWS Meilleures pratiques fondamentales en matière de sécurité
- Benchmark v1.2.0 des AWS fondations du Centre pour la sécurité Internet (CIS)

Si vous ne souhaitez pas activer ces normes, définissez `EnableDefaultStandards` sur `false`.

Vous pouvez également utiliser le `Tags` paramètre pour attribuer des valeurs de balise à la ressource du hub.

AWS CLI

Exécutez la commande `enable-security-hub`. Pour activer les normes par défaut, incluez`--enable-default-standards`. Pour ne pas activer les normes par défaut, incluez`--no-enable-default-standards`. Les normes de sécurité par défaut sont les suivantes :

- AWS Meilleures pratiques fondamentales en matière de sécurité
- Benchmark v1.2.0 des AWS fondations du Centre pour la sécurité Internet (CIS)

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Exemple

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Multi-account script d'activation

> **Note**
>
> Au lieu de ce script, nous vous recommandons d'utiliser une configuration centralisée pour activer et configurer Security Hub CSPM sur plusieurs comptes et régions.

Le script d'activation multi-comptes Security Hub CSPM vous GitHub permet d'activer Security Hub CSPM sur l'ensemble des comptes et des régions. Le script automatise également le processus d'envoi d'invitations aux comptes des membres et d'activation AWS Config.

Le script active automatiquement l'enregistrement AWS Config des ressources pour toutes les ressources, y compris les ressources globales, dans toutes les régions. Il ne limite pas l'enregistrement des ressources mondiales à une seule région. Pour réduire les coûts, nous vous recommandons d'enregistrer les ressources mondiales dans une seule région. Si vous utilisez la configuration centrale ou l'agrégation entre régions, il doit s'agir de votre région d'origine. Pour de plus amples informations, veuillez consulter Enregistrer des ressources dans AWS Config.

Il existe un script correspondant pour désactiver Security Hub CSPM sur tous les comptes et toutes les régions.

Prochaines étapes : gestion de la posture et intégrations

Après avoir activé Security Hub CSPM, nous vous recommandons d'activer les normes et contrôles de sécurité pour surveiller votre niveau de sécurité. Une fois que vous avez activé les contrôles, Security Hub CSPM commence à exécuter des contrôles de sécurité et à générer des résultats de contrôle qui vous aident à détecter les erreurs de configuration dans votre environnement. AWS Pour recevoir les résultats des contrôles, vous devez activer et configurer AWS Config Security Hub

CSPM. Pour de plus amples informations, veuillez consulter Activation et configuration AWS Config pour Security Hub CSPM.

Après avoir activé Security Hub CSPM, vous pouvez également tirer parti des intégrations entre Security Hub CSPM Services AWS et d'autres solutions tierces pour consulter leurs résultats dans Security Hub CSPM. Security Hub CSPM regroupe les résultats provenant de différentes sources et les ingère dans un format cohérent. Pour de plus amples informations, veuillez consulter Comprendre les intégrations dans Security Hub CSPM.

Activation et configuration AWS Config pour Security Hub CSPM

AWS Security Hub CSPM utilise des AWS Config règles pour exécuter des contrôles de sécurité et générer des résultats pour la plupart des contrôles. AWS Config fournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS. Il utilise des règles pour établir une configuration de base pour vos ressources et un enregistreur de configuration pour détecter si une ressource particulière enfreint les conditions d'une règle.

Certaines règles, appelées règles AWS Config gérées, sont prédéfinies et développées par AWS Config. Les autres règles sont des AWS Config règles personnalisées développées par Security Hub CSPM. AWS Config les règles utilisées par Security Hub CSPM pour les contrôles sont appelées règles liées aux services. Service-linked les règles permettent Services AWS , comme Security Hub CSPM, de créer des AWS Config règles dans votre compte.

Si AWS Security Hub CSPM et Security Hub sont activés, Security Hub CSPM crée automatiquement un enregistreur de configuration lié au service pour évaluer vos contrôles de sécurité. Il n'est pas nécessaire de l'activer ou de le configurer manuellement AWS Config. Pour de plus amples informations, veuillez consulter Utilisation de l'enregistreur de configuration lié au service.

Si Security Hub CSPM est activé sans Security Hub, vous devez activer AWS Config et activer manuellement l'enregistrement des ressources. Pour de plus amples informations, veuillez consulter Configuration manuelle AWS Config.

Les AWS Config prérequis décrits sur cette page s'appliquent uniquement aux normes de AWS sécurité, telles que les meilleures pratiques de sécurité AWS fondamentales et le benchmark des AWS fondations du CIS. Les normes multicloud, telles que CIS Azure Foundations Benchmark v4.0.0, ne vous obligent pas à activer l' AWS Config enregistrement ou à configurer un enregistreur de configuration. Le connecteur multicloud Security Hub CSPM configure automatiquement un enregistreur lié à un service pour évaluer les ressources cloud externes. La seule condition préalable aux normes multicloud est un connecteur Security Hub CSPM pour le fournisseur de cloud externe.

Rubriques

- Utilisation de l'enregistreur de configuration lié au service
- Configuration manuelle AWS Config
- Comprendre le Config.1 contrôle
- Génération de règles liées à un service

Utilisation de l'enregistreur de configuration lié au service

Lorsque AWS Security Hub CSPM et Security Hub sont activés, Security Hub CSPM crée et gère automatiquement un enregistreur de configuration lié à un service pour tous vos comptes et régions. Il n'est pas nécessaire de l'activer ou de le configurer manuellement AWS Config.

Le nom de cet enregistreur de configuration est`AWSConfigurationRecorderForSecurityHubCSPM`. Security Hub CSPM crée un enregistreur de configuration lié au service correspondant pour chaque compte et région dans lesquels Security Hub CSPM et Security Hub sont activés. Lorsque vous activez Security Hub CSPM pour de nouveaux Compte AWS s et Région AWS s, Security Hub CSPM crée automatiquement l'enregistreur de configuration lié au service.

Security Hub CSPM gère la configuration des ressources de l'enregistreur de configuration lié au service, en veillant à ce que l'enregistrement soit activé pour toutes les ressources liées aux contrôles pris en charge par Security Hub. Pour obtenir la liste des ressources requises, voirObligatoireAWS Configressources pour les résultats des contrôles.

Lorsque Security Hub CSPM crée cet enregistreur de configuration lié à un service, Security Hub n'utilise pas l'enregistreur de configuration géré par le client dans. AWS Config

Pour plus d'informations sur les enregistreurs de configuration, voir Utilisation de l'enregistreur de configuration dans le Guide du AWS Config développeur.

Configuration manuelle AWS Config

Les étapes suivantes s'appliquent lorsque Security Hub CSPM est activé sans Security Hub. Dans ce cas, vous devez activer AWS Config pour votre compte et activer l'enregistrement des ressources pour les types de ressources évalués par vos contrôles activés. Ensuite, Security Hub CSPM crée les AWS Config règles appropriées et commence à exécuter des contrôles de sécurité pour générer des résultats.

Considérations avant l'activation et la configuration AWS Config

Pour recevoir les résultats de contrôle dans Security Hub CSPM, celui-ci AWS Config doit être activé pour votre compte dans chaque Région AWS cas où Security Hub CSPM est activé. Si vous utilisez Security Hub CSPM pour un environnement multi-comptes, celui-ci AWS Config doit être activé dans chaque région pour le compte administrateur et tous les comptes membres.

Nous vous recommandons vivement d'activer l'enregistrement des ressources AWS Config avant d'activer les normes et contrôles CSPM du Security Hub. Cela vous permet de vous assurer que les résultats de vos contrôles sont exacts.

Pour activer l'enregistrement des ressources dans AWS Config, vous devez disposer des autorisations suffisantes pour enregistrer les ressources dans le rôle Gestion des identités et des accès AWS (IAM) attaché à l'enregistreur de configuration. En outre, assurez-vous qu'aucune politique ou AWS Organizations politique IAM n' AWS Config empêche d'avoir l'autorisation d'enregistrer vos ressources. Les contrôles CSPM du Security Hub évaluent directement les configurations des ressources et ne tiennent pas compte AWS Organizations des politiques. Pour plus d'informations sur AWS Config l'enregistrement, consultez la section Utilisation de l'enregistreur de configuration dans le Guide du AWS Config développeur.

Si vous activez une norme dans Security Hub CSPM mais que vous ne l'avez pas activée AWS Config, Security Hub CSPM essaie de créer des AWS Config règles liées au service selon le calendrier suivant :

- Le jour où vous activez la norme.
- Le lendemain de l'activation de la norme.
- 3 jours après avoir activé la norme.
- 7 jours après l'activation de la norme, puis en continu tous les 7 jours.

Si vous utilisez la configuration centralisée, Security Hub CSPM essaie également de créer des AWS Config règles liées aux services chaque fois que vous associez une politique de configuration qui active une ou plusieurs normes aux comptes, aux unités organisationnelles (UO) ou à la racine.

Enregistrer des ressources dans AWS Config

Lorsque vous l'activez AWS Config, vous devez spécifier les AWS ressources que l'enregistreur AWS Config de configuration doit enregistrer. Grâce aux règles liées au service, l'enregistreur de configuration permet à Security Hub CSPM de détecter les modifications apportées à la configuration de vos ressources.

Pour que Security Hub CSPM génère des résultats de contrôle précis, vous devez activer l'enregistrement AWS Config pour les types de ressources correspondant à vos contrôles activés. Il s'agit principalement de contrôles activés avec un type de calendrier déclenché par des modifications qui nécessitent un enregistrement des ressources. Certains contrôles dotés d'un type de calendrier périodique nécessitent également un enregistrement des ressources. Pour obtenir la liste de ces contrôles et des ressources correspondantes, consultezObligatoireAWS Configressources pour les résultats des contrôles.

> **Warning**
>
> Si vous ne configurez pas correctement AWS Config l'enregistrement pour les contrôles Security Hub CSPM, cela peut entraîner des résultats de contrôle inexacts, en particulier dans les cas suivants :
>
> - Vous n'avez jamais enregistré la ressource pour un contrôle donné, ou vous avez désactivé l'enregistrement d'une ressource avant de créer ce type de ressource. Dans ces cas, vous recevez un `WARNING` résultat pour le contrôle en question, même si vous avez peut-être créé des ressources dans le cadre du contrôle après avoir désactivé l'enregistrement. Il `WARNING` s'agit d'un résultat par défaut qui n'évalue pas réellement l'état de configuration de la ressource.
> - Vous désactivez l'enregistrement pour une ressource évaluée par un contrôle particulier. Dans ce cas, Security Hub CSPM conserve les résultats du contrôle générés avant que vous ne désactiviez l'enregistrement, même si le contrôle n'évalue pas les ressources nouvelles ou mises à jour. Security Hub CSPM modifie également le statut de conformité des résultats en. `WARNING` Ces résultats conservés peuvent ne pas refléter avec précision l'état de configuration actuel d'une ressource.

Par défaut, AWS Config enregistre toutes les ressources régionales prises en charge qu'il découvre dans le Région AWS système dans lequel il s'exécute. Pour recevoir tous les résultats du contrôle CSPM du Security Hub, vous devez également configurer AWS Config pour enregistrer les ressources globales. Pour réduire les coûts, nous recommandons d'enregistrer les ressources mondiales dans une seule région uniquement. Si vous utilisez la configuration centrale ou l'agrégation entre régions, cette région doit être votre région d'origine.

Dans AWS Config, vous pouvez choisir entre un enregistrement continu et un enregistrement quotidien des modifications de l'état des ressources. Si vous optez pour un enregistrement quotidien, AWS Config fournit les données de configuration des ressources à la fin de chaque période de

24 heures en cas de modification de l'état des ressources. S'il n'y a aucune modification, aucune donnée n'est transmise. Cela peut retarder la génération des résultats CSPM du Security Hub pour les contrôles déclenchés par des modifications jusqu'à ce qu'une période de 24 heures soit terminée.

Pour plus d'informations sur AWS Config l'enregistrement, consultez la section AWS Ressources relatives à l'enregistrement dans le Guide du AWS Config développeur.

Méthodes d'activation et de configuration AWS Config

Vous pouvez activer AWS Config et activer l'enregistrement des ressources de l'une des manières suivantes :

- AWS Config console — Vous pouvez activer un compte AWS Config à l'aide de la AWS Config console. Pour obtenir des instructions, consultez la section Configuration AWS Config avec la console dans le guide du AWS Config développeur.
- AWS CLI ou SDK : vous pouvez activer AWS Config un compte en utilisant le AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, consultez la section Configuration AWS Config avec le AWS CLI dans le guide du AWS Config développeur. AWS des kits de développement logiciel (SDK) sont également disponibles pour de nombreux langages de programmation.
- CloudFormation modèle — Pour l'activer AWS Config pour de nombreux comptes, nous vous recommandons d'utiliser le AWS CloudFormation modèle nommé Enable AWS Config. Pour accéder à ce modèle, consultez les AWS CloudFormation StackSet exemples de modèles dans le guide de AWS CloudFormation l'utilisateur.

  Par défaut, ce modèle exclut l'enregistrement pour les ressources globales IAM. Assurez-vous d'activer l'enregistrement pour les ressources mondiales IAM en une seule fois afin de réduire Région AWS les coûts d'enregistrement. Si l'agrégation entre régions est activée, il doit s'agir de votre région d'origine du Security Hub CSPM. Sinon, il peut s'agir de n'importe quelle région dans laquelle Security Hub CSPM est disponible et qui prend en charge l'enregistrement des ressources mondiales IAM. Nous vous recommandons d'en exécuter un StackSet pour enregistrer toutes les ressources, y compris les ressources globales IAM, dans la région d'origine ou dans une autre région sélectionnée. Exécutez ensuite une seconde StackSet pour enregistrer toutes les ressources, à l'exception des ressources globales IAM des autres régions.
- GitHub script : Security Hub CSPM propose un GitHubscript qui active Security Hub CSPM AWS Config pour plusieurs comptes dans toutes les régions. Ce script est utile si vous ne vous êtes pas intégré à une AWS Organizations organisation ou si vous possédez des comptes membres qui ne font pas partie d'une organisation.

Pour plus d'informations, consultez le billet de blog suivant sur le blog de AWS sécurité : Optimize AWS Config for AWS Security Hub CSPM pour gérer efficacement votre posture de sécurité dans le cloud.

Considérations de coût

Security Hub CSPM peut avoir un impact sur les coûts de votre enregistreur AWS Config de configuration en mettant à jour l'élément de `AWS::Config::ResourceCompliance` configuration. Des mises à jour peuvent avoir lieu chaque fois qu'un contrôle Security Hub CSPM associé à une AWS Config règle change d'état de conformité, est activé ou désactivé, ou comporte des mises à jour de paramètres. Si vous utilisez l'enregistreur de AWS Config configuration uniquement pour Security Hub CSPM et que vous n'utilisez pas cet élément de configuration à d'autres fins, nous vous recommandons de désactiver l'enregistrement dans. AWS Config Cela peut réduire vos AWS Config coûts. Vous n'avez pas besoin de vous enregistrer `AWS::Config::ResourceCompliance` pour que les contrôles de sécurité fonctionnent dans Security Hub CSPM.

Pour plus d'informations sur les coûts associés à l'enregistrement des ressources, consultez AWS la section Tarification et AWS Config tarification de Security Hub CSPM.

Comprendre le Config.1 contrôle

> **Note**
>
> Lorsque AWS Security Hub CSPM et Security Hub sont tous deux activés, le Config.1 contrôle a toujours un statut de. `PASSED` Security Hub CSPM a un accès direct aux éléments de configuration via un enregistreur de configuration lié à un service. Pour de plus amples informations, veuillez consulter Utilisation de l'enregistreur de configuration lié au service.

Dans Security Hub CSPM, le Config.1contrôle génère des `FAILED` résultats dans votre compte s'il AWS Config est désactivé. Il génère également des `FAILED` résultats dans votre compte s'il AWS Config est activé mais que l'enregistrement des ressources n'est pas activé.

Si cette option AWS Config est activée et que l'enregistrement des ressources est activé, mais que l'enregistrement des ressources n'est pas activé pour un type de ressource vérifié par un contrôle activé, Security Hub CSPM génère un `FAILED` résultat pour le Config.1 contrôle. Outre ce `FAILED` résultat, Security Hub CSPM génère des `WARNING` résultats concernant le contrôle activé et les types de ressources que le contrôle contrôle. Par exemple, si vous activez le KMS.5contrôle et que l'enregistrement des ressources n'est pas activé pour AWS KMS keys, Security Hub CSPM génère

un `FAILED` résultat pour le Config.1 contrôle. Security Hub CSPM génère également des `WARNING` résultats pour le KMS.5 contrôle et vos clés KMS.

Pour recevoir un `PASSED` résultat pour le Config.1 contrôle, activez l'enregistrement des ressources pour tous les types de ressources correspondant aux contrôles activés. Désactivez également les contrôles qui ne sont pas obligatoires pour votre organisation. Cela permet de s'assurer que vous ne présentez aucune lacune de configuration lors de vos contrôles de sécurité. Cela permet également de garantir que vous recevez des informations précises sur les ressources mal configurées.

Si vous êtes l'administrateur délégué du Security Hub CSPM d'une organisation, l' AWS Config enregistrement doit être correctement configuré pour votre compte et les comptes de vos membres. Si vous utilisez l'agrégation entre régions, AWS Config l'enregistrement doit être correctement configuré dans la région d'origine et dans toutes les régions liées. Les ressources mondiales n'ont pas besoin d'être enregistrées dans les régions liées.

Génération de règles liées à un service

Pour chaque contrôle utilisant une AWS Config règle liée à un service, Security Hub CSPM crée des instances de la règle requise dans votre environnement. AWS

Ces règles liées aux services sont spécifiques à Security Hub CSPM. Security Hub CSPM crée ces règles liées aux services même si d'autres instances des mêmes règles existent déjà. La règle liée au service est ajoutée `securityhub` avant le nom de règle d'origine et un identifiant unique après le nom de règle. Par exemple, pour la règle AWS Config géréevpc-flow-logs-enabled, le nom de la règle liée au service peut être. `securityhub-vpc-flow-logs-enabled-12345`

Il existe des quotas pour le nombre de règles AWS Config gérées qui peuvent être utilisées pour évaluer les contrôles. AWS Config les règles créées par Security Hub CSPM ne sont pas prises en compte dans ces quotas. Vous pouvez activer une norme de sécurité même si vous avez déjà atteint le AWS Config quota de règles gérées dans votre compte. Pour en savoir plus sur les quotas pour AWS Config les règles, consultez la section Limites AWS Config de service du Guide du AWS Config développeur.

> **Note**
>
> Si vous utilisez Security Hub (CSPM) et Security Hub, vous pouvez voir les règles liées aux services, AWS Config mais vous ne pourrez pas voir les ressources conformes ou non conformes associées à la règle. Les ressources conformes et non conformes ne seront visibles que dans Security Hub CSPM et Security Hub.

Comprendre la configuration locale dans Security Hub CSPM

La configuration locale est la méthode par défaut utilisée par défaut pour configurer une AWS organisation dans Security Hub CSPM. Si vous n'acceptez pas et n'activez pas la configuration centralisée, votre organisation utilise la configuration locale par défaut.

Dans le cadre de la configuration locale, le compte administrateur délégué du Security Hub CSPM dispose d'un contrôle limité sur les paramètres de configuration. Les seuls paramètres que l'administrateur délégué peut appliquer sont l'activation automatique du Security Hub CSPM et des normes de sécurité par défaut dans les nouveaux comptes d'entreprise. Ces paramètres s'appliquent uniquement dans la région dans laquelle vous avez désigné le compte d'administrateur délégué. Les normes de sécurité par défaut sont AWS Foundational Security Best Practices (FSBP) et Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Les paramètres de configuration locaux ne s'appliquent pas aux comptes d'organisation existants ni aux régions autres que celle dans laquelle le compte d'administrateur délégué a été désigné.

Outre l'activation du Security Hub CSPM et des normes par défaut dans les nouveaux comptes d'organisation d'une même région, vous devez configurer les autres paramètres du Security Hub CSPM, notamment les normes et les contrôles, séparément dans chaque région et chaque compte. Comme ce processus peut être dupliqué, nous vous recommandons d'utiliser une configuration centralisée pour un environnement multi-comptes si une ou plusieurs des conditions suivantes s'appliquent à vous :

- Vous souhaitez des paramètres de configuration différents pour les différentes parties de votre organisation (par exemple, différentes normes activées ou différents contrôles pour différentes équipes).
- Vous opérez dans plusieurs régions et souhaitez réduire le temps et la complexité liés à la configuration du service dans ces régions.
- Vous souhaitez que les nouveaux comptes utilisent des paramètres de configuration spécifiques lorsqu'ils rejoignent l'organisation.
- Vous souhaitez que les comptes d'organisation héritent des paramètres de configuration spécifiques d'un compte parent ou root.

Pour plus d'informations sur la configuration centrale, consultezComprendre la configuration centrale dans Security Hub CSPM.

Comprendre la configuration centrale dans Security Hub CSPM

La configuration centrale est une fonctionnalité AWS Security Hub CSPM qui vous aide à configurer et à gérer le Security Hub CSPM sur plusieurs et. Comptes AWS Régions AWS Pour utiliser la configuration centralisée, vous devez d'abord intégrer Security Hub CSPM et. AWS Organizations Vous pouvez intégrer les services en créant une organisation et en désignant un compte administrateur Security Hub CSPM délégué pour l'organisation.

À partir du compte administrateur délégué du Security Hub CSPM, vous pouvez activer le Security Hub CSPM pour les comptes et les unités organisationnelles (UO) de votre organisation dans toutes les régions. Vous pouvez également activer, configurer et désactiver les normes de sécurité et les contrôles de sécurité individuels pour les comptes et les unités d'organisation dans toutes les régions. Vous pouvez configurer ces paramètres en quelques étapes à partir d'une région principale, appelée région d'origine.

Lorsque vous utilisez la configuration centralisée, l'administrateur délégué peut choisir les comptes et les unités d'organisation à configurer. Si l'administrateur délégué désigne un compte membre ou une unité d'organisation comme étant autogéré, le membre peut configurer ses propres paramètres séparément dans chaque région. Si l'administrateur délégué désigne un compte membre ou une unité d'organisation comme étant géré de manière centralisée, seul l'administrateur délégué peut configurer le compte de membre ou l'unité d'organisation dans toutes les régions. Vous pouvez désigner tous les comptes et unités d'organisation de votre organisation comme étant gérés de manière centralisée, tous autogérés ou une combinaison des deux.

Pour configurer des comptes gérés de manière centralisée, l'administrateur délégué utilise les politiques de configuration CSPM de Security Hub. Les politiques de configuration permettent à l'administrateur délégué de spécifier si Security Hub CSPM est activé ou désactivé, et quelles normes et contrôles sont activés ou désactivés. Ils peuvent également être utilisés pour personnaliser les paramètres de certaines commandes.

Les politiques de configuration prennent effet dans la région d'origine et dans toutes les régions associées. L'administrateur délégué spécifie la région d'origine de l'organisation et les régions associées avant de commencer à utiliser la configuration centrale. La spécification de régions liées est facultative. L'administrateur délégué peut créer une politique de configuration unique pour l'ensemble de l'organisation ou créer plusieurs politiques de configuration pour configurer des paramètres variables pour différents comptes et unités d'organisation.

> **Tip**
>
> Si vous n'utilisez pas la configuration centralisée, vous devez configurer Security Hub CSPM séparément dans chaque compte et région. C'est ce qu'on appelle la configuration locale. Dans le cadre de la configuration locale, l'administrateur délégué peut automatiquement activer Security Hub CSPM et un ensemble limité de normes de sécurité dans les nouveaux comptes d'organisation de la région actuelle. La configuration locale ne s'applique pas aux comptes d'organisation existants ni aux régions autres que la région actuelle. La configuration locale ne prend pas non plus en charge l'utilisation de politiques de configuration.

Cette section fournit une vue d'ensemble de la configuration centrale.

Avantages de l'utilisation de la configuration centralisée

Les avantages de la configuration centralisée sont les suivants :

Simplifier la configuration du service et des fonctionnalités du Security Hub CSPM

Lorsque vous utilisez la configuration centralisée, Security Hub CSPM vous guide tout au long du processus de configuration des meilleures pratiques de sécurité pour votre entreprise. Il déploie également automatiquement les politiques de configuration qui en résultent sur des comptes et des unités d'organisation spécifiés. Si vous disposez de paramètres Security Hub CSPM existants, tels que l'activation automatique de nouveaux contrôles de sécurité, vous pouvez les utiliser comme point de départ pour vos politiques de configuration. En outre, la page de configuration de la console Security Hub CSPM affiche un résumé en temps réel de vos politiques de configuration et indique quels comptes et unités d'organisation utilisent chaque politique.

Configuration sur plusieurs comptes et régions

Vous pouvez utiliser la configuration centralisée pour configurer Security Hub CSPM sur plusieurs comptes et régions. Cela permet de garantir que chaque partie de votre organisation conserve une configuration cohérente et une couverture de sécurité adéquate.

Adapter différentes configurations aux différents comptes et unités d'organisation

Grâce à la configuration centralisée, vous pouvez choisir de configurer les comptes et les unités d'organisation de différentes manières. Par exemple, vos comptes de test et de production peuvent nécessiter des configurations différentes. Vous pouvez également créer une politique de configuration qui couvre les nouveaux comptes lorsqu'ils rejoignent l'organisation.

Empêcher la dérive de configuration

Une dérive de configuration se produit lorsqu'un utilisateur apporte une modification à un service ou à une fonctionnalité qui entre en conflit avec les sélections de l'administrateur délégué. La configuration centrale empêche cette dérive. Lorsque vous désignez un compte ou une unité d'organisation comme étant géré de manière centralisée, il n'est configurable que par l'administrateur délégué de l'organisation. Si vous préférez qu'un compte ou une unité d'organisation spécifique configure ses propres paramètres, vous pouvez le désigner comme autogéré.

Quand utiliser la configuration centralisée ?

La configuration centralisée est particulièrement avantageuse pour les AWS environnements qui incluent plusieurs comptes Security Hub CSPM. Il est conçu pour vous aider à gérer de manière centralisée le Security Hub CSPM pour plusieurs comptes.

Vous pouvez utiliser la configuration centralisée pour configurer le service Security Hub CSPM, les normes de sécurité et les contrôles de sécurité. Vous pouvez également l'utiliser pour personnaliser les paramètres de certaines commandes. Pour plus d'informations sur les normes de sécurité, consultezComprendre les normes de sécurité dans Security Hub CSPM. Pour plus d'informations sur les contrôles de sécurité, consultezComprendre les contrôles de sécurité dans Security Hub CSPM.

Termes et concepts de configuration centrale

La compréhension des termes et concepts clés suivants peut vous aider à utiliser la configuration centrale de Security Hub CSPM.

Configuration centrale

Une fonctionnalité Security Hub CSPM qui aide le compte administrateur Security Hub CSPM délégué d'une organisation à configurer le service Security Hub CSPM, les normes de sécurité et les contrôles de sécurité sur plusieurs comptes et régions. Pour configurer ces paramètres, l'administrateur délégué crée et gère les politiques de configuration Security Hub CSPM pour les comptes gérés de manière centralisée au sein de son organisation. Self-managed les comptes peuvent configurer leurs propres paramètres séparément dans chaque région. Pour utiliser la configuration centralisée, vous devez intégrer Security Hub CSPM et. AWS Organizations

Région d'origine

Région AWS À partir duquel l'administrateur délégué configure le Security Hub CSPM de manière centralisée, en créant et en gérant des politiques de configuration. Les politiques de configuration prennent effet dans la région d'origine et dans toutes les régions associées.

La région d'origine sert également de région d'agrégation CSPM du Security Hub, recevant les résultats, les informations et autres données des régions liées.

Les régions AWS introduites le 20 mars 2019 ou après cette date sont appelées régions optionnelles. Une région optionnelle ne peut pas être la région d'origine, mais elle peut être une région liée. Pour obtenir la liste des régions optionnelles, consultez la section Considérations à prendre en compte avant d'activer et de désactiver les régions dans le Guide de référence sur la gestion des AWS comptes.

Région liée

Et Région AWS qui est configurable depuis la région d'origine. Les politiques de configuration sont créées par l'administrateur délégué dans la région d'origine. Les politiques entrent en vigueur dans la région d'origine et dans toutes les régions associées. La spécification de régions liées est facultative.

Une région liée envoie également des résultats, des informations et d'autres données à la région d'origine.

Les régions AWS introduites le 20 mars 2019 ou après cette date sont appelées régions optionnelles. Vous devez activer une telle région pour un compte avant qu'une politique de configuration puisse lui être appliquée. Le compte de gestion des Organizations peut activer l'option « Régions » pour un compte membre. Pour plus d'informations, voir Spécifier les comptes que Régions AWS votre compte peut utiliser dans le Guide de référence sur la gestion des AWS comptes.

Cible

Une Compte AWS unité organisationnelle (UO) ou la racine de l'organisation.

Politique de configuration CSPM de Security Hub

Ensemble de paramètres Security Hub CSPM que l'administrateur délégué peut configurer pour des cibles gérées de manière centralisée. Cela inclut notamment les éléments suivants :

- S'il faut activer ou désactiver Security Hub CSPM.

- S'il faut activer une ou plusieurs normes de sécurité.
- Quels contrôles de sécurité activer dans le cadre des normes activées. L'administrateur délégué peut le faire en fournissant une liste de contrôles spécifiques qui doivent être activés, et Security Hub CSPM désactive tous les autres contrôles (y compris les nouveaux contrôles lorsqu'ils sont publiés). L'administrateur délégué peut également fournir une liste de contrôles spécifiques qui doivent être désactivés, et Security Hub CSPM active tous les autres contrôles (y compris les nouveaux contrôles lorsqu'ils sont publiés).
- Vous pouvez éventuellement personnaliser les paramètres pour sélectionner les commandes activées selon les normes activées.

Une politique de configuration prend effet dans la région d'origine et dans toutes les régions associées une fois qu'elle est associée à au moins un compte, une unité organisationnelle (UO) ou la racine.

Sur la console Security Hub CSPM, l'administrateur délégué peut choisir la politique de configuration recommandée par Security Hub CSPM ou créer des politiques de configuration personnalisées. Avec l'API CSPM de Security Hub AWS CLI, l'administrateur délégué ne peut créer que des politiques de configuration personnalisées. L'administrateur délégué peut créer un maximum de 20 politiques de configuration personnalisées.

Dans la politique de configuration recommandée, Security Hub CSPM, la norme AWS Foundational Security Best Practices (FSBP) et tous les contrôles FSBP existants et nouveaux sont activés. Les contrôles qui acceptent des paramètres utilisent les valeurs par défaut. La politique de configuration recommandée s'applique à l'ensemble de l'organisation.

Pour appliquer différents paramètres à l'organisation ou appliquer différentes politiques de configuration à différents comptes et unités d'organisation, créez une politique de configuration personnalisée.

> **Note**
>
> Les politiques de configuration prennent uniquement en charge les normes et les contrôles de AWS sécurité. Les normes multicloud, telles que CIS Azure Foundations Benchmark v4.0.0, et leurs contrôles multicloud associés ne peuvent pas être inclus dans une politique de configuration. Pour activer ou configurer les normes multicloud, utilisez les mécanismes de configuration locaux directement dans le périphérique souhaité. Compte AWS

Configuration locale

Type de configuration par défaut pour une organisation, après avoir intégré Security Hub CSPM et. AWS Organizations Avec la configuration locale, l'administrateur délégué peut choisir d'activer automatiquement le Security Hub CSPM et les normes de sécurité par défaut dans les nouveaux comptes d'organisation de la région actuelle. Si l'administrateur délégué active automatiquement les normes par défaut, tous les contrôles inclus dans ces normes sont également automatiquement activés avec les paramètres par défaut pour les nouveaux comptes d'organisation. Ces paramètres ne s'appliquent pas aux comptes existants. Une modification de la configuration est donc possible une fois qu'un compte a rejoint l'organisation. La désactivation de contrôles spécifiques faisant partie des normes par défaut et la configuration de normes et de contrôles supplémentaires doivent être effectuées séparément dans chaque compte et région.

La configuration locale ne prend pas en charge l'utilisation de politiques de configuration. Pour utiliser les politiques de configuration, vous devez passer à la configuration centralisée.

Gestion manuelle des comptes

Si vous n'intégrez pas Security Hub CSPM à Security Hub AWS Organizations ou si vous possédez un compte autonome, vous devez définir les paramètres de chaque compte séparément dans chaque région. La gestion manuelle des comptes ne prend pas en charge l'utilisation de politiques de configuration.

API de configuration centralisées

Opérations Security Hub CSPM que seul l'administrateur CSPM délégué au Security Hub peut utiliser dans la région d'origine pour gérer les politiques de configuration des comptes gérés de manière centralisée. Les opérations incluent :

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`

- `ListConfigurationPolicyAssociations`

Account-specific API

Opérations CSPM du Security Hub qui peuvent être utilisées pour activer ou désactiver le Security Hub CSPM, les normes et les contrôles compte par compte. Ces opérations sont utilisées dans chaque région.

Self-managed les comptes peuvent utiliser des opérations spécifiques au compte pour configurer leurs propres paramètres. Les comptes gérés de manière centralisée ne peuvent pas utiliser les opérations spécifiques suivantes dans la région d'origine et dans les régions associées. Dans ces régions, seul l'administrateur délégué peut configurer des comptes gérés de manière centralisée par le biais d'opérations de configuration et de politiques de configuration centralisées.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Pour vérifier l'état du compte, le propriétaire d'un compte géré de manière centralisée peut utiliser n'importe quelle `Get` `Describe` opération de l'API Security Hub CSPM.

Si vous utilisez la configuration locale ou la gestion manuelle des comptes, ces opérations spécifiques au compte peuvent être utilisées au lieu d'une configuration centralisée.

Self-managed les comptes peuvent également utiliser `*Invitations` et effectuer `*Members` des opérations. Toutefois, nous recommandons que les comptes autogérés n'utilisent pas ces opérations. Les associations de politiques peuvent échouer si un compte membre possède ses propres membres qui font partie d'une organisation différente de celle de l'administrateur délégué.

Unité d'organisation (UO)

Dans AWS Organizations and Security Hub CSPM, un conteneur pour un groupe de. Comptes AWS Une unité organisationnelle (UO) peut également contenir d'autres UO, ce qui vous permet de créer une hiérarchie qui ressemble à une arborescence renversée, avec une UO parent en haut et des branches d'UO descendantes pour aboutir à des comptes qui sont les feuilles de l'arbre. Une unité organisationnelle peut avoir exactement un parent, et chaque compte d'organisation peut être membre d'une seule unité organisationnelle.

Vous pouvez gérer les unités d'organisation dans AWS Organizations ou AWS Control Tower. Pour plus d'informations, voir Gestion des unités organisationnelles dans le Guide de l'AWS Organizations utilisateur ou Gouverner les organisations et les comptes avec AWS Control Tower dans le Guide de AWS Control Tower l'utilisateur.

L'administrateur délégué peut associer des politiques de configuration à des comptes ou à des unités d'organisation spécifiques, ou à la racine pour couvrir tous les comptes et unités d'organisation d'une organisation.

Géré de manière centralisée

Une cible que seul l'administrateur délégué peut configurer dans toutes les régions à l'aide de politiques de configuration.

Le compte d'administrateur délégué indique si une cible est gérée de manière centralisée. L'administrateur délégué peut également modifier le statut d'une cible de gestion centralisée à autogéré, ou inversement.

Self-managed

Une cible qui gère ses propres paramètres Security Hub CSPM. Une cible autogérée utilise des opérations spécifiques au compte pour configurer Security Hub CSPM séparément dans chaque région. Cela contraste avec les cibles gérées de manière centralisée, qui ne sont configurables que par l'administrateur délégué dans toutes les régions via des politiques de configuration.

Le compte d'administrateur délégué indique si une cible est autogérée. L'administrateur délégué peut appliquer un comportement autogéré à une cible. Un compte ou une unité d'organisation peut également hériter du comportement autogéré d'un parent.

Le compte d'administrateur délégué peut lui-même être un compte autogéré. Le compte d'administrateur délégué peut faire passer le statut d'une cible d'autogéré à géré de manière centralisée, ou inversement.

Association de politiques de configuration

Lien entre une politique de configuration et un compte, une unité organisationnelle (UO) ou un root. Lorsqu'une association de politiques existe, le compte, l'unité d'organisation ou le root utilise les paramètres définis par la politique de configuration. Une association existe dans l'un ou l'autre des cas suivants :

- Lorsque l'administrateur délégué applique directement une politique de configuration à un compte, à une unité d'organisation ou à un root

- Lorsqu'un compte ou une unité d'organisation hérite d'une politique de configuration d'une unité d'organisation parent ou de la racine

Une association existe jusqu'à ce qu'une configuration différente soit appliquée ou héritée.

Politique de configuration appliquée

Type d'association de politique de configuration dans lequel l'administrateur délégué applique directement une politique de configuration aux comptes cibles, aux unités d'organisation ou à la racine. Les cibles sont configurées conformément à la politique de configuration, et seul l'administrateur délégué peut modifier leur configuration. Si elle est appliquée à root, la politique de configuration affecte tous les comptes et unités d'organisation de l'organisation qui n'utilisent pas de configuration différente par le biais d'une application ou d'un héritage du parent le plus proche.

L'administrateur délégué peut également appliquer une configuration autogérée à des comptes spécifiques, à des unités d'organisation ou à la racine.

Politique de configuration héritée

Type d'association de politique de configuration dans lequel un compte ou une unité d'organisation adopte la configuration de l'unité d'organisation parent la plus proche ou de la racine. Si une politique de configuration n'est pas directement appliquée à un compte ou à une unité d'organisation, elle hérite de la configuration du parent le plus proche. Tous les éléments d'une politique sont hérités. En d'autres termes, un compte ou une unité d'organisation ne peut pas choisir d'hériter de manière sélective de certaines parties d'une politique. Si le parent le plus proche est autogéré, le compte enfant ou l'unité d'organisation hérite du comportement autogéré du parent.

L'héritage ne peut pas remplacer une configuration appliquée. En d'autres termes, si une politique de configuration ou une configuration autogérée est directement appliquée à un compte ou à une unité d'organisation, elle utilise cette configuration et n'hérite pas de la configuration du parent.

Racine

Dans AWS Organizations and Security Hub CSPM, le nœud parent de niveau supérieur d'une organisation. Si l'administrateur délégué applique une politique de configuration à root, celle-ci est associée à tous les comptes et unités d'organisation de l'organisation, sauf s'ils utilisent une stratégie différente, par le biais d'une application ou d'un héritage, ou s'ils sont désignés comme autogérés. Si l'administrateur désigne le root comme étant autogéré, tous les comptes et unités d'organisation de l'organisation sont autogérés, sauf s'ils utilisent une politique de configuration via une application ou un héritage. Si le root est autogéré et qu'aucune politique de configuration

n'existe actuellement, tous les nouveaux comptes de l'organisation conservent leurs paramètres actuels.

Les nouveaux comptes qui rejoignent une organisation sont considérés comme root jusqu'à ce qu'ils soient affectés à une unité d'organisation spécifique. Si aucun nouveau compte n'est attribué à une unité d'organisation, il hérite de la configuration racine, sauf si l'administrateur délégué le désigne comme un compte autogéré.

Activation de la configuration centralisée dans Security Hub CSPM

Le compte administrateur délégué du AWS Security Hub CSPM peut utiliser la configuration centrale pour configurer le Security Hub CSPM, les normes et les contrôles pour plusieurs comptes et unités organisationnelles (UO) répartis sur plusieurs comptes. Régions AWS

Pour obtenir des informations générales sur les avantages de la configuration centralisée et son fonctionnement, consultezComprendre la configuration centrale dans Security Hub CSPM.

Cette section explique les conditions requises pour la configuration centralisée et explique comment commencer à l'utiliser.

Prérequis pour une configuration centralisée

Avant de commencer à utiliser la configuration centralisée, vous devez intégrer Security Hub CSPM à une région d'origine AWS Organizations et lui désigner une région d'origine. Si vous utilisez la console Security Hub CSPM, ces prérequis sont inclus dans le flux de travail optionnel pour la configuration centralisée.

Intégrer aux Organisations

Vous devez intégrer Security Hub CSPM et Organizations pour utiliser la configuration centralisée.

Pour intégrer ces services, vous devez commencer par créer une organisation dans Organizations. À partir du compte de gestion Organizations, vous désignez ensuite un compte d'administrateur délégué Security Hub CSPM. Pour obtenir des instructions, veuillez consulter Intégration de Security Hub CSPM àAWS Organizations.

Assurez-vous de désigner votre administrateur délégué dans la région d'origine de votre choix. Lorsque vous commencez à utiliser la configuration centralisée, le même administrateur délégué est également automatiquement défini dans toutes les régions liées. Le compte de gestion des Organisations ne peut pas être défini comme compte d'administrateur délégué.

> **Important**
>
> Lorsque vous utilisez la configuration centralisée, vous ne pouvez pas utiliser la console Security Hub CSPM ou les API Security Hub CSPM pour modifier ou supprimer le compte administrateur délégué. Si le compte de gestion des Organizations utilise des AWS Organizations API pour modifier ou supprimer l'administrateur délégué du Security Hub CSPM, le Security Hub CSPM arrête automatiquement la configuration centrale. Vos politiques de configuration sont également dissociées et supprimées. Les comptes membres conservent la configuration qu'ils avaient avant le changement ou la suppression de l'administrateur délégué.

Désigner une région d'origine

Vous devez désigner une région d'origine pour utiliser la configuration centralisée. La région d'origine est la région à partir de laquelle l'administrateur délégué configure l'organisation.

> **Note**
>
> La région d'origine ne peut pas être une région désignée comme région optionnelle. AWS Une région optionnelle est désactivée par défaut. Pour obtenir la liste des régions optionnelles, consultez la section Considérations à prendre en compte avant d'activer et de désactiver les régions dans le Guide de référence sur la gestion des AWS comptes.

Vous pouvez éventuellement spécifier une ou plusieurs régions liées configurables à partir de la région d'origine.

L'administrateur délégué peut créer et gérer des politiques de configuration uniquement à partir de la région d'origine. Les politiques de configuration prennent effet dans la région d'origine et dans toutes les régions associées. Vous ne pouvez pas créer une politique de configuration qui s'applique uniquement à un sous-ensemble de ces régions, et pas à d'autres. Les contrôles impliquant des ressources globales font exception à cette règle. Si vous utilisez une configuration centralisée, Security Hub CSPM désactive automatiquement les contrôles impliquant des ressources globales dans toutes les régions, à l'exception de la région d'origine. Pour de plus amples informations, veuillez consulter Contrôles utilisant des ressources globales.

La région d'origine est également la région d'agrégation CSPM de votre Security Hub qui reçoit les résultats, les informations et autres données des régions liées.

Si vous avez déjà défini une région d'agrégation pour l'agrégation entre régions, il s'agit de votre région d'origine par défaut pour la configuration centrale. Vous pouvez modifier la région d'origine avant de commencer à utiliser la configuration centrale en supprimant votre agrégateur de recherche actuel et en créant un nouveau dans la région d'origine de votre choix. Un agrégateur de résultats est une ressource Security Hub CSPM qui indique la région d'origine et les régions associées.

Pour désigner une région d'origine, consultez les étapes de définition d'une région d'agrégation. Si vous possédez déjà une région d'origine, vous pouvez appeler l'GetFindingAggregatorAPI pour en savoir plus, notamment pour savoir quelles régions y sont actuellement liées.

Instructions pour activer la configuration centralisée

Choisissez votre méthode préférée et suivez les étapes pour activer la configuration centralisée pour votre organisation.

Security Hub CSPM console

Pour activer la configuration centrale (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Paramètres et configuration. Choisissez ensuite Démarrer la configuration centrale.

   Si vous vous inscrivez à Security Hub CSPM, choisissez Go to Security Hub CSPM.
3. Sur la page Désigner un administrateur délégué, sélectionnez votre compte d'administrateur délégué ou entrez son identifiant de compte. Le cas échéant, nous vous recommandons de choisir le même administrateur délégué que celui que vous avez défini pour les autres services AWS de sécurité et de conformité. Choisissez Définir un administrateur délégué.
4. Sur la page Centraliser l'organisation, dans la section Régions, sélectionnez votre région d'origine. Vous devez être connecté à votre région d'origine pour continuer. Si vous avez déjà défini une région d'agrégation pour l'agrégation entre régions, elle est affichée en tant que région d'origine. Pour modifier la région d'origine, choisissez Modifier les paramètres de la région. Vous pouvez ensuite sélectionner votre région d'origine préférée et revenir à ce flux de travail.
5. Sélectionnez au moins une région pour créer un lien vers la région d'origine. Vous pouvez également choisir si vous souhaitez lier automatiquement les futures régions prises en charge à la région d'origine. Les régions que vous sélectionnez ici seront configurables depuis

la région d'origine par l'administrateur délégué. Les politiques de configuration entrent en vigueur dans votre région d'origine et dans toutes les régions associées.

6. Choisissez Confirmer et continuez.
7. Vous pouvez désormais utiliser la configuration centralisée. Continuez à suivre les instructions de la console pour créer votre première politique de configuration. Si vous n'êtes pas encore prêt à créer une politique de configuration, choisissez Je ne suis pas encore prêt à configurer. Vous pouvez créer une politique ultérieurement en choisissant Paramètres et configuration dans le volet de navigation. Pour obtenir des instructions sur la création d'une politique de configuration, consultezCréation et association de politiques de configuration.

Security Hub CSPM API

Pour activer la configuration centrale (API)

1. À l'aide des informations d'identification du compte administrateur délégué, appelez l'UpdateOrganizationConfigurationAPI depuis la région d'origine.
2. Réglez le `AutoEnable` champ sur`false`.
3. Définissez le `ConfigurationType` champ de l'`OrganizationConfiguration`objet sur`CENTRAL`. Cette action a les conséquences suivantes :

   - Désigne le compte d'appel en tant qu'administrateur délégué du Security Hub CSPM dans toutes les régions liées.
   - Active le Security Hub CSPM dans le compte d'administrateur délégué dans toutes les régions liées.
   - Désigne le compte appelant en tant qu'administrateur délégué du Security Hub CSPM pour les comptes nouveaux et existants qui utilisent le Security Hub CSPM et appartiennent à l'organisation. Cela se produit dans la région d'origine et dans toutes les régions associées. Le compte appelant est défini comme administrateur délégué pour les nouveaux comptes d'organisation uniquement s'ils sont associés à une politique de configuration dans laquelle Security Hub CSPM est activé. Le compte d'appel est défini comme administrateur délégué pour les comptes d'organisation existants uniquement s'ils ont déjà activé Security Hub CSPM.
   - Définit AutoEnablesur `false` dans toutes les régions liées, et définit AutoEnableStandardssur `NONE` dans la région d'origine et toutes les régions liées. Ces paramètres ne sont pas pertinents dans les régions d'origine et associées lorsque vous utilisez la configuration centralisée, mais vous pouvez activer automatiquement le Security

Hub CSPM et les normes de sécurité par défaut dans les comptes de l'organisation en utilisant des politiques de configuration.

4. Vous pouvez désormais utiliser la configuration centralisée. L'administrateur délégué peut créer des politiques de configuration pour configurer Security Hub CSPM dans votre organisation. Pour obtenir des instructions sur la création d'une politique de configuration, consultezCréation et association de politiques de configuration.

Exemple de demande d'API :

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Pour activer la configuration centralisée (AWS CLI)

1. À l'aide des informations d'identification du compte administrateur délégué, exécutez la update-organization-configurationcommande depuis la région d'origine.
2. Incluez le paramètre `no-auto-enable`.
3. Définissez le `ConfigurationType` champ de l'`organization-configuration`objet sur`CENTRAL`. Cette action a les conséquences suivantes :

   - Désigne le compte d'appel en tant qu'administrateur délégué du Security Hub CSPM dans toutes les régions liées.
   - Active le Security Hub CSPM dans le compte d'administrateur délégué dans toutes les régions liées.
   - Désigne le compte appelant en tant qu'administrateur délégué du Security Hub CSPM pour les comptes nouveaux et existants qui utilisent le Security Hub CSPM et appartiennent à l'organisation. Cela se produit dans la région d'origine et dans toutes les régions associées. Le compte d'appel est défini comme administrateur délégué pour les nouveaux comptes d'organisation uniquement s'ils sont associés à une politique de configuration dans laquelle

Security Hub est activé. Le compte d'appel est défini comme administrateur délégué pour les comptes d'organisation existants uniquement s'ils ont déjà activé Security Hub CSPM.

- Définit l'option d'activation automatique sur « no-auto-enabledans toutes les régions liées », et sur « NONE dans la région auto-enable-standardsd'origine » et dans toutes les régions liées. Ces paramètres ne sont pas pertinents dans les régions d'origine et associées lorsque vous utilisez la configuration centralisée, mais vous pouvez activer automatiquement le Security Hub CSPM et les normes de sécurité par défaut dans les comptes de l'organisation en utilisant des politiques de configuration.

4. Vous pouvez désormais utiliser la configuration centralisée. L'administrateur délégué peut créer des politiques de configuration pour configurer Security Hub CSPM dans votre organisation. Pour obtenir des instructions sur la création d'une politique de configuration, consultezCréation et association de politiques de configuration.

Exemple de commande :

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Cibles gérées de manière centralisée et cibles autogérées

Lorsque vous activez la configuration centralisée, l'administrateur délégué du AWS Security Hub CSPM peut désigner chaque compte d'organisation, chaque unité organisationnelle (UO) et la racine comme étant gérés de manière centralisée ou autogérée. Le type de gestion d'une cible détermine la manière dont vous pouvez spécifier ses paramètres Security Hub CSPM.

Pour obtenir des informations générales sur les avantages de la configuration centralisée et son fonctionnement, consultezComprendre la configuration centrale dans Security Hub CSPM.

Cette section explique les différences entre une désignation gérée de manière centralisée et une désignation autogérée et explique comment choisir le type de gestion d'un compte, d'une unité d'organisation ou de la racine.

Self-managed

Le propriétaire d'un compte autogéré, d'une unité d'organisation ou d'un root doit configurer ses paramètres séparément dans chacun Région AWS d'eux. L'administrateur délégué ne peut pas créer de politiques de configuration pour les cibles autogérées.

Géré de manière centralisée

Seul l'administrateur délégué du Security Hub CSPM peut configurer les paramètres des comptes gérés de manière centralisée, des unités d'organisation ou de la racine dans la région d'origine et les régions associées. Les politiques de configuration peuvent être associées à des comptes et à des unités d'organisation gérés de manière centralisée.

L'administrateur délégué peut changer le statut d'une cible entre autogéré et géré de manière centralisée. Par défaut, tous les comptes et unités d'organisation sont autogérés lorsque vous démarrez la configuration centralisée via l'API Security Hub CSPM. Dans la console, le type de gestion dépend de votre première politique de configuration. Les comptes et les unités d'organisation que vous associez à votre première politique sont gérés de manière centralisée. Les autres comptes et unités d'organisation sont autogérés par défaut.

Si vous associez une politique de configuration à un compte précédemment autogéré, les paramètres de stratégie remplacent la désignation autogérée. Le compte est géré de manière centralisée et adopte les paramètres reflétés dans la politique de configuration.

Si vous remplacez un compte géré de manière centralisée par un compte autogéré, les paramètres précédemment appliqués au compte par le biais d'une politique de configuration restent en place. Par exemple, un compte géré de manière centralisée peut initialement être associé à une politique activant Security Hub CSPM, activant les meilleures pratiques de sécurité AWS fondamentales et désactivée. CloudTrail.1 Si vous indiquez ensuite que le compte est autogéré, tous les paramètres restent inchangés. Toutefois, le titulaire du compte peut modifier indépendamment les paramètres du compte à l'avenir.

Les comptes enfants et les unités d'organisation peuvent hériter du comportement autogéré d'un parent autogéré, de la même manière que les comptes enfants et les unités d'organisation peuvent hériter des politiques de configuration d'un parent géré de manière centralisée. Pour de plus amples informations, veuillez consulter Association des politiques par le biais de l'application et de l'héritage.

Un compte ou une unité d'organisation autogéré ne peut pas hériter d'une politique de configuration d'un nœud parent ou de la racine. Par exemple, si vous souhaitez que tous les comptes et unités d'organisation de votre organisation héritent d'une politique de configuration provenant de la racine,

vous devez remplacer le type de gestion des nœuds autogérés par des nœuds gérés de manière centralisée.

Options pour configurer les paramètres dans les comptes autogérés

Self-managed les comptes doivent configurer leurs propres paramètres séparément dans chaque région.

Les propriétaires de comptes autogérés peuvent invoquer les opérations suivantes de l'API Security Hub CSPM dans chaque région pour configurer leurs paramètres :

- `EnableSecurityHub`et `DisableSecurityHub` pour activer ou désactiver le service Security Hub CSPM (si un compte autogéré dispose d'un administrateur Security Hub CSPM délégué, l'administrateur doit dissocier le compte avant que le propriétaire du compte puisse désactiver Security Hub CSPM).
- `BatchEnableStandards`et `BatchDisableStandards` pour activer ou désactiver les normes
- `BatchUpdateStandardsControlAssociations`ou `UpdateStandardsControl` pour activer ou désactiver les commandes

Self-managed les comptes peuvent également utiliser `*Invitations` et effectuer `*Members` des opérations. Toutefois, nous recommandons que les comptes autogérés n'utilisent pas ces opérations. Les associations de politiques peuvent échouer si un compte membre possède ses propres membres qui font partie d'une organisation différente de celle de l'administrateur délégué.

Pour obtenir une description des actions de l'API CSPM de Security Hub, consultez le document de référence de l'API CSPM du AWS Security Hub.

Self-managed les comptes peuvent également utiliser la console Security Hub CSPM ou AWS CLI configurer leurs paramètres dans chaque région.

Self-managed les comptes ne peuvent invoquer aucune API liée aux politiques de configuration et aux associations de politiques du Security Hub CSPM. Seul l'administrateur délégué peut invoquer des API de configuration centrales et utiliser des politiques de configuration pour configurer des comptes gérés de manière centralisée.

Choix du type de gestion d'une cible

Choisissez votre méthode préférée et suivez les étapes pour désigner un compte ou une unité d'organisation comme étant géré de manière centralisée ou autogérée dans AWS Security Hub CSPM.

Security Hub CSPM console

Pour choisir le type de gestion d'un compte ou d'une unité d'organisation

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Choisissez Configuration.
3. Dans l'onglet Organisation, sélectionnez le compte ou l'unité d'organisation cible. Choisissez Modifier.
4. Sur la page Définir la configuration, pour Type de gestion, choisissez Gestion centralisée si vous souhaitez que l'administrateur délégué configure le compte ou l'unité d'organisation cible. Choisissez ensuite Appliquer une politique spécifique si vous souhaitez associer une politique de configuration existante à la cible. Choisissez Hériter de mon organisation si vous souhaitez que la cible hérite de la configuration de son parent le plus proche. Choisissez Self-managedsi vous souhaitez que le compte ou l'unité d'organisation configure ses propres paramètres.
5. Choisissez Suivant. Passez en revue vos modifications, puis choisissez Enregistrer.

Security Hub CSPM API

Pour choisir le type de gestion d'un compte ou d'une unité d'organisation

1. Appelez l'StartConfigurationPolicyAssociationAPI depuis le compte d'administrateur délégué CSPM de Security Hub dans la région d'origine.
2. Dans le `ConfigurationPolicyIdentifier` champ, indiquez `SELF_MANAGED_SECURITY_HUB` si vous souhaitez que le compte ou l'unité d'organisation contrôle ses propres paramètres. Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration appropriée si vous souhaitez que l'administrateur délégué contrôle les paramètres du compte ou de l'unité d'organisation.
3. Pour le `Target` champ, indiquez l'Compte AWSID, l'ID de l'UO ou l'ID racine de la cible dont vous souhaitez modifier le type de gestion. Cela associe le comportement autogéré ou la politique de configuration spécifiée à la cible. Les comptes enfants de la cible peuvent hériter du comportement autogéré ou de la politique de configuration.

Exemple de demande d'API pour désigner un compte autogéré :

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Pour choisir le type de gestion d'un compte ou d'une unité d'organisation

1. Exécutez la start-configuration-policy-associationcommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine.
2. Dans le `configuration-policy-identifier` champ, indiquez `SELF_MANAGED_SECURITY_HUB` si vous souhaitez que le compte ou l'unité d'organisation contrôle ses propres paramètres. Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration appropriée si vous souhaitez que l'administrateur délégué contrôle les paramètres du compte ou de l'unité d'organisation.
3. Pour le `target` champ, indiquez l'Compte AWSID, l'ID de l'UO ou l'ID racine de la cible dont vous souhaitez modifier le type de gestion. Cela associe le comportement autogéré ou la politique de configuration spécifiée à la cible. Les comptes enfants de la cible peuvent hériter du comportement autogéré ou de la politique de configuration.

Exemple de commande pour désigner un compte autogéré :

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Fonctionnement des politiques de configuration dans Security Hub CSPM

L'administrateur délégué du AWS Security Hub CSPM peut créer des politiques de configuration pour configurer le Security Hub CSPM, les normes de sécurité et les contrôles de sécurité pour une organisation. Après avoir créé une politique de configuration, l'administrateur délégué peut l'associer à des comptes spécifiques, à des unités organisationnelles (UO) ou à la racine. La politique prend ensuite effet dans les comptes, les unités d'organisation ou la racine spécifiés.

Pour obtenir des informations générales sur les avantages de la configuration centralisée et son fonctionnement, consultezComprendre la configuration centrale dans Security Hub CSPM.

Cette section fournit un aperçu détaillé des politiques de configuration.

Considérations relatives aux politiques

Avant de créer une politique de configuration dans Security Hub CSPM, prenez en compte les informations suivantes.

- Les politiques de configuration doivent être associées pour prendre effet : après avoir créé une politique de configuration, vous pouvez l'associer à un ou plusieurs comptes, unités organisationnelles (UO) ou à la racine. Une politique de configuration peut être associée à des comptes ou à des unités d'organisation par le biais d'une application directe ou par héritage d'une unité d'organisation parent.
- Un compte ou une unité d'organisation ne peut être associé qu'à une seule stratégie de configuration : pour éviter tout conflit de paramètres, un compte ou une unité d'organisation ne peut être associé qu'à une seule politique de configuration à la fois. Un compte ou une unité d'organisation peut également être autogéré.
- Les politiques de configuration sont complètes : les politiques de configuration fournissent une spécification complète des paramètres. Par exemple, un compte enfant ne peut pas accepter les paramètres de certains contrôles d'une politique et les paramètres d'autres contrôles d'une autre politique. Lorsque vous associez une politique à un compte enfant, assurez-vous que la politique spécifie tous les paramètres que vous souhaitez que le compte enfant utilise.
- Les politiques de configuration ne peuvent pas être annulées : il n'est pas possible d'annuler une politique de configuration une fois que vous l'avez associée à des comptes ou à des unités d'organisation. Par exemple, si vous associez une politique de configuration qui désactive les CloudWatch contrôles à un compte spécifique, puis que vous dissociez cette politique, les CloudWatch contrôles continuent d'être désactivés dans ce compte. Pour réactiver CloudWatch les contrôles, vous pouvez associer le compte à une nouvelle politique qui active les contrôles. Vous pouvez également transformer le compte en compte autogéré et activer chaque CloudWatch contrôle du compte.
- Les politiques de configuration prennent effet dans votre région d'origine et dans toutes les régions liées : une politique de configuration affecte tous les comptes associés dans la région d'origine et toutes les régions liées. Vous ne pouvez pas créer une politique de configuration qui ne s'applique que dans certaines de ces régions et pas dans d'autres. Les contrôles qui utilisent des ressources

globales font exception à cette règle. Security Hub CSPM désactive automatiquement les contrôles impliquant des ressources globales dans toutes les régions, à l'exception de la région d'origine.

Les régions AWS introduites le 20 mars 2019 ou après cette date sont appelées régions optionnelles. Vous devez activer une telle région pour un compte avant qu'une politique de configuration n'y prenne effet. Le compte de gestion des Organizations peut activer l'option « Régions » pour un compte membre. Pour obtenir des instructions sur l'activation des régions optionnelles, voir Spécifier les régions que Régions AWS votre compte peut utiliser dans le Guide de référence AWS sur la gestion des comptes.

Si votre politique configure un contrôle qui n'est pas disponible dans la région d'origine ou dans une ou plusieurs régions liées, Security Hub CSPM ignore la configuration du contrôle dans les régions non disponibles mais applique la configuration dans les régions où le contrôle est disponible. Vous n'êtes pas couvert pour un contrôle qui n'est pas disponible dans la région d'origine ou dans l'une des régions associées.

- Les politiques de configuration sont des ressources : en tant que ressource, une politique de configuration possède un Amazon Resource Name (ARN) et un identifiant unique universel (UUID). L'ARN utilise le format suivant : `arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`* Une configuration autogérée ne possède ni ARN ni UUID. L'identifiant d'une configuration autogérée est`SELF_MANAGED_SECURITY_HUB`.
- Les normes multicloud ne sont pas prises en charge dans les politiques de configuration. Les politiques de configuration ne peuvent inclure que des normes et des contrôles AWS de sécurité. Les normes multicloud, telles que CIS Azure Foundations Benchmark v4.0.0, et leurs contrôles associés (par exemple,`Azure.Storage.1`) ne peuvent pas être inclus dans une politique de configuration. Si vous incluez un ARN ou un ID de contrôle standard multicloud dans une politique de configuration, la demande renvoie un`InvalidInputException`. Pour activer ou configurer les normes multicloud, utilisez les mécanismes de configuration locaux directement dans le périphérique souhaité. Compte AWS

Types de politiques de configuration

Chaque politique de configuration définit les paramètres suivants :

- Activez ou désactivez Security Hub CSPM.
- Activez une ou plusieurs normes de sécurité.

- Indiquez quels contrôles de sécurité sont activés dans le cadre des normes activées. Vous pouvez le faire en fournissant une liste de contrôles spécifiques qui doivent être activés, et Security Hub CSPM désactive tous les autres contrôles, y compris les nouveaux contrôles lorsqu'ils sont publiés. Vous pouvez également fournir une liste de contrôles spécifiques qui doivent être désactivés, et Security Hub CSPM active tous les autres contrôles, y compris les nouveaux contrôles lorsqu'ils sont publiés.
- Vous pouvez éventuellement personnaliser les paramètres pour sélectionner les contrôles activés selon les normes activées.

Les politiques de configuration centrales n'incluent pas les paramètres de l' AWS Config enregistreur. Vous devez activer AWS Config et activer séparément l'enregistrement pour les ressources requises afin que Security Hub CSPM puisse générer des résultats de contrôle. Pour de plus amples informations, veuillez consulter Considérations avant l'activation et la configuration AWS Config.

Si vous utilisez une configuration centralisée, Security Hub CSPM désactive automatiquement les contrôles impliquant des ressources globales dans toutes les régions, à l'exception de la région d'origine. Les autres contrôles que vous choisissez d'activer par le biais d'une politique de configuration sont activés dans toutes les régions où ils sont disponibles. Pour limiter les résultats de ces contrôles à une seule région, vous pouvez mettre à jour les paramètres de votre AWS Config enregistreur et désactiver l'enregistrement des ressources globales dans toutes les régions, à l'exception de la région d'origine.

Si un contrôle activé impliquant des ressources globales n'est pas pris en charge dans la région d'origine, Security Hub CSPM essaie d'activer le contrôle dans une région liée où le contrôle est pris en charge. Avec la configuration centralisée, vous ne pouvez pas couvrir un contrôle qui n'est pas disponible dans la région d'origine ou dans l'une des régions associées.

Pour obtenir la liste des contrôles impliquant des ressources globales, voirContrôles utilisant des ressources globales.

Politique de configuration recommandée

Lorsque vous créez une politique de configuration pour la première fois dans la console Security Hub CSPM, vous avez la possibilité de choisir la politique recommandée par Security Hub CSPM.

La politique recommandée active Security Hub CSPM, la norme AWS Foundational Security Best Practices (FSBP) et tous les contrôles FSBP existants et nouveaux. Les contrôles qui acceptent des paramètres utilisent les valeurs par défaut. La politique recommandée s'applique au root (tous les

comptes et unités d'organisation, qu'ils soient nouveaux ou existants). Après avoir créé la politique recommandée pour votre organisation, vous pouvez la modifier à partir du compte d'administrateur délégué. Par exemple, vous pouvez activer des normes ou des contrôles supplémentaires ou désactiver des contrôles FSBP spécifiques. Pour obtenir des instructions sur la modification d'une politique de configuration, consultezMise à jour des politiques de configuration.

Politique de configuration personnalisée

Au lieu de la stratégie recommandée, l'administrateur délégué peut créer jusqu'à 20 politiques de configuration personnalisées. Vous pouvez associer une seule politique personnalisée à l'ensemble de votre organisation ou différentes politiques personnalisées à différents comptes et unités d'organisation. Pour une politique de configuration personnalisée, vous devez spécifier les paramètres souhaités. Par exemple, vous pouvez créer une politique personnalisée qui active le FSBP, le Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 et tous les contrôles de ces normes, à l'exception des contrôles Amazon Redshift. Le niveau de granularité que vous utilisez dans les politiques de configuration personnalisées dépend de l'étendue de la couverture de sécurité prévue dans l'ensemble de votre organisation.

> **Note**
>
> Vous ne pouvez pas associer une politique de configuration qui désactive Security Hub CSPM au compte d'administrateur délégué. Une telle politique peut être associée à d'autres comptes mais ignore l'association avec l'administrateur délégué. Le compte d'administrateur délégué conserve sa configuration actuelle.

Après avoir créé une politique de configuration personnalisée, vous pouvez passer à la stratégie de configuration recommandée en mettant à jour votre stratégie de configuration afin de refléter la configuration recommandée. Cependant, vous ne voyez pas la possibilité de créer la politique de configuration recommandée dans la console Security Hub CSPM après la création de votre première politique.

Association des politiques par le biais de l'application et de l'héritage

Lorsque vous optez pour la première fois pour la configuration centralisée, votre organisation n'a aucune association et se comporte de la même manière qu'avant l'inscription. L'administrateur délégué peut ensuite établir des associations entre une politique de configuration ou un comportement autogéré et des comptes, des unités d'organisation ou la racine. Les associations peuvent être créées par voie de demande ou d'héritage.

À partir du compte d'administrateur délégué, vous pouvez appliquer directement une politique de configuration à un compte, à une unité d'organisation ou à la racine. L'administrateur délégué peut également appliquer directement une désignation autogérée à un compte, à une unité d'organisation ou à la racine.

En l'absence d'application directe, un compte ou une unité d'organisation hérite des paramètres du parent le plus proche doté d'une politique de configuration ou d'un comportement autogéré. Si le parent le plus proche est associé à une politique de configuration, l'enfant hérite de cette politique et n'est configurable que par l'administrateur délégué de la région d'origine. Si le parent le plus proche est autogéré, l'enfant hérite du comportement autogéré et a la possibilité de spécifier ses propres paramètres dans chacun d'eux. Région AWS

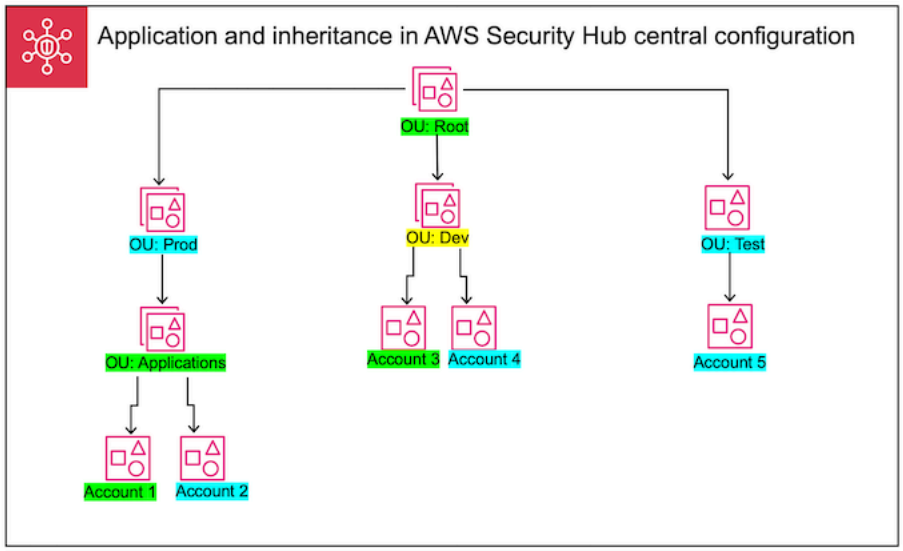
L'application a la priorité sur l'héritage. En d'autres termes, l'héritage ne remplace pas une politique de configuration ou une désignation autogérée que l'administrateur délégué a directement appliquée à un compte ou à une unité d'organisation.

Si vous appliquez directement une politique de configuration à un compte autogéré, cette politique remplace la désignation autogérée. Le compte est géré de manière centralisée et adopte les paramètres reflétés dans la politique de configuration.

Nous recommandons d'appliquer directement une politique de configuration à la racine. Si vous appliquez une politique à la racine, les nouveaux comptes qui rejoignent votre organisation hériteront automatiquement de la politique racine, sauf si vous les associez à une autre stratégie ou si vous les désignez comme autogérés.

Une seule politique de configuration peut être associée à un compte ou à une unité d'organisation à la fois, par le biais d'une application ou d'un héritage. Ceci est conçu pour éviter les conflits de paramètres.

Le schéma suivant illustre le fonctionnement de l'application des politiques et de l'héritage dans une configuration centrale.



Dans cet exemple, une politique de configuration est appliquée à un nœud surligné en vert. Aucune politique de configuration n'est appliquée à un nœud surligné en bleu. Un nœud surligné en jaune a été désigné comme étant autogéré. Chaque compte et unité d'organisation utilise la configuration suivante :

- OU:Root (Vert) — Cette unité d'organisation utilise la politique de configuration qui lui a été appliquée.
- OU:Prod (Bleu) — Cette unité d'organisation hérite de la politique de configuration de OU:Root.
- OU:Applications (Vert) — Cette unité d'organisation utilise la politique de configuration qui lui a été appliquée.
- Compte 1 (vert) — Ce compte utilise la politique de configuration qui lui a été appliquée.
- Compte 2 (bleu) — Ce compte hérite de la politique de configuration de OU:Applications.
- OU:Dev (Jaune) — Cette UO est autogérée.
- Compte 3 (vert) — Ce compte utilise la politique de configuration qui lui a été appliquée.
- Compte 4 (bleu) — Ce compte hérite du comportement autogéré de. OU:Dev
- OU:Test (Bleu) — Ce compte hérite de la politique de configuration de OU:Root.
- Compte 5 (bleu) — Ce compte hérite de la politique de configuration OU:Root puisque son parent immédiat n'est pas associé à une politique de configuration. OU:Test

Tester une politique de configuration

Pour vous assurer de bien comprendre le fonctionnement des politiques de configuration, nous vous recommandons d'en créer une et de l'associer à un compte de test ou à une unité d'organisation.

Pour tester une politique de configuration

1. Créez une politique de configuration personnalisée et vérifiez que les paramètres spécifiés pour l'activation, les normes et les contrôles de Security Hub CSPM sont corrects. Pour obtenir des instructions, veuillez consulter Création et association de politiques de configuration.
2. Appliquez la politique de configuration à un compte de test ou à une unité d'organisation qui ne possède aucun compte enfant ou unité d'organisation.
3. Vérifiez que le compte de test ou l'unité d'organisation utilise la politique de configuration de la manière prévue dans votre région d'origine et dans toutes les régions associées. Vous pouvez également vérifier que tous les autres comptes et unités d'organisation de votre organisation restent autogérés et peuvent modifier leurs propres paramètres dans chaque région.

Après avoir testé une politique de configuration dans un seul compte ou unité d'organisation, vous pouvez l'associer à d'autres comptes et unités d'organisation.

Création et association de politiques de configuration

Le compte administrateur délégué du AWS Security Hub CSPM peut créer des politiques de configuration qui spécifient la manière dont le Security Hub CSPM, les normes et les contrôles sont configurés dans des comptes et des unités d'organisation (UO) spécifiés. Une politique de configuration ne prend effet qu'une fois que l'administrateur délégué l'a associée à au moins un compte ou une unité organisationnelle (UO), ou à la racine. L'administrateur délégué peut également associer une configuration autogérée à des comptes, à des unités d'organisation ou à l'utilisateur root.

Si c'est la première fois que vous créez une politique de configuration, nous vous recommandons de la vérifier d'abordFonctionnement des politiques de configuration dans Security Hub CSPM.

> **Note**
>
> Les politiques de configuration ne prennent en charge que les AWS normes et les contrôles. Vous ne pouvez pas inclure de normes multicloud (telles que CIS Azure Foundations Benchmark v4.0.0) ou de contrôles Azure dans une politique de configuration. Incluant un ARN standard multicloud ou un identifiant de contrôle, `InvalidInputException` renvois. Pour activer ou configurer les normes multicloud, utilisez les mécanismes de configuration locaux directement dans le périphérique souhaité. Compte AWS

Choisissez votre méthode d'accès préférée et suivez les étapes pour créer et associer une politique de configuration ou une configuration autogérée. Lorsque vous utilisez la console Security Hub CSPM, vous pouvez associer une configuration à plusieurs comptes ou unités d'organisation en même temps. Lorsque vous utilisez l'API Security Hub CSPM ou AWS CLI, vous ne pouvez associer une configuration qu'à un seul compte ou unité d'organisation par demande.

> **Note**
>
> Si vous utilisez une configuration centralisée, Security Hub CSPM désactive automatiquement les contrôles impliquant des ressources globales dans toutes les régions, à l'exception de la région d'origine. Les autres contrôles que vous choisissez d'activer par le biais d'une politique de configuration sont activés dans toutes les régions où ils sont disponibles. Pour limiter les résultats de ces contrôles à une seule région, vous pouvez mettre à jour les paramètres de votre AWS Config enregistreur et désactiver l'enregistrement des ressources globales dans toutes les régions, à l'exception de la région d'origine.
> Si un contrôle activé impliquant des ressources globales n'est pas pris en charge dans la région d'origine, Security Hub CSPM essaie d'activer le contrôle dans une région liée où le contrôle est pris en charge. Avec la configuration centralisée, vous ne pouvez pas couvrir un contrôle qui n'est pas disponible dans la région d'origine ou dans l'une des régions associées. Pour obtenir la liste des contrôles impliquant des ressources globales, voirContrôles utilisant des ressources globales.

Security Hub CSPM console

Pour créer et associer des politiques de configuration

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, choisissez Configuration et l'onglet Politiques. Choisissez ensuite Create policy.
3. Sur la page Configurer l'organisation, si c'est la première fois que vous créez une politique de configuration, trois options s'affichent sous Type de configuration. Si vous avez déjà créé au moins une politique de configuration, seule l'option Politique personnalisée s'affiche.

- Choisissez Utiliser la configuration CSPM de Security Hub AWS recommandée dans l'ensemble de mon organisation pour appliquer notre politique recommandée. La politique recommandée active le Security Hub CSPM dans tous les comptes de l'organisation, applique la norme AWS Foundational Security Best Practices (FSBP) et active tous les contrôles FSBP nouveaux et existants. Les commandes utilisent les valeurs de paramètres par défaut.
- Choisissez Je ne suis pas encore prêt à configurer pour créer une politique de configuration ultérieurement.
- Choisissez Politique personnalisée pour créer une politique de configuration personnalisée. Spécifiez s'il faut activer ou désactiver Security Hub CSPM, les normes à activer et les contrôles à activer selon ces normes. Spécifiez éventuellement des valeurs de paramètres personnalisés pour un ou plusieurs contrôles activés qui prennent en charge les paramètres personnalisés.

4. Dans la section Comptes, choisissez les comptes cibles, les unités d'organisation ou la racine auxquels vous souhaitez que votre politique de configuration s'applique.

   - Choisissez Tous les comptes si vous souhaitez appliquer la politique de configuration à la racine. Cela inclut tous les comptes et unités d'organisation de l'organisation auxquels aucune autre politique n'est appliquée ou dont aucune autre politique n'est héritée.
   - Choisissez Comptes spécifiques si vous souhaitez appliquer la politique de configuration à des comptes ou à des unités d'organisation spécifiques. Entrez les identifiants de compte ou sélectionnez les comptes et les unités d'organisation dans la structure de l'organisation. Vous pouvez appliquer la politique à un maximum de 15 cibles (comptes, unités d'organisation ou root) lorsque vous la créez. Pour spécifier un nombre plus élevé, modifiez votre politique après sa création et appliquez-la à des cibles supplémentaires.
   - Choisissez L'administrateur délégué uniquement pour appliquer la politique de configuration au compte d'administrateur délégué actuel.

5. Choisissez Suivant.
6. Sur la page Vérifier et appliquer, passez en revue les détails de votre politique de configuration. Choisissez ensuite Créer une politique et appliquez. Dans votre région d'origine et dans les régions associées, cette action remplace les paramètres de configuration existants des comptes associés à cette politique de configuration. Les comptes peuvent être associés à la politique de configuration par le biais d'une application ou d'un héritage d'un nœud parent. Les comptes enfants et les unités d'organisation des cibles appliquées

hériteront automatiquement de cette politique de configuration, sauf s'ils sont spécifiquement exclus, autogérés ou s'ils utilisent une politique de configuration différente.

Security Hub CSPM API

Pour créer et associer des politiques de configuration

1. Appelez l'CreateConfigurationPolicyAPI depuis le compte d'administrateur délégué CSPM de Security Hub dans la région d'origine.
2. Pour`Name`, fournissez un nom unique pour la politique de configuration. Facultativement`Description`, pour, fournissez une description de la politique de configuration.
3. Pour le `ServiceEnabled` champ, indiquez si vous souhaitez que Security Hub CSPM soit activé ou désactivé dans cette politique de configuration.
4. Dans le `EnabledStandardIdentifiers` champ, spécifiez les normes CSPM du Security Hub que vous souhaitez activer dans cette politique de configuration.
5. Pour l'`SecurityControlsConfiguration`objet, spécifiez les contrôles que vous souhaitez activer ou désactiver dans cette politique de configuration. Choisir `EnabledSecurityControlIdentifiers` signifie que les commandes spécifiées sont activées. Les autres contrôles qui font partie de vos normes activées (y compris les contrôles récemment publiés) sont désactivés. Choisir `DisabledSecurityControlIdentifiers` signifie que les commandes spécifiées sont désactivées. Les autres contrôles qui font partie de vos normes activées (y compris les contrôles récemment publiés) sont activés.
6. Spécifiez éventuellement les contrôles activés pour le `SecurityControlCustomParameters` champ dont vous souhaitez personnaliser les paramètres. Indiquez `CUSTOM` le `ValueType` champ et la valeur du paramètre personnalisé pour le `Value` champ. La valeur doit correspondre au type de données correct et se situer dans les plages valides spécifiées par Security Hub CSPM. Seules certaines commandes prennent en charge les valeurs de paramètres personnalisées. Pour de plus amples informations, veuillez consulter Comprendre les paramètres de contrôle dans Security Hub CSPM.
7. Pour appliquer votre politique de configuration aux comptes ou aux unités d'organisation, appelez l'StartConfigurationPolicyAssociationAPI depuis le compte d'administrateur délégué Security Hub CSPM de la région d'origine.

8. Pour le `ConfigurationPolicyIdentifier` champ, indiquez le nom de ressource Amazon (ARN) ou l'identifiant unique universel (UUID) de la politique. L'ARN et l'UUID sont renvoyés par l'`CreateConfigurationPolicy`API. Pour une configuration autogérée, le `ConfigurationPolicyIdentifier` champ est égal à`SELF_MANAGED_SECURITY_HUB`.
9. Pour le `Target` champ, indiquez l'unité d'organisation, le compte ou l'ID racine auquel vous souhaitez que cette politique de configuration s'applique. Vous ne pouvez fournir qu'une seule cible par demande d'API. Les comptes enfants et les unités d'organisation de la cible sélectionnée hériteront automatiquement de cette politique de configuration à moins qu'ils ne soient autogérés ou qu'ils n'utilisent une stratégie de configuration différente.

Exemple de demande d'API pour créer une politique de configuration :

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
```

```
            }
        }
    }
}
```

Exemple de demande d'API pour associer une politique de configuration :

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Pour créer et associer des politiques de configuration

1. Exécutez la create-configuration-policycommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine.
2. Pourname, fournissez un nom unique pour la politique de configuration. Facultativementdescription, pour, fournissez une description de la politique de configuration.
3. Pour le `ServiceEnabled` champ, indiquez si vous souhaitez que Security Hub CSPM soit activé ou désactivé dans cette politique de configuration.
4. Dans le `EnabledStandardIdentifiers` champ, spécifiez les normes CSPM du Security Hub que vous souhaitez activer dans cette politique de configuration.
5. Pour le `SecurityControlsConfiguration` champ, spécifiez les contrôles que vous souhaitez activer ou désactiver dans cette politique de configuration. Choisir `EnabledSecurityControlIdentifiers` signifie que les commandes spécifiées sont activées. Les autres contrôles qui font partie de vos normes activées (y compris les contrôles récemment publiés) sont désactivés. Choisir `DisabledSecurityControlIdentifiers` signifie que les commandes spécifiées sont désactivées. Les autres contrôles qui s'appliquent à vos normes activées (y compris les contrôles récemment publiés) sont activés.
6. Spécifiez éventuellement les contrôles activés pour le `SecurityControlCustomParameters` champ dont vous souhaitez personnaliser les paramètres. Indiquez `CUSTOM` le `ValueType` champ et la valeur du paramètre personnalisé

pour le `Value` champ. La valeur doit correspondre au type de données correct et se situer dans les plages valides spécifiées par Security Hub CSPM. Seules certaines commandes prennent en charge les valeurs de paramètres personnalisées. Pour de plus amples informations, veuillez consulter Comprendre les paramètres de contrôle dans Security Hub CSPM.

7. Pour appliquer votre politique de configuration aux comptes ou aux unités d'organisation, exécutez la start-configuration-policy-associationcommande depuis le compte d'administrateur délégué Security Hub CSPM de la région d'origine.
8. Pour le `configuration-policy-identifier` champ, indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration. Cet ARN et cet ID sont renvoyés par la `create-configuration-policy` commande.
9. Pour le `target` champ, indiquez l'unité d'organisation, le compte ou l'ID racine auquel vous souhaitez que cette politique de configuration s'applique. Vous ne pouvez fournir qu'une seule cible à chaque fois que vous exécutez la commande. Les enfants de la cible sélectionnée hériteront automatiquement de cette politique de configuration à moins qu'ils ne soient autogérés ou qu'ils n'utilisent une stratégie de configuration différente.

Exemple de commande pour créer une politique de configuration :

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

Exemple de commande pour associer une politique de configuration :

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

L'`StartConfigurationPolicyAssociation`API renvoie un champ appelé`AssociationStatus`. Ce champ indique si une association de politiques est en attente ou en état de réussite ou d'échec. Le passage du statut à `SUCCESS` ou peut prendre jusqu'à 24 heures`FAILURE`. `PENDING` Pour plus d'informations sur le statut de l'association, consultezRévision de l'état d'association d'une politique de configuration.

Examen de l'état et des détails des politiques de configuration

L'administrateur délégué du AWS Security Hub CSPM peut consulter les politiques de configuration d'une organisation et leurs détails. Cela inclut les comptes et les unités organisationnelles (UO) auxquels une politique est associée.

Pour obtenir des informations générales sur les avantages de la configuration centralisée et son fonctionnement, consultezComprendre la configuration centrale dans Security Hub CSPM.

Choisissez votre méthode préférée et suivez les étapes pour consulter vos politiques de configuration.

Security Hub CSPM console

Pour consulter les politiques de configuration (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, sélectionnez Paramètres et configuration.
3. Cliquez sur l'onglet Politiques pour obtenir un aperçu de vos politiques de configuration.
4. Sélectionnez une politique de configuration, puis choisissez Afficher les détails pour obtenir des informations supplémentaires à son sujet, notamment les comptes et les unités d'organisation auxquels elle est associée.

Security Hub CSPM API

Pour afficher une liste récapitulative de toutes vos politiques de configuration, utilisez le ListConfigurationPoliciesfonctionnement de l'API Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la list-configuration-policiescommande. Le compte administrateur délégué du Security Hub CSPM doit appeler l'opération dans la région d'origine.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Pour afficher les détails d'une politique de configuration spécifique, utilisez l'GetConfigurationPolicyopération. Si vous utilisez leAWS CLI, lancez le get-configuration-policy. Le compte d'administrateur délégué doit invoquer l'opération dans la région d'origine. Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration dont vous souhaitez consulter les détails.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Pour afficher une liste récapitulative de toutes vos politiques de configuration et de leurs associations de comptes, utilisez l'ListConfigurationPolicyAssociationsopération use the. Si vous utilisez leAWS CLI, exécutez la list-configuration-policy-associationscommande. Le compte d'administrateur délégué doit invoquer l'opération dans la région d'origine. Vous pouvez éventuellement fournir des paramètres de pagination ou filtrer les résultats en fonction d'un ID de politique, d'un type d'association ou d'un statut d'association spécifique.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Pour afficher les associations associées à un compte spécifique, utilisez l'GetConfigurationPolicyAssociationopération. Si vous utilisez leAWS CLI, exécutez la get-configuration-policy-associationcommande. Le compte d'administrateur délégué doit invoquer l'opération dans la région d'origine. Pour`target`, indiquez le numéro de compte, l'ID de l'unité d'organisation ou l'identifiant root.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Révision de l'état d'association d'une politique de configuration

Les opérations d'API de configuration centrale suivantes renvoient un champ appelé `AssociationStatus` :

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Ce champ est renvoyé à la fois lorsque la configuration sous-jacente est une politique de configuration et lorsqu'il s'agit d'un comportement autogéré.

La valeur de `AssociationStatus` indique si une association de politiques est en attente ou en cours de réussite ou d'échec pour un compte spécifique. Le passage de l'état à `SUCCESS` ou peut prendre jusqu'`PENDING`à 24 heures`FAILED`. Un statut de `SUCCESS` signifie que tous les paramètres spécifiés dans la politique de configuration sont associés au compte. Un statut de `FAILED` signifie qu'un ou plusieurs paramètres spécifiés dans la politique de configuration n'ont pas pu être associés au compte. Malgré un `FAILED` statut, le compte peut être partiellement configuré conformément à la politique. Par exemple, vous pouvez essayer d'associer un compte à une politique de configuration qui active le Security Hub CSPM, active les meilleures pratiques de sécurité AWS fondamentales et le désactive. CloudTrail.1 Les deux réglages initiaux peuvent réussir, mais le CloudTrail.1 réglage peut échouer. Dans cet exemple, le statut de l'association est `FAILED` même si certains paramètres ont été correctement configurés.

Le statut d'association d'une unité d'organisation parent ou de la racine dépend du statut de ses enfants. Si le statut d'association de tous les enfants est le `SUCCESS` même, le statut d'association du parent l'est`SUCCESS`. Si le statut d'association d'un ou de plusieurs enfants est le même`FAILED`, le statut d'association du parent l'est`FAILED`.

La valeur de `AssociationStatus` dépend du statut associatif de la politique dans toutes les régions concernées. Si l'association réussit dans la région d'origine et dans toutes les régions associées, la valeur de `AssociationStatus` est`SUCCESS`. Si l'association échoue dans une ou plusieurs de ces régions, la valeur de `AssociationStatus` est`FAILED`.

Le comportement suivant a également un impact sur la valeur de `AssociationStatus` :

- Si la cible est une unité d'organisation parent ou la racine, elle possède un statut `AssociationStatus` de `SUCCESS` ou `FAILED` uniquement lorsque tous les enfants ont le `FAILED` statut `SUCCESS` ou. Si le statut d'association d'un compte enfant ou d'une unité d'organisation change (par exemple, lorsqu'une région associée est ajoutée ou supprimée) après avoir associé le parent pour la première fois à une configuration, la modification

ne met pas à jour le statut d'association du parent, sauf si vous appelez à nouveau l'`StartConfigurationPolicyAssociation`API.

- Si la cible est un compte, elle possède un `AssociationStatus` compte `SUCCESS` ou `FAILED` uniquement si l'association a un résultat `FAILED` dans `SUCCESS` ou dans la région d'origine et toutes les régions associées. Si le statut d'association d'un compte cible change (par exemple, lorsqu'une région associée est ajoutée ou supprimée) une fois que vous l'avez associée pour la première fois à une configuration, son statut d'association est mis à jour. Toutefois, la modification ne met pas à jour le statut d'association du parent, sauf si vous invoquez à nouveau l'`StartConfigurationPolicyAssociation`API.

Si vous ajoutez une nouvelle région liée, Security Hub CSPM réplique vos associations existantes qui se trouvent dans une `PENDINGSUCCESS`, ou un `FAILED` état de la nouvelle région.

Même lorsque le statut de l'association est défini`SUCCESS`, le statut d'activation d'une norme faisant partie de la politique peut passer à un état incomplet. Dans ce cas, Security Hub CSPM ne peut pas générer de résultats pour les contrôles de la norme. Pour de plus amples informations, veuillez consulter Vérifier l'état d'une norme.

Résolution des problèmes d'association

Dans AWS Security Hub CSPM, une association de politiques de configuration peut échouer pour les raisons courantes suivantes.

- Le compte de gestion des Organizations n'est pas membre : si vous souhaitez associer une politique de configuration au compte de gestion Organizations, AWS Security Hub CSPM doit déjà être activé sur ce compte. Le compte de gestion devient ainsi un compte membre de l'organisation.
- AWS Confign'est pas activé ou correctement configuré : pour activer les normes dans une politique de configuration, AWS Config il doit être activé et configuré pour enregistrer les ressources pertinentes.
- L'association doit être effectuée à partir d'un compte d'administrateur délégué : vous ne pouvez associer une politique à des comptes cibles et à des unités d'organisation que lorsque vous êtes connecté au compte administrateur délégué du Security Hub CSPM.
- Vous devez vous associer depuis votre région d'origine : vous ne pouvez associer une politique à des comptes cibles et à des unités d'organisation que lorsque vous êtes connecté à votre région d'origine.
- Opt-in Région non activée : l'association de politiques échoue pour un compte membre ou une unité d'organisation dans une région associée s'il s'agit d'une région optionnelle que

l'administrateur délégué n'a pas activée. Vous pouvez réessayer après avoir activé la région à partir du compte d'administrateur délégué.

- Compte de membre suspendu : l'association de règles échoue si vous essayez d'associer une politique à un compte de membre suspendu.

Mise à jour des politiques de configuration

Après avoir créé une politique de configuration, le compte administrateur délégué du AWS Security Hub CSPM peut mettre à jour les détails de la politique et les associations de politiques. Lorsque les détails de la politique sont mis à jour, les comptes associés à la stratégie de configuration commencent automatiquement à utiliser la politique mise à jour.

Pour obtenir des informations générales sur les avantages de la configuration centralisée et son fonctionnement, consultezComprendre la configuration centrale dans Security Hub CSPM.

> **Note**
>
> Les politiques de configuration ne prennent en charge que les AWS normes et les contrôles. Vous ne pouvez pas inclure de normes multicloud (telles que CIS Azure Foundations Benchmark v4.0.0) ou de contrôles Azure dans une politique de configuration. Incluant un ARN standard multicloud ou un identifiant de contrôle, `InvalidInputException` renvois. Pour activer ou configurer les normes multicloud, utilisez les mécanismes de configuration locaux directement dans le périphérique souhaité. Compte AWS

L'administrateur délégué peut mettre à jour les paramètres de stratégie suivants :

- Activez ou désactivez Security Hub CSPM.
- Activez une ou plusieurs normes de sécurité.
- Indiquez quels contrôles de sécurité sont activés dans le cadre des normes activées. Vous pouvez le faire en fournissant une liste de contrôles spécifiques qui doivent être activés, et Security Hub CSPM désactive tous les autres contrôles, y compris les nouveaux contrôles lorsqu'ils sont publiés. Vous pouvez également fournir une liste de contrôles spécifiques qui doivent être désactivés, et Security Hub CSPM active tous les autres contrôles, y compris les nouveaux contrôles lorsqu'ils sont publiés.
- Vous pouvez éventuellement personnaliser les paramètres pour sélectionner les contrôles activés selon les normes activées.

Choisissez votre méthode préférée et suivez les étapes pour mettre à jour une politique de configuration.

> **Note**
>
> Si vous utilisez une configuration centralisée, Security Hub CSPM désactive automatiquement les contrôles impliquant des ressources globales dans toutes les régions, à l'exception de la région d'origine. Les autres contrôles que vous choisissez d'activer par le biais d'une politique de configuration sont activés dans toutes les régions où ils sont disponibles. Pour limiter les résultats de ces contrôles à une seule région, vous pouvez mettre à jour les paramètres de votre AWS Config enregistreur et désactiver l'enregistrement des ressources globales dans toutes les régions, à l'exception de la région d'origine.
> Si un contrôle activé impliquant des ressources globales n'est pas pris en charge dans la région d'origine, Security Hub CSPM essaie d'activer le contrôle dans une région liée où le contrôle est pris en charge. Avec la configuration centralisée, vous ne pouvez pas couvrir un contrôle qui n'est pas disponible dans la région d'origine ou dans l'une des régions associées. Pour obtenir la liste des contrôles impliquant des ressources globales, voirContrôles utilisant des ressources globales.

Console

Pour mettre à jour les politiques de configuration

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, sélectionnez Paramètres et configuration.
3. Choisissez l'onglet Politiques.
4. Sélectionnez la politique de configuration que vous souhaitez modifier, puis choisissez Modifier. Si vous le souhaitez, modifiez les paramètres de politique. Laissez cette section telle quelle si vous souhaitez conserver les paramètres de stratégie inchangés.
5. Choisissez Next. Si vous le souhaitez, modifiez les associations de politiques. Laissez cette section telle quelle si vous souhaitez conserver les associations de politiques inchangées.

Vous pouvez associer ou dissocier la politique à un maximum de 15 cibles (comptes, unités d'organisation ou root) lorsque vous la mettez à jour.

6. Choisissez Suivant.
7. Passez en revue vos modifications, puis choisissez Enregistrer et appliquer. Dans votre région d'origine et dans les régions associées, cette action remplace les paramètres de configuration existants des comptes associés à cette politique de configuration. Les comptes peuvent être associés à une politique de configuration par le biais d'une application ou d'un héritage provenant d'un nœud parent.

API

Pour mettre à jour les politiques de configuration

1. Pour mettre à jour les paramètres d'une politique de configuration, appelez l'UpdateConfigurationPolicyAPI depuis le compte d'administrateur délégué Security Hub CSPM de la région d'origine.
2. Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez mettre à jour.
3. Fournissez des valeurs mises à jour pour les champs ci-dessous`ConfigurationPolicy`. Vous pouvez éventuellement indiquer le motif de la mise à jour.
4. Pour ajouter de nouvelles associations pour cette politique de configuration, appelez l'StartConfigurationPolicyAssociationAPI depuis le compte d'administrateur délégué Security Hub CSPM de la région d'origine. Pour supprimer une ou plusieurs associations actuelles, appelez l'StartConfigurationPolicyDisassociationAPI depuis le compte d'administrateur délégué Security Hub CSPM de la région d'origine.
5. Pour le `ConfigurationPolicyIdentifier` champ, indiquez l'ARN ou l'ID de la politique de configuration dont vous souhaitez mettre à jour les associations.
6. Pour le `Target` champ, indiquez les comptes, les unités d'organisation ou l'ID racine que vous souhaitez associer ou dissocier. Cette action remplace les associations de politiques précédentes pour les unités d'organisation ou les comptes spécifiés.

> **Note**
>
> Lorsque vous appelez l'`UpdateConfigurationPolicy`API, Security Hub CSPM remplace la liste complète des champs`EnabledStandardIdentifiers`,

`EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, et`SecurityControlCustomParameters`. Chaque fois que vous invoquez cette API, fournissez la liste complète des normes que vous souhaitez activer, ainsi que la liste complète des contrôles que vous souhaitez activer ou désactiver et pour lesquels vous souhaitez personnaliser les paramètres.

Exemple de demande d'API pour mettre à jour une politique de configuration :

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
```

```
        }
    }
}
```

AWS CLI

Pour mettre à jour les politiques de configuration

1. Pour mettre à jour les paramètres d'une politique de configuration, exécutez la update-configuration-policycommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine.
2. Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez mettre à jour.
3. Fournissez des valeurs mises à jour pour les champs ci-dessous`configuration-policy`. Vous pouvez éventuellement indiquer le motif de la mise à jour.
4. Pour ajouter de nouvelles associations pour cette politique de configuration, exécutez la start-configuration-policy-associationcommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine. Pour supprimer une ou plusieurs associations actuelles, exécutez la start-configuration-policy-disassociationcommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine.
5. Pour le `configuration-policy-identifier` champ, indiquez l'ARN ou l'ID de la politique de configuration dont vous souhaitez mettre à jour les associations.
6. Pour le `target` champ, indiquez les comptes, les unités d'organisation ou l'ID racine que vous souhaitez associer ou dissocier. Cette action remplace les associations de politiques précédentes pour les unités d'organisation ou les comptes spécifiés.

> **Note**
>
> Lorsque vous exécutez la `update-configuration-policy` commande, Security Hub CSPM remplace la liste complète des champs`EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, et`SecurityControlCustomParameters`. Chaque fois que vous exécutez cette commande, fournissez la liste complète des normes que vous souhaitez activer et la liste complète des contrôles que vous souhaitez activer ou désactiver et pour lesquels vous souhaitez personnaliser les paramètres.

Exemple de commande pour mettre à jour une politique de configuration :

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

L'`StartConfigurationPolicyAssociation`API renvoie un champ appelé`AssociationStatus`. Ce champ indique si une association de politiques est en attente ou en état de réussite ou d'échec. Le passage de l'état à `SUCCESS` ou peut prendre jusqu'`PENDING`à 24 heures`FAILURE`. Pour plus d'informations sur le statut de l'association, consultezRévision de l'état d'association d'une politique de configuration.

Supprimer les politiques de configuration

Après avoir créé une politique de configuration, l'administrateur délégué du AWS Security Hub CSPM peut la supprimer. L'administrateur délégué peut également conserver la politique, mais la dissocier de comptes ou d'unités organisationnelles (UO) spécifiques, ou de la racine. Pour obtenir des instructions sur la dissociation d'une politique, consultezDissociation d'une configuration de ses cibles.

Pour obtenir des informations générales sur les avantages de la configuration centralisée et son fonctionnement, consultezComprendre la configuration centrale dans Security Hub CSPM.

Cette section explique comment supprimer les politiques de configuration.

Lorsque vous supprimez une politique de configuration, elle n'existe plus pour votre organisation. Les comptes cibles, les unités d'organisation et la racine de l'organisation ne peuvent plus utiliser la politique de configuration. Les cibles associées à une politique de configuration supprimée héritent de la politique de configuration du parent le plus proche ou deviennent autogérées si le parent le plus

proche est autogéré. Si vous souhaitez qu'une cible utilise une configuration différente, vous pouvez l'associer à une nouvelle politique de configuration. Pour de plus amples informations, veuillez consulter Création et association de politiques de configuration.

Nous vous recommandons de créer et d'associer au moins une politique de configuration à votre organisation afin de fournir une couverture de sécurité adéquate.

Avant de pouvoir supprimer une politique de configuration, vous devez dissocier la stratégie des comptes, des unités d'organisation ou de la racine auxquels elle s'applique actuellement.

Choisissez votre méthode préférée et suivez les étapes pour supprimer une politique de configuration.

Console

Pour supprimer une politique de configuration

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, sélectionnez Paramètres et configuration.
3. Choisissez l'onglet Politiques. Sélectionnez la politique de configuration que vous souhaitez supprimer, puis choisissez Supprimer. Si la politique de configuration est toujours associée à des comptes ou à des unités d'organisation, vous êtes invité à dissocier d'abord la politique de ces cibles avant de pouvoir la supprimer.
4. Consultez le message de confirmation. Entrez**`confirm`**, puis choisissez Supprimer.

API

Pour supprimer une politique de configuration

Appelez l'DeleteConfigurationPolicyAPI depuis le compte d'administrateur délégué Security Hub CSPM de la région d'origine.

Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez supprimer. Si vous recevez un `ConflictException` message d'erreur, la politique de configuration s'applique toujours aux comptes ou aux unités d'organisation de votre

organisation. Pour résoudre l'erreur, dissociez la politique de configuration de ces comptes ou unités d'organisation avant d'essayer de la supprimer.

Exemple de demande d'API pour supprimer une politique de configuration :

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Pour supprimer une politique de configuration

Exécutez la delete-configuration-policycommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine.

Indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez supprimer. Si vous recevez un `ConflictException` message d'erreur, la politique de configuration s'applique toujours aux comptes ou aux unités d'organisation de votre organisation. Pour résoudre l'erreur, dissociez la politique de configuration de ces comptes ou unités d'organisation avant d'essayer de la supprimer.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Dissociation d'une configuration de ses cibles

À partir du compte administrateur délégué du AWS Security Hub CSPM, vous pouvez dissocier une politique de configuration ou une configuration autogérée d'un compte, d'une unité d'organisation ou d'un root. La dissociation conserve la politique pour une utilisation future, mais supprime les associations existantes de comptes, d'unités d'organisation ou de racine spécifiques. Vous ne pouvez dissocier qu'une configuration appliquée directement, pas une configuration héritée. Pour modifier une configuration héritée, vous pouvez appliquer une politique de configuration ou un comportement autogéré au compte ou à l'unité d'organisation concerné. Vous pouvez également appliquer une nouvelle politique de configuration, qui inclut les modifications souhaitées, au parent le plus proche.

La dissociation ne supprime pas une politique de configuration. La politique est conservée dans votre compte afin que vous puissiez l'associer à d'autres cibles de votre organisation. Pour obtenir des instructions sur la suppression d'une politique de configuration, consultezSupprimer les politiques de configuration. Lorsque la dissociation est terminée, la cible affectée hérite de la politique de configuration ou du comportement autogéré du parent le plus proche. S'il n'existe aucune configuration héritable, une cible conserve les paramètres qu'elle avait avant la dissociation mais devient autogérée.

Choisissez votre méthode préférée et suivez les étapes pour dissocier un compte, une unité d'organisation ou un root de sa configuration actuelle.

Console

Pour dissocier un compte ou une unité d'organisation de sa configuration actuelle

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, sélectionnez Paramètres et configuration.
3. Dans l'onglet Organizations, sélectionnez le compte, l'unité d'organisation ou la racine que vous souhaitez dissocier de sa configuration actuelle. Choisissez Modifier.
4. Sur la page Définir la configuration, pour Gestion, choisissez Politique appliquée si vous souhaitez que l'administrateur délégué puisse appliquer des politiques directement à la cible. Choisissez Hierited si vous souhaitez que la cible hérite de la configuration de son parent le plus proche. Dans les deux cas, l'administrateur délégué contrôle les paramètres de la cible. Choisissez Self-managedsi vous souhaitez que le compte ou l'unité d'organisation contrôle ses propres paramètres.
5. Après avoir examiné vos modifications, choisissez Suivant et Appliquer. Cette action remplace les configurations existantes de tous les comptes ou unités d'organisation concernés, si ces configurations entrent en conflit avec vos sélections actuelles.

API

Pour dissocier un compte ou une unité d'organisation de sa configuration actuelle

1. Appelez l'StartConfigurationPolicyDisassociationAPI depuis le compte d'administrateur délégué CSPM de Security Hub dans la région d'origine.
2. Pour`ConfigurationPolicyIdentifier`, fournissez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez dissocier. Indiquez ce champ `SELF_MANAGED_SECURITY_HUB` pour dissocier les comportements autogérés.
3. Pour`Target`, indiquez les comptes, les unités d'organisation ou la racine que vous souhaitez dissocier de cette politique de configuration.

Exemple de demande d'API pour dissocier une politique de configuration :

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Pour dissocier un compte ou une unité d'organisation de sa configuration actuelle

1. Exécutez la start-configuration-policy-disassociationcommande depuis le compte d'administrateur délégué Security Hub CSPM dans la région d'origine.
2. Pour`configuration-policy-identifier`, fournissez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez dissocier. Indiquez ce champ `SELF_MANAGED_SECURITY_HUB` pour dissocier les comportements autogérés.
3. Pour`target`, indiquez les comptes, les unités d'organisation ou la racine que vous souhaitez dissocier de cette politique de configuration.

Exemple de commande pour dissocier une politique de configuration :

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
```

```
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Configuration d'une norme ou d'un contrôle en contexte

Lorsque vous utilisez la configuration centralisée dans AWS Security Hub CSPM, l'administrateur délégué de Security Hub CSPM peut créer des politiques de configuration qui spécifient la manière dont le Security Hub CSPM, les normes de sécurité et les contrôles de sécurité sont configurés pour une organisation. L'administrateur délégué peut associer des politiques à des comptes et à des unités d'organisation (UO) spécifiques. Les politiques entrent en vigueur dans votre région d'origine et dans toutes les régions associées. L'administrateur délégué peut mettre à jour les politiques de configuration si nécessaire.

Sur la console Security Hub CSPM, l'administrateur délégué peut mettre à jour les politiques de configuration de deux manières : depuis la page Configuration ou dans le contexte des flux de travail existants. Ce dernier point peut être utile car, lorsque vous consultez les résultats de sécurité, vous pouvez découvrir les normes et les contrôles les plus pertinents pour votre environnement et les configurer en même temps.

In-context la configuration n'est disponible que sur la console Security Hub CSPM. Par programmation, l'administrateur délégué doit invoquer le UpdateConfigurationPolicyfonctionnement de l'API Security Hub CSPM pour modifier la façon dont des normes ou des contrôles spécifiques sont configurés dans l'organisation.

Suivez ces étapes pour configurer une norme ou un contrôle Security Hub CSPM en contexte.

Pour configurer une norme ou un contrôle en contexte (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, choisissez l'une des options suivantes :

   - Pour configurer une norme, sélectionnez Normes de sécurité, puis choisissez une norme spécifique.
   - Pour configurer un contrôle, choisissez Controls, puis choisissez un contrôle spécifique.

3. La console répertorie vos politiques de configuration Security Hub CSPM existantes et le statut de la norme ou du contrôle sélectionné dans chacune d'elles. Choisissez les options pour activer ou désactiver la norme ou le contrôle dans chaque politique de configuration existante. Pour les contrôles, vous pouvez également choisir de personnaliser les paramètres de contrôle. Vous ne pouvez pas créer de nouvelle politique lors de la configuration contextuelle. Pour créer une nouvelle politique, vous devez accéder à la page Configuration, choisir l'onglet Stratégies, puis choisir Créer une politique.
4. Après avoir apporté vos modifications, choisissez Next.
5. Passez en revue vos modifications, puis choisissez Appliquer. Les mises à jour concernent tous les comptes et unités d'organisation associés à une politique de configuration modifiée. Les mises à jour prennent également effet dans la région d'origine et dans toutes les régions associées.

Désactivation de la configuration centrale dans Security Hub CSPM

Lorsque vous désactivez la configuration centralisée dans AWS Security Hub CSPM, l'administrateur délégué perd la possibilité de configurer le Security Hub CSPM, les normes de sécurité et les contrôles de sécurité sur plusieurs Comptes AWS unités organisationnelles (UO) et. Régions AWS Vous devez plutôt configurer la plupart des paramètres séparément pour chaque compte dans chaque région.

> **Important**
>
> Avant de désactiver la configuration centralisée, vous devez d'abord dissocier vos comptes et unités d'organisation de leur configuration actuelle, qu'il s'agisse d'une politique de configuration ou d'un comportement autogéré.
> Avant de désactiver la configuration centralisée, vous devez également supprimer les politiques de configuration existantes.

Lorsque vous désactivez la configuration centrale, les modifications suivantes se produisent :

- L'administrateur délégué ne peut plus créer de politiques de configuration pour l'organisation.
- Les comptes auxquels une politique de configuration a été appliquée ou héritée conservent leurs paramètres actuels, mais deviennent autogérés.
- Votre organisation passe à la configuration locale. Dans le cadre de la configuration locale, la majorité des paramètres Security Hub CSPM doivent être configurés séparément dans chaque

compte d'organisation et dans chaque région. L'administrateur délégué peut choisir d'activer automatiquement le Security Hub CSPM, les normes de sécurité par défaut et tous les contrôles inclus dans les normes par défaut dans les nouveaux comptes d'organisation. Les normes par défaut sont AWS Foundational Security Best Practices (FSBP) et Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Ces paramètres ne prennent effet que dans la région actuelle et n'ont d'incidence que sur les nouveaux comptes de l'organisation. L'administrateur délégué ne peut pas modifier les normes par défaut. La configuration locale ne prend pas en charge l'utilisation de politiques de configuration ou de configuration au niveau de l'unité d'organisation.

L'identité du compte d'administrateur délégué reste la même lorsque vous arrêtez d'utiliser la configuration centrale. Votre région d'origine et les régions associées restent également les mêmes (votre région d'origine est désormais appelée région d'agrégation et peut être utilisée pour rechercher une agrégation).

Choisissez votre méthode préférée et suivez les étapes pour arrêter d'utiliser la configuration centrale et passer à la configuration locale.

Security Hub CSPM console

Pour désactiver la configuration centrale (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur délégué du Security Hub CSPM dans la région d'origine.
2. Dans le volet de navigation, sélectionnez Paramètres et configuration.
3. Dans la section Vue d'ensemble, choisissez Modifier.
4. Dans la zone Modifier la configuration de l'organisation, choisissez Configuration locale. Si ce n'est pas déjà fait, vous êtes invité à dissocier et à supprimer vos politiques de configuration actuelles avant de pouvoir arrêter la configuration centralisée. Les comptes ou unités d'organisation désignés comme autogérés doivent être dissociés de leur configuration autogérée. Vous pouvez le faire dans la console en modifiant le type de gestion de chaque compte ou unité d'organisation autogéré en mode géré de manière centralisée et en héritant de mon organisation.

5. Vous pouvez éventuellement sélectionner les paramètres de configuration par défaut locaux pour les nouveaux comptes d'organisation.
6. Choisissez Confirmer.

Security Hub CSPM API

Pour désactiver la configuration centrale (API)

1. Appelez l'UpdateOrganizationConfigurationAPI.
2. Définissez le `ConfigurationType` champ de l'`OrganizationConfiguration`objet sur`LOCAL`. L'API renvoie une erreur si vous avez des politiques de configuration ou des associations de politiques existantes. Pour dissocier une politique de configuration, appelez l'`StartConfigurationPolicyDisassociation`API. Pour supprimer une politique de configuration, appelez l'`DeleteConfigurationPolicy`API.
3. Si vous souhaitez activer automatiquement le Security Hub CSPM dans les nouveaux comptes d'organisation, définissez le `AutoEnable` champ sur. `true` Par défaut, la valeur de ce champ est`false`, et Security Hub CSPM n'est pas automatiquement activé dans les nouveaux comptes d'organisation. Si vous souhaitez activer automatiquement les normes de sécurité par défaut dans les nouveaux comptes d'organisation, définissez le `AutoEnableStandards` champ sur`DEFAULT`. Il s'agit de la valeur par défaut. Si vous ne souhaitez pas activer automatiquement les normes de sécurité par défaut dans les nouveaux comptes d'organisation, définissez le `AutoEnableStandards` champ sur`NONE`.

Exemple de demande d'API :

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Pour désactiver la configuration centrale (AWS CLI)

1. Exécutez la commande update-organization-configuration.

2. Définissez le `ConfigurationType` champ de l'`organization-configuration`objet sur`LOCAL`. La commande renvoie une erreur si vous avez des politiques de configuration ou des associations de politiques existantes. Pour dissocier une politique de configuration, exécutez la `start-configuration-policy-disassociation` commande. Pour supprimer une politique de configuration, exécutez la `delete-configuration-policy` commande.
3. Si vous souhaitez activer automatiquement le Security Hub CSPM dans les nouveaux comptes d'organisation, incluez le `auto-enable` paramètre. Par défaut, la valeur de ce paramètre est`no-auto-enable`, et Security Hub CSPM n'est pas automatiquement activé dans les nouveaux comptes d'organisation. Si vous souhaitez activer automatiquement les normes de sécurité par défaut dans les nouveaux comptes d'organisation, définissez le `auto-enable-standards` champ sur`DEFAULT`. Il s'agit de la valeur par défaut. Si vous ne souhaitez pas activer automatiquement les normes de sécurité par défaut dans les nouveaux comptes d'organisation, définissez le `auto-enable-standards` champ sur`NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Gestion des comptes d'administrateur et de membre dans Security Hub CSPM

Si votre AWS environnement comporte plusieurs comptes, vous pouvez traiter les comptes qui utilisent AWS Security Hub CSPM comme des comptes membres et les associer à un seul compte administrateur. L'administrateur peut surveiller votre niveau de sécurité global et effectuer les actions autorisées sur les comptes des membres. L'administrateur peut également effectuer diverses tâches de gestion et d'administration des comptes à grande échelle, telles que le suivi des coûts d'utilisation estimés et l'évaluation des quotas de compte.

Vous pouvez associer des comptes membres à un administrateur de deux manières : en intégrant Security Hub CSPM à Security Hub CSPM AWS Organizations ou en envoyant et en acceptant manuellement des invitations d'adhésion dans Security Hub CSPM.

Gérer des comptes avecAWS Organizations

AWS Organizationsest un service de gestion de comptes global qui permet AWS aux administrateurs de consolider et de gérer plusieurs comptesComptes AWS. Il fournit des fonctionnalités de gestion des comptes et de facturation consolidée conçues pour répondre aux besoins budgétaires, de sécurité et de conformité. Il est proposé sans frais supplémentaires et s'intègre à plusieurs applicationsServices AWS, notamment AWS Security Hub CSPM, Amazon Macie et Amazon. GuardDuty Pour plus d'informations, consultez le Guide de l'utilisateur AWS Organizations.

Lorsque vous intégrez Security Hub CSPM etAWS Organizations, le compte de gestion Organizations désigne un administrateur délégué du Security Hub CSPM. Security Hub CSPM est automatiquement activé dans le compte d'administrateur délégué Région AWS dans lequel il a été désigné.

Après avoir désigné un administrateur délégué, nous vous recommandons de gérer les comptes dans Security Hub CSPM avec une configuration centralisée. C'est le moyen le plus efficace de personnaliser Security Hub CSPM et de garantir une couverture de sécurité adéquate pour votre organisation.

La configuration centralisée permet à l'administrateur délégué de personnaliser Security Hub CSPM sur plusieurs comptes et régions d'entreprise plutôt que de le configurer. Region-by-Region Vous pouvez créer une politique de configuration pour l'ensemble de votre organisation ou créer différentes politiques de configuration pour différents comptes et unités d'organisation. Les politiques précisent si Security Hub CSPM est activé ou désactivé dans les comptes associés et quelles normes et contrôles de sécurité sont activés.

L'administrateur délégué peut désigner des comptes comme étant gérés de manière centralisée ou autogérés. Les comptes gérés de manière centralisée sont configurables uniquement par l'administrateur délégué. Self-managed les comptes peuvent définir leurs propres paramètres.

Si vous n'optez pas pour la configuration centralisée, l'administrateur délégué dispose d'une capacité plus limitée pour configurer le Security Hub CSPM, appelée configuration locale. Dans le cadre de la configuration locale, l'administrateur délégué peut automatiquement activer le Security Hub CSPM et les normes de sécurité par défaut dans les nouveaux comptes d'organisation de la région actuelle. Toutefois, les comptes existants n'utilisent pas ces paramètres, de sorte qu'une modification de la configuration peut se produire une fois qu'un compte a rejoint l'organisation.

Outre ces nouveaux paramètres de compte, la configuration locale est spécifique au compte et. Region-specific Chaque compte d'organisation doit configurer le service, les normes et les contrôles

Security Hub CSPM séparément dans chaque région. La configuration locale ne prend pas non plus en charge l'utilisation de politiques de configuration.

Gestion manuelle des comptes sur invitation

Vous devez gérer manuellement les comptes des membres sur invitation dans Security Hub CSPM si vous avez un compte autonome ou si vous ne l'intégrez pas à Organizations. Un compte autonome ne peut pas s'intégrer à Organizations, il est donc nécessaire de le gérer manuellement. Nous vous recommandons d'intégrer AWS Organizations et d'utiliser la configuration centralisée si vous ajoutez des comptes supplémentaires à l'avenir.

Lorsque vous utilisez la gestion manuelle des comptes, vous désignez un compte comme administrateur du Security Hub CSPM. Le compte administrateur peut consulter les données des comptes des membres et prendre certaines mesures en fonction des résultats des comptes des membres. L'administrateur du Security Hub CSPM invite d'autres comptes à devenir membres, et la relation administrateur-membre est établie lorsqu'un compte membre potentiel accepte l'invitation.

La gestion manuelle des comptes ne prend pas en charge l'utilisation de politiques de configuration. Sans politiques de configuration, l'administrateur ne peut pas personnaliser Security Hub CSPM de manière centralisée en configurant des paramètres variables pour différents comptes. Au lieu de cela, chaque compte d'organisation doit activer et configurer Security Hub CSPM séparément dans chaque région. Il peut donc être plus difficile et fastidieux de garantir une couverture de sécurité adéquate pour tous les comptes et régions dans lesquels vous utilisez Security Hub CSPM. Cela peut également entraîner une dérive de la configuration, car les comptes membres peuvent définir leurs propres paramètres sans intervention de l'administrateur.

Pour gérer les comptes sur invitation, consultezGestion des comptes sur invitation dans Security Hub CSPM.

Recommandations pour la gestion de plusieurs comptes dans Security Hub CSPM

La section suivante résume certaines restrictions et recommandations à prendre en compte lors de la gestion des comptes de membres dans AWS Security Hub CSPM.

Nombre maximal de comptes membres

Si vous utilisez l'intégration avecAWS Organizations, Security Hub CSPM prend en charge jusqu'à 10 000 comptes membres par compte d'administrateur délégué dans chacun d'eux. Région AWS

Si vous activez et gérez Security Hub CSPM manuellement, Security Hub CSPM prend en charge jusqu'à 1 000 invitations de compte de membre par compte administrateur dans chaque région.

Création de relations administrateur-membre

> **Note**
>
> Si vous utilisez l'intégration CSPM de Security Hub et que vous n'avez invité aucun compte membre manuellement, cette section ne s'applique pas à vous. AWS Organizations

Un compte ne peut pas être à la fois un compte administrateur et un compte membre.

Un compte membre ne peut être associé qu'à un seul compte administrateur. Si un compte d'organisation est activé par le compte administrateur du Security Hub CSPM, le compte ne peut pas accepter d'invitation provenant d'un autre compte. Si un compte a déjà accepté une invitation, le compte ne peut pas être activé par le compte administrateur Security Hub CSPM de l'organisation. Il ne peut pas non plus recevoir d'invitations provenant d'autres comptes.

Pour le processus d'invitation manuel, l'acceptation d'une invitation d'adhésion est facultative.

Adhésion viaAWS Organizations

Si vous intégrez Security Hub CSPM à Security HubAWS Organizations, le compte de gestion Organizations peut désigner un compte d'administrateur délégué (DA) pour Security Hub CSPM. Le compte de gestion de l'organisation ne peut pas être défini en tant que DA dans Organizations. Bien que cela soit autorisé dans Security Hub CSPM, nous recommandons que le compte de gestion des Organizations ne soit pas le DA.

Nous vous recommandons de choisir le même compte DA dans toutes les régions. Si vous utilisez la configuration centralisée, Security Hub CSPM définit le même compte DA dans toutes les régions dans lesquelles vous configurez Security Hub CSPM pour votre organisation.

Nous vous recommandons également de choisir le même compte DA pour tous les services AWS de sécurité et de conformité afin de vous aider à gérer les problèmes liés à la sécurité de manière centralisée.

Adhésion sur invitation

Pour les comptes membres créés sur invitation, l'association administrateur-compte membre est créée uniquement dans la région d'où l'invitation est envoyée. Le compte administrateur doit activer

le Security Hub CSPM dans chaque région dans laquelle vous souhaitez l'utiliser. Le compte administrateur invite ensuite chaque compte à devenir un compte membre dans cette région.

> **Note**
>
> Nous vous recommandons d'utiliser des invitations CSPM à la AWS Organizations place du Security Hub pour gérer vos comptes de membres.

Coordination des comptes d'administrateur entre les services

Security Hub CSPM regroupe les résultats de différents AWS services, tels qu'Amazon, Amazon GuardDuty Inspector et Amazon Macie. Security Hub CSPM permet également aux utilisateurs de passer d'une GuardDuty découverte à une enquête dans Amazon Detective.

Toutefois, les relations administrateur-membre que vous configurez dans ces autres services ne s'appliquent pas automatiquement à Security Hub CSPM. Security Hub CSPM vous recommande d'utiliser le même compte que le compte administrateur pour tous ces services. Ce compte administrateur doit être un compte responsable des outils de sécurité. Le même compte doit également être le compte agrégateur pourAWS Config.

Par exemple, un utilisateur du compte GuardDuty administrateur A peut consulter les résultats relatifs aux comptes de GuardDuty membres B et C sur la GuardDuty console. Si le compte A active alors Security Hub CSPM, les utilisateurs du compte A ne voient pas automatiquement les GuardDuty résultats des comptes B et C dans Security Hub CSPM. Une relation administrateur-membre du Security Hub CSPM est également requise pour ces comptes.

Pour ce faire, définissez le compte A comme compte administrateur du Security Hub CSPM et activez les comptes B et C pour qu'ils deviennent des comptes membres du Security Hub CSPM.

Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations

Vous pouvez intégrer AWS Security Hub CSPM à Security Hub CSPMAWS Organizations, puis le gérer pour les comptes de votre organisation.

Pour intégrer Security Hub CSPM àAWS Organizations, vous devez créer une organisation dans. AWS Organizations Le compte de gestion des Organizations désigne un compte en tant

qu'administrateur délégué du Security Hub CSPM pour l'organisation. L'administrateur délégué peut ensuite activer le Security Hub CSPM pour les autres comptes de l'organisation, ajouter ces comptes en tant que comptes membres du Security Hub CSPM et effectuer les actions autorisées sur les comptes des membres. L'administrateur délégué du Security Hub CSPM peut activer et gérer le Security Hub CSPM pour un maximum de 10 000 comptes membres.

L'étendue des capacités de configuration de l'administrateur délégué dépend de l'utilisation ou non de la configuration centralisée. Lorsque la configuration centralisée est activée, vous n'avez pas besoin de configurer Security Hub CSPM séparément dans chaque compte membre et. Région AWS L'administrateur délégué peut appliquer les paramètres CSPM spécifiques du Security Hub à des comptes membres et à des unités d'organisation (UO) spécifiques dans toutes les régions.

Le compte administrateur délégué Security Hub CSPM peut effectuer les actions suivantes sur les comptes des membres :

- Si vous utilisez la configuration centralisée, configurez le Security Hub CSPM de manière centralisée pour les comptes membres et les unités d'organisation en créant des politiques de configuration Security Hub CSPM. Les politiques de configuration peuvent être utilisées pour activer et désactiver Security Hub CSPM, activer et désactiver les normes, ainsi que pour activer et désactiver les contrôles.
- Traitez automatiquement les nouveaux comptes comme des comptes membres du Security Hub CSPM lorsqu'ils rejoignent l'organisation. Si vous utilisez la configuration centralisée, une politique de configuration associée à une unité d'organisation inclut les comptes existants et nouveaux qui font partie de l'unité d'organisation.
- Traitez les comptes d'organisation existants comme des comptes membres du Security Hub CSPM. Cela se produit automatiquement si vous utilisez la configuration centralisée.
- Dissociez les comptes des membres appartenant à l'organisation. Si vous utilisez la configuration centralisée, vous ne pouvez dissocier un compte membre qu'après l'avoir désigné comme étant autogéré. Vous pouvez également associer une politique de configuration qui désactive Security Hub CSPM à des comptes membres spécifiques gérés de manière centralisée.

Si vous n'optez pas pour la configuration centralisée, votre organisation utilise le type de configuration par défaut appelé configuration locale. Dans le cadre de la configuration locale, la capacité de l'administrateur délégué à appliquer les paramètres aux comptes des membres est plus limitée. Pour de plus amples informations, veuillez consulter Comprendre la configuration locale dans Security Hub CSPM.

Pour obtenir la liste complète des actions que l'administrateur délégué peut effectuer sur les comptes des membres, consultezActions autorisées par les comptes administrateur et membre dans Security Hub CSPM.

Les rubriques de cette section expliquent comment intégrer Security Hub CSPM à Security Hub CSPM AWS Organizations et comment gérer le Security Hub CSPM pour les comptes d'une organisation. Le cas échéant, chaque section identifie les avantages et les différences de gestion pour les utilisateurs de la configuration centralisée.

Rubriques

- Intégration de Security Hub CSPM àAWS Organizations
- Activation automatique du Security Hub CSPM dans les nouveaux comptes d'entreprise
- Activation manuelle du Security Hub CSPM dans les nouveaux comptes d'organisation
- Dissocier les comptes membres du Security Hub CSPM de votre organisation

Intégration de Security Hub CSPM àAWS Organizations

Pour intégrer AWS Security Hub CSPMAWS Organizations, vous devez créer une organisation dans Organizations et utiliser le compte de gestion de l'organisation pour désigner un compte administrateur Security Hub CSPM délégué. Cela permet à Security Hub CSPM de devenir un service fiable dans les Organizations. Il active également Security Hub CSPM en cours Région AWS pour le compte administrateur délégué, et il permet à l'administrateur délégué d'activer Security Hub CSPM pour les comptes membres, de consulter les données des comptes membres et d'effectuer d'autres actions autorisées sur les comptes membres.

Si vous utilisez la configuration centralisée, l'administrateur délégué peut également créer des politiques de configuration Security Hub CSPM qui spécifient comment le service, les normes et les contrôles Security Hub CSPM doivent être configurés dans les comptes de l'organisation.

Création d'une organisation

Une organisation est une entité que vous créez pour consolider les vôtres Comptes AWS afin de pouvoir les administrer en tant qu'unité unique.

Vous pouvez créer une organisation à l'aide de la AWS Organizations console ou à l'aide d'une commande provenant de l'API du SDK AWS CLI ou de l'une des API. Pour obtenir des instructions détaillées, voir Création d'une organisation dans le guide de AWS Organizations l'utilisateur.

Vous pouvez l'utiliser AWS Organizations pour visualiser et gérer de manière centralisée tous les comptes de votre organisation. Une organisation possède un compte de gestion avec zéro ou plusieurs comptes membres. Vous pouvez organiser les comptes dans une structure hiérarchique arborescente avec une racine en haut et des unités organisationnelles (UO) imbriquées sous la racine. Chaque compte peut être placé directement sous la racine ou dans l'une des unités d'organisation de la hiérarchie. Une UO est un conteneur pour des comptes spécifiques. Par exemple, vous pouvez créer une unité d'organisation financière qui inclut tous les comptes liés aux opérations financières.

Recommandations pour le choix de l'administrateur délégué du Security Hub CSPM

Si vous avez créé un compte administrateur à la suite du processus d'invitation manuel et que vous êtes en train de passer à la gestion des comptes avecAWS Organizations, nous vous recommandons de désigner ce compte en tant qu'administrateur délégué du Security Hub CSPM.

Bien que les API et la console Security Hub CSPM permettent au compte de gestion de l'organisation d'être l'administrateur délégué du Security Hub CSPM, nous vous recommandons de choisir deux comptes différents. Cela est dû au fait que les utilisateurs qui ont accès au compte de gestion de l'organisation pour gérer la facturation sont susceptibles d'être différents des utilisateurs qui ont besoin d'accéder au Security Hub CSPM pour la gestion de la sécurité.

Nous recommandons d'utiliser le même administrateur délégué dans toutes les régions. Si vous optez pour la configuration centralisée, Security Hub CSPM désigne automatiquement le même administrateur délégué dans votre région d'origine et dans toutes les régions associées.

Vérifiez les autorisations pour configurer l'administrateur délégué

Pour désigner et supprimer un compte administrateur Security Hub CSPM délégué, le compte de gestion de l'organisation doit disposer des autorisations nécessaires pour les `DisableOrganizationAdminAccount` actions `EnableOrganizationAdminAccount` et dans Security Hub CSPM. Le compte de gestion Organizations doit également disposer d'autorisations administratives pour les Organizations.

Pour accorder toutes les autorisations requises, associez les politiques gérées par Security Hub CSPM suivantes au principal IAM du compte de gestion de l'organisation :

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Désignation de l'administrateur délégué

Pour désigner le compte administrateur Security Hub CSPM délégué, vous pouvez utiliser la console Security Hub CSPM, l'API Security Hub CSPM ou. AWS CLI Security Hub CSPM définit l'administrateur délégué Région AWS uniquement dans la version actuelle, et vous devez répéter l'action dans les autres régions. Si vous commencez à utiliser la configuration centralisée, Security Hub CSPM définit automatiquement le même administrateur délégué dans la région d'origine et dans les régions associées.

Il n'est pas nécessaire que le compte de gestion de l'organisation active Security Hub CSPM soit activé pour désigner le compte administrateur délégué du Security Hub CSPM.

Nous recommandons que le compte de gestion de l'organisation ne soit pas le compte administrateur délégué du Security Hub CSPM. Toutefois, si vous choisissez le compte de gestion de l'organisation comme administrateur délégué de Security Hub CSPM, Security Hub CSPM doit être activé sur le compte de gestion. Si Security Hub CSPM n'est pas activé sur le compte de gestion, vous devez activer Security Hub CSPM manuellement. Security Hub CSPM ne peut pas être activé automatiquement pour le compte de gestion de l'organisation.

Vous devez désigner l'administrateur délégué du Security Hub CSPM à l'aide de l'une des méthodes suivantes. La désignation de l'administrateur délégué du Security Hub CSPM avec les API Organizations ne se reflète pas dans le Security Hub CSPM.

Choisissez votre méthode préférée et suivez les étapes pour désigner le compte administrateur délégué du Security Hub CSPM.

Security Hub CSPM console

Pour désigner l'administrateur délégué lors de l'intégration

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Go to Security Hub CSPM. Vous êtes invité à vous connecter au compte de gestion de l'organisation.
3. Sur la page Désigner un administrateur délégué, dans la section Compte d'administrateur délégué, spécifiez le compte d'administrateur délégué. Nous vous recommandons de choisir le même administrateur délégué que celui que vous avez défini pour les autres services AWS de sécurité et de conformité.

4. Choisissez Définir un administrateur délégué. Vous êtes invité à vous connecter au compte d'administrateur délégué (si ce n'est pas déjà fait) pour poursuivre l'intégration grâce à la configuration centralisée. Si vous ne souhaitez pas démarrer la configuration centralisée, choisissez Annuler. Votre administrateur délégué est configuré, mais vous n'utilisez pas encore la configuration centralisée.

Pour désigner l'administrateur délégué à partir du Settings page

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation Security Hub CSPM, choisissez Settings. Choisissez ensuite Général.
3. Si un compte administrateur Security Hub CSPM est actuellement attribué, vous devez supprimer le compte actuel avant de pouvoir désigner un nouveau compte.

   Sous Administrateur délégué, pour supprimer le compte actuel, choisissez Supprimer.
4. Entrez l'identifiant du compte que vous souhaitez désigner comme compte administrateur Security Hub CSPM.

   Vous devez désigner le même compte administrateur Security Hub CSPM dans toutes les régions. Si vous désignez un compte différent de celui désigné dans d'autres régions, la console renvoie un message d'erreur.
5. Choisisssez Delegate (Déléguer).

Security Hub CSPM API,AWS CLI

Depuis le compte de gestion de l'organisation, utilisez le EnableOrganizationAdminAccountfonctionnement de l'API Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la enable-organization-admin-accountcommande. Indiquez l'Compte AWSID de l'administrateur délégué du Security Hub CSPM.

L'exemple suivant désigne l'administrateur délégué du Security Hub CSPM. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Supprimer ou modifier l'administrateur délégué

Seul le compte de gestion de l'organisation peut supprimer le compte administrateur délégué du Security Hub CSPM.

Pour modifier l'administrateur délégué du Security Hub CSPM, vous devez d'abord supprimer le compte administrateur délégué actuel, puis en désigner un nouveau.

> **Warning**
>
> Lorsque vous utilisez la configuration centralisée, vous ne pouvez pas utiliser la console Security Hub CSPM ou les API Security Hub CSPM pour modifier ou supprimer le compte administrateur délégué. Si le compte de gestion de l'organisation utilise la AWS Organizations console ou les AWS Organizations API pour modifier ou supprimer l'administrateur délégué de Security Hub CSPM, Security Hub CSPM arrête automatiquement la configuration centrale et supprime vos politiques de configuration et vos associations de politiques. Les comptes membres conservent les configurations qu'ils avaient avant le changement ou la suppression de l'administrateur délégué.

Si vous utilisez la console Security Hub CSPM pour supprimer l'administrateur délégué dans une région, il est automatiquement supprimé dans toutes les régions.

L'API Security Hub CSPM supprime uniquement le compte administrateur Security Hub CSPM délégué de la région dans laquelle l'appel ou la commande d'API est émis. Vous devez répéter l'action dans les autres régions.

Si vous utilisez l'API Organizations pour supprimer le compte administrateur délégué de Security Hub CSPM, celui-ci est automatiquement supprimé dans toutes les régions.

Suppression de l'administrateur délégué (API Organizations,AWS CLI)

Vous pouvez utiliser Organizations pour supprimer l'administrateur délégué du Security Hub CSPM dans toutes les régions.

Si vous utilisez la configuration centralisée pour gérer les comptes, la suppression du compte d'administrateur délégué entraîne la suppression de vos politiques de configuration et de vos associations de politiques. Les comptes membres conservent les configurations qu'ils avaient avant le changement ou la suppression de l'administrateur délégué. Toutefois, ces comptes ne peuvent

plus être gérés par le compte d'administrateur délégué supprimé. Ils deviennent des comptes autogérés qui doivent être configurés séparément dans chaque région.

Choisissez votre méthode préférée et suivez les instructions pour supprimer le compte administrateur délégué de Security Hub CSPM avec. AWS Organizations

Organizations API,AWS CLI

Pour supprimer l'administrateur délégué du Security Hub CSPM

Depuis le compte de gestion de l'organisation, utilisez le DeregisterDelegatedAdministratorfonctionnement de l'API Organizations. Si vous utilisez leAWS CLI, exécutez la commande deregister-delegated-administrator. Indiquez l'ID de compte de l'administrateur délégué et le principal de service pour Security Hub CSPM, à savoir. `securityhub.amazonaws.com`

L'exemple suivant supprime l'administrateur délégué du Security Hub CSPM. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Supprimer l'administrateur délégué (console Security Hub CSPM)

Vous pouvez utiliser la console Security Hub CSPM pour supprimer l'administrateur CSPM délégué de Security Hub dans toutes les régions.

Lorsque le compte administrateur CSPM délégué du Security Hub est supprimé, les comptes des membres sont dissociés du compte administrateur délégué du Security Hub CSPM supprimé.

Security Hub CSPM est toujours activé dans les comptes des membres. Ils deviennent des comptes autonomes jusqu'à ce qu'un nouvel administrateur Security Hub CSPM les autorise en tant que comptes membres.

Si le compte de gestion de l'organisation n'est pas un compte activé dans Security Hub CSPM, utilisez l'option sur la page Welcome to Security Hub CSPM.

Pour supprimer le compte administrateur Security Hub CSPM délégué du Bienvenue sur Security Hub CSPM page

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Go to Security Hub.
3. Sous Administrateur délégué, choisissez Supprimer.

Si le compte de gestion de l'organisation est un compte activé dans Security Hub, utilisez l'option de l'onglet Général de la page Paramètres.

Pour supprimer le compte administrateur Security Hub CSPM délégué du Settings page

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation Security Hub CSPM, choisissez Settings. Choisissez ensuite Général.
3. Sous Administrateur délégué, choisissez Supprimer.

Suppression de l'administrateur délégué (API Security Hub CSPM),AWS CLI)

Vous pouvez utiliser l'API Security Hub CSPM ou les opérations Security Hub CSPM pour supprimer l'AWS CLIadministrateur CSPM délégué du Security Hub. Lorsque vous supprimez l'administrateur délégué à l'aide de l'une de ces méthodes, il n'est supprimé que dans la région où l'appel ou la commande d'API a été émis. Security Hub CSPM ne met pas à jour les autres régions et ne supprime pas le compte d'administrateur délégué dans. AWS Organizations

Choisissez votre méthode préférée et suivez ces étapes pour supprimer le compte administrateur délégué de Security Hub CSPM auprès de Security Hub CSPM.

Security Hub CSPM API,AWS CLI

Pour supprimer l'administrateur délégué du Security Hub CSPM

Depuis le compte de gestion de l'organisation, utilisez le DisableOrganizationAdminAccountfonctionnement de l'API Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la disable-organization-admin-accountcommande. Indiquez l'ID de compte de l'administrateur délégué du Security Hub CSPM.

L'exemple suivant supprime l'administrateur délégué du Security Hub CSPM. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Désactivation de l'intégration de Security Hub CSPM avecAWS Organizations

Une fois qu'une AWS Organizations organisation est intégrée à AWS Security Hub CSPM, le compte de gestion des Organizations peut ensuite désactiver l'intégration. En tant qu'utilisateur du compte de gestion des Organizations, vous pouvez le faire en désactivant l'accès sécurisé pour Security Hub CSPM dans. AWS Organizations

Lorsque vous désactivez l'accès sécurisé pour Security Hub CSPM, les événements suivants se produisent :

- Security Hub CSPM perd son statut de service de confiance en. AWS Organizations
- Le compte administrateur délégué du Security Hub CSPM perd l'accès aux paramètres, aux données et aux ressources du Security Hub CSPM pour tous les comptes membres du Security Hub CSPM. Régions AWS
- Si vous utilisiez la configuration centralisée, Security Hub CSPM cesse automatiquement de l'utiliser pour votre organisation. Vos politiques de configuration et vos associations de politiques sont supprimées. Les comptes conservent les configurations qu'ils avaient avant que vous ne désactiviez l'accès sécurisé.
- Tous les comptes membres du Security Hub CSPM deviennent des comptes autonomes et conservent leurs paramètres actuels. Si Security Hub CSPM a été activé pour un compte membre dans une ou plusieurs régions, le Security Hub CSPM continue d'être activé pour le compte dans ces régions. Les normes et contrôles activés restent également inchangés. Vous pouvez modifier ces paramètres séparément dans chaque compte et région. Toutefois, le compte n'est plus associé à un administrateur délégué dans aucune région.

Pour plus d'informations sur les conséquences de la désactivation de l'accès aux services sécurisés, consultez la section Utilisation AWS Organizations avec d'autres personnes Services AWS dans le Guide de l'AWS Organizationsutilisateur.

Pour désactiver l'accès sécurisé, vous pouvez utiliser la AWS Organizations console, l'API Organizations ou leAWS CLI. Seul un utilisateur du compte de gestion des Organizations peut

désactiver l'accès aux services sécurisés pour Security Hub CSPM. Pour plus de détails sur les autorisations dont vous avez besoin, consultez la section Autorisations requises pour désactiver l'accès sécurisé dans le Guide de AWS Organizations l'utilisateur.

Avant de désactiver l'accès sécurisé, nous vous recommandons de contacter l'administrateur délégué de votre organisation afin de désactiver le Security Hub CSPM dans les comptes membres et de nettoyer les ressources Security Hub CSPM de ces comptes.

Choisissez votre méthode préférée et suivez les étapes pour désactiver l'accès sécurisé pour Security Hub CSPM.

Organizations console

Pour désactiver l'accès sécurisé pour Security Hub CSPM

1. Connectez-vous à l'Console de gestion AWSaide des informations d'identification du compte AWS Organizations de gestion.
2. Ouvrez la console Organizations à l'adresse https://console.aws.amazon.com/organizations/.
3. Dans le panneau de navigation, choisissez Services.
4. Sous Services intégrés, choisissez AWSSecurity Hub CSPM.
5. Choisissez Disable trusted access (Désactiver l'accès approuvé).
6. Confirmez que vous souhaitez désactiver l'accès sécurisé.

Organizations API

Pour désactiver l'accès sécurisé pour Security Hub CSPM

Invoquez le DisableAWSServiceAccessfonctionnement de l'AWS OrganizationsAPI. Pour le `ServicePrincipal` paramètre, spécifiez le principal du service Security Hub CSPM ()`securityhub.amazonaws.com`.

AWS CLI

Pour désactiver l'accès sécurisé pour Security Hub CSPM

Exécutez la commande disable-aws-service-access de l'API. AWS Organizations Pour le `service-principal` paramètre, spécifiez le principal du service Security Hub CSPM ()`securityhub.amazonaws.com`.

Exemple :

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Activation automatique du Security Hub CSPM dans les nouveaux comptes d'entreprise

Lorsque de nouveaux comptes rejoignent votre organisation, ils sont ajoutés à la liste sur la page Comptes de la console AWS Security Hub CSPM. Pour les comptes de l'organisation, le type est Par organisation. Par défaut, les nouveaux comptes ne deviennent pas membres du Security Hub CSPM lorsqu'ils rejoignent l'organisation. Leur statut est Non membre. Le compte d'administrateur délégué peut automatiquement ajouter de nouveaux comptes en tant que membres et activer Security Hub CSPM sur ces comptes lorsqu'ils rejoignent l'organisation.

> **Note**
>
> Bien que plusieurs d'entre Régions AWS elles soient actives par défaut pour votre régionCompte AWS, vous devez activer certaines régions manuellement. Ces régions sont appelées « régions optionnelles » dans ce document. Pour activer automatiquement le Security Hub CSPM sur un nouveau compte dans une région optionnelle, cette région doit d'abord être activée sur le compte. Seul le titulaire du compte peut activer la région opt-in. Pour plus d'informations sur les régions optionnelles, voir Spécifier celles que Régions AWS votre compte peut utiliser.

Ce processus est différent selon que vous utilisez la configuration centrale (recommandée) ou la configuration locale.

Activation automatique des nouveaux comptes d'entreprise (configuration centrale)

Si vous utilisez la configuration centralisée, vous pouvez activer automatiquement le Security Hub CSPM dans les comptes d'organisation nouveaux et existants en créant une politique de configuration dans laquelle le Security Hub CSPM est activé. Vous pouvez ensuite associer la politique à la racine de l'organisation ou à des unités organisationnelles (UO) spécifiques.

Si vous associez une politique de configuration dans laquelle Security Hub CSPM est activé à une unité d'organisation spécifique, Security Hub CSPM est automatiquement activé dans tous les

comptes (existants et nouveaux) appartenant à cette unité d'organisation. Les nouveaux comptes qui n'appartiennent pas à l'unité d'organisation sont autogérés et le Security Hub CSPM n'est pas automatiquement activé. Si vous associez une politique de configuration dans laquelle Security Hub CSPM est activé à la racine, Security Hub CSPM est automatiquement activé dans tous les comptes (existants et nouveaux) qui rejoignent l'organisation. Les exceptions sont les cas où un compte utilise une politique différente par le biais d'une application ou d'un héritage, ou s'il est autogéré.

Dans votre politique de configuration, vous pouvez également définir les normes et contrôles de sécurité qui doivent être activés dans l'unité d'organisation. Pour générer des résultats de contrôle pour les normes activées, les comptes de l'unité d'organisation doivent être AWS Config activés et configurés pour enregistrer les ressources requises. Pour plus d'informations sur AWS Config l'enregistrement, consultez la section Activation et configuration AWS Config.

Pour obtenir des instructions sur la création d'une politique de configuration, consultezCréation et association de politiques de configuration.

Activation automatique des nouveaux comptes d'organisation (configuration locale)

Lorsque vous utilisez la configuration locale et que vous activez l'activation automatique des normes par défaut, Security Hub CSPM ajoute de nouveaux comptes d'organisation en tant que membres et active Security Hub CSPM dans ces comptes dans la région actuelle. Les autres régions ne sont pas concernées. En outre, l'activation automatique n'active pas le Security Hub CSPM dans les comptes d'organisation existants, sauf s'ils ont déjà été ajoutés en tant que comptes membres.

Une fois l'activation automatique activée, les normes de sécurité par défaut sont activées pour les nouveaux comptes membres de la région actuelle lorsqu'ils rejoignent l'organisation. Les normes par défaut sont AWS Foundational Security Best Practices (FSBP) et Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Vous ne pouvez pas modifier les normes par défaut. Si vous souhaitez activer d'autres normes au sein de votre organisation, ou activer des normes pour certains comptes et unités d'organisation, nous vous recommandons d'utiliser une configuration centralisée.

Pour générer des résultats de contrôle pour les normes par défaut (et les autres normes activées), les comptes de votre organisation doivent avoir été AWS Config activés et configurés pour enregistrer les ressources requises. Pour plus d'informations sur AWS Config l'enregistrement, consultez la section Activation et configuration AWS Config.

Choisissez votre méthode préférée et suivez les étapes pour activer automatiquement le Security Hub CSPM dans les nouveaux comptes d'entreprise. Ces instructions s'appliquent uniquement si vous utilisez une configuration locale.

Security Hub CSPM console

Pour activer automatiquement les nouveaux comptes d'organisation en tant que membres du Security Hub CSPM

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Sign utilise les informations d'identification du compte d'administrateur délégué.
2. Dans le volet de navigation Security Hub CSPM, sous Paramètres, sélectionnez Configuration.
3. Dans la section Comptes, activez les Auto-enable comptes.

Security Hub CSPM API

Pour activer automatiquement les nouveaux comptes d'organisation en tant que membres du Security Hub CSPM

Appelez l'`UpdateOrganizationConfiguration`API depuis le compte d'administrateur délégué. Définissez le `AutoEnable` champ sur `true` pour activer automatiquement le Security Hub CSPM dans les nouveaux comptes d'organisation.

AWS CLI

Pour activer automatiquement les nouveaux comptes d'organisation en tant que membres du Security Hub CSPM

Exécutez la `update-organization-configuration`commande depuis le compte d'administrateur délégué. Incluez le `auto-enable` paramètre permettant d'activer automatiquement le Security Hub CSPM dans les nouveaux comptes d'organisation.

```
aws securityhub update-organization-configuration --auto-enable
```

Activation manuelle du Security Hub CSPM dans les nouveaux comptes d'organisation

Si vous n'activez pas automatiquement le Security Hub CSPM dans les nouveaux comptes d'organisation lorsqu'ils rejoignent l'organisation, vous pouvez ajouter ces comptes en tant que membres et y activer le Security Hub CSPM manuellement une fois qu'ils ont rejoint l'organisation.

Vous devez également activer manuellement le Security Hub CSPM dans Comptes AWS le cas où vous vous êtes précédemment dissocié d'une organisation.

> **Note**
>
> Cette section ne s'applique pas à vous si vous utilisez la configuration centralisée. Si vous utilisez la configuration centralisée, vous pouvez créer des politiques de configuration qui activent le Security Hub CSPM dans des comptes membres et des unités organisationnelles (UO) spécifiques. Vous pouvez également activer des normes et des contrôles spécifiques dans ces comptes et unités d'organisation.

Vous ne pouvez pas activer Security Hub CSPM dans un compte s'il s'agit déjà d'un compte membre au sein d'une autre organisation.

Vous ne pouvez pas non plus activer Security Hub CSPM dans un compte actuellement suspendu. Si vous essayez d'activer le service sur un compte suspendu, le statut du compte passe à Compte suspendu.

- Si Security Hub CSPM n'est pas activé sur le compte, Security Hub CSPM est activé sur ce compte. La norme AWS Foundational Security Best Practices (FSBP) et le CIS AWS Foundations Benchmark v1.2.0 sont également activés dans le compte, sauf si vous désactivez les normes de sécurité par défaut.

  L'exception à cette règle est le compte de gestion des Organizations. Security Hub CSPM ne peut pas être activé automatiquement dans le compte de gestion des Organizations. Vous devez activer manuellement Security Hub CSPM dans le compte de gestion des Organizations avant de pouvoir l'ajouter en tant que compte membre.
- Si Security Hub CSPM est déjà activé sur le compte, Security Hub CSPM n'apporte aucune autre modification au compte. Cela permet uniquement l'adhésion.

Pour que Security Hub CSPM puisse générer des résultats de contrôle, les comptes membres doivent être AWS Config activés et configurés pour enregistrer les ressources requises. Pour plus d'informations, consultez Activation et configuration de AWS Config.

Choisissez votre méthode préférée et suivez les étapes pour activer un compte d'organisation en tant que compte membre du Security Hub CSPM.

Security Hub CSPM console

Pour activer manuellement les comptes d'organisation en tant que membres du Security Hub CSPM

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte d'administrateur délégué.
2. Dans le volet de navigation Security Hub CSPM, sous Paramètres, sélectionnez Configuration.
3. Dans la liste des comptes, sélectionnez chaque compte d'organisation que vous souhaitez activer.
4. Choisissez Actions, puis Add member (Ajouter un membre).

Security Hub CSPM API

Pour activer manuellement les comptes d'organisation en tant que membres du Security Hub CSPM

Appelez l'`CreateMembers`API depuis le compte d'administrateur délégué. Pour chaque compte à activer, indiquez l'identifiant du compte.

Contrairement au processus d'invitation manuel, lorsque vous appelez `CreateMembers` pour activer un compte d'organisation, vous n'avez pas besoin d'envoyer d'invitation.

AWS CLI

Pour activer manuellement les comptes d'organisation en tant que membres du Security Hub CSPM

Exécutez la `create-members`commande depuis le compte d'administrateur délégué. Pour chaque compte à activer, indiquez l'identifiant du compte.

Contrairement au processus d'invitation manuel, lorsque vous lancez un appel `create-members` pour activer un compte d'organisation, vous n'avez pas besoin d'envoyer d'invitation.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Exemple

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Dissocier les comptes membres du Security Hub CSPM de votre organisation

Pour arrêter de recevoir et de consulter les résultats d'un compte membre du AWS Security Hub CSPM, vous pouvez dissocier le compte membre de votre organisation.

> **Note**
>
> Si vous utilisez la configuration centralisée, la dissociation fonctionne différemment. Vous pouvez créer une politique de configuration qui désactive Security Hub CSPM dans un ou plusieurs comptes membres gérés de manière centralisée. Par la suite, ces comptes font toujours partie de l'organisation, mais ne généreront pas les résultats du Security Hub CSPM. Si vous utilisez la configuration centralisée mais que vous avez également des comptes de membres invités manuellement, vous pouvez dissocier un ou plusieurs comptes invités manuellement.

Les comptes membres gérés à l'aide de ne AWS Organizations peuvent pas dissocier leurs comptes du compte administrateur. Seul le compte administrateur peut dissocier un compte membre.

La dissociation d'un compte membre ne ferme pas le compte. Au lieu de cela, il supprime le compte du membre de l'organisation. Le compte de membre dissocié devient un compte autonome Compte AWS qui n'est plus géré par l'intégration de Security Hub CSPM avec. AWS Organizations

Choisissez votre méthode préférée et suivez les étapes pour dissocier un compte membre de l'organisation.

Security Hub CSPM console

Pour dissocier un compte membre de l'organisation

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte d'administrateur délégué.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Configuration.

3. Dans la section Comptes, sélectionnez les comptes que vous souhaitez dissocier. Si vous utilisez la configuration centrale, vous pouvez sélectionner un compte invité manuellement à dissocier de l'onglet. `Invitation accounts` Cet onglet n'est visible que si vous utilisez la configuration centralisée.
4. Choisissez Actions, puis Dissocier le compte.

Security Hub CSPM API

Pour dissocier un compte membre de l'organisation

Appelez l'`DisassociateMembers`API depuis le compte d'administrateur délégué. Vous devez fournir les Compte AWS identifiants des comptes membres à dissocier. Pour consulter la liste des comptes des membres, appelez l'`ListMembers`API.

AWS CLI

Pour dissocier un compte membre de l'organisation

Exécutez la `disassociate-members` commande > depuis le compte d'administrateur délégué. Vous devez fournir les Compte AWS identifiants des comptes membres à dissocier. Pour afficher la liste des comptes des membres, exécutez la `list-members` commande >.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Exemple

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Vous pouvez également utiliser la AWS Organizations console ou AWS CLI AWS les SDK pour dissocier un compte membre de votre organisation. Pour plus d'informations, consultez la section Suppression d'un compte membre de votre organisation dans le Guide de AWS Organizations l'utilisateur.

Gestion des comptes sur invitation dans Security Hub CSPM

Vous pouvez gérer de manière centralisée plusieurs comptes AWS Security Hub CSPM de deux manières : en intégrant Security Hub CSPM à Security Hub AWS Organizations ou en envoyant et en acceptant manuellement des invitations d'adhésion. Vous devez utiliser le processus manuel si

vous possédez un compte autonome ou si vous ne l'intégrez pas àAWS Organizations. Dans le cadre de la gestion manuelle des comptes, l'administrateur du Security Hub CSPM invite les comptes à devenir membres. La relation administrateur-membre est établie lorsqu'un membre potentiel accepte l'invitation. Un compte administrateur Security Hub CSPM peut gérer Security Hub CSPM pour un maximum de 1 000 comptes membres sur invitation.

> **Note**
>
> Si vous créez une organisation basée sur des invitations dans Security Hub CSPM, vous pouvez ensuite passer à l'utilisation à la place. AWS Organizations Si vous avez plusieurs comptes membres, nous vous recommandons d'utiliser les invitations CSPM à la AWS Organizations place de Security Hub pour gérer vos comptes membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

Cross-Region l'agrégation des résultats et d'autres données est disponible pour les comptes que vous invitez par le biais du processus d'invitation manuel. Toutefois, l'administrateur doit inviter le compte membre de la région d'agrégation et de toutes les régions associées pour que l'agrégation entre régions fonctionne. En outre, Security Hub CSPM doit être activé dans la région d'agrégation et dans toutes les régions associées pour permettre à l'administrateur de consulter les résultats du compte membre.

Les politiques de configuration ne sont pas prises en charge pour les comptes de membres invités manuellement. Au lieu de cela, vous devez configurer les paramètres Security Hub CSPM séparément dans chaque compte membre et Région AWS lorsque vous utilisez le processus d'invitation manuel.

Vous devez également utiliser le processus manuel basé sur les invitations pour les comptes qui n'appartiennent pas à votre organisation. Par exemple, il se peut que vous n'incluiez pas de compte de test dans votre organisation. Vous pouvez également regrouper les comptes de plusieurs organisations sous un seul compte administrateur Security Hub CSPM. Le compte administrateur du Security Hub CSPM doit envoyer des invitations aux comptes appartenant à d'autres organisations.

Sur la page de configuration de la console Security Hub CSPM, les comptes ajoutés sur invitation sont répertoriés dans l'onglet Comptes d'invitation. Si vous utilisez la configuration centralisée, mais que vous invitez également des comptes extérieurs à votre organisation, vous pouvez consulter les résultats des comptes basés sur des invitations dans cet onglet. Toutefois, l'administrateur CSPM de

Security Hub ne peut pas configurer de comptes basés sur des invitations dans toutes les régions en utilisant des politiques de configuration.

Les rubriques de cette section expliquent comment gérer les comptes des membres par le biais d'invitations.

Rubriques

- Ajouter et inviter des comptes membres dans Security Hub CSPM
- Répondre à une invitation à devenir membre du Security Hub CSPM
- Dissociation des comptes membres dans Security Hub CSPM
- Supprimer des comptes de membres dans Security Hub CSPM
- Dissociation d'un compte administrateur Security Hub CSPM
- Transition vers Organizations pour gérer les comptes dans Security Hub CSPM

Ajouter et inviter des comptes membres dans Security Hub CSPM

> **Note**
>
> Nous vous recommandons d'utiliser des invitations CSPM à la AWS Organizations place du Security Hub pour gérer vos comptes de membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

Votre compte devient l'administrateur du AWS Security Hub CSPM pour les comptes qui acceptent votre invitation à devenir un compte membre du Security Hub CSPM.

Lorsque vous acceptez une invitation provenant d'un autre compte, votre compte devient un compte membre, et ce compte devient votre administrateur.

Si votre compte est un compte administrateur, vous ne pouvez pas accepter une invitation à devenir membre.

L'ajout d'un compte membre comprend les étapes suivantes :

1. Le compte administrateur ajoute le compte du membre à sa liste de comptes membres.
2. Le compte administrateur envoie une invitation au compte membre.
3. Le compte membre accepte l'invitation.

Ajouter des comptes de membres

Depuis la console Security Hub CSPM, vous pouvez ajouter des comptes à votre liste de comptes membres. Dans la console Security Hub CSPM, vous pouvez sélectionner des comptes individuellement ou télécharger un `.csv` fichier contenant les informations du compte.

Pour chaque compte, vous devez fournir l'identifiant du compte et une adresse e-mail. L'adresse e-mail doit être l'adresse e-mail à contacter pour tout problème de sécurité lié au compte. Il n'est pas utilisé pour vérifier le compte.

Choisissez votre méthode préférée et suivez les étapes pour ajouter des comptes de membre.

Security Hub CSPM console

Pour ajouter des comptes à votre liste de comptes membres

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur.
2. Dans le volet de gauche, choisissez Settings (Paramètres).
3. Sur la page Paramètres, sélectionnez Comptes, puis Ajouter des comptes. Vous pouvez ensuite ajouter des comptes individuellement ou télécharger un `.csv` fichier contenant la liste des comptes.
4. Pour sélectionner les comptes, effectuez l'une des opérations suivantes :

   - Pour ajouter les comptes individuellement, sous Entrez les comptes, entrez l'ID du compte et l'adresse e-mail du compte à ajouter, puis choisissez Ajouter.

     Répétez cette procédure pour chaque compte.
   - Pour utiliser un fichier de valeurs séparées par des virgules (.csv) pour ajouter plusieurs comptes, créez d'abord le fichier. Le fichier doit contenir l'identifiant du compte et l'adresse e-mail de chaque compte à ajouter.

     Dans votre `.csv` liste, les comptes doivent apparaître un par ligne. La première ligne du `.csv` fichier doit contenir l'en-tête. Dans l'en-tête, la première colonne est **`Account ID`** et la deuxième colonne est**`Email`**.

     Chaque ligne suivante doit contenir un ID de compte et une adresse e-mail valides pour le compte à ajouter.

Voici un exemple de `.csv` fichier affiché dans un éditeur de texte.

```
Account ID,Email
111111111111,user@example.com
```

Dans un tableur, les champs apparaissent dans des colonnes distinctes. Le format sous-jacent est toujours séparé par des virgules. Vous devez formater les identifiants de compte sous forme de nombres non décimaux. Par exemple, l'ID de compte 444455556666 ne peut pas être formaté sous la forme 444455556666.0. Assurez-vous également que le formatage des nombres ne supprime aucun zéro en tête de l'identifiant du compte.

Pour sélectionner le fichier, sur la console, choisissez Upload list (.csv). Choisissez ensuite Parcourir.

Après avoir sélectionné le fichier, choisissez Ajouter des comptes.

5. Une fois que vous avez terminé d'ajouter des comptes, sous Comptes à ajouter, sélectionnez Suivant.

Security Hub CSPM API

Pour ajouter des comptes à votre liste de comptes membres

Appelez l'`CreateMembers`API depuis le compte administrateur. Pour chaque compte membre à ajouter, vous devez fournir l'Compte AWSidentifiant.

AWS CLI

Pour ajouter des comptes à votre liste de comptes membres

Exécutez la `create-members`commande depuis le compte administrateur. Pour chaque compte membre à ajouter, vous devez fournir l'Compte AWSidentifiant.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Exemple

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Inviter des comptes membres

Après avoir ajouté les comptes de membre, vous envoyez une invitation au compte de membre. Vous pouvez également renvoyer une invitation à un compte que vous avez dissocié de l'administrateur.

Security Hub CSPM console

Pour inviter des comptes de membres potentiels

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur.
2. Dans le volet de navigation, choisissez Paramètres, puis Comptes.
3. Pour le compte à inviter, choisissez Invite (Inviter) dans la colonne Status (Statut).
4. Lorsque vous êtes invité à confirmer, choisissez Inviter.

> **Note**
>
> Pour renvoyer des invitations à des comptes dissociés, sélectionnez chaque compte dissocié sur la page Comptes. Pour Actions, choisissez Renvoyer l'invitation.

Security Hub CSPM API

Pour inviter des comptes de membres potentiels

Appelez l'`InviteMembers`API depuis le compte administrateur. Pour chaque compte à inviter, vous devez fournir l'Compte AWSidentifiant.

AWS CLI

Pour inviter des comptes de membres potentiels

Exécutez la `invite-members`commande depuis le compte administrateur. Pour chaque compte à inviter, vous devez fournir l'Compte AWSidentifiant.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Exemple

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Répondre à une invitation à devenir membre du Security Hub CSPM

> **Note**
>
> Nous vous recommandons d'utiliser des invitations CSPM à la AWS Organizations place du Security Hub pour gérer vos comptes de membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

Vous pouvez accepter ou refuser une invitation à devenir membre du AWS Security Hub CSPM.

Si vous acceptez une invitation, votre compte devient un compte membre du Security Hub CSPM. Le compte qui a envoyé l'invitation devient votre compte administrateur Security Hub CSPM. L'utilisateur du compte administrateur peut consulter les résultats de votre compte membre dans Security Hub CSPM.

Si vous refusez l'invitation, votre compte est marqué comme Désigné sur la liste des comptes membres du compte administrateur.

Vous ne pouvez accepter qu'une seule invitation pour créer un compte membre.

Avant d'accepter ou de refuser une invitation, vous devez activer Security Hub CSPM.

N'oubliez pas que tous les comptes Security Hub CSPM doivent être AWS Config activés et configurés pour enregistrer toutes les ressources. Pour plus de détails sur la configuration requiseAWS Config, voir Activation et configuration AWS Config.

Acceptation d'une invitation

Vous pouvez envoyer une invitation pour devenir membre du Security Hub CSPM depuis le compte administrateur. Vous pouvez ensuite accepter l'invitation après vous être connecté au compte membre.

Choisissez la méthode que vous préférez et suivez les étapes pour accepter une invitation à devenir membre.

Security Hub CSPM console

Pour accepter une invitation d'adhésion

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Paramètres, puis Comptes.
3. Dans la section Compte administrateur, activez Accepter, puis sélectionnez Accepter l'invitation.

Security Hub CSPM API

Pour accepter une invitation d'adhésion

Appelez l'`AcceptAdministratorInvitation`API. Vous devez fournir l'identifiant de l'invitation et l'Compte AWSidentifiant du compte administrateur. Pour récupérer les détails de l'invitation, utilisez l'`ListInvitations`opération.

AWS CLI

Pour accepter une invitation d'adhésion

Exécutez la commande `accept-administrator-invitation`. Vous devez fournir l'identifiant de l'invitation et l'Compte AWSidentifiant du compte administrateur. Pour récupérer les détails de l'invitation, exécutez la `list-invitations`commande.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Exemple

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> La console Security Hub CSPM continue de fonctionner. `AcceptInvitation`
> Il finira par changer d'usage`AcceptAdministratorInvitation`. Toutes les

politiques IAM qui contrôlent spécifiquement l'accès à cette fonction doivent continuer à être utiliséesAcceptInvitation. Vous devez également compléter vos politiques AcceptAdministratorInvitation pour vous assurer que les autorisations appropriées sont en place une fois que la console commence à être utiliséeAcceptAdministratorInvitation.

Refuser une invitation

Vous pouvez refuser une invitation à devenir membre du Security Hub CSPM. Lorsque vous refusez une invitation dans la console Security Hub CSPM, votre compte est marqué comme Désigné dans la liste des comptes membres du compte administrateur. Le statut Résigné apparaît uniquement lorsque vous vous connectez à la console Security Hub CSPM à l'aide du compte administrateur. Toutefois, l'invitation reste inchangée dans la console du compte membre jusqu'à ce que vous vous connectiez au compte administrateur et que vous supprimiez l'invitation.

Pour refuser une invitation, vous devez vous connecter au compte membre qui a reçu l'invitation.

Choisissez votre méthode préférée et suivez les étapes pour refuser une invitation à devenir membre.

Security Hub CSPM console

Pour refuser une invitation d'adhésion

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Paramètres, puis Comptes.
3. Dans la section Compte administrateur, choisissez Refuser l'invitation.

Security Hub CSPM API

Pour refuser une invitation d'adhésion

Appelez l'DeclineInvitationsAPI. Vous devez fournir l'Compte AWSID du compte administrateur qui a émis l'invitation. Pour consulter les informations relatives à vos invitations, utilisez l'ListInvitationsopération.

AWS CLI

Pour refuser une invitation d'adhésion

Exécutez la commande `decline-invitations`. Vous devez fournir l'Compte AWSID du compte administrateur qui a émis l'invitation. Pour afficher les informations relatives à vos invitations, exécutez la `list-invitations`commande.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Exemple

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Dissociation des comptes membres dans Security Hub CSPM

> **Note**
>
> Nous vous recommandons d'utiliser des invitations CSPM à la AWS Organizations place du Security Hub pour gérer vos comptes de membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

Un compte administrateur AWS Security Hub CSPM peut dissocier un compte membre pour ne plus recevoir ni consulter les résultats de ce compte. Vous devez dissocier un compte membre avant de pouvoir le supprimer.

Lorsque vous dissociez un compte membre, il reste dans votre liste de comptes membres avec le statut Supprimé (Dissocié). Votre compte est supprimé des informations du compte administrateur du compte membre.

Pour continuer à recevoir les résultats relatifs au compte, vous pouvez renvoyer l'invitation. Pour supprimer complètement le compte membre, vous pouvez le supprimer.

Choisissez votre méthode préférée et suivez les étapes pour dissocier un compte de membre invité manuellement du compte d'administrateur.

Security Hub CSPM console

Pour dissocier un compte de membre invité manuellement

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

Connectez-vous à l'aide des informations d'identification du compte administrateur.

2. Dans le volet de navigation, sous Paramètres, sélectionnez Configuration.
3. Dans la section Comptes, sélectionnez les comptes que vous souhaitez dissocier.
4. Choisissez Actions, puis Dissocier le compte.

Security Hub CSPM API

Pour dissocier un compte de membre invité manuellement

Appelez l'`DisassociateMembers`API depuis le compte administrateur. Vous devez fournir les Compte AWS identifiants des comptes membres que vous souhaitez dissocier. Pour afficher la liste des comptes des membres, utilisez l'`ListMembers`opération.

AWS CLI

Pour dissocier un compte de membre invité manuellement

Exécutez la `disassociate-members`commande depuis le compte administrateur. Vous devez fournir les Compte AWS identifiants des comptes membres que vous souhaitez dissocier. Pour afficher la liste des comptes des membres, exécutez la `list-members`commande.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Exemple

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Supprimer des comptes de membres dans Security Hub CSPM

> **Note**
>
> Nous vous recommandons d'utiliser des invitations CSPM à la AWS Organizations place du Security Hub pour gérer vos comptes de membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

En tant que compte administrateur AWS Security Hub CSPM, vous pouvez supprimer les comptes de membres ajoutés sur invitation. Avant de pouvoir supprimer un compte activé, vous devez le dissocier.

Lorsque vous supprimez un compte membre, il est complètement supprimé de la liste. Pour rétablir l'adhésion au compte, vous devez l'ajouter et l'inviter à nouveau comme s'il s'agissait d'un tout nouveau compte de membre.

Vous ne pouvez pas supprimer les comptes qui appartiennent à une organisation et qui sont gérés à l'aide de l'intégration avecAWS Organizations.

Choisissez votre méthode préférée et suivez les étapes pour supprimer les comptes de membres invités manuellement.

Security Hub CSPM console

Pour supprimer un compte de membre invité manuellement

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide du compte administrateur.
2. Dans le volet de navigation, choisissez Paramètres, puis Configuration.
3. Choisissez l'onglet Comptes d'invitation. Sélectionnez ensuite les comptes à supprimer.
4. Choisissez Actions, puis Supprimer. Cette option n'est disponible que si vous avez dissocié le compte. Vous devez dissocier un compte membre avant de le supprimer.

Security Hub CSPM API

Pour supprimer un compte de membre invité manuellement

Appelez l'`DeleteMembers`API depuis le compte administrateur. Vous devez fournir les Compte AWS identifiants des comptes membres que vous souhaitez supprimer. Pour récupérer la liste des comptes membres, appelez l'`ListMembers`API.

AWS CLI

Pour supprimer un compte de membre invité manuellement

Exécutez la `delete-members`commande depuis le compte administrateur. Vous devez fournir les Compte AWS identifiants des comptes membres que vous souhaitez supprimer. Pour récupérer la liste des comptes membres, exécutez la `list-members`commande.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Exemple

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Dissociation d'un compte administrateur Security Hub CSPM

> **Note**
>
> Nous vous recommandons d'utiliser des invitations CSPM à la AWS Organizations place du Security Hub pour gérer vos comptes de membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

Si votre compte a été ajouté en tant que compte membre du AWS Security Hub CSPM sur invitation, vous pouvez dissocier le compte membre du compte administrateur. Une fois que vous avez dissocié un compte membre, Security Hub CSPM n'envoie pas les résultats du compte au compte administrateur.

Les comptes membres gérés à l'aide de l'intégration avec ne AWS Organizations peuvent pas dissocier leurs comptes du compte administrateur. Seul l'administrateur délégué du Security Hub CSPM peut dissocier les comptes membres gérés par des Organizations.

Lorsque vous vous dissociez de votre compte administrateur, celui-ci reste dans la liste des membres du compte administrateur avec le statut Désigné. Cependant, le compte administrateur ne reçoit aucune information concernant votre compte.

Une fois que vous vous êtes dissocié du compte administrateur, l'invitation à devenir membre est toujours valable. Vous pourrez accepter à nouveau l'invitation à l'avenir.

Security Hub CSPM console

Pour vous dissocier de votre compte administrateur

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Paramètres, puis Comptes.
3. Dans la section Compte administrateur, désactivez Accepter, puis choisissez Mettre à jour.

Security Hub CSPM API

Pour vous dissocier de votre compte administrateur

Appelez l'`DisassociateFromAdministratorAccount`API.

AWS CLI

Pour vous dissocier de votre compte administrateur

Exécutez la commande `disassociate-from-administrator-account`.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> La console Security Hub CSPM continue de fonctionner. `DisassociateFromMasterAccount` Il finira par changer d'usage`DisassociateFromAdministratorAccount`. Toutes les politiques IAM qui contrôlent spécifiquement l'accès à cette fonction doivent continuer à être utilisées`DisassociateFromMasterAccount`. Vous devez également compléter vos politiques `DisassociateFromAdministratorAccount` pour vous assurer que les autorisations appropriées sont en place une fois que la console commence à être utilisée`DisassociateFromAdministratorAccount`.

Transition vers Organizations pour gérer les comptes dans Security Hub CSPM

Lorsque vous gérez des comptes manuellement dans AWS Security Hub CSPM, vous devez inviter des comptes de membres potentiels et configurer chaque compte de membre séparément dans chacun d'eux. Région AWS

En intégrant Security Hub CSPMAWS Organizations, vous pouvez éliminer le besoin d'envoyer des invitations et mieux contrôler la façon dont Security Hub CSPM est configuré et personnalisé au sein de votre organisation. C'est pourquoi nous vous recommandons d'utiliser les invitations Security Hub CSPM à la AWS Organizations place des invitations Security Hub pour gérer vos comptes de membres. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations.

Il est possible d'utiliser une approche combinée dans laquelle vous utilisez l'AWS Organizationsintégration, mais vous pouvez également inviter manuellement des comptes extérieurs à votre organisation. Cependant, nous vous recommandons d'utiliser exclusivement l'intégration Organizations. La configuration centralisée, une fonctionnalité qui vous aide à gérer Security Hub CSPM sur plusieurs comptes et régions, n'est disponible que lorsque vous intégrez des Organizations.

Cette section explique comment passer de la gestion manuelle des comptes basée sur les invitations à la gestion des comptes avec. AWS Organizations

Intégration de Security Hub CSPM àAWS Organizations

Tout d'abord, vous devez intégrer Security Hub CSPM et. AWS Organizations

Vous pouvez intégrer ces services en suivant les étapes suivantes :

- Créez une organisation dansAWS Organizations. Pour obtenir des instructions, voir Création d'une organisation dans le guide de AWS Organizations l'utilisateur.
- Dans le compte de gestion des Organizations, désignez un compte d'administrateur délégué Security Hub CSPM.

> **Note**
>
> Le compte de gestion de l'organisation ne peut pas être défini comme compte DA.

Pour obtenir des instructions complètes, consultez Intégration de Security Hub CSPM àAWS Organizations.

En effectuant les étapes précédentes, vous accordez un accès sécurisé à Security Hub CSPM dans. AWS Organizations Cela active également Security Hub CSPM en cours Région AWS pour le compte administrateur délégué.

L'administrateur délégué peut gérer l'organisation dans Security Hub CSPM, principalement en ajoutant les comptes de l'organisation en tant que comptes membres du Security Hub CSPM. L'administrateur peut également accéder à certains paramètres, données et ressources du Security Hub CSPM pour ces comptes.

Lorsque vous passez à la gestion des comptes à l'aide d'Organizations, les comptes basés sur des invitations ne deviennent pas automatiquement membres du Security Hub CSPM. Seuls les comptes que vous ajoutez à votre nouvelle organisation peuvent devenir membres du Security Hub CSPM.

Après avoir activé l'intégration, vous pouvez gérer les comptes auprès des Organizations. Pour plus d'informations, consultez Gestion du Security Hub CSPM pour plusieurs comptes avecAWS Organizations. La gestion des comptes varie en fonction du type de configuration de votre organisation.

Actions autorisées par les comptes administrateur et membre dans Security Hub CSPM

Les comptes administrateur et membre ont accès aux actions CSPM du AWS Security Hub indiquées dans les tableaux suivants. Dans les tableaux, les valeurs ont les significations suivantes :

- N'importe lequel : le compte peut exécuter l'action pour n'importe quel compte membre sous le même administrateur.
- Actuel : le compte ne peut effectuer l'action que pour lui-même (le compte auquel vous êtes actuellement connecté).
- Dash — Indique que le compte ne peut pas effectuer l'action.

Comme indiqué dans les tableaux, les actions autorisées varient selon que vous les intégrez ou non AWS Organizations et selon le type de configuration utilisé par votre organisation. Pour plus d'informations sur la différence entre la configuration centrale et la configuration locale, consultezGérer des comptes avecAWS Organizations.

Security Hub CSPM ne copie pas les résultats des comptes des membres dans le compte administrateur. Dans Security Hub CSPM, tous les résultats sont ingérés dans une région spécifique pour un compte spécifique. Dans chaque région, le compte administrateur peut consulter et gérer les résultats de ses comptes membres dans cette région.

Si vous définissez une région d'agrégation, le compte administrateur peut consulter et gérer les résultats des comptes des membres provenant des régions liées qui sont répliqués dans la région d'agrégation. Pour plus d'informations sur l'agrégation entre régions, consultez la section Cross-Region Agrégation.

Les tableaux suivants indiquent les autorisations par défaut pour les comptes d'administrateur et de membre. Vous pouvez utiliser des politiques IAM personnalisées pour restreindre davantage l'accès aux fonctionnalités et fonctions du Security Hub CSPM. Pour obtenir des conseils et des exemples, consultez le billet de blog Aligning IAM policies to user personas for AWS Security Hub CSPM.

Actions autorisées si vous intégrez à Organizations et utilisez une configuration centralisée

Les comptes administrateur et membre peuvent accéder aux actions CSPM de Security Hub comme suit si vous intégrez Organizations et utilisez une configuration centralisée.

Action	Compte administrateur délégué Security Hub CSPM	Compte membre géré de manière centralisée	Self-managed compte membre
Création et gestion des politiques de configuration CSPM de Security Hub	Pour les comptes gérés de manière autonome ou centralisée	–	–
Afficher les comptes de l'organisation	N'importe lequel	–	–
Dissocier le compte membre	N'importe lequel	–	–
Supprimer le compte membre	Tout compte n'appartenant pas à une organisation	–	–

Action	Compte administrateur délégué Security Hub CSPM	Compte membre géré de manière centralisée	Self-managed compte membre
Désactiver Security Hub CSPM	Pour les comptes courants et les comptes gérés de manière centralisée	–	En cours (doit être dissocié du compte administrateur)
Afficher les résultats et retrouver l'historique	N'importe lequel	Current	Current
Mettre à jour les résultats	N'importe lequel	Current	Current
Afficher les résultats d'analyse	N'importe lequel	Current	Current
Afficher les détails du contrôle	N'importe lequel	Current	Current
Activer ou désactiver les résultats de contrôle consolidés	N'importe lequel	–	–
Activer et désactiver les normes	Pour les comptes courants et les comptes gérés de manière centralisée	–	Current
Activer et désactiver les contrôles	Pour les comptes courants et les comptes gérés de manière centralisée	–	Current
Activer et désactiver les intégrations	Current	Current	Current

Action	Compte administrateur délégué Security Hub CSPM	Compte membre géré de manière centralisée	Self-managed compte membre
Configurer l'agrégation entre régions	N'importe lequel	–	–
Sélectionnez la région d'origine et les régions associées	N'importe laquelle (vous devez arrêter et redémarrer la configuration centrale pour changer de région d'origine)	–	–
Configurer des actions personnalisées	Current	Current	Current
Configuration des règles d'automatisation	N'importe lequel	–	–
Configurer des informations personnalisées	Current	Current	Current

Actions autorisées si vous intégrez des organisations et utilisez une configuration locale

Les comptes d'administrateur et de membre peuvent accéder aux actions CSPM de Security Hub comme suit si vous les intégrez à Organizations et utilisez une configuration locale.

Action	Compte administrateur délégué Security Hub CSPM	Compte membre
Création et gestion des politiques de configuration CSPM de Security Hub	–	–

Action	Compte administrateur délégué Security Hub CSPM	Compte membre
Afficher les comptes de l'organisation	N'importe lequel	–
Dissocier le compte membre	N'importe lequel	–
Supprimer le compte membre	–	–
Désactiver Security Hub CSPM	–	En cours (si le compte est dissocié de l'administrateur délégué)
Afficher les résultats et retrouver l'historique	N'importe lequel	Current
Mettre à jour les résultats	N'importe lequel	Current
Afficher les résultats d'analyse	N'importe lequel	Current
Afficher les détails du contrôle	N'importe lequel	Current
Activer ou désactiver les résultats de contrôle consolidés	N'importe lequel	–
Activer et désactiver les normes	Current	Current
Activez automatiquement le Security Hub CSPM et les normes par défaut dans les nouveaux comptes d'entreprise	Pour les comptes courants et les nouveaux comptes de l'organisation	–
Activer et désactiver les contrôles	Current	Current

Action	Compte administrateur délégué Security Hub CSPM	Compte membre
Activer et désactiver les intégrations	Current	Current
Configurer l'agrégation entre régions	N'importe lequel	–
Configurer des actions personnalisées	Current	Current
Configuration des règles d'automatisation	N'importe lequel	–
Configurer des informations personnalisées	Current	Current

Actions autorisées pour les comptes basés sur des invitations

Les comptes d'administrateur et de membre peuvent accéder aux actions CSPM de Security Hub comme suit si vous utilisez la méthode basée sur les invitations pour gérer manuellement les comptes au lieu de les intégrer. AWS Organizations

Action	Compte administrateur Security Hub CSPM	Compte membre
Création et gestion des politiques de configuration CSPM de Security Hub	–	–
Afficher les comptes de l'organisation	N'importe lequel	–
Dissocier le compte membre	N'importe lequel	Current
Supprimer le compte membre	N'importe lequel	–

Action	Compte administrateur Security Hub CSPM	Compte membre
Désactiver Security Hub CSPM	En cours (si aucun compte de membre n'est activé)	En cours (si le compte est dissocié du compte administrateur)
Afficher les résultats et retrouver l'historique	N'importe lequel	Current
Mettre à jour les résultats	N'importe lequel	Current
Afficher les résultats d'analyse	N'importe lequel	Current
Afficher les détails du contrôle	N'importe lequel	Current
Activer ou désactiver les résultats de contrôle consolidés	N'importe lequel	–
Activer et désactiver les normes	Current	Current
Activez automatiquement le Security Hub CSPM et les normes par défaut dans les nouveaux comptes d'entreprise	–	–
Activer et désactiver les contrôles	Current	Current
Activer et désactiver les intégrations	Current	Current
Configurer l'agrégation entre régions	N'importe lequel	–

Action	Compte administrateur Security Hub CSPM	Compte membre
Configurer des actions personnalisées	Current	Current
Configuration des règles d'automatisation	N'importe lequel	–
Configurer des informations personnalisées	Current	Current

Effet des actions du compte sur les données CSPM du Security Hub

Ces actions de compte ont les effets suivants sur les données CSPM du AWS Security Hub.

Security Hub CSPM désactivé

Si vous utilisez la configuration centralisée, l'administrateur délégué (DA) peut créer des politiques de configuration Security Hub CSPM qui désactivent le AWS Security Hub CSPM dans des comptes et des unités d'organisation (UO) spécifiques. Dans ce cas, le Security Hub CSPM est désactivé dans les comptes et les unités d'organisation spécifiés dans votre région d'origine et dans toutes les régions associées. Si vous n'utilisez pas la configuration centralisée, vous devez désactiver Security Hub CSPM séparément dans chaque compte et région où vous l'avez activé. Vous ne pouvez pas utiliser la configuration centralisée si Security Hub CSPM est désactivé dans le compte DA.

Aucun résultat n'est généré ou mis à jour pour le compte administrateur si Security Hub CSPM est désactivé dans le compte administrateur. Les résultats archivés existants sont supprimés au bout de 30 jours. Les résultats actifs existants sont supprimés au bout de 90 jours.

Les intégrations avec les autres Services AWS sont supprimées.

Les normes et contrôles de sécurité activés sont désactivés.

Les autres données et paramètres du Security Hub CSPM, notamment les actions personnalisées, les informations et les abonnements à des produits tiers, sont conservés pendant 90 jours.

Compte membre dissocié du compte administrateur

Lorsqu'un compte membre est dissocié du compte administrateur, le compte administrateur perd l'autorisation de consulter les résultats du compte membre. Cependant, Security Hub CSPM est toujours activé dans les deux comptes.

Si vous utilisez la configuration centralisée, le DA ne peut pas configurer le Security Hub CSPM pour un compte membre dissocié du compte DA.

Les paramètres personnalisés ou les intégrations définis pour le compte administrateur ne sont pas appliqués aux résultats de l'ancien compte membre. Par exemple, une fois les comptes dissociés, vous pouvez avoir une action personnalisée dans le compte administrateur utilisée comme modèle d'événement dans une EventBridge règle Amazon. Toutefois, cette action personnalisée ne peut pas être utilisée dans le compte du membre.

Dans la liste des comptes du compte administrateur Security Hub CSPM, le statut Dissocié est attribué à un compte supprimé.

Le compte de membre est supprimé d'une organisation

Lorsqu'un compte membre est supprimé d'une organisation, le compte administrateur du Security Hub CSPM perd l'autorisation de consulter les résultats du compte membre. Cependant, Security Hub CSPM est toujours activé dans les deux comptes avec les mêmes paramètres qu'avant sa suppression.

Si vous utilisez la configuration centralisée, vous ne pouvez pas configurer le Security Hub CSPM pour un compte membre une fois celui-ci supprimé de l'organisation à laquelle appartient l'administrateur délégué. Toutefois, le compte conserve les paramètres qu'il avait avant sa suppression, sauf si vous les modifiez manuellement.

Dans la liste des comptes du compte administrateur Security Hub CSPM, le statut d'un compte supprimé est Deleted.

Le compte est suspendu

Lorsqu'un compte Compte AWS est suspendu, le compte perd l'autorisation de consulter ses résultats dans Security Hub CSPM. Aucun résultat n'est généré ou mis à jour pour ce compte. Le compte administrateur d'un compte suspendu peut consulter les résultats existants concernant le compte.

Pour un compte d'organisation, le statut du compte membre peut également passer à Compte suspendu. Cela se produit si le compte est suspendu au moment où le compte administrateur tente de l'activer. Le compte administrateur d'un compte suspendu ne peut pas consulter les résultats relatifs à ce compte. Dans le cas contraire, le statut suspendu n'affecte pas le statut du compte du membre.

Si vous utilisez la configuration centralisée, l'association de politiques échoue si l'administrateur délégué essaie d'associer une politique de configuration à un compte suspendu.

Après 90 jours, le compte est soit résilié, soit réactivé. Lorsque le compte est réactivé, ses autorisations Security Hub CSPM sont restaurées. Si le statut du compte membre est Compte suspendu, le compte administrateur doit activer le compte manuellement.

Le compte est fermé

Lorsqu'un Compte AWS est fermé, Security Hub CSPM répond à la fermeture comme suit.

Si le compte est un compte administrateur Security Hub CSPM, il est supprimé en tant que compte administrateur et tous les comptes membres sont supprimés. S'il s'agit d'un compte membre, il est dissocié et supprimé en tant que membre du compte administrateur Security Hub CSPM.

Security Hub CSPM conserve les résultats archivés existants dans le compte pendant 30 jours. Pour une constatation de contrôle, le calcul de 30 jours est basé sur la valeur du `UpdatedAt` champ de la constatation. Pour un autre type de résultat, le calcul est basé sur la valeur du `ProcessedAt` champ `UpdatedAt` ou du résultat, quelle que soit la date la plus récente. À la fin de cette période de 30 jours, Security Hub CSPM supprime définitivement le résultat du compte.

Security Hub CSPM conserve les résultats actifs existants dans le compte pendant 90 jours. Pour une constatation de contrôle, le calcul de 90 jours est basé sur la valeur du `UpdatedAt` champ de la constatation. Pour un autre type de résultat, le calcul est basé sur la valeur du `ProcessedAt` champ `UpdatedAt` ou du résultat, quelle que soit la date la plus récente. À la fin de cette période de 90 jours, Security Hub CSPM supprime définitivement le résultat du compte.

Pour conserver à long terme les résultats existants, vous pouvez les exporter vers un compartiment S3. Vous pouvez le faire en utilisant une action personnalisée avec une EventBridge règle Amazon. Pour de plus amples informations, veuillez consulter Utilisation à EventBridge des fins de réponse et de correction automatisées.

> **Important**
>
> Pour les clients inscritsAWS GovCloud (US) Regions, sauvegardez puis supprimez les données de votre politique et les autres ressources de votre compte avant de fermer votre compte. Vous n'aurez pas accès aux ressources et aux données après la fermeture de votre compte.

Pour plus d'informations, voir Fermer un Compte AWS dans le guide Gestion de compte AWS de référence.

Comprendre l'agrégation entre régions dans Security Hub CSPM

> **Note**
>
> La région d'agrégation est désormais appelée région d'origine. Certaines opérations de l'API CSPM du Security Hub utilisent toujours l'ancien terme « région d'agrégation ».

En utilisant l'agrégation entre régions dans AWS Security Hub CSPM, vous pouvez agréger les résultats, trouver des mises à jour, des informations, contrôler les états de conformité et les scores de sécurité de plusieurs régions d'origine Régions AWS vers une seule. Vous pouvez ensuite gérer toutes ces données depuis votre région d'origine.

Supposons que vous définissiez USA Est (Virginie du Nord) comme région d'origine, et USA Ouest (Oregon) et USA Ouest (Californie du Nord) comme régions liées. Lorsque vous consultez la page des résultats dans l'est des États-Unis (Virginie du Nord), vous voyez les résultats des trois régions. Les mises à jour de ces résultats sont également prises en compte dans les trois régions.

> **Note**
>
> DansAWS GovCloud (US), l'agrégation entre régions n'est prise en charge que pour les résultats, la recherche de mises à jour et les informations AWS GovCloud (US) croisées. Plus précisément, vous pouvez uniquement agréger les résultats, rechercher des mises à jour et des informations entre AWS GovCloud (US-East) et AWS GovCloud (US-West). Dans les régions de Chine, l'agrégation entre régions n'est prise en charge que pour les résultats, les mises à jour et les informations sur les régions de Chine. Plus précisément, vous ne pouvez

agréger les résultats, trouver des mises à jour et des informations qu'entre la Chine (Pékin) et la Chine (Ningxia).

Si un contrôle est activé dans une région liée mais désactivé dans la région d'origine, vous pouvez voir l'état de conformité du contrôle depuis la région d'origine, mais vous ne pouvez pas activer ou désactiver ce contrôle depuis la région d'origine. L'exception est si vous utilisez la configuration centralisée. Si vous utilisez la configuration centralisée, l'administrateur délégué du Security Hub CSPM peut configurer les contrôles dans la région d'origine et dans les régions associées à partir de la région d'origine.

Si vous avez défini une région d'origine, les scores de sécurité tiennent compte des statuts de contrôle dans tous Régions liées. Pour consulter les scores de sécurité et les états de conformité entre régions, ajoutez les autorisations suivantes à votre rôle IAM qui utilise Security Hub CSPM :

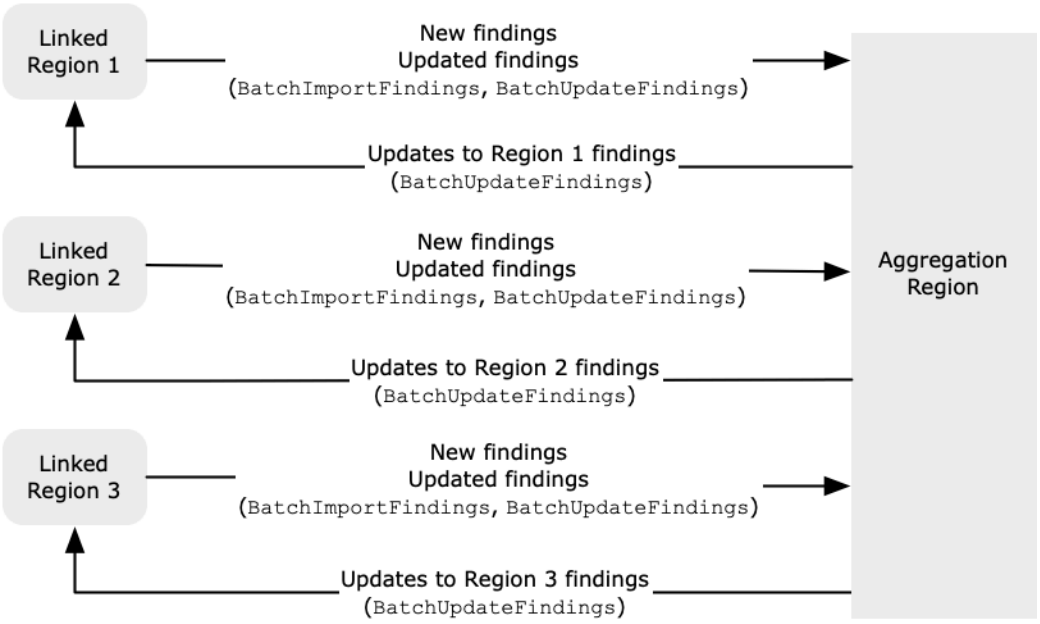
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

Types de données agrégées

Lorsque l'agrégation entre régions est activée avec une ou plusieurs régions liées, Security Hub CSPM réplique les données suivantes des régions liées vers la région d'origine. Cela se produit dans tous les comptes pour lesquels l'agrégation entre régions est activée.

- Résultats
- Informations
- Contrôlez les statuts de conformité
- Scores de sécurité

Outre les nouvelles données de la liste précédente, Security Hub CSPM réplique également les mises à jour de ces données entre les régions liées et la région d'origine. Les mises à jour effectuées dans une région liée sont répliquées dans la région d'origine. Les mises à jour effectuées dans la région d'origine sont répliquées dans la région associée. En cas de conflit entre les mises à jour de la région d'origine et de la région associée, c'est la mise à jour la plus récente qui est utilisée.



Cross-Region l'agrégation n'augmente pas le coût du Security Hub CSPM. Vous n'êtes pas débité lorsque Security Hub CSPM réplique de nouvelles données ou des mises à jour.

Dans la région d'origine, la page Résumé fournit une vue de vos résultats actifs dans les régions liées. Pour plus d'informations, voir Affichage d'un résumé interrégional des résultats par gravité. Les autres panneaux de la page de résumé qui analysent les résultats affichent également des informations provenant des régions liées.

Vos scores de sécurité dans la région d'origine sont calculés en comparant le nombre de contrôles passés au nombre de contrôles activés dans toutes les régions associées. En outre, si un contrôle est activé dans au moins une région liée, il est visible sur les pages de détails des normes de sécurité de la région d'origine. L'état de conformité des contrôles sur les pages détaillées des normes reflète les résultats obtenus dans les régions liées. Si un contrôle de sécurité associé à un contrôle échoue dans une ou plusieurs régions liées, le statut de conformité de ce contrôle s'affiche comme Échec sur les pages de détails des normes de la région d'origine. Le nombre de contrôles de sécurité inclut les résultats de toutes les régions liées.

Security Hub CSPM agrège uniquement les données des régions où Security Hub CSPM est activé sur un compte. Security Hub CSPM n'est pas automatiquement activé pour un compte en fonction de la configuration d'agrégation entre régions.

Il est possible d'activer l'agrégation entre régions sans qu'aucune région liée ne soit sélectionnée. Dans ce cas, aucune réplication de données n'a lieu.

Agrégation pour les comptes d'administrateur et de membre

Les comptes autonomes, les comptes membres et les comptes administrateurs peuvent configurer l'agrégation entre régions. Si elle est configurée par un administrateur, la présence du compte administrateur est essentielle pour que l'agrégation entre régions fonctionne dans les comptes administrés. Si le compte administrateur est supprimé ou dissocié d'un compte membre, l'agrégation entre régions pour le compte membre cesse. Cela est vrai même si l'agrégation entre régions était activée sur le compte avant le début de la relation administrateur-membre.

Lorsqu'un compte administrateur active l'agrégation entre régions, Security Hub CSPM réplique les données générées par le compte administrateur dans toutes les régions associées à la région d'origine. En outre, Security Hub CSPM identifie les comptes membres associés à cet administrateur, et chaque compte de membre hérite des paramètres d'agrégation entre régions de l'administrateur. Security Hub CSPM reproduit les données générées par un compte membre dans toutes les régions associées à la région d'origine.

L'administrateur peut accéder aux résultats de sécurité de tous les comptes membres des régions administrées et les gérer. Toutefois, en tant qu'administrateur Security Hub CSPM, vous devez être connecté à la région d'origine pour consulter les données agrégées de tous les comptes membres et des régions associées.

En tant que compte membre du Security Hub CSPM, vous devez être connecté à la région d'origine pour consulter les données agrégées de votre compte provenant de toutes les régions associées. Les comptes membres ne sont pas autorisés à consulter les données des autres comptes membres.

Un compte administrateur peut inviter manuellement des comptes de membres ou servir d'administrateur délégué d'une organisation intégrée àAWS Organizations. Pour un compte de membre invité manuellement, l'administrateur doit inviter le compte depuis la région d'origine et toutes les régions associées pour que l'agrégation entre régions fonctionne. En outre, Security Hub CSPM doit être activé dans la région d'origine et dans toutes les régions associées pour permettre à l'administrateur de consulter les résultats du compte membre. Si vous n'utilisez pas la région d'origine à d'autres fins, vous pouvez désactiver les normes CSPM et les intégrations du Security Hub dans cette région pour éviter les frais.

Si vous envisagez d'utiliser l'agrégation entre régions et que vous possédez plusieurs comptes d'administrateur, nous vous recommandons de suivre les bonnes pratiques suivantes :

- Chaque compte administrateur possède des comptes de membre différents.
- Chaque compte administrateur possède les mêmes comptes de membre dans toutes les régions.

- Chaque compte administrateur utilise une région d'origine différente.

> **Note**
>
> Pour comprendre l'impact de l'agrégation entre régions sur la configuration centrale, voirImpact de la configuration centrale sur l'agrégation entre régions.

Impact de la configuration centrale sur l'agrégation entre régions

La configuration centrale est une fonctionnalité optionnelle de AWS Security Hub CSPM que vous pouvez utiliser si vous l'intégrez. AWS Organizations Si vous utilisez la configuration centralisée, le compte administrateur délégué peut configurer le service Security Hub CSPM, les normes et les contrôles pour les comptes et les unités organisationnelles (UO) de l'organisation. Pour configurer les comptes et les unités d'organisation, l'administrateur délégué crée des politiques de configuration Security Hub CSPM. Les politiques de configuration peuvent être utilisées pour définir si Security Hub CSPM est activé ou désactivé, et quelles normes et contrôles sont activés. L'administrateur délégué associe les politiques de configuration à des comptes spécifiques, à des unités d'organisation ou à la racine (l'ensemble de l'organisation).

L'administrateur délégué peut créer et gérer des politiques de configuration pour l'organisation uniquement à partir de la région d'origine. En outre, les politiques de configuration entrent en vigueur dans la région d'origine et dans toutes les régions associées. Vous ne pouvez pas créer une politique de configuration qui s'applique uniquement à certaines régions liées et pas à d'autres. Pour plus d'informations sur l'agrégation entre régions, consultez la section Cross-Region Agrégation.

Pour utiliser la configuration centralisée, vous devez désigner une région d'origine. Vous pouvez éventuellement choisir une ou plusieurs régions comme régions liées. Vous pouvez également choisir de désigner une région d'origine sans aucune région liée.

La modification de vos paramètres d'agrégation entre régions peut avoir un impact sur vos politiques de configuration. Lorsque vous ajoutez une région liée, vos politiques de configuration prennent effet dans cette région. Si la région est une région optionnelle, elle doit être activée pour que vos politiques de configuration y prennent effet. À l'inverse, lorsque vous supprimez une région liée, les politiques de configuration ne s'appliquent plus dans cette région. Dans cette région, les comptes conservent les paramètres qu'ils avaient lorsque la région associée a été supprimée. Vous pouvez modifier ces paramètres, mais vous devez le faire séparément pour chaque compte et chaque région.

Si vous supprimez ou modifiez la région d'origine, vos politiques de configuration et vos associations de politiques sont supprimées. Vous ne pouvez plus utiliser la configuration centralisée ni créer de politiques de configuration dans aucune région. Les comptes conservent les paramètres qu'ils avaient avant la modification ou la suppression de la région d'origine. Vous pouvez modifier ces paramètres à tout moment, mais comme vous n'utilisez plus la configuration centralisée, les paramètres doivent être modifiés séparément dans chaque compte et région. Vous pouvez utiliser la configuration centralisée et créer à nouveau des politiques de configuration si vous désignez une nouvelle région d'origine.

Pour plus d'informations sur la configuration centrale, consultezComprendre la configuration centrale dans Security Hub CSPM.

Activation de l'agrégation entre régions

> **Note**
>
> La région d'agrégation est désormais appelée région d'origine. Certaines opérations de l'API CSPM du Security Hub utilisent toujours l'ancien terme « région d'agrégation ».

Vous devez activer l'agrégation entre régions à partir de la région Région AWS que vous souhaitez désigner comme région d'origine.

Pour activer l'agrégation entre régions, vous devez créer une ressource Security Hub CSPM appelée agrégateur de recherche. La ressource d'agrégation de recherche indique votre région d'origine et les régions associées (le cas échéant).

Vous ne pouvez pas utiliser une Région AWS région désactivée par défaut comme région d'origine. Pour obtenir la liste des régions désactivées par défaut, consultez la section Activation d'une région dans le Références générales AWS.

Lorsque vous activez l'agrégation entre régions, vous choisissez de spécifier une ou plusieurs régions liées si vous le souhaitez. Vous pouvez également choisir de lier automatiquement les nouvelles régions lorsque Security Hub CSPM commence à les prendre en charge et que vous les acceptez.

Security Hub CSPM console

Pour activer l'agrégation entre régions

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. À l'aide du Région AWS sélecteur, connectez-vous à la région que vous souhaitez utiliser comme région d'agrégation.
3. Dans le menu de navigation du Security Hub CSPM, sélectionnez Paramètres, puis Régions.
4. Pour Rechercher une agrégation, choisissez Configurer une agrégation de recherche.

   Par défaut, la région d'origine est définie sur Aucune région d'agrégation.
5. Sous Région d'agrégation, sélectionnez l'option permettant de désigner la région actuelle comme région d'origine.
6. Facultativement, pour les régions liées, sélectionnez les régions à partir desquelles agréger les données.
7. Pour agréger automatiquement les données des nouvelles régions dans la partition lorsque Security Hub CSPM les prend en charge et que vous les acceptez, sélectionnez Lier les futures régions.
8. Choisissez Enregistrer.

Security Hub CSPM API

Dans la région que vous souhaitez utiliser comme région d'origine, utilisez l'`CreateFindingAggregator`API Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la commande create-finding-aggregator.

Pour `RegionLinkingMode`, choisissez l'une des options suivantes :

- `ALL_REGIONS`— Security Hub CSPM agrège les données de toutes les régions. Security Hub CSPM agrège également les données des nouvelles régions au fur et à mesure qu'elles sont prises en charge et que vous les acceptez.
- `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub CSPM agrège les données de toutes les régions, à l'exception des régions que vous souhaitez exclure. Security Hub CSPM agrège également les données des nouvelles régions au fur et à mesure qu'elles sont prises en charge et que vous les acceptez. `Regions`À utiliser pour fournir la liste des régions à exclure de l'agrégation.

- `SPECIFIED_REGIONS`— Security Hub CSPM agrège les données d'une liste sélectionnée de régions. Security Hub CSPM n'agrège pas automatiquement les données des nouvelles régions. `Regions`À utiliser pour fournir la liste des régions à partir desquelles effectuer l'agrégation.
- `NO_REGIONS`— Security Hub CSPM n'agrège pas les données car vous ne sélectionnez aucune région liée.

L'exemple suivant configure l'agrégation entre régions. La région d'origine est l'est des États-Unis (Virginie du Nord). Les régions associées sont l'ouest des États-Unis (Californie du Nord) et l'ouest des États-Unis (Oregon). Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Révision des paramètres d'agrégation entre régions

> **Note**
>
> La région d'agrégation est désormais appelée région d'origine. Certaines opérations de l'API CSPM du Security Hub utilisent toujours l'ancien terme « région d'agrégation ».

Vous pouvez consulter la configuration actuelle d'agrégation entre régions dans AWS Security Hub CSPM depuis n'importe quel endroit. Région AWS La configuration inclut la région d'origine, les régions associées (le cas échéant) et indique s'il convient de lier automatiquement les nouvelles régions dans la mesure où Security Hub CSPM les prend en charge.

Les comptes membres peuvent consulter les paramètres d'agrégation entre régions configurés par le compte administrateur.

Choisissez votre méthode préférée et suivez les étapes pour afficher vos paramètres d'agrégation entre régions actuels.

Security Hub CSPM console

Pour afficher les paramètres d'agrégation entre régions (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Paramètres, puis l'onglet Régions.

Si l'agrégation entre régions n'est pas activée, l'onglet Régions affiche l'option permettant d'activer l'agrégation entre régions. Seuls les comptes d'administrateur et les comptes autonomes peuvent activer l'agrégation entre régions.

Si l'agrégation entre régions est activée, l'onglet Régions affiche les informations suivantes :

- La Région d'accueil
- S'il faut agréger automatiquement les résultats, les informations, les statuts de contrôle et les scores de sécurité des nouvelles régions prises en charge par Security Hub CSPM et auxquelles vous avez souscrit
- La liste des régions liées (si certaines sont sélectionnées)

Security Hub CSPM API

Pour consulter les paramètres d'agrégation entre régions (API Security Hub CSPM)

Utilisez le `GetFindingAggregator`fonctionnement de l'API Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la commande get-finding-aggregator.

Lorsque vous faites la demande, fournissez l'ARN de l'agrégateur de recherche. Pour obtenir l'ARN de l'agrégateur de recherche, utilisez la commande `ListFindingAggregators`operation ou list-finding-aggregators.

L'exemple suivant montre les paramètres d'agrégation entre régions pour l'ARN d'agrégateur de recherche spécifié. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne inversée (\) pour améliorer la lisibilité

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

Mise à jour des paramètres d'agrégation entre régions

> **Note**
>
> La région d'agrégation est désormais appelée région d'origine. Certaines opérations de l'API CSPM du Security Hub utilisent toujours l'ancien terme « région d'agrégation ».

Vous pouvez mettre à jour vos paramètres d'agrégation entre régions actuels dans AWS Security Hub CSPM en modifiant les régions liées ou la région d'origine actuelle. Vous pouvez également choisir d'agréger automatiquement les données provenant de nouvelles versions dans Régions AWS lesquelles Security Hub CSPM est pris en charge.

Les modifications apportées à l'agrégation entre régions ne sont pas mises en œuvre pour une région optionnelle tant que vous n'activez pas la région dans votre. Compte AWS Les régions AWS introduites le 20 mars 2019 ou après cette date sont des régions optionnelles.

Lorsque vous arrêtez d'agréger les données d'une région liée, AWS Security Hub CSPM ne supprime aucune donnée agrégée existante de cette région accessible dans la région d'origine.

Vous ne pouvez pas utiliser les procédures de mise à jour décrites dans cette section pour modifier la région d'origine. Pour modifier la région d'origine, vous devez effectuer les opérations suivantes :

1. Arrêtez l'agrégation entre régions. Pour obtenir des instructions, veuillez consulter the section called “Arrêt de l'agrégation”.
2. Choisissez la région que vous souhaitez utiliser comme nouvelle région d'origine.
3. Activez l'agrégation entre régions. Pour obtenir des instructions, veuillez consulter the section called “Activer l'agrégation”.

Vous devez mettre à jour la configuration d'agrégation entre régions à partir de la région d'origine actuelle.

Security Hub CSPM console

Pour modifier les régions liées

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

Connectez-vous à la région d'agrégation actuelle.

2. Dans le menu de navigation du Security Hub CSPM, sélectionnez Paramètres, puis Régions.
3. Pour Rechercher une agrégation, choisissez Modifier.
4. Pour les régions liées, mettez à jour les régions liées sélectionnées.
5. Si nécessaire, modifiez si l'option Lier les futures régions est sélectionnée. Ce paramètre détermine si Security Hub CSPM lie automatiquement les nouvelles régions au fur et à mesure qu'il les prend en charge et que vous les acceptez.
6. Choisissez Enregistrer.

Security Hub CSPM API

Utilisez l'`UpdateFindingAggregator`opération. Si vous utilisez leAWS CLI, exécutez la commande update-finding-aggregator. Pour identifier l'agrégateur de recherche, vous devez fournir l'ARN de l'agrégateur de recherche. Pour obtenir l'ARN de l'agrégateur de recherche, utilisez l'`ListFindingAggregators`opération ou la commande list-finding-aggregators.

Si le mode de liaison est `ALL_REGIONS_EXCEPT_SPECIFIED` ou`SPECIFIED_REGIONS`, vous pouvez modifier la liste des régions exclues ou incluses. Si vous souhaitez passer au mode de liaison des régions`NO_REGIONS`, vous ne devez pas fournir de liste de régions.

Lorsque vous modifiez la liste des régions exclues ou incluses, vous devez fournir la liste complète avec les mises à jour. Supposons, par exemple, que vous agrégez actuellement les résultats de l'est des États-Unis (Ohio) et que vous souhaitez également agréger les résultats de l'ouest des États-Unis (Oregon). Vous devez fournir une `Regions` liste contenant à la fois l'est des États-Unis (Ohio) et l'ouest des États-Unis (Oregon).

L'exemple suivant met à jour l'agrégation entre régions pour les régions sélectionnées. La commande est exécutée depuis la région d'origine actuelle, à savoir l'est des États-Unis (Virginie du Nord). Les régions associées sont l'ouest des États-Unis (Californie du Nord) et l'ouest des États-Unis (Oregon). Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Arrêt de l'agrégation entre régions

> **Note**
>
> La région d'agrégation est désormais appelée région d'origine. Certaines opérations de l'API CSPM du Security Hub utilisent toujours l'ancien terme « région d'agrégation ».

Si vous ne souhaitez pas que AWS Security Hub CSPM agrège les données, vous pouvez supprimer votre agrégateur de recherches. Vous pouvez également conserver votre agrégateur de recherches mais ne pas le lier Régions AWS à la région d'origine en mettant à jour l'agrégateur existant en mode de `NO_REGIONS` liaison.

Pour modifier votre région d'origine, vous devez supprimer votre agrégateur de recherche actuel et en créer un nouveau.

Lorsque vous supprimez votre agrégateur de recherches, Security Hub CSPM arrête d'agréger les données. Cela ne supprime aucune donnée agrégée existante de la région d'origine.

Suppression de l'agrégateur de recherches (console)

Vous ne pouvez supprimer votre agrégateur de résultats que dans la région d'origine actuelle.

Dans les régions autres que la région d'origine, le panneau d'agrégation de recherche de la console Security Hub CSPM affiche un message indiquant que vous devez modifier la configuration dans la région d'origine. Choisissez ce message pour afficher un lien permettant de passer à la région d'origine.

Security Hub CSPM console

Pour arrêter l'agrégation entre régions (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Assurez-vous d'être connecté à votre région d'origine actuelle.
3. Dans le menu de navigation du Security Hub CSPM, sélectionnez Paramètres, puis Régions.
4. Sous Recherche d'une agrégation, sélectionnez Modifier.
5. Sous Région d'agrégation, sélectionnez Aucune région d'agrégation.
6. Choisissez Enregistrer.

7. Dans la boîte de dialogue de confirmation, dans le champ de confirmation, tapez**Confirm**.
8. Choisissez Confirmer.

Security Hub CSPM API

Utilisez le DeleteFindingAggregatorfonctionnement de l'API Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la delete-finding-aggregatorcommande.

Pour identifier l'agrégateur de recherche à supprimer, fournissez l'ARN de l'agrégateur de recherche. Pour obtenir l'ARN de l'agrégateur de recherche, utilisez l'ListFindingAggregatorsopération ou la list-finding-aggregatorscommande.

L'exemple suivant supprime l'agrégateur de résultats. La commande est exécutée depuis la région d'origine actuelle, à savoir l'est des États-Unis (Virginie du Nord). Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-
east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --
region us-east-1
```

Comprendre les normes de sécurité dans Security Hub CSPM

Dans AWS Security Hub CSPM, une norme de sécurité est un ensemble d'exigences basées sur les cadres réglementaires, les meilleures pratiques du secteur ou les politiques de l'entreprise. Pour plus de détails sur les normes actuellement prises en charge par Security Hub CSPM, y compris les contrôles de sécurité qui s'appliquent à chacune d'elles, consultez le. Référence des normes pour Security Hub CSPM

Lorsque vous activez une norme, Security Hub CSPM active automatiquement tous les contrôles qui s'appliquent à la norme. Security Hub CSPM exécute ensuite des contrôles de sécurité, ce qui génère les résultats du Security Hub CSPM. Vous pouvez désactiver puis réactiver des contrôles individuels si nécessaire. Vous pouvez également désactiver complètement une norme. Si vous désactivez une norme, Security Hub CSPM arrête d'exécuter des contrôles de sécurité sur les contrôles qui s'appliquent à la norme. Les résultats ne sont plus générés pour les contrôles.

Outre les résultats, Security Hub CSPM génère un score de sécurité pour chaque norme que vous activez. Le score est basé sur l'état des contrôles qui s'appliquent à la norme. Si vous définissez

une région d'agrégation, le score de sécurité d'une norme reflète l'état des contrôles dans toutes les régions liées. Si vous êtes l'administrateur Security Hub CSPM d'une organisation, le score reflète l'état des contrôles pour tous les comptes de votre organisation. Pour de plus amples informations, veuillez consulter Calcul des scores de sécurité.

Pour consulter et gérer les normes, vous pouvez utiliser la console Security Hub CSPM ou l'API Security Hub CSPM. Sur la console, la page Normes de sécurité affiche toutes les normes de sécurité actuellement prises en charge par Security Hub CSPM. Cela inclut une description de chaque norme et l'état actuel de la norme. Si vous activez une norme, vous pouvez également utiliser cette page pour accéder à des informations supplémentaires sur la norme. Par exemple, vous pouvez consulter :

- Le score de sécurité actuel de la norme.
- Statistiques agrégées pour les contrôles qui s'appliquent à la norme.
- Liste des contrôles qui s'appliquent à la norme et sont actuellement activés, y compris l'état de conformité de chacun d'entre eux.
- Liste des contrôles qui s'appliquent à la norme mais qui sont actuellement désactivés.

Pour une analyse plus approfondie, vous pouvez filtrer et trier les données, puis effectuer une analyse détaillée pour examiner les détails des contrôles individuels qui s'appliquent à la norme.

Vous pouvez activer les normes individuellement pour un seul compte et Région AWS. Toutefois, pour gagner du temps et réduire la dérive de configuration dans les environnements multicomptes et multirégions, nous vous recommandons d'utiliser une configuration centralisée pour activer et gérer les normes. Grâce à la configuration centralisée, l'administrateur délégué de Security Hub CSPM peut créer des politiques qui spécifient comment configurer une norme pour plusieurs comptes et régions.

Rubriques

- Référence des normes pour Security Hub CSPM
- Mise en place d'une norme de sécurité
- Révision des détails d'une norme de sécurité
- Désactivation des normes de sécurité activées automatiquement
- Désactivation d'une norme de sécurité

Référence des normes pour Security Hub CSPM

Dans AWS Security Hub CSPM, une norme de sécurité est un ensemble d'exigences basées sur les cadres réglementaires, les meilleures pratiques du secteur ou les politiques de l'entreprise. Security Hub CSPM associe ces exigences aux contrôles et effectue des contrôles de sécurité sur les contrôles afin de déterminer si les exigences d'une norme sont respectées. Chaque norme comprend plusieurs commandes.

Security Hub CSPM prend actuellement en charge les normes suivantes :

- AWS Meilleures pratiques fondamentales en matière de sécurité : développée par des professionnels du secteur AWS et développée par des professionnels du secteur, cette norme est une compilation des meilleures pratiques de sécurité pour les organisations, quels que soient leur secteur ou leur taille. Il fournit un ensemble de contrôles qui détectent lorsque vous Comptes AWS et vos ressources s'écartent des meilleures pratiques de sécurité. Il fournit également des conseils prescriptifs sur la manière d'améliorer et de maintenir votre posture de sécurité.
- Meilleures pratiques en matière de sécurité de l'IA : développée par des experts en AWS sécurité, cette norme fournit un ensemble de contrôles sélectionnés qui détectent les cas où les ressources d'IA déployées ne sont pas conformes aux meilleures pratiques de sécurité. Il vous aide à identifier les domaines dans lesquels vos charges de travail d'IA s'écartent des configurations de sécurité recommandées, dans des domaines tels que l'isolation du réseau, le chiffrement, le placement des VPC et AWS KMS l'utilisation des clés.
- AWS Balisage des ressources : développée par Security Hub CSPM, cette norme peut vous aider à déterminer si vos AWS ressources comportent des balises. Une balise est une paire clé-valeur qui fait office de méta-donnée pour une AWS ressource. Les balises peuvent vous aider à identifier, classer, gérer et rechercher des AWS ressources. Par exemple, vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire ou environnement.
- CIS AWS Foundations Benchmark — Développée par le Center for Internet Security (CIS), cette norme fournit des directives de configuration sécurisée pour AWS. Il spécifie un ensemble de directives de configuration de sécurité et de meilleures pratiques pour un sous-ensemble de Services AWS ressources, en mettant l'accent sur les paramètres fondamentaux, testables et indépendants de l'architecture. Les directives comprennent des procédures de mise en œuvre et d'évaluation claires et étape par étape.
- NIST SP 800-53 Revision 5 — Cette norme est conforme aux exigences du National Institute of Standards and Technology (NIST) en matière de protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information et des ressources critiques. Le cadre associé s'applique généralement aux U.S agences fédérales ou aux organisations qui travaillent avec U.S. agences

fédérales ou systèmes d'information. Cependant, les organisations privées peuvent également utiliser les exigences comme cadre directeur.

- NIST SP 800-171 Revision 2 — Cette norme est conforme aux recommandations et exigences de sécurité du NIST pour protéger la confidentialité des informations contrôlées non classifiées (CUI) dans les systèmes et les organisations qui ne font pas partie du gouvernement fédéral. U.S Les CUI sont des informations qui ne répondent pas aux critères de classification du gouvernement, mais qui sont considérées comme sensibles et qui sont créées ou détenues par le U.S gouvernement fédéral ou d'autres entités au nom du gouvernement fédéral U.S.
- PCI DSS — Cette norme s'aligne sur le cadre de conformité à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) défini par le PCI Security Standards Council (SSC). Le cadre fournit un ensemble de règles et de directives pour traiter en toute sécurité les informations relatives aux cartes de crédit et de débit. Le cadre s'applique généralement aux organisations qui stockent, traitent ou transmettent les données des titulaires de cartes.
- Service-managed standard, AWS Control Tower — Cette norme vous aide à configurer les contrôles de détection fournis par Security Hub CSPM à partir de. AWS Control Tower AWS Control Tower offre un moyen simple de configurer et de gérer un environnement AWS multi-comptes, en suivant les meilleures pratiques prescriptives.

Les normes et contrôles de Security Hub CSPM ne garantissent pas la conformité aux cadres réglementaires ou aux audits. Ils fournissent plutôt un moyen d'évaluer et de surveiller l'état de vos ressources Comptes AWS et de vos ressources. Nous vous recommandons d'activer chaque norme adaptée aux besoins de votre entreprise, à votre secteur d'activité ou à votre cas d'utilisation.

Les contrôles individuels peuvent s'appliquer à plusieurs normes. Si vous activez plusieurs normes, nous vous recommandons d'activer également les résultats de contrôle consolidés. Dans ce cas, Security Hub CSPM génère un résultat unique pour chaque contrôle, même si le contrôle s'applique à plusieurs normes. Si vous n'activez pas les résultats des contrôles consolidés, Security Hub CSPM génère un résultat distinct pour chaque norme activée à laquelle un contrôle s'applique. Par exemple, si vous activez deux normes et qu'un contrôle s'applique aux deux, vous recevez deux résultats distincts pour le contrôle, un pour chaque norme. Si vous activez les résultats de contrôle consolidés, vous ne recevez qu'un seul résultat pour le contrôle. Pour de plus amples informations, veuillez consulter Conclusions de contrôle consolidées.

Référence détaillée par norme

- AWS Norme fondamentale des meilleures pratiques de sécurité dans Security Hub CSPM
- Norme relative aux meilleures pratiques en matière de sécurité de l'IA dans Security Hub CSPM

- AWS Norme de balisage des ressources dans Security Hub CSPM
- CIS AWS Point de référence des fondations en matière de sécurité CSPM
- NIST SP 800-53 Révision 5 dans Security Hub CSPM
- NIST SP 800-171 Revision 2 dans Security Hub CSPM
- PCI DSS dans Security Hub CSPM
- Service-managed normes du Security Hub CSPM

AWS Norme fondamentale des meilleures pratiques de sécurité dans Security Hub CSPM

Développée par AWS des professionnels du secteur, la norme FSBP (AWS Foundational Security Best Practices) est une compilation des meilleures pratiques de sécurité pour les organisations, quels que soient leur secteur ou leur taille. Il fournit un ensemble de contrôles qui détectent quand Comptes AWS et quand les ressources s'écartent des meilleures pratiques de sécurité. Il fournit également des conseils prescriptifs sur la manière d'améliorer et de maintenir la posture de sécurité de votre organisation.

Dans AWS Security Hub CSPM, la norme des meilleures pratiques de sécurité AWS fondamentales inclut des contrôles qui évaluent en permanence vos charges de travail Comptes AWS et vous aident à identifier les domaines qui s'écartent des meilleures pratiques de sécurité. Les contrôles incluent les meilleures pratiques de sécurité pour les ressources provenant de plusieurs sources Services AWS. Chaque contrôle se voit attribuer une catégorie qui reflète la fonction de sécurité à laquelle le contrôle s'applique. Pour obtenir la liste des catégories et des informations supplémentaires, consultezCatégories de contrôle.

Contrôles qui s'appliquent à la norme

La liste suivante indique les contrôles CSPM AWS de Security Hub qui s'appliquent à la norme AWS Foundational Security Best Practices (v1.0.0). Pour consulter les détails d'un contrôle, choisissez-le.

[Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS

[ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée

[ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits

[APIGateway.1] API Gateway REST et la journalisation de l'exécution des WebSocket API doivent être activés

[APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend

[APIGateway.3] Les étapes de l'API REST API Gateway doivent avoir AWS X-Ray traçage activé

[APIGateway.4] API Gateway doit être associée à une ACL Web WAF

[APIGateway.5] Les données du cache de l'API REST API Gateway doivent être chiffrées au repos

[APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation

[APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2

[APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées

[APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées

[AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos

[AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée

[AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API

[AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport

[Athena.4] La journalisation des groupes de travail Athena doit être activée

[AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB

[AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité

[AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)

[Autoscaling.5] Les instances Amazon EC2 lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresses IP publiques

[AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité

[AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2

[Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos

[BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC

[BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes

[BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public

[BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock

[CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles

[CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés

[CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut

[CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit

[CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré

[CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée

[CloudFront.6] CloudFront les distributions doivent avoir le WAF activé

[CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés

[CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS

[CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées

[CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées

[CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

[CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine

[CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée

[CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda

[CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies

[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs

[CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles

[CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair

[CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés

[CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée

[CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos

[Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées

[Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste

[Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée

[Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito

[Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

[Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée

[DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos

[DataSync.1] la journalisation des DataSync tâches doit être activée

[DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques

[DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée

[DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée

[DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée

[DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL

[DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune

[DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé

[DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS

[DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité

[DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos

[DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

[DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics

[DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch

[DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée

[DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport

[DynamoDB.1] Les tables DynamoDB doivent automatiquement adapter la capacité à la demande

[DynamoDB.2] La restauration instantanée des tables DynamoDB doit être activée

[DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos

[DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée

[DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit

[EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

[EC2.3] Les volumes Amazon EBS joints doivent être chiffrés au repos

[EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

[EC2.7] Le chiffrement par défaut d'EBS doit être activé

[EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

[EC2.9] Les instances Amazon EC2 ne doivent pas avoir d'adresse IPv4 publique

[EC2.10] Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2

[EC2.15] Les sous-réseaux Amazon EC2 ne doivent pas attribuer automatiquement d'adresses IP publiques

[EC2.16] Les listes de contrôle d'accès réseau non utilisées doivent être supprimées

[EC2.17] Les instances Amazon EC2 ne doivent pas utiliser plusieurs ENI

[EC2.18] Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés

[EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé

[EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active

[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389

[EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC

[EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés

[EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau

[EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2

[EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR

[EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry

[EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager

[EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager

[EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager

[EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

[EC2.171] La journalisation des connexions VPN EC2 doit être activée

[EC2.172] Les paramètres d'accès public EC2 VPC Block devraient bloquer le trafic de passerelle Internet

[EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés

[EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2

[EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés

[EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS

[EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2

[ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée

[ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée

[ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée

[ECS.2] Aucune adresse IP publique ne doit être attribuée automatiquement aux services ECS

[ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte

[ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés

[ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine

[ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur

[ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation

[ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate

[ECS.12] Les clusters ECS doivent utiliser Container Insights

[ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques

[ECS.18] Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS

[ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée

[ECS.20] Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux

[ECS.21] Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows

[EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS

[EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde

[EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine

[EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur

[EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS

[EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos

[EKS.1] Les points de terminaison du cluster EKS ne doivent pas être accessibles au public

[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge

[EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés

[EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée

[EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge

[ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées

[ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters

[ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication

[ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos

[ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport

[ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé

[ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut

[ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés

[ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées

[ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch

[ELB.1] L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS

[ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager

[ELB.3] Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS

[ELB.4] L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP non valides

[ELB.5] La journalisation des applications et des équilibreurs de charge classiques doit être activée

[ELB.6] La protection contre la suppression doit être activée pour les équilibreurs de charge des applications, des passerelles et du réseau

[ELB.7] Le drainage des connexions doit être activé pour les équilibreurs de charge classiques

[ELB.8] Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie qui est solide AWS Config durée

[ELB.9] L'équilibrage de charge entre zones doit être activé pour les équilibreurs de charge classiques

[ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité

[ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict

[ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité

[ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict

[ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées

[ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit

[ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés

[ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés

[EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques

[EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé

[EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos

[EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport

[ES.1] Le chiffrement au repos doit être activé pour les domaines Elasticsearch

[ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public

[ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds

[ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée

[ES.5] La journalisation des audits doit être activée pour les domaines Elasticsearch

[ES.6] Les domaines Elasticsearch doivent comporter au moins trois nœuds de données

[ES.7] Les domaines Elasticsearch doivent être configurés avec au moins trois nœuds principaux dédiés

[ES.8] Les connexions aux domaines Elasticsearch doivent être chiffrées conformément à la dernière politique de sécurité TLS

[EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources

[FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes

[FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes

[FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ

[FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ

[FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement

[Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos

[Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue

[GuardDuty.1] GuardDuty doit être activé

[GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée

[GuardDuty.6] La protection GuardDuty Lambda doit être activée

[GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée

[GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée

[GuardDuty.9] GuardDuty La protection RDS doit être activée

[GuardDuty.10] La protection GuardDuty S3 doit être activée

[GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée

[GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée

[GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée

[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets

[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes

[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées

[IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services

[Inspector.1] La numérisation Amazon Inspector EC2 doit être activée

[Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée

[Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée

[Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé

[Kinesis.1] Les flux Kinesis doivent être chiffrés au repos

[Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate

[KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS

[KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS

[KMS.3]AWS KMS keysne doit pas être supprimé par inadvertance

[KMS.5] Les clés KMS ne doivent pas être accessibles au public

[Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public

[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge

[Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité

[Macie.1] Amazon Macie devrait être activé

[Macie.2] La découverte automatique des données sensibles par Macie doit être activée

[MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch

[MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier

[MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport

[MSK.4] L'accès public aux clusters MSK doit être désactivé

[MSK.5] La journalisation des connecteurs MSK doit être activée

[MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié

[Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos

[Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch

[Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics

[Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée

[Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées

[Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos

[Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune

[Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés

[NetworkFirewall.2] La journalisation du Network Firewall doit être activée

[NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles

[NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.

[NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.

[NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide

[NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall

[NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall

[Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines

[Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public

[Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds

[Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée

[Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines

[Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données

[Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé

[Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS

[Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée

[PCA.1]CA privée AWSI'autorité de certification racine doit être désactivée

[Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS

[RDS.1] L'instantané RDS doit être privé

[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration

[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé

[RDS.4] Les instantanés du cluster RDS et les instantanés de base de données doivent être chiffrés au repos

[RDS.5] Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité

[RDS.6] Une surveillance améliorée doit être configurée pour les instances de base de données RDS

[RDS.7] La protection contre la suppression des clusters RDS doit être activée

[RDS.8] La protection contre la suppression des instances de base de données RDS doit être activée

[RDS.9] Les instances de base de données RDS doivent publier des CloudWatch journaux dans Logs

[RDS.10] L'authentification IAM doit être configurée pour les instances RDS

[RDS.11] Les sauvegardes automatiques doivent être activées sur les instances RDS

[RDS.12] L'authentification IAM doit être configurée pour les clusters RDS

[RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées

[RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora

[RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité

[RDS.16] Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données

[RDS.17] Les instances de base de données RDS doivent être configurées pour copier les balises dans les instantanés

[RDS.19] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements de cluster critiques

[RDS.20] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques

[RDS.21] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de groupe de paramètres de base de données critiques

[RDS.22] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements critiques du groupe de sécurité des bases de données

[RDS.23] Les instances RDS ne doivent pas utiliser le port par défaut d'un moteur de base de données

[RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

[RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

[RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos

[RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs

[RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée

[RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch

[RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch

[RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs

[RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit

[RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch

[RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions

[RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit

[RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL

[RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet

[RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données

[RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données

[RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante

[RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge

[Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public

[Redshift.2] Les connexions aux clusters Amazon Redshift doivent être chiffrées pendant le transit

[Redshift.3] Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift

[Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift

[Redshift.6] Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures

[Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré

[Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut

[Redshift.10] Les clusters Redshift doivent être chiffrés au repos

[Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes

[Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ

[RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré

[RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL

[RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public

[RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut

[RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

[S3.2] Les compartiments S3 à usage général devraient bloquer l'accès public en lecture

[S3.3] Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

[S3.6] Les politiques de bucket à usage général S3 devraient restreindre l'accès aux autres Comptes AWS

[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public

[S3.9] Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée

[S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3

[S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie

[S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés

[S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

[S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie

[SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet

[SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé

[SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes

[SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1

[SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée

[SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge

[SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé

[SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

[SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée

[SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée

[SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé

[SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée

[SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

[SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux

[SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés

[SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs

[SecretsManager.1] La rotation automatique des secrets des secrets de Secrets Manager doit être activée

[SecretsManager.2] Les secrets de Secrets Manager configurés avec une rotation automatique devraient être correctement pivotés

[SecretsManager.3] Supprimer les secrets inutilisés du Gestionnaire de Secrets

[SecretsManager.4] Les secrets de Secrets Manager doivent être renouvelés dans un délai spécifié

[ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement

[SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails

[SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public

[SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos

[SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public

[SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager

[SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif

[SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT

[SSM.4] Les documents SSM ne doivent pas être publics

[SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation

[SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM

[StepFunctions.1] La journalisation des machines à états Step Functions doit être activée

[Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux

[Transfer.3] La journalisation des connecteurs Transfer Family doit être activée

[WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée

[WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition

[WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle

[WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles

[WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition

[WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle

[WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

[WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles

[WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles

[WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos

[WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Norme relative aux meilleures pratiques en matière de sécurité de l'IA dans Security Hub CSPM

La norme AI Security Best Practices est un ensemble de contrôles de sécurité automatisés qui détectent lorsque les ressources IA déployées ne sont pas conformes aux meilleures pratiques de sécurité. Développée par des experts en AWS sécurité, cette norme fournit un ensemble de contrôles sélectionnés qui vous aident à identifier les domaines dans lesquels vos charges de travail d'IA s'écartent des configurations de sécurité recommandées.

Dans AWS Security Hub CSPM, la norme AI Security Best Practices inclut des contrôles qui évaluent en permanence vos ressources. Les contrôles couvrent les domaines de sécurité, y compris, mais sans s'y limiter, l'isolation du réseau, le chiffrement au repos et en transit, le placement des VPC, l'utilisation des AWS KMS clés et les exigences relatives au registre privé. Chaque contrôle se voit attribuer une catégorie qui reflète la fonction de sécurité à laquelle le contrôle s'applique. Pour obtenir la liste des catégories et des informations supplémentaires, consultezCatégories de contrôle dans Security Hub CSPM.

La norme AI Security Best Practices porte le nom de ressource Amazon (ARN) suivant :`arn:aws:securityhub:`*`region`*`::standards/ai-security-best-practices/v/1.0.0`, où se *`region`* trouve le code de région correspondant à la ressource applicable Région AWS. Vous pouvez également utiliser le GetEnabledStandards fonctionnement de l'API CSPM Security Hub pour récupérer l'ARN d'une norme actuellement activée.

Contrôles qui s'appliquent à la norme

La liste suivante indique les contrôles CSPM AWS de Security Hub qui s'appliquent à la norme AI Security Best Practices (v1.0.0). Pour consulter les détails d'un contrôle, choisissez-le.

- [Bedrock.1] Les sources de données Amazon Bedrock doivent être cryptées et gérées par le clientAWS KMSclés

- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [BedrockAgentCore.7] Les interpréteurs de code AgentCore personnalisés de Bedrock doivent utiliser une configuration de réseau privé
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée

- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SageMaker.20] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.21] les instances de SageMaker bloc-notes doivent être chiffrées avec la gestion par le client AWS KMS clés
- [SageMaker.22] les calendriers SageMaker de surveillance doivent avoir activé le cryptage du trafic inter-conteneurs
- [SageMaker.23] les expériences SageMaker d'inférence doivent avoir un volume de stockage d'instance chiffré et géré par le client AWS KMS clés
- [SageMaker.24] les expériences SageMaker d'inférence doivent avoir un stockage de données crypté et géré par le client AWS KMS clés
- [SageMaker.25] les définitions de tâches relatives à la qualité des SageMaker modèles doivent avoir l'isolation réseau activée

AWS Norme de balisage des ressources dans Security Hub CSPM

La norme AWS Resource Tagging, développée par AWS Security Hub CSPM, vous aide à déterminer s'il manque des balises à vos AWS ressources. Les balises sont des paires clé-valeur qui font office de métadonnées pour l'organisation AWS des ressources. Pour la plupart des AWS ressources, vous avez la possibilité d'ajouter des balises à une ressource lorsque vous créez la ressource ou après la création de la ressource. Les exemples de ressources incluent les CloudFront distributions Amazon, les instances Amazon Elastic Compute Cloud (Amazon EC2) et les secrets

dans AWS Secrets Manager. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer AWS les ressources.

Chaque balise se compose de deux parties :

- Une clé de balise, par exemple `CostCenterEnvironment`, ou. `Project` Les touches des tags distinguent les majuscules et minuscules.
- Une valeur de balise, par exemple, `111122223333` ou. `Production` Les valeurs de balise sont sensibles à la casse, tout comme les clés de balise.

Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour plus d'informations sur l'ajout de balises aux AWS ressources, consultez le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Pour chaque contrôle qui s'applique à la norme AWS Resource Tagging dans Security Hub CSPM, vous pouvez éventuellement utiliser le paramètre pris en charge pour spécifier les clés de balise que vous souhaitez que le contrôle vérifie. Si vous ne spécifiez aucune clé de balise, le contrôle vérifie uniquement l'existence d'au moins une clé de balise et échoue si une ressource ne possède aucune clé de balise.

Avant d'activer la norme AWS Resource Tagging, il est important d'activer et de configurer l'enregistrement des ressources dans AWS Config. Lorsque vous configurez l'enregistrement des ressources, veillez également à l'activer pour tous les types de AWS ressources qui sont vérifiés par les contrôles qui s'appliquent à la norme. Dans le cas contraire, Security Hub CSPM pourrait ne pas être en mesure d'évaluer les ressources appropriées et de générer des résultats précis pour les contrôles qui s'appliquent à la norme. Pour plus d'informations, y compris une liste des types de ressources à enregistrer, consultezAWS ConfigRessources requises pour les résultats des contrôles.

Une fois que vous avez activé la norme de balisage AWS des ressources, vous commencez à recevoir les résultats des contrôles qui s'appliquent à la norme. Notez que Security Hub CSPM peut prendre jusqu'à 18 heures pour générer des résultats pour les contrôles qui utilisent la même règle AWS Config liée aux services que les contrôles qui s'appliquent à d'autres normes activées. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

La norme AWS Resource Tagging possède le nom de ressource Amazon (ARN) suivant :`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`, où se *`region`* trouve le code de région correspondant à la ressource applicable Région

AWS. Vous pouvez également utiliser le GetEnabledStandards fonctionnement de l'API CSPM Security Hub pour récupérer l'ARN d'une norme actuellement activée.

> **Note**
>
> La norme AWS Resource Tagging n'est pas disponible dans les régions Asie-Pacifique (Nouvelle-Zélande) et Asie-Pacifique (Taipei).

Contrôles applicables à la norme

La liste suivante indique les contrôles CSPM AWS de Security Hub qui s'appliquent à la norme AWS Resource Tagging (v1.0.0). Pour consulter les détails d'un contrôle, choisissez-le.

- [ACM.3] Les certificats ACM doivent être balisés
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées
- [Athena.2] Les catalogues de données Athena doivent être balisés
- [Athena.3] Les groupes de travail Athena doivent être étiquetés
- [AutoScaling.10] Les groupes EC2 Auto Scaling doivent être balisés
- [Backup.2]AWS Backuples points de récupération doivent être étiquetés
- [Backup.3]AWS Backuples coffres-forts doivent être étiquetés
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Backup.5]AWS Backuples plans de sauvegarde doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées

- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [CloudFormation.2] les CloudFormation piles doivent être étiquetées
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudTrail.9] les CloudTrail sentiers doivent être balisés
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DynamoDB.5] Les tables DynamoDB doivent être balisées
- [EC2.33] Les pièces jointes de la passerelle de transit EC2 doivent être étiquetées
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.35] Les interfaces réseau EC2 doivent être étiquetées
- [EC2.36] Les passerelles client EC2 doivent être étiquetées
- [EC2.37] Les adresses IP Elastic EC2 doivent être balisées
- [EC2.38] Les instances EC2 doivent être étiquetées
- [EC2.39] Les passerelles Internet EC2 doivent être étiquetées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.41] Les ACL du réseau EC2 doivent être balisées
- [EC2.42] Les tables de routage EC2 doivent être étiquetées
- [EC2.43] Les groupes de sécurité EC2 doivent être balisés

- [EC2.44] Les sous-réseaux EC2 doivent être balisés
- [EC2.45] Les volumes EC2 doivent être balisés
- [EC2.46] Les Amazon VPC doivent être balisés
- [EC2.47] Les services de point de terminaison Amazon VPC doivent être balisés
- [EC2.48] Les journaux de flux Amazon VPC doivent être balisés
- [EC2.49] Les connexions d'appairage Amazon VPC doivent être étiquetées
- [EC2.50] Les passerelles VPN EC2 doivent être étiquetées
- [EC2.52] Les passerelles de transit EC2 doivent être étiquetées
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECS.13] Les services ECS doivent être balisés
- [ECS.14] Les clusters ECS doivent être balisés
- [ECS.15] Les définitions de tâches ECS doivent être étiquetées
- [EFS.5] Les points d'accès EFS doivent être balisés
- [EKS.6] Les clusters EKS doivent être balisés
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées
- [ES.9] Les domaines Elasticsearch doivent être balisés
- [EventBridge.2] les bus EventBridge d'événements doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.1]AWS Glueles emplois doivent être étiquetés

- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [GuardDuty.3] Les GuardDuty IPsets doivent être balisés
- [GuardDuty.4] les GuardDuty détecteurs doivent être étiquetés
- [IAM.23] Les analyseurs IAM Access Analyzer doivent être étiquetés
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.2] Les flux Kinesis doivent être balisés

- [Lambda.6] Les fonctions Lambda doivent être balisées
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [NetworkFirewall.7] Les pare-feux Network Firewall doivent être étiquetés
- [NetworkFirewall.8] Les politiques de pare-feu de Network Firewall doivent être étiquetées
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.28] Les clusters de bases de données RDS doivent être balisés
- [RDS.29] Les instantanés du cluster de bases de données RDS doivent être balisés
- [RDS.30] Les instances de base de données RDS doivent être balisées
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.32] Les instantanés de base de données RDS doivent être balisés
- [RDS.33] Les groupes de sous-réseaux de base de données RDS doivent être balisés
- [Redshift.11] Les clusters Redshift doivent être balisés
- [Redshift.12] Les abonnements aux notifications d'événements Redshift doivent être balisés
- [Redshift.13] Les instantanés du cluster Redshift doivent être balisés
- [Redshift.14] Les groupes de sous-réseaux du cluster Redshift doivent être balisés
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SecretsManager.5] Les secrets de Secrets Manager doivent être balisés
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SNS.3] Les sujets SNS doivent être balisés
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SSM.5] Les documents SSM doivent être balisés
- [StepFunctions.2] Les activités de Step Functions doivent être étiquetées
- [Transfer.1]AWS Transfer Familyles flux de travail doivent être balisés
- [Transfer.4] Les accords Transfer Family doivent être étiquetés

- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés

CIS AWS Point de référence des fondations en matière de sécurité CSPM

Le benchmark des AWS fondations du Center for Internet Security (CIS) constitue un ensemble de meilleures pratiques de configuration de sécurité pour AWS. Ces meilleures pratiques reconnues par l'industrie vous fournissent des procédures de mise en œuvre et d'évaluation claires, étape par étape. Qu'il s'agisse de systèmes d'exploitation, de services cloud ou de périphériques réseau, les contrôles présentés dans ce benchmark vous aident à protéger les systèmes spécifiques utilisés par votre organisation.

AWS Security Hub CSPM prend en charge les versions 5.0.0, 3.0.0, 1.4.0 et 1.2.0 de CIS AWS Foundations Benchmark. Cette page répertorie les contrôles de sécurité pris en charge par chaque version. Il fournit également une comparaison des versions.

CIS AWS Foundations Benchmark version 5.0.0

Security Hub CSPM prend en charge la version 5.0.0 (v5.0.0) du benchmark CIS Foundations. AWS Security Hub CSPM a satisfait aux exigences de la certification des logiciels de sécurité CIS et a obtenu la certification des logiciels de sécurité CIS pour les benchmarks CIS suivants :

- Indice de référence CIS pour AWS les fondations de la CEI, v5.0.0, niveau 1
- Indice de référence CIS pour AWS les fondations de la CEI, v5.0.0, niveau 2

Contrôles qui s'appliquent au CIS AWS Foundations Benchmark version 5.0.0

[Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS

[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

[EC2.7] Le chiffrement par défaut d'EBS doit être activé

[EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389

[EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants

[EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants

[EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS

[EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos

[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.9] La MFA doit être activée pour l'utilisateur root

[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support

[IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées

[IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés

[IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM

[IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé

[KMS.4]AWS KMSla rotation des touches doit être activée

[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration

[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé

[RDS.5] Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité

[RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées

[RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public

[S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général

[S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet

[S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet

CIS AWS Foundations Benchmark version 3.0.0

Security Hub CSPM prend en charge la version 3.0.0 (v3.0.0) du benchmark CIS Foundations. AWS Security Hub CSPM a satisfait aux exigences de la certification des logiciels de sécurité CIS et a obtenu la certification des logiciels de sécurité CIS pour les benchmarks CIS suivants :

- Indice de référence CIS pour AWS les fondations de la CEI, v3.0.0, niveau 1
- Indice de référence CIS pour AWS les fondations de la CEI, v3.0.0, niveau 2

Contrôles qui s'appliquent au CIS AWS Foundations Benchmark version 3.0.0

[Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS

[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

[EC2.7] Le chiffrement par défaut d'EBS doit être activé

[EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389

[EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants

[EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants

[EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS

[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.9] La MFA doit être activée pour l'utilisateur root

[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support

[IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées

[IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés

[IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM

[IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé

[KMS.4]AWS KMSla rotation des touches doit être activée

[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration

[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé

[RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public

[S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général

[S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet

[S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet

CIS AWS Foundations Benchmark version 1.4.0

Security Hub CSPM prend en charge la version 1.4.0 (v1.4.0) du benchmark CIS Foundations. AWS

Contrôles qui s'appliquent au CIS AWS Foundations Benchmark version 1.4.0

[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs

[CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public

[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3

[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »

[CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM

[CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration

[CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification

[CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client

[CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3

[CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration

[CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité

[CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)

[CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau

[CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage

[CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

[EC2.7] Le chiffrement par défaut d'EBS doit être activé

[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389

[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.9] La MFA doit être activée pour l'utilisateur root

[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support

[IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées

[KMS.4]AWS KMSla rotation des touches doit être activée

[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public

[S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général

CIS AWS Foundations Benchmark version 1.2.0

Security Hub CSPM prend en charge la version 1.2.0 (v1.2.0) du benchmark CIS Foundations. AWS Security Hub CSPM a satisfait aux exigences de la certification des logiciels de sécurité CIS et a obtenu la certification des logiciels de sécurité CIS pour les benchmarks CIS suivants :

- Indice de référence de la CEI pour AWS les fondations de la CEI, v1.2.0, niveau 1

- Indice de référence de la CEI pour AWS les fondations de la CEI, v1.2.0, niveau 2

Contrôles qui s'appliquent au CIS AWS Foundations Benchmark version 1.2.0

[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs

[CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public

[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3

[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »

[CloudWatch.2] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les appels d'API non autorisés

[CloudWatch.3] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la connexion à la console de gestion sans MFA

[CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM

[CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration

[CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification

[CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client

[CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3

[CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration

[CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité

[CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)

[CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau

[CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage

[CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22

[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389

[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets

[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées

[IAM.9] La MFA doit être activée pour l'utilisateur root

[IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule

[IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule

[IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole

[IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre

[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

[IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins

[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support

[KMS.4]AWS KMSla rotation des touches doit être activée

Comparaison des versions pour CIS AWS Indice de référence des fondations

Cette section résume les différences entre les versions spécifiques du test de référence du Center for Internet Security (CIS) AWS Foundations : v5.0.0, v3.0.0, v1.4.0 et v1.2.0. AWS Security Hub CSPM prend en charge chacune de ces versions du référentiel CIS AWS Foundations. Cependant, nous vous recommandons d'utiliser la version 5.0.0 pour vous tenir au courant des meilleures pratiques de sécurité. Vous pouvez activer plusieurs versions des normes CIS AWS Foundations Benchmark en même temps. Pour plus d'informations sur les normes habilitantes, consultezMise en place d'une norme de sécurité. Si vous souhaitez passer à la version 5.0.0, activez-la avant de désactiver une ancienne version. Cela permet d'éviter des lacunes dans vos contrôles de sécurité. Si vous utilisez l'intégration de Security Hub CSPM AWS Organizations et que vous souhaitez activer la version 5.0.0 par lots sur plusieurs comptes, nous vous recommandons d'utiliser une configuration centralisée. ???

Mise en correspondance des contrôles avec les exigences du CIS dans chaque version

Découvrez les contrôles pris en charge par chaque version du CIS AWS Foundations Benchmark.

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS	1.2	1.2	1.2	1,18
[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture	3.1	3.1	3.1	2.1
[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé	3,5	3,5	3.7	2.7
[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée	3.2	3.2	3.2	2.2
[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	3.4	2,4
[CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	3.3	2.3

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3	3.4	3.4	3.6	2.6
[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4.3	3.3
[CloudWatch.2] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les appels d'API non autorisés	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	3.1
[CloudWatch.3] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la connexion à la console de gestion sans MFA	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	3.2
[CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,4	3.4

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,5	3,5
[CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,6	3.6
[CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,7	3.7
[CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,8	3.8
[CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,9	3.9

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,10	3,10
[CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,11	3,11
[CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,12	3,12
[CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,13	3.13

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	4,14	3,14
[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources	3.3	3.3	3,5	2,5
[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant	5.5	5,4	5.3	4.3
[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC	3.7	3.7	3.9	2,9
[EC2.7] Le chiffrement par défaut d'EBS doit être activé	5.1.1	2.2.1	2.2.1	Non pris en charge
[EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)	5.7	5.6	Non pris en charge	Non pris en charge
[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22	Non pris en charge — remplacé par les exigences 5.3 et 5.4	Non pris en charge — remplacé par les exigences 5.2 et 5.3	Non pris en charge — remplacé par les exigences 5.2 et 5.3	4.1

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389	Non pris en charge — remplacé par les exigences 5.3 et 5.4	Non pris en charge — remplacé par les exigences 5.2 et 5.3	Non pris en charge — remplacé par les exigences 5.2 et 5.3	4.2
[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389	5.2	5.1	5.1	Non pris en charge
[EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants	5.3	5.2	Non pris en charge	Non pris en charge
[EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants	5,4	5.3	Non pris en charge	Non pris en charge
[EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS	2.3.1	2.4.1	Non pris en charge	Non pris en charge
[EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos	2.3.1	Non pris en charge	Non pris en charge	Non pris en charge

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets	Non pris en charge	Non pris en charge	1.16	1,22
[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM	1.14	1.15	Non pris en charge	1.16
[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins	1.13	1.14	1.14	1.4
[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister	1.3	1.4	1.4	1.12
[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console	1.9	1.10	1.10	1.2
[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root	1.5	1.6	1.6	1.14

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées	Non pris en charge — voir à la [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées place	Non pris en charge — voir à la [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées place	Non pris en charge — voir à la [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées place	1.3
[IAM.9] La MFA doit être activée pour l'utilisateur root	1.4	1.5	1.5	1.13
[IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	1.5
[IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	1.6

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	1,7
[IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	1.8
[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus	1,7	1.8	1.8	1.9
[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe	1.8	1.9	1.9	1.10
[IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	1.11

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support	1.16	1,17	1,17	1.2
[IAM.20] Évitez d'utiliser l'utilisateur root	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	Non pris en charge — CIS a supprimé cette exigence	1.1
[IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées	1.11	1.12	1.12	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés	1,18	1,19	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM	1,21	1,22	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé	1,19	1,20	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[KMS.4]AWS KMSla rotation des touches doit être activée	3.6	3.6	3.8	2,8
[Macie.1] Amazon Macie devrait être activé	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle	Non pris en charge — vérification manuelle

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration	2.2.3	2.3.3	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé	2.2.1	2.3.1	2.3.1	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[RDS.5] Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité	2.2.4	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées	2.2.2	2.3.2	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité	2.2.4	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés	2.1.4	2.1.4	2.1.5	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures

ID et titre du contrôle	Exigences relatives à la version 5.0.0 de CIS	Configuration requise pour CIS v3.0.0	Exigence CIS v1.4.0	Exigence CIS v1.2.0
[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS	2.1.1	2.1.1	2.1.2	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public	2.1.4	2.1.4	2.1.5	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures
[S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général	2.1.2	2.1.2	2.1.3	Non pris en charge — CIS a ajouté cette exigence dans les versions ultérieures

ARN pour la CEI AWS Points de référence des fondations

Lorsque vous activez une ou plusieurs versions du test CIS AWS Foundations Benchmark, vous commencez à recevoir les résultats au format ASFF (AWS Security Finding Format). Dans ASFF, chaque version utilise le nom de ressource Amazon (ARN) suivant :

Indice de référence CIS AWS Foundations v5.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/5.0.0
```

Indice de référence CIS AWS Foundations v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

Indice de référence CIS AWS Foundations v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

Indice de référence CIS AWS Foundations v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Vous pouvez utiliser le GetEnabledStandards fonctionnement de l'API CSPM Security Hub pour trouver l'ARN d'une norme activée.

Les valeurs précédentes sont pour`StandardsArn`. Toutefois, `StandardsSubscriptionArn` fait référence à la ressource d'abonnement standard que Security Hub CSPM crée lorsque vous vous abonnez à une norme BatchEnableStandards en appelant dans une région.

> **Note**
>
> Lorsque vous activez une version de CIS AWS Foundations Benchmark, Security Hub CSPM peut mettre jusqu'à 18 heures à générer des résultats pour les contrôles qui utilisent la même règle AWS Config liée aux services que les contrôles activés dans d'autres normes activées. Pour plus d'informations sur le calendrier de génération des résultats de contrôle, consultezPlanification de l'exécution des vérifications de sécurité.

Les champs de recherche diffèrent si vous activez les résultats de contrôle consolidés. Pour plus d'informations sur ces différences, consultezImpact de la consolidation sur les champs et les valeurs ASFF. Pour les résultats du contrôle des échantillons, voirÉchantillons de résultats de contrôle.

Exigences CIS qui ne sont pas prises en charge dans Security Hub CSPM

Comme indiqué dans le tableau précédent, Security Hub CSPM ne prend pas en charge toutes les exigences du CIS dans toutes les versions du CIS AWS Foundations Benchmark. La plupart des exigences non prises en charge ne peuvent être évaluées qu'en examinant manuellement l'état de vos AWS ressources.

NIST SP 800-53 Révision 5 dans Security Hub CSPM

La publication spéciale 800-53 Revision 5 du NIST (NIST SP 800-53 Rev. 5) est un cadre de cybersécurité et de conformité développé par le National Institute of Standards and Technology (NIST), une agence qui fait partie du. U.S Département du commerce. Ce cadre de conformité fournit un catalogue d'exigences en matière de sécurité et de confidentialité pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information et des ressources critiques. U.S. les agences du gouvernement fédéral et les sous-traitants doivent se conformer à ces exigences pour protéger leurs systèmes et leurs organisations. Les organisations privées peuvent également utiliser volontairement les exigences comme cadre directeur pour réduire les risques de cybersécurité. Pour plus d'informations sur le framework et ses exigences, consultez le NIST SP 800-53 Rev. 5 dans le NIST Computer Security Resource Center.

AWS Security Hub CSPM fournit des contrôles de sécurité qui prennent en charge un sous-ensemble des exigences de la norme NIST SP 800-53, révision 5. Les contrôles effectuent des contrôles de sécurité automatisés pour certaines Services AWS ressources. Pour activer et gérer ces contrôles, vous pouvez activer le framework NIST SP 800-53 Revision 5 en standard dans Security Hub CSPM. Notez que les commandes ne sont pas conformes aux exigences de la norme NIST SP 800-53, révision 5, qui nécessitent des vérifications manuelles.

Contrairement à d'autres frameworks, le framework NIST SP 800-53 Revision 5 n'est pas prescriptif quant à la manière dont ses exigences doivent être évaluées. Le cadre fournit plutôt des lignes directrices. Dans Security Hub CSPM, la norme et les contrôles NIST SP 800-53 Revision 5 témoignent de la compréhension de ces directives par le service.

Rubriques

- Configuration de l'enregistrement des ressources pour les contrôles qui s'appliquent à la norme
- Déterminer les contrôles qui s'appliquent à la norme

Configuration de l'enregistrement des ressources pour les contrôles qui s'appliquent à la norme

Pour optimiser la couverture et la précision des résultats, il est important d'activer et de configurer l'enregistrement des ressources AWS Config avant d'activer la norme NIST SP 800-53 Revision 5 dans AWS Security Hub CSPM. Lorsque vous configurez l'enregistrement des ressources, veillez également à l'activer pour tous les types de AWS ressources qui sont vérifiés par les contrôles qui s'appliquent à la norme. Cela concerne principalement les contrôles dont le type de planification est déclenché par des modifications. Cependant, certains contrôles avec un type de planification périodique nécessitent également l'enregistrement des ressources. Si l'enregistrement des ressources n'est pas activé ou configuré correctement, Security Hub CSPM risque de ne pas être en mesure d'évaluer les ressources appropriées et de générer des résultats précis pour les contrôles qui s'appliquent à la norme.

Pour plus d'informations sur la manière dont Security Hub CSPM utilise l'enregistrement des ressources dans AWS Config, consultez. Activation et configuration AWS Config pour Security Hub CSPM Pour plus d'informations sur la configuration de l'enregistrement des ressources dans AWS Config, consultez la section Utilisation de l'enregistreur de configuration dans le Guide du AWS Config développeur.

Le tableau suivant indique les types de ressources à enregistrer pour les contrôles qui s'appliquent à la norme NIST SP 800-53 Revision 5 dans Security Hub CSPM.

Service AWS	Types de ressources
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Base rocheuse de l'Amazonie AgentCore	`AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`

Service AWS	Types de ressources
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`

Service AWS	Types de ressources
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
Gestion des identités et des accès AWS (AIM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Service Amazon	`AWS::OpenSearch::Domain`

Service AWS	Types de ressources
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`

Service AWS	Types de ressources
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Déterminer les contrôles qui s'appliquent à la norme

La liste suivante indique les contrôles qui prennent en charge les exigences du NIST SP 800-53 Revision 5 et qui s'appliquent à la norme NIST SP 800-53 Revision 5 dans AWS Security Hub CSPM. Pour plus de détails sur les exigences spécifiques prises en charge par un contrôle, choisissez le contrôle. Reportez-vous ensuite au champ Exigences associées dans les détails du contrôle. Ce champ spécifie chaque exigence NIST prise en charge par le contrôle. Si le champ ne spécifie aucune exigence NIST particulière, le contrôle ne prend pas en charge cette exigence.

- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [APIGateway.1] API Gateway REST et la journalisation de l'exécution des WebSocket API doivent être activés
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.3] Les étapes de l'API REST API Gateway doivent avoir AWS X-Ray traçage activé
- [APIGateway.4] API Gateway doit être associée à une ACL Web WAF
- [APIGateway.5] Les données du cache de l'API REST API Gateway doivent être chiffrées au repos
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité

- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [Autoscaling.5] Les instances Amazon EC2 lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresses IP publiques
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture
- [CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé
- [CloudTrail.4] la validation du fichier CloudTrail journal doit être activée
- [CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys

- [CloudWatch.15] CloudWatch les actions spécifiées doivent être configurées pour les alarmes
- [CloudWatch.16] les groupes de CloudWatch journaux doivent être conservés pendant une période spécifiée
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics

- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DynamoDB.1] Les tables DynamoDB doivent automatiquement adapter la capacité à la demande
- [DynamoDB.2] La restauration instantanée des tables DynamoDB doit être activée
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement
- [EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant
- [EC2.3] Les volumes Amazon EBS joints doivent être chiffrés au repos
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC
- [EC2.7] Le chiffrement par défaut d'EBS doit être activé
- [EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.9] Les instances Amazon EC2 ne doivent pas avoir d'adresse IPv4 publique
- [EC2.10] Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2
- [EC2.12] Les EIP Amazon EC2 non utilisés doivent être supprimés
- [EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22
- [EC2.15] Les sous-réseaux Amazon EC2 ne doivent pas attribuer automatiquement d'adresses IP publiques
- [EC2.16] Les listes de contrôle d'accès réseau non utilisées doivent être supprimées
- [EC2.17] Les instances Amazon EC2 ne doivent pas utiliser plusieurs ENI
- [EC2.18] Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés

- [EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé
- [EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry
- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.2] Aucune adresse IP publique ne doit être attribuée automatiquement aux services ECS
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine

- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EKS.1] Les points de terminaison du cluster EKS ne doivent pas être accessibles au public
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés

- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ELB.1] L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.3] Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS
- [ELB.4] L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP non valides
- [ELB.5] La journalisation des applications et des équilibreurs de charge classiques doit être activée
- [ELB.6] La protection contre la suppression doit être activée pour les équilibreurs de charge des applications, des passerelles et du réseau
- [ELB.7] Le drainage des connexions doit être activé pour les équilibreurs de charge classiques
- [ELB.8] Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie qui est solide AWS Config durée
- [ELB.9] L'équilibrage de charge entre zones doit être activé pour les équilibreurs de charge classiques
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.16] Les équilibreurs de charge des applications doivent être associés à un AWS WAF ACL web
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé

- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.1] Le chiffrement au repos doit être activé pour les domaines Elasticsearch
- [ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public
- [ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [ES.5] La journalisation des audits doit être activée pour les domaines Elasticsearch
- [ES.6] Les domaines Elasticsearch doivent comporter au moins trois nœuds de données
- [ES.7] Les domaines Elasticsearch doivent être configurés avec au moins trois nœuds principaux dédiés
- [ES.8] Les connexions aux domaines Elasticsearch doivent être chiffrées conformément à la dernière politique de sécurité TLS
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.1] GuardDuty doit être activé
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.3]AWS KMS keysne doit pas être supprimé par inadvertance
- [KMS.4]AWS KMSla rotation des touches doit être activée
- [Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public
- [Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge
- [Lambda.3] Les fonctions Lambda doivent se trouver dans un VPC
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch

- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines

- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [RDS.1] L'instantané RDS doit être privé
- [RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration
- [RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé
- [RDS.4] Les instantanés du cluster RDS et les instantanés de base de données doivent être chiffrés au repos
- [RDS.5] Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité
- [RDS.6] Une surveillance améliorée doit être configurée pour les instances de base de données RDS
- [RDS.7] La protection contre la suppression des clusters RDS doit être activée
- [RDS.8] La protection contre la suppression des instances de base de données RDS doit être activée
- [RDS.9] Les instances de base de données RDS doivent publier des CloudWatch journaux dans Logs
- [RDS.10] L'authentification IAM doit être configurée pour les instances RDS
- [RDS.11] Les sauvegardes automatiques doivent être activées sur les instances RDS
- [RDS.12] L'authentification IAM doit être configurée pour les clusters RDS
- [RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité
- [RDS.16] Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données

- [RDS.17] Les instances de base de données RDS doivent être configurées pour copier les balises dans les instantanés
- [RDS.19] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements de cluster critiques
- [RDS.20] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques
- [RDS.21] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de groupe de paramètres de base de données critiques
- [RDS.22] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements critiques du groupe de sécurité des bases de données
- [RDS.23] Les instances RDS ne doivent pas utiliser le port par défaut d'un moteur de base de données
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public
- [Redshift.2] Les connexions aux clusters Amazon Redshift doivent être chiffrées pendant le transit
- [Redshift.3] Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift

- [Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift
- [Redshift.6] Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures
- [Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés
- [S3.2] Les compartiments S3 à usage général devraient bloquer l'accès public en lecture
- [S3.3] Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture
- [S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS
- [S3.6] Les politiques de bucket à usage général S3 devraient restreindre l'accès aux autres Comptes AWS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
- [S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public
- [S3.9] Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.14] Les compartiments S3 à usage général doivent avoir le contrôle de version activé
- [S3.15] Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé

- [S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SecretsManager.1] La rotation automatique des secrets des secrets de Secrets Manager doit être activée
- [SecretsManager.2] Les secrets de Secrets Manager configurés avec une rotation automatique devraient être correctement pivotés
- [SecretsManager.3] Supprimer les secrets inutilisés du Gestionnaire de Secrets
- [SecretsManager.4] Les secrets de Secrets Manager doivent être renouvelés dans un délai spécifié
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.1] Les sujets SNS doivent être chiffrés au repos à l'aide deAWS KMS
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager
- [SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
- [SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT
- [SSM.4] Les documents SSM ne doivent pas être publics
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée

- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.11]AWS WAFla journalisation des ACL Web doit être activée
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles

NIST SP 800-171 Revision 2 dans Security Hub CSPM

La publication spéciale 800-171 Revision 2 du NIST (NIST SP 800-171 Rev. 2) est un cadre de cybersécurité et de conformité développé par le National Institute of Standards and Technology (NIST), une agence qui fait partie du. U.S Département du commerce. Ce cadre de conformité fournit des exigences de sécurité recommandées pour protéger la confidentialité des informations contrôlées non classifiées dans les systèmes et les organisations qui ne font pas partie du gouvernement fédéral U.S. Les informations contrôlées non classifiées, également appelées CUI, sont des informations sensibles qui ne répondent pas aux critères de classification gouvernementaux mais qui doivent être protégées. Il s'agit d'informations considérées comme sensibles et créées ou détenues par le U.S gouvernement fédéral ou d'autres entités pour le compte du gouvernement fédéral U.S.

Le NIST SP 800-171 Rev. 2 fournit des exigences de sécurité recommandées pour protéger la confidentialité du CUI lorsque :

- L'information se trouve dans des systèmes et des organisations non fédéraux,
- L'organisation non fédérale ne collecte ni ne conserve d'informations pour le compte d'une agence fédérale ni n'utilise ou n'exploite un système pour le compte d'une agence, et
- Il n'existe aucune exigence de sauvegarde spécifique pour protéger la confidentialité des CUI prescrite par la loi, la réglementation ou la politique gouvernementale d'autorisation pour la catégorie CUI répertoriée dans le registre CUI.

Les exigences s'appliquent à tous les composants des systèmes et organisations non fédéraux qui traitent, stockent ou transmettent des CUI, ou assurent la protection de sécurité des composants. Pour plus d'informations, consultez le NIST SP 800-171 Rev. 2 dans le Centre de ressources sur la sécurité informatique du NIST.

AWS Security Hub CSPM fournit des contrôles de sécurité qui prennent en charge un sous-ensemble des exigences de la NIST SP 800-171, révision 2. Les contrôles effectuent des contrôles de sécurité automatisés pour certaines Services AWS ressources. Pour activer et gérer ces contrôles, vous pouvez activer le framework NIST SP 800-171 Revision 2 en standard dans Security Hub CSPM. Notez que les commandes ne sont pas conformes aux exigences de la norme NIST SP 800-171, révision 2, qui nécessitent des vérifications manuelles.

Rubriques

- Configuration de l'enregistrement des ressources pour les contrôles qui s'appliquent à la norme
- Déterminer les contrôles qui s'appliquent à la norme

Configuration de l'enregistrement des ressources pour les contrôles qui s'appliquent à la norme

Pour optimiser la couverture et la précision des résultats, il est important d'activer et de configurer l'enregistrement des ressources AWS Config avant d'activer la norme NIST SP 800-171 Revision 2 dans AWS Security Hub CSPM. Lorsque vous configurez l'enregistrement des ressources, veillez également à l'activer pour tous les types de AWS ressources qui sont vérifiés par les contrôles qui s'appliquent à la norme. Dans le cas contraire, Security Hub CSPM pourrait ne pas être en mesure d'évaluer les ressources appropriées et de générer des résultats précis pour les contrôles qui s'appliquent à la norme.

Pour plus d'informations sur la manière dont Security Hub CSPM utilise l'enregistrement des ressources dans AWS Config, consultez. Activation et configuration AWS Config pour Security Hub CSPM Pour plus d'informations sur la configuration de l'enregistrement des ressources dans AWS Config, consultez la section Utilisation de l'enregistreur de configuration dans le Guide du AWS Config développeur.

Le tableau suivant indique les types de ressources à enregistrer pour les contrôles qui s'appliquent à la norme NIST SP 800-171 Revision 2 dans Security Hub CSPM.

Service AWS	Types de ressources
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`

Service AWS	Types de ressources
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
Gestion des identités et des accès AWS(AIM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Service de stockage Amazon Simple (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SMS)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Déterminer les contrôles qui s'appliquent à la norme

La liste suivante indique les contrôles qui prennent en charge les exigences du NIST SP 800-171 Revision 2 et qui s'appliquent à la norme NIST SP 800-171 Revision 2 dans AWS Security Hub CSPM. Pour plus de détails sur les exigences spécifiques prises en charge par un contrôle,

choisissez le contrôle. Reportez-vous ensuite au champ Exigences associées dans les détails du contrôle. Ce champ spécifie chaque exigence NIST prise en charge par le contrôle. Si le champ ne spécifie aucune exigence NIST particulière, le contrôle ne prend pas en charge cette exigence.

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé
- [CloudTrail.3] Au moins une CloudTrail piste doit être activée
- [CloudTrail.4] la validation du fichier CloudTrail journal doit être activée
- [CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »
- [CloudWatch.2] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les appels d'API non autorisés
- [CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM
- [CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration
- [CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification
- [CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client
- [CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3
- [CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration
- [CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité
- [CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)

- [CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau
- [CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage
- [CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC
- [CloudWatch.15] CloudWatch les actions spécifiées doivent être configurées pour les alarmes
- [EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC
- [EC2.10] Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2
- [EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22
- [EC2.16] Les listes de contrôle d'accès réseau non utilisées doivent être supprimées
- [EC2.18] Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés
- [EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé
- [EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.3] Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS
- [ELB.8] Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie qui est solide AWS Config durée
- [GuardDuty.1] GuardDuty doit être activé
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets

- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS
- [S3.6] Les politiques de bucket à usage général S3 devraient restreindre l'accès aux autres Comptes AWS

- [S3.9] Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.14] Les compartiments S3 à usage général doivent avoir le contrôle de version activé
- [S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys
- [SNS.1] Les sujets SNS doivent être chiffrés au repos à l'aide deAWS KMS
- [SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles

PCI DSS dans Security Hub CSPM

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) est un cadre de conformité tiers qui fournit un ensemble de règles et de directives pour traiter en toute sécurité les informations relatives aux cartes de crédit et de débit. Le Conseil des normes de sécurité PCI (SSC) crée et met à jour ce cadre.

AWS Security Hub CSPM fournit une norme PCI DSS qui peut vous aider à rester en conformité avec ce framework tiers. Vous pouvez utiliser cette norme pour découvrir des failles de sécurité dans les AWS ressources qui gèrent les données des titulaires de cartes. Nous vous recommandons d'activer cette norme si Comptes AWS vous disposez de ressources qui stockent, traitent ou transmettent les données du titulaire de la carte ou des données d'authentification sensibles. Les évaluations effectuées par le PCI SSC ont validé cette norme.

Security Hub CSPM prend en charge les normes PCI DSS v3.2.1 et PCI DSS v4.0.1. Nous vous recommandons d'utiliser la version 4.0.1 pour vous tenir au courant des meilleures pratiques en matière de sécurité. Les deux versions de la norme peuvent être activées en même temps. Pour plus d'informations sur les normes habilitantes, consultezMise en place d'une norme de sécurité. Si vous utilisez actuellement la version 3.2.1 mais que vous souhaitez utiliser uniquement la version 4.0.1, activez la version la plus récente avant de désactiver l'ancienne version. Cela permet d'éviter des lacunes dans vos contrôles de sécurité. Si vous utilisez l'intégration de Security Hub CSPM avec la version 4.0.1 AWS Organizations et que vous souhaitez activer par lots la version 4.0.1 sur plusieurs comptes, nous vous recommandons d'utiliser une configuration ??? centralisée pour ce faire.

Les sections suivantes indiquent les contrôles qui s'appliquent à la norme PCI DSS v3.2.1 et à la norme PCI DSS v4.0.1.

Contrôles applicables à la norme PCI DSS v3.2.1

La liste suivante indique les contrôles CSPM de Security Hub qui s'appliquent à la norme PCI DSS v3.2.1. Pour consulter les détails d'un contrôle, choisissez-le.

[AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.3] Au moins une CloudTrail piste doit être activée

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs

[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »

[CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles

[CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

[DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques

[EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

[EC2.12] Les EIP Amazon EC2 non utilisés doivent être supprimés

[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22

[ELB.1] L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS

[ES.1] Le chiffrement au repos doit être activé pour les domaines Elasticsearch

[ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public

[GuardDuty.1] GuardDuty doit être activé

[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets

[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées

[IAM.9] La MFA doit être activée pour l'utilisateur root

[IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes

[IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM

[KMS.4]AWS KMSla rotation des touches doit être activée

[Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public

[Lambda.3] Les fonctions Lambda doivent se trouver dans un VPC

[Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines

[Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public

[RDS.1] L'instantané RDS doit être privé

[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration

[Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

[S3.2] Les compartiments S3 à usage général devraient bloquer l'accès public en lecture

[S3.3] Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

[S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions

[SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet

[SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager

[SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif

[SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT

Contrôles qui s'appliquent à la norme PCI DSS v4.0.1

La liste suivante indique les contrôles CSPM de Security Hub qui s'appliquent à la norme PCI DSS v4.0.1. Pour consulter les détails d'un contrôle, choisissez-le.

[ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée

[ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits

[APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2

[AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée

[AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)

[Autoscaling.5] Les instances Amazon EC2 lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresses IP publiques

[CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut

[CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées

[CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

[CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit

[CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée

[CloudFront.6] CloudFront les distributions doivent avoir le WAF activé

[CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

[CloudTrail.3] Au moins une CloudTrail piste doit être activée

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

[CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public

[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3

[CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles

[CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair

[CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés

[DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques

[DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune

[DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé

[DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS

[DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée

[DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée

[DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée

[DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL

[DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

[DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics

[DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch

[DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit

[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22

[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389

[EC2.15] Les sous-réseaux Amazon EC2 ne doivent pas attribuer automatiquement d'adresses IP publiques

[EC2.16] Les listes de contrôle d'accès réseau non utilisées doivent être supprimées

[EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

[EC2.171] La journalisation des connexions VPN EC2 doit être activée

[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389

[EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau

[EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2

[EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants

[EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants

[EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

[ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée

[ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate

[ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques

[ECS.2] Aucune adresse IP publique ne doit être attribuée automatiquement aux services ECS

[ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur

[EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur

[EKS.1] Les points de terminaison du cluster EKS ne doivent pas être accessibles au public

[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge

[EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés

[EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée

[ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters

[ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport

[ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé

[ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées

[ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch

[ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict

[ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict

[ELB.3] Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS

[ELB.4] L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP non valides

[ELB.8] Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie qui est solide AWS Config durée

[EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques

[EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé

[ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public

[ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds

[ES.5] La journalisation des audits doit être activée pour les domaines Elasticsearch

[ES.8] Les connexions aux domaines Elasticsearch doivent être chiffrées conformément à la dernière politique de sécurité TLS

[EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources

[GuardDuty.1] GuardDuty doit être activé

[GuardDuty.10] La protection GuardDuty S3 doit être activée

[GuardDuty.6] La protection GuardDuty Lambda doit être activée

[GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée

[GuardDuty.9] GuardDuty La protection RDS doit être activée

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

[IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes

[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées

[IAM.9] La MFA doit être activée pour l'utilisateur root

[IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule

[IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule

[IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre

[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

[IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins

[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support

[IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM

[Inspector.1] La numérisation Amazon Inspector EC2 doit être activée

[Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée

[Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée

[Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé

[KMS.4]AWS KMSla rotation des touches doit être activée

[Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public

[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge

[MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch

[MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier

[MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport

[Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch

[Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics

[Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée

[Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines

[RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées

[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration

[RDS.20] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques

[RDS.21] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de groupe de paramètres de base de données critiques

[RDS.22] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements critiques du groupe de sécurité des bases de données

[RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

[RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

[RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs

[RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée

[RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch

[RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch

[RDS.9] Les instances de base de données RDS doivent publier des CloudWatch journaux dans Logs

[Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public

[Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes

[Redshift.2] Les connexions aux clusters Amazon Redshift doivent être chiffrées pendant le transit

[Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift

[Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

[S3.15] Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé

[S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys

[S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés

[S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet

[S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet

[S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public

[S3.9] Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée

[SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet

[SecretsManager.1] La rotation automatique des secrets des secrets de Secrets Manager doit être activée

[SecretsManager.2] Les secrets de Secrets Manager configurés avec une rotation automatique devraient être correctement pivotés

[SecretsManager.4] Les secrets de Secrets Manager doivent être renouvelés dans un délai spécifié

[SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif

[SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT

[StepFunctions.1] La journalisation des machines à états Step Functions doit être activée

[Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux

[WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée

[WAF.11]AWS WAFla journalisation des ACL Web doit être activée

Service-managed normes du Security Hub CSPM

Une norme gérée par les services est une norme de sécurité gérée par un autre Service AWS mais que vous pouvez consulter dans Security Hub CSPM. Par exemple, Service-Managed Standard : AWS Control Tower est une norme gérée par des services qui AWS Control Tower gère. Une norme gérée par les services diffère d'une norme de sécurité que AWS Security Hub CSPM gère de la manière suivante :

- Création et suppression de normes : vous créez et supprimez une norme gérée par un service à l'aide de la console ou de l'API du service de gestion, ou à l'aide du. AWS CLI Tant que vous n'avez pas créé la norme dans le service de gestion de l'une de ces manières, la norme n'apparaît pas dans la console Security Hub CSPM et n'est pas accessible par l'API Security Hub CSPM ou. AWS CLI
- Aucune activation automatique des contrôles — Lorsque vous créez une norme de gestion de services, Security Hub CSPM et le service de gestion n'activent pas automatiquement les contrôles qui s'appliquent à la norme. De plus, lorsque Security Hub CSPM publie de nouveaux contrôles pour la norme, ils ne sont pas automatiquement activés. Il s'agit d'un écart par rapport aux normes gérées par Security Hub CSPM. Pour plus d'informations sur la manière habituelle de configurer les contrôles dans Security Hub CSPM, consultez. Comprendre les contrôles de sécurité dans Security Hub CSPM
- Activation et désactivation des contrôles : nous vous recommandons d'activer et de désactiver les contrôles dans le service de gestion pour éviter toute dérive.
- Disponibilité des contrôles : le service de gestion choisit les contrôles disponibles dans le cadre de la norme de gestion des services. Les contrôles disponibles peuvent inclure l'ensemble ou un sous-ensemble des contrôles CSPM Security Hub existants.

Une fois que le service de gestion a créé la norme gérée par le service et rendu les contrôles disponibles pour celle-ci, vous pouvez accéder aux résultats de vos contrôles, à leurs états de contrôle et au score de sécurité standard dans la console Security Hub CSPM, l'API Security Hub

CSPM ou. AWS CLI Certaines ou toutes ces informations peuvent également être disponibles dans le service de gestion.

Sélectionnez une norme gérée par les services dans la liste suivante pour en savoir plus.

Service-managed normes

- Service-Managed Norme : AWS Control Tower

Service-Managed Norme : AWS Control Tower

Cette section fournit des informations sur Service-Managed Standard : AWS Control Tower.

Qu'est-ce que Service-Managed Standard : AWS Control Tower?

Service-Managed Standard : AWS Control Tower est une norme gérée par des services qui AWS Control Tower gère et prend en charge un sous-ensemble de contrôles Security Hub. Cette norme est conçue pour les utilisateurs de AWS Security Hub CSPM et. AWS Control Tower Il vous permet de configurer les contrôles de détection de Security Hub CSPM à partir du AWS Control Tower service.

Les contrôles de détection détectent la non-conformité des ressources (par exemple, les mauvaises configurations) au sein de votre. Comptes AWS

> **Tip**
>
> Service-managed les normes diffèrent des normes gérées par AWS Security Hub CSPM. Par exemple, vous devez créer et supprimer une norme de service gérée dans le service de gestion. Pour de plus amples informations, veuillez consulter Service-managed normes du Security Hub CSPM.

Lorsque vous activez un contrôle Security Hub CSPM via AWS Control Tower, Control Tower active également Security Hub CSPM pour vous dans ces comptes et régions spécifiques, si ce n'est pas déjà fait. Dans la console et l'API Security Hub CSPM, vous pouvez afficher Service-Managed Standard : à AWS Control Tower côté des autres normes Security Hub CSPM, une fois que la norme est activée depuis. AWS Control Tower

Pour plus d'informations sur cette norme, consultez la section Contrôles CSPM de Security Hub dans le Guide de l'AWS Control Tower utilisateur.

Création de la norme

Cette norme est disponible dans Security Hub CSPM uniquement si vous activez les contrôles Security Hub CSPM depuis. AWS Control Tower AWS Control Tower crée la norme lorsque vous activez un contrôle applicable pour la première fois à l'aide de l'une des méthodes suivantes :

- AWS Control Tower console
- AWS Control Tower API (appelez l'`EnableControl`API)
- AWS CLI (exécutez la `enable-control` commande)

Lorsque vous activez un contrôle Security Hub CSPM via AWS Control Tower, si vous n'avez pas encore activé Security Hub CSPM, activez AWS Control Tower également Security Hub CSPM pour vous dans ces comptes et régions spécifiques.

Pour identifier un contrôle CSPM Security Hub par ID de contrôle dans Control Catalog, vous pouvez utiliser le champ dans`Implementation.Identifier`. AWS Control Tower Ce champ correspond à l'ID de contrôle CSPM de Security Hub et peut être utilisé pour filtrer un ID de contrôle spécifique. Pour récupérer les métadonnées de contrôle d'un contrôle CSPM Security Hub spécifique (par exemple, CodeBuild.1 « ») dans AWS Control Tower, vous pouvez utiliser l'`ListControls`API :

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Vous ne pouvez pas afficher ou accéder à cette norme dans la console Security Hub CSPM, l'API Security Hub CSPM, ou AWS CLI sans avoir préalablement configuré AWS Control Tower et activé les contrôles Security Hub CSPM à l' AWS Control Tower aide de l'une des méthodes précédentes.

Cette norme n'est disponible que Régions AWS là où elle AWS Control Tower est disponible.

Activation et désactivation des commandes dans la norme

Une fois que vous avez activé les contrôles CSPM de Security Hub AWS Control Tower et que la Service-Managed norme AWS Control Tower Standard : a été créée, vous pouvez consulter la norme et ses contrôles disponibles dans Security Hub CSPM.

Lorsque Security Hub CSPM ajoute de nouveaux contrôles à la Service-Managed norme : AWS Control Tower standard, ils ne sont pas automatiquement activés pour les clients qui ont activé la norme. Vous devez activer et désactiver les commandes du formulaire standard à AWS Control Tower l'aide de l'une des méthodes suivantes :

- AWS Control Tower console
- AWS Control Tower API (appelez les `DisableControl` API `EnableControl` et)
- AWS CLI (exécutez les `disable-control` commandes `enable-control` et)

Lorsque vous modifiez l'état d'activation d'un contrôle dans AWS Control Tower, la modification est également reflétée dans Security Hub CSPM.

Cependant, la désactivation d'un contrôle activé dans Security Hub CSPM AWS Control Tower entraîne une dérive du contrôle. L'état du contrôle s' AWS Control Tower affiche sous la forme`Drifted`. Vous pouvez résoudre cette dérive en utilisant l'ResetEnabledControlAPI pour réinitialiser le contrôle qui est en dérive, ou en sélectionnant OU dans la AWS Control Tower console, Re-register ou en désactivant et réactivant le contrôle à l' AWS Control Tower aide de l'une des méthodes précédentes.

L'exécution des actions d'activation et de désactivation dans vous AWS Control Tower permet d'éviter toute dérive des commandes.

Lorsque vous activez ou désactivez les contrôles dans AWS Control Tower, l'action s'applique à tous les comptes et régions régis par AWS Control Tower. Si vous activez et désactivez les contrôles dans Security Hub CSPM (non recommandé pour cette norme), l'action s'applique uniquement au compte et à la région actuels.

> **Note**
>
> La configuration centrale ne peut pas être utilisée pour gérer Service-Managed Standard : AWS Control Tower. Vous ne pouvez utiliser que le AWS Control Tower service pour activer et désactiver les commandes de cette norme.

Affichage de l'état d'activation et de l'état du contrôle

Vous pouvez consulter l'état d'activation d'un contrôle à l'aide de l'une des méthodes suivantes :

- console Security Hub CSPM, API Security Hub CSPM ou AWS CLI
- AWS Control Tower console
- AWS Control Tower API pour voir la liste des contrôles activés (appelez l'`ListEnabledControls`API)

- AWS CLI pour voir la liste des contrôles activés (exécutez la `list-enabled-controls` commande)

Un contrôle que vous désactivez AWS Control Tower a un statut d'activation `Disabled` dans Security Hub CSPM, sauf si vous activez explicitement ce contrôle dans Security Hub CSPM.

Security Hub CSPM calcule l'état des contrôles en fonction de l'état du flux de travail et de l'état de conformité des résultats des contrôles. Pour plus d'informations sur l'état d'activation et l'état de contrôle, consultezExaminer les détails des contrôles dans Security Hub CSPM.

Sur la base des statuts de contrôle, Security Hub CSPM calcule un score de sécurité pour Standard :. Service-Managed AWS Control Tower Ce score n'est disponible que dans Security Hub CSPM. En outre, vous pouvez uniquement consulter les résultats des contrôles dans Security Hub CSPM. Le score de sécurité standard et les résultats des contrôles ne sont pas disponibles dans AWS Control Tower.

> **Note**
>
> Lorsque vous activez les contrôles pour Service-Managed Standard : AWS Control Tower, Security Hub CSPM peut prendre jusqu'à 18 heures pour générer des résultats pour les contrôles qui utilisent une règle liée à un AWS Config service existante. Vous disposez peut-être de règles liées aux services existantes si vous avez activé d'autres normes et contrôles dans Security Hub CSPM. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

Supprimer la norme

Vous pouvez supprimer cette norme de service gérée en AWS Control Tower désactivant tous les contrôles applicables à l'aide de l'une des méthodes suivantes :

- AWS Control Tower console
- AWS Control Tower API (appelez l'`DisableControl`API)
- AWS CLI (exécutez la `disable-control` commande)

La désactivation de tous les contrôles supprime la norme dans tous les comptes gérés et les régions gouvernées dans. AWS Control Tower La suppression de la norme dans AWS Control Tower

entraîne sa suppression de la page Standards de la console Security Hub CSPM, et vous ne pouvez plus y accéder à l'aide de l'API Security Hub CSPM ou. AWS CLI

> **Note**
>
> La désactivation de tous les contrôles de la norme dans Security Hub CSPM ne désactive ni ne supprime la norme.

La désactivation du service Security Hub CSPM supprime Service-Managed Standard : AWS Control Tower et toutes les autres normes que vous avez activées.

Format de champ de recherche pour Service-Managed Standard : AWS Control Tower

Lorsque vous créez Service-Managed Standard : AWS Control Tower et que vous activez les contrôles correspondants, vous commencez à recevoir les résultats des contrôles dans Security Hub CSPM. Security Hub CSPM rapporte les résultats des contrôles dans le. AWS Format de recherche de sécurité (ASFF) Voici les valeurs ASFF pour le nom de ressource Amazon (ARN) de cette norme et `GeneratorId` :

- ARN standard — `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

Pour un exemple de résultat pour Service-Managed Standard : AWS Control Tower, voirÉchantillons de résultats de contrôle.

Contrôles applicables à Service-Managed Standard : AWS Control Tower

Service-Managed Standard : AWS Control Tower prend en charge un sous-ensemble de contrôles qui font partie de la norme FSBP (AWS Foundational Security Best Practices). Choisissez un contrôle pour afficher les informations le concernant, y compris les étapes à suivre pour remédier aux erreurs de détection.

Pour savoir quels contrôles CSPM de Security Hub sont pris en charge AWS Control Tower, vous pouvez utiliser l'une des méthodes suivantes :

- AWS Console Control Catalog dans laquelle vous pouvez filtrer `“Control owner = AWS Security Hub”`

- AWS API Control Catalog (appelez l'`ListControls`API) avec filtre `Implementations` pour `Types` vérifier `AWS::SecurityHub::SecurityControl`
- AWS CLI (exécutez la `list-controls` commande) avec filtre pour`Implementations`. Exemple de commande CLI :

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Les limites régionales des contrôles CSPM de Security Hub lorsqu'elles sont activées via la norme Control Tower peuvent ne pas correspondre aux limites régionales des contrôles sous-jacents.

Dans Security Hub CSPM, si les résultats de contrôle consolidés sont désactivés dans votre compte, le `ProductFields.ControlId` champ des résultats générés utilise l'ID de contrôle standard. L'identifiant de contrôle standard est au format CT. ***`ControlId`***(par exemple, CT.CodeBuild.1).

Pour plus d'informations sur cette norme, consultez la section Contrôles CSPM de Security Hub dans le Guide de l'AWS Control Tower utilisateur.

Mise en place d'une norme de sécurité

Lorsque vous activez une norme de sécurité dans AWS Security Hub CSPM, Security Hub CSPM crée et active automatiquement tous les contrôles qui s'appliquent à la norme. Security Hub CSPM commence également à exécuter des contrôles de sécurité et à générer des résultats pour les contrôles.

Pour optimiser la couverture et la précision des résultats, activez et configurez l'enregistrement des ressources AWS Config avant d'activer une norme. Lorsque vous configurez l'enregistrement des ressources, veillez également à l'activer pour tous les types de ressources qui sont vérifiés par les contrôles qui s'appliquent à la norme. Dans le cas contraire, Security Hub CSPM pourrait ne pas être en mesure d'évaluer les ressources appropriées et de générer des résultats précis pour les contrôles qui s'appliquent à la norme. Pour de plus amples informations, veuillez consulter Activation et configuration AWS Config pour Security Hub CSPM.

Les normes de sécurité multicloud, telles que CIS Azure Foundations Benchmark v4.0.0, ont des exigences différentes des normes. AWS Les normes multicloud nécessitent un connecteur CSPM Security Hub pour le fournisseur de cloud externe et ne vous obligent pas à configurer AWS Config ou à créer manuellement un enregistreur de configuration. Le connecteur multicloud Security Hub

CSPM configure automatiquement un enregistreur lié à un service pour évaluer les ressources dans l'environnement cloud externe.

Après avoir activé une norme, vous pouvez désactiver ou réactiver ultérieurement les contrôles individuels qui s'appliquent à la norme. Si vous désactivez un contrôle pour une norme, Security Hub CSPM arrête de générer des résultats pour le contrôle. En outre, Security Hub CSPM ignore le contrôle lorsqu'il calcule le score de sécurité de la norme. Le score de sécurité est le pourcentage de contrôles qui ont réussi l'évaluation, par rapport au nombre total de contrôles qui s'appliquent à la norme, sont activés et comportent des données d'évaluation.

Lorsque vous activez une norme, Security Hub CSPM génère un score de sécurité préliminaire pour la norme, généralement dans les 30 minutes suivant votre première visite sur la page Résumé ou sur les normes de sécurité de la console Security Hub CSPM. Les scores de sécurité sont générés uniquement pour les normes activées lorsque vous visitez ces pages sur la console. De plus, l'enregistrement des ressources doit être configuré AWS Config pour que les scores apparaissent. Dans les régions de Chine et AWS GovCloud (US) Regions, la génération d'un score de sécurité préliminaire pour une norme par Security Hub CSPM peut prendre jusqu'à 24 heures. Une fois que Security Hub CSPM a généré un score préliminaire, il le met à jour toutes les 24 heures. Pour déterminer la date de dernière mise à jour d'un score de sécurité, vous pouvez vous référer à l'horodatage fourni par Security Hub CSPM pour le score. Pour de plus amples informations, veuillez consulter Calcul des scores de sécurité.

La manière dont vous activez une norme varie selon que vous utilisez une configuration centralisée pour gérer Security Hub CSPM pour plusieurs comptes et. Régions AWS Nous vous recommandons d'utiliser la configuration centrale si vous souhaitez activer les normes dans des environnements multicomptes et multirégions. Vous pouvez utiliser la configuration centralisée si vous intégrez Security Hub CSPM à. AWS Organizations Si vous n'utilisez pas la configuration centralisée, vous devez activer chaque norme séparément dans chaque compte et chaque région.

Rubriques

- Activation d'une norme dans plusieurs comptes et Régions AWS
- Activation d'une norme dans un seul compte et Région AWS
- Vérifier l'état d'une norme

Activation d'une norme dans plusieurs comptes et Régions AWS

Pour activer et configurer une norme de sécurité sur plusieurs comptes Régions AWS, utilisez la configuration centralisée. Grâce à la configuration centralisée, l'administrateur délégué de

Security Hub CSPM peut créer des politiques de configuration CSPM de Security Hub qui activent une ou plusieurs normes. L'administrateur peut ensuite associer une politique de configuration à des comptes individuels, à des unités organisationnelles (UO) ou à la racine. Une politique de configuration affecte la région d'origine, également appelée région d'agrégation, et toutes les régions liées.

Les politiques de configuration offrent des options de personnalisation. Par exemple, vous pouvez choisir d'activer uniquement la norme FSBP (AWS Foundational Security Best Practices) pour une unité d'organisation. Pour une autre unité d'organisation, vous pouvez choisir d'activer à la fois la norme FSBP et la norme Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0. Pour plus d'informations sur la création d'une politique de configuration qui active les normes spécifiques que vous spécifiez, consultezCréation et association de politiques de configuration.

Si vous utilisez une configuration centralisée, Security Hub CSPM n'active automatiquement aucune norme dans les comptes nouveaux ou existants. Au lieu de cela, l'administrateur Security Hub CSPM spécifie les normes à activer dans les différents comptes lorsqu'il crée des politiques de configuration Security Hub CSPM pour son organisation. Security Hub CSPM propose une politique de configuration recommandée dans laquelle seule la norme FSBP est activée. Pour de plus amples informations, veuillez consulter Types de politiques de configuration.

> **Note**
>
> L'administrateur CSPM de Security Hub peut utiliser des politiques de configuration pour activer n'importe quelle norme à l'exception de la norme gérée par les AWS Control Tower services. Pour activer cette norme, l'administrateur doit utiliser AWS Control Tower directement. Ils doivent également utiliser AWS Control Tower pour activer ou désactiver les contrôles individuels de cette norme pour un compte géré de manière centralisée.

Si vous souhaitez que certains comptes activent et configurent des normes pour leurs propres comptes, l'administrateur CSPM de Security Hub peut désigner ces comptes comme des comptes autogérés. Self-managed les comptes doivent activer et configurer les normes séparément dans chaque région.

Activation d'une norme dans un seul compte et Région AWS

Si vous n'utilisez pas la configuration centralisée ou si vous possédez un compte autogéré, vous ne pouvez pas utiliser de politiques de configuration pour activer les normes de sécurité de manière centralisée sur plusieurs comptes ou Régions AWS. Cependant, vous pouvez activer une norme

dans un seul compte et une seule région. Vous pouvez le faire à l'aide de la console Security Hub CSPM ou de l'API Security Hub CSPM.

Security Hub CSPM console

Suivez ces étapes pour activer une norme dans un compte et une région à l'aide de la console Security Hub CSPM.

Pour activer une norme dans un compte et une région

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, choisissez la région dans laquelle vous souhaitez activer la norme.
3. Dans le volet de navigation, sélectionnez Normes de sécurité. La page Normes de sécurité répertorie toutes les normes actuellement prises en charge par Security Hub CSPM. Si vous avez déjà activé une norme, la section relative à la norme inclut le score de sécurité actuel et des informations supplémentaires sur la norme.
4. Dans la section correspondant à la norme que vous souhaitez activer, choisissez Activer la norme.

Pour activer la norme dans d'autres régions, répétez les étapes précédentes dans chaque région supplémentaire.

Security Hub CSPM API

Pour activer une norme par programmation dans un seul compte et une seule région, utilisez l'BatchEnableStandardsopération. Ou, si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la batch-enable-standards commande.

Dans votre demande, utilisez le `StandardsArn` paramètre pour spécifier l'Amazon Resource Name (ARN) de la norme que vous souhaitez activer. Spécifiez également la région à laquelle s'applique votre demande. Par exemple, la commande suivante active la norme FSBP (AWS Foundational Security Best Practices) :

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

Où se *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0* trouve l'ARN de la norme FSBP dans la région de l'Est des États-Unis (Virginie du Nord) et *us-east-1* la région dans laquelle l'activer.

Pour obtenir l'ARN d'une norme, utilisez l'DescribeStandardsopération ou, si vous utilisez le AWS CLI, exécutez la describe-standards commande.

Pour consulter d'abord la liste des normes actuellement activées sur votre compte, vous pouvez utiliser l'GetEnabledStandardsopération. Si vous utilisez le AWS CLI, vous pouvez exécuter la commande get-enabled-standards pour récupérer cette liste.

Une fois que vous avez activé une norme, Security Hub CSPM commence à effectuer des tâches pour activer la norme dans le compte et la région spécifiée. Cela inclut la création de tous les contrôles qui s'appliquent à la norme. Pour suivre l'état de ces tâches, vous pouvez vérifier l'état de la norme pour le compte et la région.

Vérifier l'état d'une norme

Lorsque vous activez une norme de sécurité pour un compte, Security Hub CSPM commence à créer tous les contrôles qui s'appliquent à la norme dans le compte. Security Hub CSPM effectue également des tâches supplémentaires pour activer la norme pour le compte, telles que la génération d'un score de sécurité préliminaire pour la norme. Pendant que Security Hub CSPM exécute ces tâches, le statut de la norme est celui du Pending compte. L'état de la norme passe ensuite par des états supplémentaires, que vous pouvez surveiller et vérifier.

> **Note**
>
> Les modifications apportées aux contrôles individuels d'une norme n'affectent pas l'état général de la norme. Par exemple, si vous activez un contrôle que vous avez précédemment désactivé, votre modification n'affectera pas le statut de la norme. De même, si vous modifiez la valeur d'un paramètre pour un contrôle activé, votre modification n'affecte pas le statut de la norme.

Pour vérifier l'état d'une norme à l'aide de la console Security Hub CSPM, sélectionnez Normes de sécurité dans le volet de navigation. La page Normes de sécurité répertorie toutes les normes actuellement prises en charge par Security Hub CSPM. Si Security Hub CSPM effectue actuellement des tâches pour activer la norme, la section relative à la norme indique que Security Hub CSPM

génère toujours un score de sécurité pour la norme. Si une norme est activée, la section de la norme inclut le score actuel. Choisissez Afficher les résultats pour consulter des informations supplémentaires, notamment l'état des contrôles individuels qui s'appliquent à la norme. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

Pour vérifier l'état d'une norme par programmation à l'aide de l'API Security Hub CSPM, utilisez l'opération. GetEnabledStandards Dans votre demande, utilisez éventuellement le `StandardsSubscriptionArns` paramètre pour spécifier l'Amazon Resource Name (ARN) de la norme dont vous souhaitez vérifier le statut. Si vous utilisez le AWS Command Line Interface (AWS CLI), vous pouvez exécuter la commande get-enabled-standards pour vérifier l'état d'une norme. Pour spécifier l'ARN de la norme à vérifier, utilisez le `standards-subscription-arns` paramètre. Pour déterminer l'ARN à spécifier, vous pouvez utiliser l'DescribeStandardsopération ou, pour le AWS CLI, exécuter la describe-standards commande.

Si votre demande aboutit, Security Hub CSPM répond avec un tableau d'objets. `StandardsSubscription` Un abonnement standard est une AWS ressource que Security Hub CSPM crée dans un compte lorsqu'une norme est activée pour ce compte. Chaque `StandardsSubscription` objet fournit des informations sur une norme actuellement activée ou en cours d'activation ou de désactivation pour le compte. Dans chaque objet, le `StandardsStatus` champ indique l'état actuel de la norme pour le compte.

Le statut d'une norme (`StandardsStatus`) peut être l'un des suivants.

PENDING

Security Hub CSPM exécute actuellement des tâches visant à activer la norme pour le compte. Cela inclut la création des contrôles qui s'appliquent à la norme et la génération d'un score de sécurité préliminaire pour la norme. L'exécution de toutes les tâches par Security Hub CSPM peut prendre plusieurs minutes. Une norme peut également avoir ce statut si elle est déjà activée pour le compte et si Security Hub CSPM ajoute actuellement de nouveaux contrôles à la norme.

Si une norme possède ce statut, il est possible que vous ne puissiez pas récupérer les détails des contrôles individuels qui s'appliquent à la norme. En outre, il se peut que vous ne puissiez pas configurer ou désactiver des commandes individuelles pour la norme. Par exemple, si vous essayez de désactiver un contrôle à l'aide de cette UpdateStandardsControl opération, une erreur se produit.

Pour déterminer si vous pouvez configurer ou gérer des contrôles individuels pour la norme, reportez-vous à la valeur du `StandardsControlsUpdatable` champ. Si la valeur de ce champ est`READY_FOR_UPDATES`, vous pouvez commencer à gérer les contrôles individuels

pour la norme. Sinon, attendez que Security Hub CSPM termine des tâches de traitement supplémentaires pour activer la norme.

READY

La norme est actuellement activée pour le compte. Security Hub CSPM peut effectuer des contrôles de sécurité et générer des résultats pour tous les contrôles qui s'appliquent à la norme et qui sont actuellement activés. Security Hub CSPM peut également calculer un score de sécurité pour la norme.

Si une norme possède ce statut, vous pouvez récupérer les détails des contrôles individuels qui s'appliquent à la norme. En outre, vous pouvez configurer, désactiver ou réactiver les commandes. Vous pouvez également désactiver la norme.

INCOMPLETE

Security Hub CSPM n'a pas été en mesure d'activer complètement la norme pour le compte. Security Hub CSPM ne peut pas exécuter de contrôles de sécurité et générer des résultats pour tous les contrôles qui s'appliquent à la norme et qui sont actuellement activés. De plus, Security Hub CSPM ne peut pas calculer de score de sécurité pour la norme.

Pour les normes multicloud, l'abonnement entre `INCOMPLETE` avec un statut pour la raison suivante : `NO_AVAILABLE_MULTICLOUD_CONNECTOR` si vous activez la norme sans connecteur CSPM. L'abonnement passe automatiquement au `READY` moment où un connecteur devient disponible.

Pour déterminer pourquoi la norme n'a pas pu être complètement activée, reportez-vous aux informations du `StandardsStatusReason` tableau. Ce tableau indique les problèmes qui ont empêché Security Hub CSPM d'activer la norme. Si une erreur interne s'est produite, essayez de réactiver la norme pour le compte. Pour d'autres types de problèmes, vérifiez vos AWS Config paramètres. Vous pouvez également désactiver des commandes individuelles que vous ne souhaitez pas vérifier, ou désactiver complètement la norme.

DELETING

Security Hub CSPM traite actuellement une demande visant à désactiver la norme pour le compte. Cela inclut la désactivation des contrôles qui s'appliquent à la norme et la suppression du score de sécurité associé. Le traitement de la demande par Security Hub CSPM peut prendre plusieurs minutes.

Si un standard possède ce statut, vous ne pouvez pas le réactiver ou essayer de le désactiver à nouveau pour le compte. Security Hub CSPM doit d'abord terminer le traitement de la demande

en cours. De plus, vous ne pouvez pas récupérer les détails des contrôles individuels qui s'appliquent à la norme ni gérer les contrôles.

FAILED

Security Hub CSPM n'a pas pu désactiver la norme pour le compte. Une ou plusieurs erreurs se sont produites lorsque Security Hub CSPM a tenté de désactiver la norme. De plus, Security Hub CSPM ne peut pas calculer de score de sécurité pour la norme.

Pour déterminer pourquoi la norme n'a pas été complètement désactivée, reportez-vous aux informations du `StandardsStatusReason` tableau. Ce tableau indique les problèmes qui ont empêché Security Hub CSPM de désactiver la norme.

Si une norme possède ce statut, vous ne pouvez pas récupérer les détails des contrôles individuels qui s'appliquent à la norme ni gérer les contrôles. Vous pouvez toutefois réactiver la norme pour le compte. Si vous résolvez les problèmes qui ont empêché Security Hub CSPM de désactiver la norme, vous pouvez également essayer de la désactiver à nouveau.

Si le statut d'une norme est défini`READY`, Security Hub CSPM effectue des contrôles de sécurité et génère des résultats pour tous les contrôles qui s'appliquent à la norme et sont actuellement activés. Pour les autres statuts, Security Hub CSPM peut exécuter des contrôles et générer des résultats pour certains contrôles activés, mais pas pour tous. La génération ou la mise à jour des résultats de contrôle peuvent prendre jusqu'à 24 heures. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

Révision des détails d'une norme de sécurité

Après avoir activé une norme de sécurité dans AWS Security Hub CSPM, vous pouvez utiliser la console pour consulter les détails de la norme. Sur la console, la page de détails d'une norme inclut les informations suivantes :

- Le score de sécurité actuel de la norme.
- Tableau des contrôles qui s'appliquent à la norme.
- Statistiques agrégées pour les contrôles qui s'appliquent à la norme.
- Résumé visuel de l'état des contrôles qui s'appliquent à la norme.
- Résumé visuel des contrôles de sécurité pour les contrôles qui sont activés et s'appliquent à la norme. Si vous intégrez à AWS Organizations, les contrôles qui sont activés dans au moins un compte d'organisation sont considérés comme activés.

Pour consulter ces informations, sélectionnez Normes de sécurité dans le volet de navigation de la console. Ensuite, dans la section relative à la norme, choisissez Afficher les résultats. Pour une analyse plus approfondie, vous pouvez filtrer et trier les données, puis effectuer une analyse détaillée pour examiner les détails des contrôles individuels qui s'appliquent à la norme.

Rubriques

- Comprendre le score de sécurité standard
- Révision des contrôles pour une norme

Comprendre le score de sécurité standard

Sur la console AWS Security Hub CSPM, la page de détails d'une norme affiche le score de sécurité de cette norme. Le score est le pourcentage de contrôles qui ont réussi l'évaluation, par rapport au nombre total de contrôles qui s'appliquent à la norme, sont activés et comportent des données d'évaluation. Sous le score se trouve un graphique qui résume les contrôles de sécurité pour les contrôles activés pour la norme. Cela inclut le nombre de contrôles de sécurité réussis et échoués. Pour les comptes administrateurs, le score standard et le graphique sont agrégés pour le compte administrateur et tous les comptes membres. Pour vérifier les échecs des contrôles de sécurité présentant un niveau de gravité spécifique, choisissez le niveau de gravité.

Lorsque vous activez une norme, Security Hub CSPM génère un score de sécurité préliminaire pour la norme, généralement dans les 30 minutes suivant votre première visite sur la page de résumé ou sur la page des normes de sécurité de la console Security Hub CSPM. Les scores sont générés uniquement pour les normes qui sont activées lorsque vous visitez ces pages. De plus, l'enregistrement AWS Config des ressources doit être configuré pour que les scores apparaissent. Dans les régions de Chine et AWS GovCloud (US) Regions, la génération d'un score préliminaire par Security Hub CSPM peut prendre jusqu'à 24 heures. Une fois que Security Hub CSPM a généré un score préliminaire pour une norme, il le met à jour toutes les 24 heures. Pour de plus amples informations, veuillez consulter Calcul des scores de sécurité.

Toutes les données figurant sur les pages détaillées des normes de sécurité sont spécifiques à la version actuelle, Région AWS sauf si vous définissez une région d'agrégation. Si vous définissez une région d'agrégation, les scores de sécurité s'appliquent à toutes les régions et incluent les résultats pour toutes les régions liées. En outre, l'état de conformité des contrôles reflète les résultats des régions liées, et le nombre de contrôles de sécurité inclut les résultats des régions liées.

Révision des contrôles pour une norme

Lorsque vous utilisez la console AWS Security Hub CSPM pour consulter les détails d'une norme que vous avez activée, vous pouvez consulter un tableau des contrôles de sécurité qui s'appliquent à la norme. Pour chaque contrôle, le tableau inclut les informations suivantes :

- L'ID et le titre du contrôle.
- État de la commande. Pour de plus amples informations, veuillez consulter Évaluation de l'état de conformité et de l'état du contrôle.
- La sévérité attribuée au contrôle.
- Le nombre de contrôles échoués et le nombre total de contrôles. Le cas échéant, le champ Vérifications ayant échoué indique également le nombre de résultats dont le statut est Inconnu.
- Si le contrôle prend en charge les paramètres personnalisés. Pour de plus amples informations, veuillez consulter Comprendre les paramètres de contrôle dans Security Hub CSPM.

Security Hub CSPM met à jour les statuts des contrôles et le nombre de contrôles de sécurité toutes les 24 heures. Un horodatage en haut de la page indique la date à laquelle Security Hub CSPM a mis à jour ces données pour la dernière fois.

Pour les comptes administrateur, les statuts des contrôles et le nombre de contrôles de sécurité sont agrégés pour le compte administrateur et tous les comptes membres. Le nombre de contrôles activés inclut les contrôles qui sont activés pour la norme dans le compte administrateur ou dans au moins un compte membre. Le nombre de contrôles désactivés inclut les contrôles qui sont désactivés pour la norme dans le compte administrateur et dans tous les comptes membres.

Vous pouvez filtrer le tableau des contrôles qui s'appliquent à la norme. À l'aide des options Filtrer par situées à côté du tableau, vous pouvez choisir de n'afficher que les commandes activées ou désactivées pour la norme. Si vous n'affichez que les contrôles activés, vous pouvez filtrer davantage le tableau en fonction de l'état des contrôles. Vous pouvez ensuite vous concentrer sur les contrôles qui ont un statut de contrôle spécifique. Outre les options Filtrer par, vous pouvez saisir des critères de filtre dans la zone Commandes de filtrage. Par exemple, vous pouvez filtrer par ID de contrôle ou par titre.

Choisissez votre méthode d'accès préférée. Suivez ensuite les étapes pour passer en revue les contrôles qui s'appliquent à une norme que vous avez activée.

Security Hub CSPM console

Pour passer en revue les commandes d'une norme activée

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Normes de sécurité dans le volet de navigation.
3. Dans la section relative à la norme, choisissez Afficher les résultats.

Le tableau en bas de page répertorie tous les contrôles qui s'appliquent à la norme. Vous pouvez filtrer et trier le tableau. Vous pouvez également télécharger la page actuelle du tableau sous forme de fichier CSV. Pour ce faire, choisissez Télécharger au-dessus du tableau. Si vous filtrez le tableau, le fichier téléchargé inclut uniquement les commandes correspondant à vos paramètres de filtre actuels.

Security Hub CSPM API

Pour passer en revue les commandes d'une norme activée

1. Utilisez le ListSecurityControlDefinitions fonctionnement de l'API Security Hub CSPM. Si vous utilisez le AWS CLI, exécutez la commande https://docs.aws.amazon.com/cli/latest/reference/securityhub/list-security-control-definitions.html list-security-control-definitions.

   Spécifiez l'Amazon Resource Name (ARN) de la norme pour laquelle vous souhaitez revoir les contrôles. Pour obtenir des ARN pour les normes, utilisez l'DescribeStandardsopération ou exécutez la commande https://docs.aws.amazon.com/cli/latest/reference/securityhub/describe-standards.html describe-standards. Si vous ne spécifiez pas l'ARN d'une norme, Security Hub CSPM renvoie tous les ID de contrôle de sécurité.
2. Utilisez le ListStandardsControlAssociations fonctionnement de l'API CSPM Security Hub ou exécutez la commande https://docs.aws.amazon.com/cli/latest/reference/securityhub/list-standards-control-associations.html list-standards-control-associations. Cette opération vous indique dans quelles normes un contrôle est activé.

   Identifiez le contrôle en fournissant l'ID de contrôle de sécurité ou l'ARN. Les paramètres de pagination sont facultatifs.

L'exemple suivant vous indique les normes dans lesquelles le Config.1 contrôle est activé.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Désactivation des normes de sécurité activées automatiquement

Si votre organisation n'utilise pas de configuration centralisée, elle utilise un type de configuration appelé configuration locale. Avec une configuration locale, AWS Security Hub CSPM peut automatiquement activer les normes de sécurité par défaut pour les nouveaux comptes de membres lorsque ceux-ci rejoignent votre organisation. Toutes les commandes qui s'appliquent à ces normes par défaut sont également activées automatiquement.

Actuellement, les normes de sécurité par défaut sont la norme AWS Foundational Security Best Practices et la norme Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Pour plus d'informations sur ces normes, consultez leRéférence des normes pour Security Hub CSPM.

Si vous préférez activer manuellement les normes de sécurité pour les nouveaux comptes de membres, vous pouvez désactiver l'activation automatique des normes par défaut. Vous ne pouvez le faire que si vous intégrez AWS Organizations et utilisez la configuration locale. Si vous utilisez la configuration centralisée, vous pouvez plutôt créer une politique de configuration qui active les normes par défaut et associer la politique à la racine. Tous les comptes et unités d'organisation de votre organisation héritent ensuite de cette politique de configuration, sauf s'ils sont associés à une autre politique ou s'ils sont autogérés. Si vous n'effectuez pas d'intégration avec AWS Organizations, vous pouvez désactiver une norme par défaut lors de l'activation initiale de Security Hub CSPM ou d'une version ultérieure. Pour savoir comment procéder, consultez Désactivation d'une norme.

Pour désactiver l'activation automatique des normes par défaut pour les nouveaux comptes de membres, vous pouvez utiliser la console Security Hub CSPM ou l'API Security Hub CSPM.

Security Hub CSPM console

Suivez ces étapes pour désactiver l'activation automatique des normes par défaut à l'aide de la console Security Hub CSPM.

Pour désactiver l'activation automatique des normes par défaut

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur.

2. Dans le volet de navigation, sous Paramètres, choisissez Configuration.
3. Dans la section Aperçu, choisissez Modifier.
4. Sous Paramètres du nouveau compte, désactivez la case à cocher Activer les normes de sécurité par défaut.
5. Choisissez Confirmer.

Security Hub CSPM API

Pour désactiver l'activation automatique des normes par défaut par programmation, depuis le compte administrateur Security Hub CSPM, utilisez le UpdateOrganizationConfiguration fonctionnement de l'API Security Hub CSPM. Dans votre demande, spécifiez `NONE` le `AutoEnableStandards` paramètre.

Si vous utilisez le AWS CLI, exécutez la update-organization-configuration commande pour désactiver l'activation automatique des normes par défaut. Pour le paramètre `auto-enable-standards`, spécifiez `NONE`. Par exemple, la commande suivante active automatiquement Security Hub CSPM pour les comptes des nouveaux membres et désactive l'activation automatique des normes par défaut pour les comptes.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Désactivation d'une norme de sécurité

Lorsque vous désactivez une norme de sécurité dans AWS Security Hub CSPM, les événements suivants se produisent :

- Toutes les commandes qui s'appliquent à la norme sont désactivées, sauf si elles sont associées à une autre norme actuellement activée.
- Les contrôles de sécurité pour les contrôles désactivés ne sont plus effectués et aucun résultat supplémentaire n'est généré pour les contrôles désactivés.
- Les résultats existants pour les commandes désactivées sont automatiquement archivés au bout de 3 à 5 jours environ.
- AWS Config les règles que Security Hub CSPM a créées pour les contrôles désactivés sont supprimées.

La suppression des AWS Config règles appropriées se produit généralement quelques minutes après la désactivation d'une norme. Cependant, cela peut prendre plus de temps. Si la première demande ne parvient pas à supprimer les règles, Security Hub CSPM réessaie toutes les 12 heures. Toutefois, si vous avez désactivé Security Hub CSPM ou si aucune autre norme n'est activée, Security Hub CSPM ne peut pas réessayer, ce qui signifie qu'il ne peut pas supprimer les règles. Si cela se produit et que vous devez supprimer les règles, contactez AWS Support.

Rubriques

- Désactivation d'une norme dans plusieurs comptes et Régions AWS
- Désactiver une norme dans un seul compte et Région AWS

Désactivation d'une norme dans plusieurs comptes et Régions AWS

Pour désactiver une norme de sécurité sur plusieurs comptes Régions AWS, utilisez la configuration centralisée. Grâce à la configuration centralisée, l'administrateur délégué de Security Hub CSPM peut créer des politiques de configuration CSPM de Security Hub qui désactivent une ou plusieurs normes. L'administrateur peut ensuite associer une politique de configuration à des comptes individuels, à des unités organisationnelles (UO) ou à la racine. Une politique de configuration affecte la région d'origine, également appelée région d'agrégation, et toutes les régions liées.

Les politiques de configuration offrent des options de personnalisation. Par exemple, vous pouvez choisir de désactiver la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) dans une unité d'organisation. Pour une autre unité d'organisation, vous pouvez choisir de désactiver à la fois la norme PCI DSS et la norme SP 800-53 Rev. 5 du National Institute of Standards and Technology (NIST). Pour plus d'informations sur la création d'une politique de configuration qui active ou désactive les normes individuelles que vous spécifiez, consultezCréation et association de politiques de configuration.

> **Note**
>
> L'administrateur CSPM de Security Hub peut utiliser des politiques de configuration pour désactiver n'importe quelle norme à l'exception de la norme gérée par les AWS Control Tower services. Pour désactiver cette norme, l'administrateur doit utiliser AWS Control Tower directement. Ils doivent également être utilisés AWS Control Tower pour désactiver ou activer les contrôles individuels de cette norme pour un compte géré de manière centralisée.

Si vous souhaitez que certains comptes configurent ou désactivent des normes pour leurs propres comptes, l'administrateur CSPM de Security Hub peut désigner ces comptes comme des comptes autogérés. Self-managed les comptes doivent désactiver les normes séparément dans chaque région.

Désactiver une norme dans un seul compte et Région AWS

Si vous n'utilisez pas la configuration centralisée ou si vous possédez un compte autogéré, vous ne pouvez pas utiliser de politiques de configuration pour désactiver les normes de sécurité de manière centralisée sur plusieurs comptes ou Régions AWS. Cependant, vous pouvez désactiver une norme dans un seul compte et une seule région. Vous pouvez le faire à l'aide de la console Security Hub CSPM ou de l'API Security Hub CSPM.

Security Hub CSPM console

Suivez ces étapes pour désactiver une norme dans un compte et une région à l'aide de la console Security Hub CSPM.

Pour désactiver une norme dans un compte et une région

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, choisissez la région dans laquelle vous souhaitez désactiver la norme.
3. Dans le volet de navigation, sélectionnez Normes de sécurité.
4. Dans la section correspondant à la norme que vous souhaitez désactiver, choisissez Désactiver la norme.

Pour désactiver la norme dans d'autres régions, répétez les étapes précédentes dans chaque région supplémentaire.

Security Hub CSPM API

Pour désactiver une norme par programmation dans un seul compte et une seule région, utilisez l'BatchDisableStandardsopération. Ou, si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la batch-disable-standards commande.

Dans votre demande, utilisez le `StandardsSubscriptionArns` paramètre pour spécifier l'Amazon Resource Name (ARN) de la norme que vous souhaitez désactiver. Si vous utilisez

le AWS CLI, utilisez le `standards-subscription-arns` paramètre pour spécifier l'ARN. Spécifiez également la région à laquelle s'applique votre demande. Par exemple, la commande suivante désactive la norme FSBP (AWS Foundational Security Best Practices) pour un compte () : *123456789012*

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

Où *arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0* se trouvent l'ARN de la norme FSBP pour le compte dans la région USA Est (Virginie du Nord) et *us-east-1* la région dans laquelle le désactiver.

Pour obtenir l'ARN d'une norme, vous pouvez utiliser l'GetEnabledStandardsopération. Cette opération permet de récupérer des informations sur les normes actuellement activées sur votre compte. Si vous utilisez le AWS CLI, vous pouvez exécuter la commande get-enabled-standards pour récupérer ces informations.

Une fois que vous avez désactivé une norme, Security Hub CSPM commence à exécuter des tâches pour désactiver la norme dans le compte et la région spécifiée. Cela inclut la désactivation de toutes les commandes qui s'appliquent à la norme. Pour suivre l'état de ces tâches, vous pouvez vérifier l'état de la norme pour le compte et la région.

Comprendre les contrôles de sécurité dans Security Hub CSPM

Dans AWS Security Hub CSPM, un contrôle de sécurité, également appelé contrôle, est une garantie au sein d'une norme de sécurité qui aide une organisation à protéger la confidentialité, l'intégrité et la disponibilité de ses informations. Dans Security Hub CSPM, un contrôle est lié à une ressource spécifique AWS .

Lorsque vous activez un contrôle dans une ou plusieurs normes, Security Hub CSPM commence à exécuter des contrôles de sécurité sur celui-ci. Les contrôles de sécurité aboutissent aux résultats du Security Hub CSPM. Lorsque vous désactivez un contrôle, Security Hub CSPM arrête d'exécuter des contrôles de sécurité sur celui-ci et les résultats ne sont plus générés.

Vous pouvez activer ou désactiver les contrôles individuellement pour un seul compte et Région AWS. Pour gagner du temps et réduire la dérive de configuration dans les environnements multicomptes, nous vous recommandons d'utiliser une configuration centralisée pour activer ou désactiver les contrôles. Grâce à la configuration centralisée, l'administrateur délégué de Security Hub CSPM peut créer des politiques qui spécifient comment un contrôle doit être configuré sur plusieurs comptes et régions. Pour plus d'informations sur l'activation et la désactivation des contrôles, consultezActivation des contrôles dans Security Hub CSPM.

Vue consolidée des contrôles

La page Contrôles de la console Security Hub CSPM affiche tous les contrôles disponibles actuellement Région AWS (vous pouvez afficher les contrôles dans le contexte d'une norme en accédant à la page Normes de sécurité et en choisissant une norme activée). Security Hub CSPM attribue aux contrôles un identifiant, un titre et une description de contrôle de sécurité cohérents pour toutes les normes. Les identifiants des contrôles incluent le numéro pertinent Service AWS et un numéro unique (par exemple, CodeBuild.3).

Les informations suivantes sont disponibles sur la page Contrôles de la console Security Hub CSPM :

- Un score de sécurité global basé sur la proportion de contrôles réussis par rapport au nombre total de contrôles activés contenant des données
- Répartition des états de contrôle de tous les contrôles CSPM Security Hub pris en charge
- Nombre total de contrôles de sécurité réussis et échoués.
- Le nombre de contrôles de sécurité ayant échoué pour des contrôles de gravité variable et des liens permettant d'afficher plus de détails sur ces contrôles ayant échoué.
- Liste des contrôles CSPM de Security Hub, avec des filtres permettant d'afficher des sous-ensembles de contrôles spécifiques.

Sur la page Contrôles, vous pouvez choisir un contrôle pour afficher ses détails et prendre des mesures en fonction des résultats générés par le contrôle. À partir de cette page, vous pouvez également activer ou désactiver un contrôle de sécurité dans vos paramètres actuels Compte AWS et Région AWS. Les actions d'activation et de désactivation de la page Contrôles s'appliquent à toutes les normes. Pour de plus amples informations, veuillez consulter Activation des contrôles dans Security Hub CSPM.

Pour les comptes d'administrateur, la page Contrôles reflète l'état des contrôles sur les comptes des membres. Si une vérification de contrôle échoue dans au moins un compte membre, le statut du contrôle est Échec. Si vous avez défini une région d'agrégation, la page Contrôles reflète l'état des contrôles dans toutes les régions liées. Si une vérification de contrôle échoue dans au moins une région liée, le statut du contrôle est Échec.

La vue des contrôles consolidés entraîne des modifications des champs de recherche de contrôle dans le format ASFF (AWS Security Finding Format) qui peuvent affecter les flux de travail. Pour de plus amples informations, veuillez consulter Vue consolidée des contrôles — modifications de l'ASFF.

Score de sécurité récapitulatif pour les contrôles

La page Contrôles affiche un score de sécurité récapitulatif compris entre 0 et 100 %. Le score de sécurité récapitulatif est calculé en fonction de la proportion de contrôles réussis par rapport au nombre total de contrôles activés dont les données sont conformes aux normes.

> **Note**
>
> Pour afficher le score de sécurité global des contrôles, vous devez ajouter l'autorisation d'**`BatchGetControlEvaluations`**appeler le rôle IAM que vous utilisez pour accéder à Security Hub CSPM. Cette autorisation n'est pas requise pour consulter les scores de sécurité correspondant à des normes spécifiques.

Lorsque vous activez Security Hub CSPM, Security Hub CSPM calcule le score de sécurité initial dans les 30 minutes suivant votre première visite sur la page Résumé ou sur la page des normes de sécurité de la console Security Hub CSPM. La génération des premiers scores de sécurité peut prendre jusqu'à 24 heures dans les régions chinoises et AWS GovCloud (US) Regions.

Outre le score de sécurité global, Security Hub CSPM calcule un score de sécurité standard pour chaque norme activée dans les 30 minutes suivant votre première visite sur la page de résumé ou sur la page des normes de sécurité. Pour afficher la liste des normes actuellement activées, utilisez l'opération `GetEnabledStandards` API.

AWS Config doit être activé avec l'enregistrement des ressources pour que les partitions apparaissent. Pour plus d'informations sur la façon dont Security Hub CSPM calcule les scores de sécurité, consultez. Calcul des scores de sécurité

Après la première génération de scores, Security Hub CSPM met à jour les scores de sécurité toutes les 24 heures. Security Hub CSPM affiche un horodatage pour indiquer la date de dernière mise à jour d'un score de sécurité.

Si vous avez défini une région d'agrégation, le score de sécurité global reflète les résultats des contrôles entre les régions liées.

Référence de contrôle pour Security Hub CSPM

Cette référence de contrôle fournit un tableau des contrôles CSPM AWS Security Hub disponibles avec des liens vers des informations supplémentaires sur chaque contrôle. Dans le tableau, les contrôles sont répertoriés par ordre alphabétique par ID de contrôle. Seuls les contrôles utilisés activement par Security Hub CSPM sont inclus ici. Les contrôles retirés sont exclus du tableau.

Le tableau fournit les informations suivantes pour chaque contrôle :

- ID de contrôle de sécurité : cet identifiant s'applique à toutes les normes Service AWS et indique la ressource et à laquelle le contrôle se rapporte. La console Security Hub CSPM affiche les identifiants de contrôle de sécurité, que les résultats des contrôles consolidés soient activés ou désactivés sur votre compte. Toutefois, les résultats du Security Hub CSPM font référence à des identifiants de contrôle de sécurité uniquement si les résultats des contrôles consolidés sont activés dans votre compte. Si les résultats de contrôle consolidés sont désactivés dans votre compte, certains identifiants de contrôle varient généralement en fonction de vos résultats de contrôle. Pour un mappage des ID de contrôle spécifiques aux normes avec les ID de contrôle de sécurité, consultez. L'impact de la consolidation sur les identifiants et titres de contrôle

  Si vous souhaitez configurer des automatisations pour les contrôles de sécurité, nous vous recommandons de filtrer en fonction de l'identifiant du contrôle plutôt que du titre ou de la description. Alors que Security Hub CSPM peut occasionnellement mettre à jour les titres ou les descriptions des contrôles, les identifiants de contrôle restent les mêmes.

  Les ID de contrôle peuvent ignorer des numéros. Il s'agit d'espaces réservés pour les contrôles futurs.
- Titre du contrôle de sécurité — Ce titre s'applique à toutes les normes. La console Security Hub CSPM affiche les titres des contrôles de sécurité, que les résultats des contrôles consolidés soient activés ou désactivés sur votre compte. Toutefois, les résultats du Security Hub CSPM font référence aux titres des contrôles de sécurité uniquement si les résultats des contrôles consolidés sont activés dans votre compte. Si les résultats de contrôle consolidés sont désactivés dans votre compte, certains titres de contrôle varient généralement en fonction de vos résultats de contrôle.

Pour un mappage des ID de contrôle spécifiques aux normes avec les ID de contrôle de sécurité, consultez. L'impact de la consolidation sur les identifiants et titres de contrôle

- Normes applicables — Indique les normes auxquelles s'applique un contrôle. Choisissez un contrôle pour passer en revue les exigences spécifiques des cadres de conformité tiers.
- Gravité — La sévérité d'un contrôle indique son importance du point de vue de la sécurité. Pour plus d'informations sur la manière dont Security Hub CSPM détermine la gravité des contrôles, consultez. Niveaux de gravité des résultats de contrôle
- Supporte les paramètres personnalisés : indique si le contrôle prend en charge les valeurs personnalisées pour un ou plusieurs paramètres. Choisissez un contrôle pour consulter les détails des paramètres. Pour de plus amples informations, veuillez consulter Comprendre les paramètres de contrôle dans Security Hub CSPM.
- Type de planification : indique quand le contrôle est évalué. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

Choisissez un contrôle pour consulter des informations supplémentaires. Les contrôles sont répertoriés par ordre alphabétique par identifiant de contrôle de sécurité.

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Account.1	Les coordonnées de sécurité doivent être fournies pour Compte AWS	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
Account.2	Compte AWS devrait faire partie d'une	NIST SP 800-53 Rév. 5	ÉLEVÉ	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
	AWS Organizations organisation				
ACM.1	ACM-issued Les certificats importés doivent être renouvelés après une période spécifiée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	Oui	Changement déclenché et périodique
ACM.2	Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v4.0.1	ÉLEVÉ	Non	Changement déclenché
ACM.3	Les certificats ACM doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Amplify.1	Les applications Amplify doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Amplify.2	Les branches Amplify doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
APIGateway.1	API Gateway REST et la journalisation de l'exécution des WebSocket API doivent être activés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Oui	Changement déclenché
APIGateway.2	Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	Non	Changement déclenché
APIGateway.3	Les étapes de l'API REST API Gateway doivent avoir le AWS X-Ray traçage activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	Non	Changement déclenché
APIGateway.4	API Gateway doit être associée à une ACL Web WAF	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
APIGateway.5	Les données du cache de l'API REST API Gateway doivent être chiffrées au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
APIGateway.8	Les routes API Gateway doivent spécifier un type d'autorisation	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊘ Oui	Périodique
APIGateway.9	La journalisation des accès doit être configurée pour les étapes API Gateway V2	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
APIGateway.10	Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
APIGateway.11	Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
AppConfig.1	AWS AppConfig les applications doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppConfig.2	AWS AppConfig les profils de configuration doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppConfig.3	AWS AppConfig les environnements doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppConfig.4	AWS AppConfig les associations d'extension doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppFlow.1	AppFlow Les flux Amazon doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppRunner.1	Les services App Runner doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppRunner.2	Les connecteurs App Runner VPC doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
AppSync.2	AWS AppSync devrait avoir la journalisation au niveau du champ activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v4.0.1	MOYEN	Oui	Changement déclenché
AppSync.4	AWS AppSync Les API GraphQL doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
AppSync.5	AWS AppSync Les API GraphQL ne doivent pas être authentifiées avec des clés d'API	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	Non	Changement déclenché
Athena.2	Les catalogues de données Athena doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Athena.3	Les groupes de travail Athena doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Athena.4	La journalisation des groupes de travail Athena doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
AutoScaling.1	Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser des contrôles de santé ELB	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
AutoScaling.2	Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊙ Oui	Changement déclenché
AutoScaling.3	Les configurations de lancement de groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Autoscaling.5	Les instances Amazon EC2 lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresses IP publiques	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
AutoScaling.6	Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
AutoScaling.9	Les groupes EC2 Auto Scaling doivent utiliser des modèles de lancement EC2	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
AutoScaling.10	Les groupes EC2 Auto Scaling doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Backup.1	AWS Backup les points de restauration doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Backup.2	AWS Backup les points de récupération doivent être marqués	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Backup.3	AWS Backup les coffres-forts doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Backup.4	AWS Backup les plans de rapport doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Backup.5	AWS Backup les plans de sauvegarde doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Batch.1	Les files d'attente des tâches par lots doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Batch.2	Les politiques de planification par lots doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Batch.3	Les environnements de calcul par lots doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Batch.4	Les propriétés des ressources de calcul dans les environnements de calcul par lots gérés doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Bedrock.1	Les sources de données Amazon Bedrock doivent être chiffrées à l'aide de clés gérées par AWS KMS le client	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Changement déclenché
BedrockAgentCore.1	Les environnements d' AgentCore exécution de Bedrock doivent être configurés avec le mode réseau VPC	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	Non	Changement déclenché
BedrockAgentCore.2	Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
BedrockAgentCore.3	AgentCore La mémoire Bedrock doit être chiffrée à l'aide de clés gérées par AWS KMS le client	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
BedrockAgentCore.4	Bedrock AgentCore Gateway doit être chiffré avec des clés gérées par AWS KMS le client	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
BedrockAgentCore.5	Les navigateurs AgentCore personnalisés Bedrock ne doivent pas utiliser le mode réseau public	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Changement déclenché
BedrockAgentCore.6	L'enregistrement de session doit être activé dans les navigateurs AgentCore personnalisés Bedrock	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
BedrockAgentCore.7	Les interpréteurs de code AgentCore personnalisés Bedrock doivent utiliser une configuration de réseau privé	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Changement déclenché
CloudFormation.2	CloudFormation les piles doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
CloudFormation.3	CloudFormation la protection contre les terminaisons doit être activée sur les piles	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
CloudFormation.4	CloudFormation les piles doivent avoir des rôles de service associés	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
CloudFront.1	CloudFront les distributions doivent avoir un objet racine par défaut configuré	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudFront.3	CloudFront les distributions devraient nécessiter un chiffrement en transit	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
CloudFront.4	CloudFront les distributions doivent avoir le basculement d'origine configuré	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
CloudFront.5	CloudFront les distributions doivent avoir la journalisation activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
CloudFront.6	CloudFront WAF doit être activé pour les distributions	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
CloudFront.7	CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudFront.8	CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
CloudFront.9	CloudFront les distributions doivent crypter le trafic vers des origines personnalisées	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
CloudFront.10	CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
CloudFront.12	CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudFront.13	CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
CloudFront.14	CloudFront les distributions doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
CloudFront.15	CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
CloudFront.16	CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
CloudFront.17	CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudTrail.1	CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudTrail.2	CloudTrail le chiffrement au repos doit être activé	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, CIS AWS AWS Foundations Benchmark v1.4.0 Bonnes pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
CloudTrail.3	Au moins une CloudTrail piste doit être activée	NIST SP 800-171 Rév. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	ÉLEVÉ	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudTrail.4	CloudTrail la validation des fichiers journaux doit être activée	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	FAIBLE	⊗ Non	Périodique
CloudTrail.5	CloudTrail les sentiers doivent être intégrés à Amazon CloudWatch Logs	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudTrail.6	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	Benchmark CIS AWS Foundations v1.2.0, Benchmark CIS AWS Foundations v1.4.0, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Changement déclenché et périodique
CloudTrail.7	Assurez-vous que la journalisation de l'accès au compartiment S3 est activée sur le compartiment CloudTrail S3	Benchmark CIS AWS Foundations v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1 AWS	FAIBLE	⊗ Non	Périodique
CloudTrail.9	CloudTrail les sentiers doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
CloudTrail.10	CloudTrail Les magasins de données sur les événements de Lake doivent être cryptés et gérés par le client AWS KMS keys	NIST SP 800-53 Rév. 5	MOYEN	⊙ Oui	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudWatch.1	Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	FAIBLE	⊗ Non	Périodique
CloudWatch.2	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les appels d'API non autorisés	Indice de référence CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.3	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour la connexion à la console de gestion sans MFA	Indice de référence CIS AWS Foundations v1.2.0	FAIBLE	⊗ Non	Périodique
CloudWatch.4	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique IAM	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudWatch.5	Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.6	Assurez-vous qu'un filtre de mesure du journal et une alarme existent en cas Console de gestion AWS d'échec d'authentification	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.7	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour la désactivation ou la suppression planifiée des clés CMK créées par le client	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudWatch.8	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.9	Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications AWS Config de configuration	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.10	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des groupes de sécurité	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudWatch.11	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des listes de contrôle d'accès réseau (ACL réseau)	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.12	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.13	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique
CloudWatch.14	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications VPC	Benchmark CIS AWS Foundations v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CloudWatch.15	CloudWatch les actions spécifiées doivent être configurées pour les alarmes	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2	ÉLEVÉ	Oui	Changement déclenché
CloudWatch.16	CloudWatch les groupes de journaux doivent être conservés pendant une période spécifiée	NIST SP 800-53 Rév. 5	MOYEN	Oui	Périodique
CloudWatch.17	CloudWatch les actions d'alarme doivent être activées	NIST SP 800-53 Rév. 5	ÉLEVÉ	Non	Changement déclenché
CodeArtifact.1	CodeArtifact les référentiels doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
CodeBuild.1	CodeBuild Les URL du référentiel source Bitbucket ne doivent pas contenir d'informations d'identification sensibles	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CodeBuild.2	CodeBuild les variables d'environnement du projet ne doivent pas contenir d'informations d'identification en texte clair	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Changement déclenché
CodeBuild.3	CodeBuild Les journaux S3 doivent être chiffrés	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	FAIBLE	⊗ Non	Changement déclenché
CodeBuild.4	CodeBuild les environnements de projet doivent avoir une configuration de journalisation	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
CodeBuild.7	CodeBuild les exportations de groupes de rapports doivent être cryptées au repos	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
CodeGuruProfiler.1	CodeGuru Les groupes de profilage du profileur doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
CodeGuruReviewer.1	CodeGuru Les associations de référentiels de réviseurs doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Cognito.1	La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Oui	Changement déclenché
Cognito.2	Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Changement déclenché
Cognito.3	Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Cognito.4	La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
Cognito.5	Le MFA doit être activé pour les groupes d'utilisateurs Cognito	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
Cognito.6	La protection contre la suppression doit être activée pour les groupes d'utilisateurs Cognito	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Config.1	AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1	CRITIQUE	✓ Oui	Périodique
Connect.1	Les types d'objets Connect Customer Customer Profiles doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
Connect.2	Les instances Connect Customer doivent avoir la CloudWatch journalisation activée	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	✗ Non	Changement déclenché
DataFirehose.1	Les flux de diffusion Firehose doivent être chiffrés au repos	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	✗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
DataSync.1	DataSync la journalisation des tâches doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Changement déclenché
DataSync.2	DataSync les tâches doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Detective.1	Les graphiques du comportement des détectives doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
DMS.1	Les instances de réplication du service de migration de base de données ne doivent pas être publiques	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	Non	Périodique
DMS.2	Les certificats DMS doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
DMS.3	Les abonnements aux événements DMS doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
DMS.4	Les instances de réplication DMS doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
DMS.5	Les groupes de sous-réseaux de réplication DMS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
DMS.6	La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	✗ Non	Changement déclenché
DMS.7	La journalisation des tâches de réplication DMS pour la base de données cible doit être activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	✗ Non	Changement déclenché
DMS.8	La journalisation des tâches de réplication DMS pour la base de données source doit être activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	✗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
DMS.9	Les points de terminaison DMS doivent utiliser le protocole SSL	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
DMS.10	L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
DMS.11	Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
DMS.12	TLS doit être activé sur les points de terminaison DMS pour Redis OSS	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
DMS.13	Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
DocumentDB.1	Les clusters Amazon DocumentDB doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
DocumentDB.2	Les clusters Amazon DocumentDB doivent bénéficier d'une période de conservation des sauvegardes adéquate	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊙ Oui	Changement déclenché
DocumentDB.3	Les instantanés de cluster manuels d'Amazon DocumentDB ne doivent pas être publics	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
DocumentDB.4	Les clusters Amazon DocumentDB doivent publier des journaux d'audit dans Logs CloudWatch	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
DocumentDB.5	La protection contre la suppression des clusters Amazon DocumentDB doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
DocumentDB.6	Les clusters Amazon DocumentDB doivent être chiffrés en transit	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
DynamoDB.1	Les tables DynamoDB devraient automatiquement adapter leur capacité à la demande	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	✓ Oui	Périodique
DynamoDB.2	La restauration instantanée des tables DynamoDB doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
DynamoDB 3	Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
DynamoDB 4	Les tables DynamoDB doivent figurer dans un plan de sauvegarde	NIST SP 800-53 Rév. 5	MOYEN	⊙ Oui	Périodique
DynamoDB 5	Les tables DynamoDB doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
DynamoDB 6	La protection contre la suppression des tables DynamoDB doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
DynamoDB 7	Les clusters DynamoDB Accelerator doivent être chiffrés en transit	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.1	Les instantanés EBS ne doivent pas être restaurables publiquement	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Périodique
EC2.2	Les groupes de sécurité par défaut du VPC ne doivent pas autoriser le trafic entrant ou sortant	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	ÉLEVÉ	⊗ Non	Changement déclenché
EC2.3	Les volumes EBS attachés doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.4	Les instances EC2 arrêtées doivent être supprimées après une période spécifiée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Oui	Périodique
EC2.6	La journalisation des flux VPC doit être activée dans tous les VPC	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST AWS SP 800-171 Rev. 2	MOYEN	Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.7	Le chiffrement EBS par défaut doit être activé	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
EC2.8	Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
EC2.9	Les instances EC2 ne doivent pas avoir d'adresse IPv4 publique	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.10	Amazon EC2 doit être configuré pour utiliser des points de terminaison VPC créés pour le service Amazon EC2	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Périodique
EC2.12	Les EIP EC2 non utilisés doivent être supprimés	PCI DSS v3.2.1, NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché
EC2.13	Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 sur le port 22	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ÉLEVÉ	⊗ Non	Changement déclenché et périodique
EC2.14	Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389	Benchmark CIS AWS Foundations v1.2.0, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché et périodique
EC2.15	Les sous-réseaux EC2 ne doivent pas attribuer automatiquement des adresses IP publiques	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.16	Les listes de contrôle d'accès réseau non utilisées doivent être supprimées	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1,	FAIBLE	⊗ Non	Changement déclenché
EC2.17	Les instances EC2 ne doivent pas utiliser plusieurs ENI	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
EC2.18	Les groupes de sécurité ne doivent autoriser le trafic entrant sans restriction que pour les ports autorisés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ÉLEVÉ	✓ Oui	Changement déclenché
EC2.19	Les groupes de sécurité ne devraient pas autoriser un accès illimité aux ports présentant un risque élevé	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	CRITIQUE	⊗ Non	Changement déclenché et périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.20	Les deux tunnels VPN pour une connexion AWS Site-to-Site VPN doivent être opérationnels	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Changement déclenché
EC2.21	Les ACL réseau ne devraient pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers le port 22 ou le port 3389	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
EC2.22	Les groupes de sécurité EC2 non utilisés doivent être supprimés		MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.23	Les passerelles de transit EC2 ne devraient pas accepter automatiquement les demandes de pièces jointes VPC	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché
EC2.24	Les types d'instances paravirtuelles EC2 ne doivent pas être utilisés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
EC2.25	Les modèles de lancement EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
EC2.28	Les volumes EBS doivent figurer dans un plan de sauvegarde	NIST SP 800-53 Rév. 5	FAIBLE	⊙ Oui	Périodique
EC2.33	Les pièces jointes de la passerelle de transit EC2 doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.34	Les tables de routage de la passerelle de transit EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.35	Les interfaces réseau EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.36	Les passerelles clients EC2 doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.37	Les adresses IP Elastic EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.38	Les instances EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.39	Les passerelles Internet EC2 doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.40	Les passerelles NAT EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.41	Les ACL du réseau EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.42	Les tables de routage EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.43	Les groupes de sécurité EC2 doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.44	Les sous-réseaux EC2 doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.45	Les volumes EC2 doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.46	Les VPC Amazon doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.47	Les services de point de terminaison Amazon VPC doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.48	Les journaux de flux Amazon VPC doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.49	Les connexions d'appairage Amazon VPC doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.50	Les passerelles VPN EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.51	La journalisation des connexions client doit être activée sur les points de terminaison du VPN client EC2	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	FAIBLE	Non	Changement déclenché
EC2.52	Les passerelles de transit EC2 doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.53	Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration du serveur distant	Benchmark CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
EC2.54	Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration du serveur distant	Benchmark CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
EC2.55	Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊘ Oui	Périodique
EC2.56	Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊘ Oui	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.57	Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	Oui	Périodique
EC2.58	Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts du gestionnaire d'incidents de Systems Manager	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	Oui	Périodique
EC2.60	Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	Oui	Périodique
EC2.170	Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	FAIBLE	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.171	La journalisation des connexions VPN EC2 doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
EC2.172	Les paramètres EC2 VPC Block Public Access devraient bloquer le trafic de la passerelle Internet	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊙ Oui	Changement déclenché
EC2.173	Les demandes EC2 Spot Fleet avec paramètres de lancement devraient permettre le chiffrement des volumes EBS attachés	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
EC2.174	Les ensembles d'options DHCP EC2 doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
EC2.175	Les modèles de lancement EC2 doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
EC2.176	Les listes de préfixes EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.177	Les sessions EC2 Traffic Mirror doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.178	Les filtres des miroirs de trafic EC2 doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.179	Les cibles du miroir de trafic EC2 doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
EC2.180	La source/destination vérification doit être activée sur les interfaces réseau EC2	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	Non	Changement déclenché
EC2.181	Les modèles de lancement EC2 devraient permettre le chiffrement des volumes EBS attachés	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	Non	Changement déclenché
EC2.182	Les instantanés EBS ne doivent pas être accessibles au public	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EC2.183	Les connexions VPN EC2 doivent utiliser le protocole IKEv2	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
ECR.1	La numérisation des images doit être configurée dans les référentiels privés ECR	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
ECR.2	Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ECR.3	Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ECR.4	Les référentiels publics ECR doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
ECR.5	Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys	NIST SP 800-53 Rév. 5	MOYEN	✓ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ECS.2	Les services ECS ne doivent pas se voir attribuer automatiquement des adresses IP publiques	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
ECS.3	Les définitions de tâches ECS ne doivent pas partager l'espace de noms des processus de l'hôte	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché
ECS.4	Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché
ECS.5	Les conteneurs ECS doivent être limités à l'accès en lecture seule aux systèmes de fichiers racine	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché
ECS.8	Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ECS.9	Les définitions de tâches ECS doivent avoir une configuration de journalisation	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché
ECS.10	Les services ECS Fargate devraient fonctionner sur la dernière version de la plateforme Fargate	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ECS.12	Les clusters ECS doivent utiliser Container Insights	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ECS.13	Les services ECS doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
ECS.14	Les clusters ECS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
ECS.15	Les définitions de tâches ECS doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ECS.16	Les ensembles de tâches ECS ne doivent pas attribuer automatiquement des adresses IP publiques	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
ECS.17	Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
ECS.18	Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
ECS.19	Les fournisseurs de capacité ECS devraient avoir activé la protection gérée contre les terminaisons	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
ECS.20	Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ECS.21	Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
EFS.1	Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
EFS.2	Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
EFS.3	Les points d'accès EFS doivent appliquer un répertoire racine	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EFS.4	Les points d'accès EFS doivent renforcer l'identité de l'utilisateur	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
EFS.5	Les points d'accès EFS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
EFS.6	Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
EFS.7	Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
EFS.8	Les systèmes de fichiers EFS doivent être chiffrés au repos	CIS AWS Foundations Benchmark v5.0.0, Bonnes pratiques AWS de sécurité fondamentales	MOYEN	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EKS.1	Les points de terminaison du cluster EKS ne doivent pas être accessibles au public	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
EKS.2	Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
EKS.3	Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
EKS.6	Les clusters EKS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
EKS.7	Les configurations du fournisseur d'identité EKS doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EKS.8	La journalisation des audits doit être activée pour les clusters EKS	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
EKS.9	Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Changement déclenché
ElastiCache.1	ElastiCache Les sauvegardes automatiques des clusters (Redis OSS) doivent être activées	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊙ Oui	Périodique
ElastiCache.2	ElastiCache les mises à niveau automatiques des versions mineures doivent être activées sur les clusters	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
ElastiCache.3	ElastiCache les groupes de réplication doivent avoir le basculement automatique activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ElastiCache.4	ElastiCache les groupes de réplication doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
ElastiCache.5	ElastiCache les groupes de réplication doivent être chiffrés en transit	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
ElastiCache.6	ElastiCache Redis OSS AUTH doit être activé pour les groupes de réplication (Redis OSS) des versions antérieures	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
ElastiCache.7	ElastiCache les clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Périodique
ElasticBeanstalk.1	Les environnements Elastic Beanstalk devraient avoir des rapports de santé améliorés activés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ElasticBeanstalk.2	Les mises à jour de la plateforme gérée Elastic Beanstalk doivent être activées	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	Oui	Changement déclenché
ElasticBeanstalk.3	Elastic Beanstalk doit diffuser les journaux vers CloudWatch	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	Oui	Changement déclenché
ELB.1	L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MOYEN	Non	Périodique
ELB.2	Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ELB.3	Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ELB.4	L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ELB.5	La journalisation des applications et des équilibreurs de charge classiques doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ELB.6	La protection contre la suppression doit être activée pour les équilibreurs de charge des applications, des passerelles et du réseau	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ELB.7	Le drainage des connexions doit être activé pour les équilibreurs de charge classiques	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
ELB.8	Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie dotée d'une configuration robuste	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ELB.9	L'équilibrage de charge entre zones doit être activé pour les équilibreurs de charge classiques	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ELB.10	L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	✓ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ELB.12	L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict.	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ELB.13	Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊙ Oui	Changement déclenché
ELB.14	L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict.	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ELB.16	Les équilibreurs de charge des applications doivent être associés à une ACL AWS Web WAF	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ELB.17	Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ELB.18	Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour chiffrer les données en transit	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
ELB.21	Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
ELB.22	Les groupes cibles ELB doivent utiliser des protocoles de transport chiffrés	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EMR.1	Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
EMR.2	Le paramètre d'accès public bloqué à Amazon EMR doit être activé	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Périodique
EMR.3	Les configurations de sécurité Amazon EMR doivent être chiffrées au repos	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
EMR.4	Les configurations de sécurité Amazon EMR doivent être chiffrées en transit	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ES.1	Les domaines Elasticsearch doivent avoir le chiffrement au repos activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ES.2	Les domaines Elasticsearch ne doivent pas être accessibles au public	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Périodique
ES.3	Les domaines Elasticsearch doivent chiffrer les données envoyées entre les nœuds	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	MOYEN	⊗ Non	Changement déclenché
ES.4	L'enregistrement des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ES.5	La journalisation des audits doit être activée pour les domaines Elasticsearch	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ES.6	Les domaines Elasticsearch doivent comporter au moins trois nœuds de données	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
ES.7	Les domaines Elasticsearch doivent être configurés avec au moins trois nœuds principaux dédiés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
ES.8	Les connexions aux domaines Elasticsearch doivent être chiffrées à l'aide de la dernière politique de sécurité TLS	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
ES.9	Les domaines Elasticsearch doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
EventBridge.2	EventBridge les bus de l'événement doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
EventBridge.3	EventBridge les bus événementiels personnalisés devraient être associés à une politique basée sur les ressources	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
EventBridge.4	EventBridge la réplication des événements doit être activée sur les terminaux globaux	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
FraudDetector.1	Les types d'entités Amazon Fraud Detector doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
FraudDetector.2	Les étiquettes d'Amazon Fraud Detector doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
FraudDetector.3	Les résultats d'Amazon Fraud Detector doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
FraudDetector.4	Les variables d'Amazon Fraud Detector doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
FSx.1	FSx pour les systèmes de fichiers OpenZFS doit être configuré pour copier les balises dans les sauvegardes et les volumes	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Périodique
FSx.2	Les systèmes de fichiers FSx pour Lustre doivent être configurés pour copier les balises dans les sauvegardes	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Périodique
FSx.3	Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
FSx.4	Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	✓ Oui	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
FSx.5	Les systèmes de fichiers FSx pour Windows File Server doivent être configurés pour le déploiement Multi-AZ	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
Glue.1	AWS Glue les offres d'emploi doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Glue.3	AWS Glue les transformations d'apprentissage automatique doivent être chiffrées au repos	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
Glue.4	AWS Glue Les tâches Spark doivent être exécutées sur les versions prises en charge de AWS Glue	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
GlobalAccelerator.1	Les accélérateurs Global Accelerator doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
GuardDuty.1	GuardDuty doit être activé	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.2	GuardDuty les filtres doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
GuardDuty.3	GuardDuty Les IPsets doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
GuardDuty.4	GuardDuty les détecteurs doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
GuardDuty.5	GuardDuty La surveillance du journal d'audit EKS doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.6	GuardDuty La protection Lambda doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
GuardDuty.7	GuardDuty La surveillance du temps d'exécution EKS doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.8	GuardDuty La protection contre les programmes malveillants pour EC2 doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.9	GuardDuty La protection RDS doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.10	GuardDuty La protection S3 doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.11	GuardDuty La surveillance du temps d'exécution doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Périodique
GuardDuty.12	GuardDuty ECS Runtime Monitoring doit être activé	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
GuardDuty.13	GuardDuty La surveillance de l'exécution d'EC2 doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
IAM.1	Les politiques IAM ne doivent pas autoriser la totalité des privilèges administratifs « * »	CIS AWS Foundations Benchmark v1.2.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ÉLEVÉ	⊗ Non	Changement déclenché
IAM.2	Les utilisateurs IAM ne doivent pas être associés à des politiques IAM	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.3	Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
IAM.4	La clé d'accès de l'utilisateur root IAM ne doit pas exister	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.5	L'authentification multifacteur doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
IAM.6	L'authentification multifacteur matérielle doit être activée pour l'utilisateur root	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.7	Les politiques de mot de passe pour les utilisateurs IAM doivent être configurées de manière robuste	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	Oui	Périodique
IAM.8	Les informations d'identification utilisateur IAM non utilisées doivent être supprimées	CIS AWS Foundations Benchmark v1.2.0, meilleures pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MOYEN	Non	Périodique
IAM.9	Le MFA doit être activé pour l'utilisateur root	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1 AWS	CRITIQUE	Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.10	Les politiques de mot de passe pour les utilisateurs IAM doivent être configurées de manière robuste	NIST SP 800-171 Rév. 2, PCI DSS v3.2.1	MOYEN	⊗ Non	Périodique
IAM.11	Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule	Indice de référence CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
IAM.12	Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule	Indice de référence CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
IAM.13	Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole	Indice de référence CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Périodique
IAM.14	Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre	Indice de référence CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.15	Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus	Benchmark CIS AWS Foundations v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST AWS SP 800-171 Rev. 2	MOYEN	⊗ Non	Périodique
IAM.16	Vérifier que la politique de mot de passe IAM empêche la réutilisation d'un mot de passe	Benchmark CIS AWS Foundations v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1 AWS	FAIBLE	⊗ Non	Périodique
IAM.17	Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans les 90 jours ou moins	Benchmark CIS AWS Foundations v1.2.0, PCI DSS v4.0.1	FAIBLE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.18	Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avec AWS Support	Benchmark CIS AWS Foundations v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1 AWS	FAIBLE	⊗ Non	Périodique
IAM.19	Le MFA doit être activé pour tous les utilisateurs IAM	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
IAM.21	Les politiques IAM gérées par les clients que vous créez ne doivent pas autoriser les actions par caractères génériques pour les services	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.22	Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées	Benchmark CIS AWS Foundations v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Périodique
IAM.23	Les analyseurs IAM Access Analyzer doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
IAM.24	Les rôles IAM doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
IAM.25	Les utilisateurs IAM doivent être tagués	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
IAM.26	SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés	Indice de référence CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IAM.27	Les identités IAM ne doivent pas être associées à la AWSCloudShellFullAccess politique	Indice de référence CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0	MOYEN	⊗ Non	Changement déclenché
IAM.28	L'analyseur d'accès externe IAM Access Analyzer doit être activé	Indice de référence CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0	ÉLEVÉ	⊗ Non	Périodique
Inspector.1	La numérisation Amazon Inspector EC2 doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
Inspector.2	La numérisation ECR d'Amazon Inspector doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
Inspector.3	L'analyse du code Lambda d'Amazon Inspector doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
Inspector.4	L'analyse standard Amazon Inspector Lambda doit être activée	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IoT.1	AWS IoT Device Defender les profils de sécurité doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoT.2	AWS IoT Core les mesures d'atténuation doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoT.3	AWS IoT Core les dimensions doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoT.4	AWS IoT Core les autorisateurs doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoT.5	AWS IoT Core les alias de rôle doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoT.6	AWS IoT Core les politiques doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTSiteWise.1	AWS IoT SiteWise les modèles d'actifs doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IoTSiteWise.2	AWS IoT SiteWise les tableaux de bord doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTSiteWise.3	AWS IoT SiteWise les passerelles doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTSiteWise.4	AWS IoT SiteWise les portails doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTSiteWise.5	AWS IoT SiteWise les projets doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTTwinMaker.1	AWS Les tâches de TwinMaker synchronisation IoT doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTTwinMaker.2	AWS Les TwinMaker espaces de travail IoT doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTTwinMaker.3	AWS TwinMaker Les scènes IoT doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
IoTTwinMaker.4	AWS TwinMaker Les entités IoT doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTWireless.1	AWS Les groupes de multidiffusion sans fil IoT doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTWireless.2	AWS Les profils de service IoT Wireless doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IoTWireless.3	AWS Les tâches IoT Wireless FUOTA doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IVS.1	Les paires de touches de lecture IVS doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IVS.2	Les configurations d'enregistrement IVS doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
IVS.3	Les chaînes IVS doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Keyspaces.1	Les espaces clés Amazon Keyspaces doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Kinesis.1	Les flux Kinesis doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
Kinesis.2	Les flux Kinesis doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Kinesis.3	Les flux Kinesis doivent avoir une période de conservation des données adéquate	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Oui	Changement déclenché
KMS.1	Les politiques IAM gérées par le client ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
KMS.2	Les directeurs IAM ne doivent pas disposer de politiques IAM en ligne qui autorisent des actions de déchiffrement sur toutes les clés KMS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
KMS.3	AWS KMS keys ne doit pas être supprimé par inadvertance	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Changement déclenché
KMS.4	AWS KMS key la rotation doit être activée	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1 AWS	MOYEN	⊗ Non	Périodique
KMS.5	Les clés KMS ne doivent pas être accessibles au public	AWS Meilleures pratiques fondamentales en matière de sécurité	CRITIQUE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Lambda.1	Les politiques relatives à la fonction Lambda devraient interdire l'accès public	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Changement déclenché
Lambda.2	Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
Lambda.3	Les fonctions Lambda doivent se trouver dans un VPC	PCI DSS v3.2.1, NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché
Lambda.5	Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊘ Oui	Changement déclenché
Lambda.6	Les fonctions Lambda doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
Lambda.7	Les fonctions Lambda doivent avoir le traçage AWS X-Ray actif activé	NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Macie.1	Amazon Macie doit être activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
Macie.2	La découverte automatique des données sensibles par Macie doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Périodique
MSK.1	Les clusters MSK doivent être chiffrés en transit entre les nœuds de courtage	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
MSK.2	Les clusters MSK doivent avoir une surveillance améliorée configurée	NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché
MSK.3	Les connecteurs MSK Connect doivent être chiffrés en transit	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
MSK.4	L'accès public doit être désactivé pour les clusters MSK	AWS Meilleures pratiques fondamentales en matière de sécurité	CRITIQUE	⊗ Non	Changement déclenché
MSK.5	Les connecteurs MSK doivent avoir la journalisation activée	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
MSK.6	Les clusters MSK doivent désactiver l'accès non authentifié	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
MQ.2	Les courtiers ActiveMQ doivent diffuser les journaux d'audit vers CloudWatch	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
MQ.4	Les courtiers Amazon MQ doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
MQ.5	Les courtiers ActiveMQ doivent utiliser active/standby le mode déploiement	NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
MQ.6	Les courtiers RabbitMQ devraient utiliser le mode de déploiement en cluster	NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché
Neptune.1	Les clusters de base de données Neptune doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Neptune.2	Les clusters de base de données Neptune doivent publier des journaux d'audit dans Logs CloudWatch	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
Neptune.3	Les instantanés du cluster de base de données Neptune ne doivent pas être publics	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Changement déclenché
Neptune.4	La protection contre la suppression doit être activée pour les clusters de base de données Neptune	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Neptune.5	Les sauvegardes automatisées doivent être activées sur les clusters de base de données Neptune	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Oui	Changement déclenché
Neptune.6	Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
Neptune.7	L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
Neptune.8	Les clusters de base de données Neptune doivent être configurés pour copier les balises dans les instantanés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	Non	Changement déclenché
Neptune.9	Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité	NIST SP 800-53 Rév. 5	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
NetworkFirewall.1	Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
NetworkFirewall.2	La journalisation du pare-feu réseau doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Périodique
NetworkFirewall.3	Les politiques de pare-feu réseau doivent être associées à au moins un groupe de règles	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Changement déclenché
NetworkFirewall.4	L'action sans état par défaut pour les politiques de pare-feu réseau doit être Drop ou Forward pour les paquets complets	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
NetworkFirewall.5	L'action sans état par défaut pour les politiques de pare-feu réseau doit être Drop ou Forward pour les paquets fragmentés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Changement déclenché
NetworkFirewall.6	Le groupe de règles de pare-feu réseau sans état ne doit pas être vide	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Changement déclenché
NetworkFirewall.7	Les pare-feux du pare-feu réseau doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
NetworkFirewall.8	Les politiques de pare-feu du pare-feu réseau doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
NetworkFirewall.9	La protection contre la suppression doit être activée sur les pare-feux du pare-feu réseau	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
NetworkFirewall.10	Les pare-feux du pare-feu réseau doivent avoir la protection contre les modifications de sous-réseau activée	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Opensearch.1	OpenSearch les domaines doivent avoir le chiffrement au repos activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Opensearch.2	OpenSearch les domaines ne doivent pas être accessibles au public	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Changement déclenché
Opensearch.3	OpenSearch les domaines doivent crypter les données envoyées entre les nœuds	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Opensearch.4	OpenSearch la journalisation des erreurs de domaine dans CloudWatch les journaux doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Opensearch.5	OpenSearch la journalisation des audits doit être activée pour les domaines	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
Opensearch.6	OpenSearch les domaines doivent avoir au moins trois nœuds de données	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Opensearch.7	OpenSearch les domaines doivent avoir un contrôle d'accès précis activé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Opensearch.8	Les connexions aux OpenSearch domaines doivent être cryptées à l'aide de la dernière politique de sécurité TLS	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Opensearch.9	OpenSearch les domaines doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
Opensearch.10	OpenSearch la dernière mise à jour logicielle doit être installée sur les domaines	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
Opensearch.11	OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés	NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Périodique
PCA.1	CA privée AWS l'autorité de certification racine doit être désactivée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
PCA.2	AWS Les autorités de certification CA privées doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
RDS.1	L'instantané RDS doit être privé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRITIQUE	Non	Changement déclenché
RDS.2	Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.3	Le chiffrement au repos doit être activé sur les instances de base de données RDS	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bonnes pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
RDS.4	Les instantanés du cluster RDS et les instantanés de base de données doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
RDS.5	Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité	CIS AWS Foundations Benchmark v5.0.0, Meilleures pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.6	Une surveillance améliorée doit être configurée pour les instances de base de données RDS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	Oui	Changement déclenché
RDS.7	La protection contre la suppression des clusters RDS doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
RDS.8	La protection contre la suppression des instances de base de données RDS doit être activée	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	Non	Changement déclenché
RDS.9	Les instances de base de données RDS doivent publier des journaux dans CloudWatch Logs	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	Non	Changement déclenché
RDS.10	L'authentification IAM doit être configurée pour les instances RDS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.11	Les sauvegardes automatiques doivent être activées sur les instances RDS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Oui	Changement déclenché
RDS.12	L'authentification IAM doit être configurée pour les clusters RDS	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
RDS.13	Les mises à niveau automatiques des versions mineures de RDS doivent être activées	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	Non	Changement déclenché
RDS.14	Le retour en arrière doit être activé sur les clusters Amazon Aurora	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.15	Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité	CIS AWS Foundations Benchmark v5.0.0, Meilleures pratiques de sécurité AWS fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
RDS.16	Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
RDS.17	Les instances de base de données RDS doivent être configurées pour copier les balises dans les instantanés	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
RDS.19	Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements critiques du cluster	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.20	Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	FAIBLE	⊗ Non	Changement déclenché
RDS.21	Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de groupe de paramètres de base de données critiques	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	FAIBLE	⊗ Non	Changement déclenché
RDS.22	Un abonnement aux notifications d'événements RDS doit être configuré pour les événements critiques du groupe de sécurité des bases de données	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.23	Les instances RDS ne doivent pas utiliser le port par défaut d'un moteur de base de données	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
RDS.24	Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
RDS.25	Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
RDS.26	Les instances de base de données RDS doivent être protégées par un plan de sauvegarde	NIST SP 800-53 Rév. 5	MOYEN	⊙ Oui	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.27	Les clusters de bases de données RDS doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
RDS.28	Les clusters de bases de données RDS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
RDS.29	Les instantanés du cluster de bases de données RDS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
RDS.30	Les instances de base de données RDS doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
RDS.31	Les groupes de sécurité RDS DB doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
RDS.32	Les instantanés de base de données RDS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.33	Les groupes de sous-réseaux de base de données RDS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
RDS.34	Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	Non	Changement déclenché
RDS.35	La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	Non	Changement déclenché
RDS.36	Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	MOYEN	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.37	Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
RDS.38	Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
RDS.39	Les instances de base de données RDS pour MySQL doivent être chiffrées en transit	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
RDS.40	Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	✓ Oui	Changement déclenché
RDS.41	Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.42	Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	Oui	Périodique
RDS.43	Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Périodique
RDS.44	Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Périodique
RDS.45	La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.46	Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Périodique
RDS.47	Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données	AWS Meilleures pratiques fondamentales en matière de sécurité	FAIBLE	⊗ Non	Changement déclenché
RDS.48	Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données	AWS Meilleures pratiques fondamentales en matière de sécurité	FAIBLE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RDS.50	Les clusters de bases de données RDS doivent disposer d'une période de rétention des sauvegardes suffisante	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Oui	Changement déclenché
RDS.51	Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Changement déclenché
Redshift.1	Les clusters Amazon Redshift devraient interdire l'accès public	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRITIQUE	⊗ Non	Changement déclenché
Redshift.2	Les connexions aux clusters Amazon Redshift doivent être chiffrées en transit	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Redshift.3	Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Oui	Changement déclenché
Redshift.4	La journalisation des audits doit être activée pour les clusters Amazon Redshift	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	Non	Changement déclenché
Redshift.6	Les mises à niveau automatiques vers les versions majeures d'Amazon Redshift devraient être activées	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
Redshift.7	Les clusters Redshift doivent utiliser un routage VPC amélioré	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché
Redshift.8	Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur administrateur par défaut	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Redshift.10	Les clusters Redshift doivent être chiffrés au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Redshift.11	Les clusters Redshift doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Redshift.12	Les notifications d'abonnement aux événements Redshift doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Redshift.13	Les instantanés du cluster Redshift doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
Redshift.14	Les groupes de sous-réseaux du cluster Redshift doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Redshift.15	Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Périodique
Redshift.16	Les groupes de sous-réseaux du cluster Redshift doivent comporter des sous-réseaux provenant de plusieurs zones de disponibilité	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
Redshift.17	Les groupes de paramètres du cluster Redshift doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	✓ Oui	Changement déclenché
Redshift.18	Les Multi-AZ déploiements des clusters Redshift doivent être activés	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RedshiftServerless.1	Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Périodique
RedshiftServerless.2	Les connexions aux groupes de travail Redshift Serverless devraient être requises pour utiliser le protocole SSL	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
RedshiftServerless.3	Les groupes de travail Redshift Serverless devraient interdire l'accès public	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Périodique
RedshiftServerless.4	Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le client AWS KMS keys	NIST SP 800-53 Rév. 5	MOYEN	⊙ Oui	Périodique
RedshiftServerless.5	Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
RedshiftServerless.6	Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique
Route53.1	Les bilans de santé de la Route 53 doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
Route53.2	Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
S3.1	Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
S3.2	Les compartiments S3 à usage général devraient bloquer l'accès public en lecture	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Changement déclenché et périodique
S3.3	Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Changement déclenché et périodique
S3.5	Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole SSL	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
S3.6	Les politiques de compartiment à usage général de S3 devraient restreindre l'accès aux autres Comptes AWS	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ÉLEVÉ	⊗ Non	Changement déclenché
S3.7	Les compartiments S3 à usage général doivent utiliser la réplication entre régions	PCI DSS v3.2.1, NIST SP 800-53 Rév. 5	FAIBLE	⊗ Non	Changement déclenché
S3.8	Les compartiments S3 à usage général devraient bloquer l'accès public	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bonnes pratiques de sécurité AWS fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
S3.9	Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
S3.10	Les compartiments S3 à usage général pour lesquels la gestion des versions est activée doivent avoir des configurations de cycle de vie	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
S3.11	Les notifications d'événements doivent être activées dans les compartiments S3 à usage général	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2	MOYEN	✓ Oui	Changement déclenché
S3.12	Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
S3.13	Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	FAIBLE	Oui	Changement déclenché
S3.14	Les compartiments S3 à usage général doivent avoir le contrôle de version activé	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2	FAIBLE	Non	Changement déclenché
S3.15	Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé	NIST SP 800-53 Rév. 5, PCI DSS v4.0.1	MOYEN	Oui	Changement déclenché
S3.17	Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2, PCI DSS v4.0.1	MOYEN	Non	Changement déclenché
S3.19	Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRITIQUE	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
S3.20	La suppression MFA doit être activée pour les compartiments S3 à usage général	Benchmark CIS AWS Foundations v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	FAIBLE	⊗ Non	Changement déclenché
S3.22	Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet	Benchmark CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
S3.23	Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet	Benchmark CIS AWS Foundations v5.0.0, Benchmark CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
S3.24	Les paramètres de blocage de l' Multi-Region accès public aux points d'accès S3 doivent être activés	AWS Meilleures pratiques de sécurité fondamentales, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
S3.25	Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie	AWS Meilleures pratiques fondamentales en matière de sécurité	FAIBLE	Oui	Changement déclenché
SageMaker.1	Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	ÉLEVÉ	Non	Périodique
SageMaker.2	SageMaker les instances de bloc-notes doivent être lancées dans un VPC personnalisé	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	Non	Changement déclenché
SageMaker.3	Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	ÉLEVÉ	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SageMaker.4	SageMaker les variantes de production des terminaux doivent avoir un nombre d'instances initial supérieur à 1	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Périodique
SageMaker.5	SageMaker l'isolation réseau doit être activée sur les modèles	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
SageMaker.6	SageMaker les configurations d'image de l'application doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
SageMaker.7	SageMaker les images doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
SageMaker.8	SageMaker les instances de bloc-notes doivent s'exécuter sur les plates-formes prises en charge	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SageMaker.9	SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
SageMaker.10	SageMaker les définitions de tâches d'explicabilité du modèle doivent avoir le cryptage du trafic inter-conteneurs activé	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
SageMaker.11	SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
SageMaker.12	SageMaker l'isolation réseau doit être activée pour les définitions de tâches liées au biais du modèle	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SageMaker.13	SageMaker les définitions de tâches relatives à la qualité des modèles doivent avoir le chiffrement du trafic inter-conteneurs activé	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
SageMaker.14	SageMaker les calendriers de surveillance doivent avoir l'isolation du réseau activée	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
SageMaker.15	SageMaker les définitions de tâches basées sur le biais du modèle doivent avoir le chiffrement du trafic inter-conteneurs activé	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	⊗ Non	Changement déclenché
SageMaker.16	SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SageMaker.17	SageMaker les magasins hors ligne des groupes de fonctionnalités doivent être cryptés avec des AWS KMS clés	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
SageMaker.18	SageMaker les boutiques en ligne de groupes de fonctionnalités avec stockage standard doivent être cryptées avec des AWS KMS clés	NIST SP 800-53 Rév. 5	MOYEN	⊗ Non	Changement déclenché
SageMaker.19	SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
SageMaker.20	SageMaker les définitions de tâches d'explicabilité du modèle doivent avoir l'isolation réseau activée	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SageMaker.21	SageMaker les instances de bloc-notes doivent être chiffrées à l'aide de AWS KMS clés gérées par le client	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
SageMaker.22	SageMaker le chiffrement du trafic entre conteneurs doit être activé dans les programmes de surveillance	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
SageMaker.23	SageMaker les expériences d'inférence doivent avoir un volume de stockage d'instance chiffré avec des clés gérées par AWS KMS le client	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
SageMaker.24	SageMaker les expériences d'inférence doivent avoir un stockage de données chiffré avec des clés gérées par AWS KMS le client	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SageMaker.25	SageMaker les définitions de tâches relatives à la qualité des modèles doivent avoir l'isolation réseau activée	AWS Meilleures pratiques fondamentales en matière de sécurité	ÉLEVÉ	⊗ Non	Changement déclenché
SecretsManager.1	La rotation automatique des secrets de Secrets Manager doit être activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊙ Oui	Changement déclenché
SecretsManager.2	Les secrets de Secrets Manager configurés avec une rotation automatique doivent être pivotés correctement	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Changement déclenché
SecretsManager.3	Supprimer les secrets non utilisés de Secrets Manager	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊙ Oui	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SecretsManager.4	Les secrets de Secrets Manager doivent faire l'objet d'une rotation dans un délai spécifié	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	Oui	Périodique
SecretsManager.5	Les secrets de Secrets Manager doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
ServiceCatalog.1	Les portefeuilles du catalogue de services ne doivent être partagés qu'au sein d'une AWS organisation	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	Non	Périodique
SES.1	Les listes de contacts SES doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
SES.2	Les ensembles de configuration SES doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
SES.3	Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SNS.1	Les sujets SNS doivent être chiffrés au repos à l'aide de AWS KMS	NIST SP 800-53 Rév. 5, NIST SP 800-171 Rév. 2	MOYEN	⊗ Non	Changement déclenché
SNS.3	Les sujets SNS doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
SNS.4	Les politiques d'accès aux rubriques SNS ne devraient pas autoriser l'accès public	AWS Meilleures pratiques fondamentales en matière de sécurité	CRITIQUE	⊗ Non	Changement déclenché
SQS.1	Les files d'attente Amazon SQS doivent être chiffrées au repos	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
SQS.2	Les files d'attente SQS doivent être balisées	AWS Norme de balisage des ressources	FAIBLE	⊙ Oui	Changement déclenché
SQS.3	Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public	AWS Meilleures pratiques fondamentales en matière de sécurité	CRITIQUE	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SSM.1	Les instances EC2 doivent être gérées par AWS Systems Manager	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
SSM.2	Les instances EC2 gérées par Systems Manager doivent avoir un statut de conformité des correctifs de COMPLIANT après l'installation d'un correctif	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	ÉLEVÉ	⊗ Non	Changement déclenché
SSM.3	Les instances EC2 gérées par Systems Manager doivent avoir un statut de conformité d'association de COMPLIANT	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	FAIBLE	⊗ Non	Changement déclenché
SSM.4	Les documents SSM ne doivent pas être publics	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	CRITIQUE	⊗ Non	Périodique

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
SSM.5	Les documents SSM doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
SSM.6	La CloudWatch journalisation de SSM Automation doit être activée	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	MOYEN	Non	Périodique
SSM.7	Le paramètre de partage public par blocs doit être activé pour les documents SSM	AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	CRITIQUE	Non	Périodique
StepFunctions.1	Step Functions indique que la journalisation doit être activée sur les machines	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, PCI DSS v4.0.1	MOYEN	Oui	Changement déclenché
StepFunctions.2	Les activités Step Functions doivent être étiquetées	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché
Transfer.1	Les flux de travail Transfer Family doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
Transfer.2	Les serveurs de la famille Transfer ne doivent pas utiliser le protocole FTP pour la connexion des terminaux	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
Transfer.3	Les connecteurs Transfer Family doivent avoir la journalisation activée	AWS Meilleures pratiques fondamentales en matière de sécurité, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
Transfer.4	Transfert Les accords familiaux doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
Transfer.5	Les certificats Transfer Family doivent être étiquetés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
Transfer.6	Les connecteurs de la famille de transferts doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché
Transfer.7	Les profils des familles de transfert doivent être balisés	AWS Norme de balisage des ressources	FAIBLE	⊘ Oui	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
WAF.1	AWS La journalisation WAF Classic Global Web ACL doit être activée	AWS Meilleures pratiques de sécurité fondamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MOYEN	⊗ Non	Périodique
WAF.2	AWS Les règles régionales de la WAF Classic doivent comporter au moins une condition	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
WAF.3	AWS Les groupes de règles régionaux WAF Classic doivent avoir au moins une règle	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
WAF.4	AWS Les ACL Web WAF Classic Regional doivent comporter au moins une règle ou un groupe de règles	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
WAF.6	AWS Les règles globales de WAF Classic doivent comporter au moins une condition	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
WAF.7	AWS Les groupes de règles globaux WAF Classic doivent avoir au moins une règle	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
WAF.8	AWS Les ACL Web globales de WAF Classic doivent comporter au moins une règle ou un groupe de règles	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
WAF.10	AWS Les ACL Web WAF doivent comporter au moins une règle ou un groupe de règles	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5	MOYEN	⊗ Non	Changement déclenché
WAF.11	AWS La journalisation des ACL Web WAF doit être activée	NIST SP 800-53 Rév. 5, PCI DSS v4.0.1	FAIBLE	⊗ Non	Périodique
WAF.12	AWS Les règles WAF doivent avoir des CloudWatch métriques activées	AWS Meilleures pratiques de sécurité fondamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MOYEN	⊗ Non	Changement déclenché

ID de contrôle de sécurité	Titre du contrôle de sécurité	Normes applicables	Sévérité	Supporte les paramètres personnalisés	Type de programme
WorkSpaces.1	WorkSpaces les volumes d'utilisateurs doivent être chiffrés au repos	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché
WorkSpaces.2	WorkSpaces les volumes racine doivent être chiffrés au repos	AWS Meilleures pratiques fondamentales en matière de sécurité	MOYEN	⊗ Non	Changement déclenché

Journal des modifications pour les contrôles CSPM de Security Hub

Le journal des modifications suivant permet de suivre les modifications importantes apportées aux contrôles CSPM existants de AWS Security Hub, qui peuvent entraîner des modifications de l'état général d'un contrôle et de l'état de conformité de ses résultats. Pour plus d'informations sur la manière dont Security Hub CSPM évalue l'état des contrôles, consultez. Évaluation de l'état de conformité et de l'état du contrôle Les modifications peuvent prendre quelques jours après leur saisie dans ce journal pour affecter toutes les Régions AWS zones dans lesquelles le contrôle est disponible.

Ce journal suit les changements survenus depuis avril 2023. Choisissez un contrôle pour consulter les informations supplémentaires le concernant. Les changements de titre sont indiqués dans la description détaillée d'un contrôle pendant 90 jours.

Date du changement	ID et titre du contrôle	Description du changement
11 septembre 2026	[RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée	Ce contrôle vérifie si la mise à niveau automatique des

Date du changement	ID et titre du contrôle	Description du changement
		versions mineures est activée pour un cluster de bases de données Amazon RDS. Security Hub CSPM a étendu le contrôle pour évaluer les clusters de bases de données Aurora, qui ne renvoyaient aucun résultat auparavant.
11 septembre 2026	[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS	Security Hub CSPM a mis à jour le titre et la description de ce contrôle pour faire référence à TLS au lieu de SSL, car le protocole SSL est obsolète.

Date du changement	ID et titre du contrôle	Description du changement
27 août 2026	[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration	Ce contrôle vérifie si les instances Amazon RDS interdise nt l'accès public. Neptune DB prenant désormais en charge les points de terminais on publics, ce contrôle évalue et génère des résultats exploitables pour les instances de base de données Neptune. Security Hub CSPM a mis à jour la description du contrôle pour refléter cette modification.

Date du changement	ID et titre du contrôle	Description du changement
12 août 2026	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon EKS s'exécute sur une version de Kubernetes prise en charge. Security Hub CSPM a modifié la valeur du paramètre pour ce contrôle, la faisant passer de à`1.33`. `1.34` Le support standard pour la version 1.33 de Kubernetes dans Amazon EKS a pris fin le 29 juillet 2026.

Date du changement	ID et titre du contrôle	Description du changement
12 août 2026	[EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un groupe de nœuds Amazon EKS s'exécute sur une version de Kubernetes prise en charge. Security Hub CSPM a modifié la valeur du paramètre pour ce contrôle, la faisant passer de à`1.33`. `1.34` Le support standard pour la version 1.33 de Kubernetes dans Amazon EKS a pris fin le 29 juillet 2026.

Date du changement	ID et titre du contrôle	Description du changement
3 août 2026	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `java17.al2023`, `java11.al2023`, `java8.al2023` la valeur de paramètre, tout comme le AWS Lambda support ajouté pour ce runtime.
3 août 2026	[EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement	Security Hub CSPM a supprimé ce contrôle de la norme FSBP (AWS Foundational Security Best Practices).

Date du changement	ID et titre du contrôle	Description du changement
31 juillet 2026	[SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge	Security Hub CSPM a modifié la valeur du paramètre pour ce contrôle, la faisant passer de à`notebook-al2-v3`. `notebook-al2023-v1` SageMaker AI a migré des plateformes d'instance de bloc-notes d'Amazon Linux 2 vers AL2023.
13 juillet 2026	[EC2.10] Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2	Security Hub CSPM a modifié la règle de sauvegarde pour ce contrôle, passant de service-vpc-endpoint-enabled à vpc-endpoint-enabled. La règle mise à jour reconnaît que les noms des services de FIPS-variant terminaux sont conformes et génère une `PASSED` recherche pour les VPC qui utilisent des points de terminaison FIPS.

Date du changement	ID et titre du contrôle	Description du changement
29 juin 2026	[EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement	Security Hub CSPM a ajouté ce contrôle aux normes applicables suivantes : la norme NIST SP 800-53 Rev. 5, la norme NIST SP 800-171 Revision 2 et la norme PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html Le 30 juillet 2026, ce contrôle sera supprimé de la norme FSBP (AWS Foundational Security Best Practices).

Date du changement	ID et titre du contrôle	Description du changement
5 juin 2026	[EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés	Security Hub CSPM a informé que ce contrôle serait retiré et retiré de toutes les normes Security Hub CSPM applicables après le 10 août 2026. À partir de la version 1.28 de Kubernetes, les clusters Amazon EKS disposent de secrets Kubernete s protégés par un cryptage d'enveloppe par défaut.
5 juin 2026	[IoTEvents.1] IoTEvents.1	Security Hub CSPM a informé que ce contrôle serait retiré et supprimé de toutes les normes Security Hub CSPM applicables après le 7 juillet 2026. AWS a annoncé la fin du support pour le service AWS IoT Events à compter du 20 mai 2026.

Date du changement	ID et titre du contrôle	Description du changement
5 juin 2026	[IoTEvents.2] IoTEvents.2	Security Hub CSPM a informé que ce contrôle serait retiré et supprimé de toutes les normes Security Hub CSPM applicables après le 7 juillet 2026. AWS a annoncé la fin du support pour le service AWS IoT Events à compter du 20 mai 2026.
5 juin 2026	[IoTEvents.3] IoTEvents.3	Security Hub CSPM a informé que ce contrôle serait retiré et supprimé de toutes les normes Security Hub CSPM applicables après le 7 juillet 2026. AWS a annoncé la fin du support pour le service AWS IoT Events à compter du 20 mai 2026.

Date du changement	ID et titre du contrôle	Description du changement
5 juin 2026	[ECS.1] Les définitions de tâches Amazon ECS doivent comporter des modes réseau sécurisés et des définitions utilisateur	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes applicables. Auparavant, le contrôle vérifiait si une définition de tâche Amazon ECS active qui utilisait le mode réseau hôte comportait également `privileged` des définitions de `user` conteneurs.
5 juin 2026	[RDS.18] Les instances RDS doivent être déployées dans un VPC	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes applicables. Depuis le retrait du EC2-Classic réseau Amazon, les instances Amazon Relational Database Service (Amazon RDS) ne peuvent plus être déployées en dehors d'un VPC. Auparavant, le contrôle vérifiait si une instance Amazon RDS était déployée sur un EC2-VPC.

Date du changement	ID et titre du contrôle	Description du changement
4 mai 2026	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge ce runtime en `ruby4.0` tant que paramètre et n'inclut plus ce runtime`nodejs20.x` , ce AWS Lambda qui est obsolète.

Date du changement	ID et titre du contrôle	Description du changement
27 avril 2026	[EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée	Security Hub CSPM a modifié la règle de sauvegarde pour ce contrôle, passant de ec2-stopped-instance à une règle CSPM Security Hub personnalisée, ec2-stopped-instance-days-check, afin de simplifier la logique d'évaluation.
7 avril 2026	[EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement	Security Hub CSPM a modifié le titre et la description de ce contrôle. Le nouveau titre et la nouvelle description reflètent plus précisément le fait que le contrôle vérifie si les instantanés Amazon EBS sont configurés pour être restaurables publiquement. Auparavant, le titre de ce contrôle était le suivant : Les instantanés Amazon EBS ne devraient pas être restaurables publiquement.

Date du changement	ID et titre du contrôle	Description du changement
7 avril 2026	[EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS	Security Hub CSPM a modifié le titre et la description de ce contrôle. Le nouveau titre et la nouvelle description reflètent plus précisément le fait que le contrôle vérifie si l'accès public bloqué au niveau du compte est activé pour les instantanés Amazon EBS. Auparavant, le titre de ce contrôle était le suivant : Les instantanés Amazon EBS ne devraient pas être accessibles au public.
6 avril 2026	[ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées	Security Hub CSPM a mis à jour la valeur du paramètre pour ce contrôle afin de refléter les politiques de sécurité recommandées.

Date du changement	ID et titre du contrôle	Description du changement
3 avril 2026	[Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste	Security Hub CSPM a étendu la plage de valeurs prises en charge pour le `temporaryPasswordValidity` paramètre de ce contrôle. Vous pouvez désormais spécifier une valeur comprise entre 1 et 365 jours. Auparavant, la fourchette était de 7 à 365 jours.
3 avril 2026	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon EKS s'exécute sur une version de Kubernetes prise en charge. Security Hub CSPM a modifié la valeur du paramètre pour ce contrôle, la faisant passer de à`1.32`. `1.33` Le support standard pour la version 1.32 de Kubernetes dans Amazon EKS a pris fin le 23 mars 2026.

Date du changement	ID et titre du contrôle	Description du changement
3 avril 2026	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 le paramètre pour les environnements d'exécution pris en charge n'est plus inclus `ruby3.2` car Lambda a rendu obsolète ce runtime.
24 mars 2026	[RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante	Security Hub CSPM a mis à jour le titre du contrôle pour indiquer que le contrôle vérifie tous les clusters de bases de données RDS.

Date du changement	ID et titre du contrôle	Description du changement
24 mars 2026	[ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine	Security Hub CSPM a mis à jour le titre et la description du contrôle pour indiquer que le contrôle vérifie les définitio ns des tâches ECS. Security Hub CSPM a également mis à jour le contrôle afin de ne pas générer de résultats pour les définitions de tâches `runtimePl atform` configuré es pour spécifier une famille de `WINDOWS_S ERVER` systèmes d'exploitation.
9 mars 2026	[AppSync.1] Les caches d' AWS AppSync API doivent être chiffrés au repos	Security Hub CSPM a retiré ce contrôle et l'a retiré de la norme FSBP (AWS Foundational Security Best Practices). AWS AppSync fournit désormais un cryptage par défaut sur tous les caches d'API actuels et futurs.

Date du changement	ID et titre du contrôle	Description du changement
9 mars 2026	[AppSync.6] Les caches d' AWS AppSync API doivent être chiffrés en transit	Security Hub CSPM a retiré ce contrôle et l'a retiré de la norme FSBP (AWS Foundational Security Best Practices). AWS AppSync fournit désormais un cryptage par défaut sur tous les caches d'API actuels et futurs.
4 mars 2026	[ECS.1] Les définitions de tâches Amazon ECS doivent comporter des modes réseau sécurisés et des définitions utilisateur	Security Hub CSPM a retiré ce contrôle et l'a retiré de la norme FSBP (AWS Foundational Security Best Practices) et de la norme NIST SP 800-53 Rev. 5.
5 février 2026	[AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos	Security Hub CSPM retirera ce contrôle et supprimera de toutes les normes Security Hub CSPM applicables le 9 mars 2026. AWS AppSync fournit un cryptage par défaut sur tous les caches d'API actuels et futurs.

Date du changement	ID et titre du contrôle	Description du changement
5 février 2026	[AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport	Security Hub CSPM retirera ce contrôle et supprimera de toutes les normes Security Hub CSPM applicables le 9 mars 2026. AWS AppSync fournit un cryptage par défaut sur tous les caches d'API actuels et futurs.
16 janvier 2026	[ECS.1] Les définitions de tâches Amazon ECS doivent comporter des modes réseau sécurisés et des définitions utilisateur	Security Hub CSPM a informé que ce contrôle serait retiré et retiré de toutes les normes Security Hub CSPM applicables après le 16 février 2026.
12 janvier 2026	[Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift	Security Hub CSPM a mis à jour ce contrôle pour supprimer le `loggingEnabled` paramètre.

Date du changement	ID et titre du contrôle	Description du changement
12 janvier 2026	[MQ.3] Les courtiers Amazon MQ devraient activer la mise à niveau automatique des versions mineures	Security Hub CSPM a retiré le contrôle et l'a retiré de toutes les normes applicables. Security Hub CSPM a retiré le contrôle en raison des exigences d'Amazon MQ pour les mises à niveau automatiques des versions mineures. Auparavant, le contrôle s'appliquait à la norme FSBP (AWS Foundational Security Best Practices), à la norme NIST SP 800-53 Rev. 5 et à la norme PCI DSS v4.0.1.

Date du changement	ID et titre du contrôle	Description du changement
12 janvier 2026	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `dotnet10` comme valeur de paramètre pour ce contrôle. AWS Lambda ajout du support pour ce runtime.

Date du changement	ID et titre du contrôle	Description du changement
15 décembre 2025	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM ne prend plus en charge `python3.9` la valeur de paramètre pour ce contrôle. AWS Lambda ne prend plus en charge ce runtime.

Date du changement	ID et titre du contrôle	Description du changement
12 décembre 2025	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon EKS s'exécute sur une version de Kubernetes prise en charge. Security Hub CSPM a modifié la valeur du paramètre de ce contrôle de à`1.31`. `1.32` Le support standard pour la version 1.31 de Kubernetes dans Amazon EKS a pris fin le 26 novembre 2025.

Date du changement	ID et titre du contrôle	Description du changement
21 novembre 2025	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `nodejs24.x` et en `python3.14` tant que valeurs de paramètre pour ce contrôle. AWS Lambda ajout de la prise en charge de ces environnements d'exécution.

Date du changement	ID et titre du contrôle	Description du changement
14 novembre 2025	[EC2.15] Les sous-réseaux Amazon EC2 ne doivent pas attribuer automatiquement d'adresses IP publiques	Security Hub CSPM a mis à jour la descripti on et la justifica tion de ce contrôle. Auparavant, le contrôle vérifiait uniquement l'attribu tion automatique des adresses IP publiques IPv4 dans les sous-réseaux Amazon VPC à l'aide de l'indicat eur. `MapPublic IpOnLaunch` Ce contrôle vérifie désormais l'attribu tion automatique des adresses IP publiques IPv4 et IPv6. La description et la justification du contrôle ont été mises à jour pour refléter ces changements.

Date du changement	ID et titre du contrôle	Description du changement
14 novembre 2025	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `java25` comme valeur de paramètre pour ce contrôle. AWS Lambda ajout du support pour ce runtime.
13 novembre 2025	[SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public	Security Hub CSPM a modifié la sévérité de ce contrôle de à`HIGH`. `CRITICAL` Autoriser l'accès public aux rubriques Amazon SNS représente un risque de sécurité important.

Date du changement	ID et titre du contrôle	Description du changement
13 novembre 2025	[SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public	Security Hub CSPM a modifié la sévérité de ce contrôle de à`HIGH`. `CRITICAL` Autoriser l'accès public aux files d'attente Amazon SQS représente un risque de sécurité important.
13 novembre 2025	[GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée	Security Hub CSPM a modifié la sévérité de ce contrôle de à`MEDIUM`. `HIGH` Ce type de surveillance de l'exécution permet de mieux détecter les menaces pour les ressources Amazon EKS.
13 novembre 2025	[MQ.3] Les courtiers Amazon MQ devraient activer la mise à niveau automatique des versions mineures	Security Hub CSPM a modifié la sévérité de ce contrôle de à`LOW`. `MEDIUM` Les mises à niveau des versions mineures incluent les correctifs de sécurité nécessaires au maintien de la sécurité d'Amazon MQ Broker.

Date du changement	ID et titre du contrôle	Description du changement
13 novembre 2025	[Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée	Security Hub CSPM a modifié la sévérité de ce contrôle de à`LOW`. `MEDIUM` Les mises à jour logicielles incluent les correctifs de sécurité nécessair es au maintien de la sécurité OpenSearch du domaine.
13 novembre 2025	[RDS.7] La protection contre la suppression des clusters RDS doit être activée	Security Hub CSPM a modifié la sévérité de ce contrôle de à`LOW`. `MEDIUM` La protection contre la suppression permet d'empêcher la suppression accidente lle des bases de données Amazon RDS et la suppression de bases de données RDS par des entités non autorisées.

Date du changement	ID et titre du contrôle	Description du changement
13 novembre 2025	[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs	Security Hub CSPM a modifié la sévérité de ce contrôle de à`LOW`. `MEDIUM` AWS CloudTrail les données d'enregis trement dans Amazon CloudWatch Logs peuvent être utilisées pour des activités d'audit, des alarmes et d'autres opérations de sécurité important es.
13 novembre 2025	[ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement	Security Hub CSPM a modifié la sévérité de ce contrôle de à`HIGH`. `MEDIUM` Le partage de AWS Service Catalog portefeuilles avec des comptes spécifiques peut être intentionnel et ne signifie pas nécessair ement qu'un portefeui lle est accessible au public.

Date du changement	ID et titre du contrôle	Description du changement
13 novembre 2025	[CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés	Security Hub CSPM a modifié la sévérité de ce contrôle de à`MEDIUM`. `LOW` Les noms `cloudfront.net` de domaine par défaut pour les CloudFront distributions Amazon sont générés de manière aléatoire, ce qui réduit les risques de sécurité.
13 novembre 2025	[ELB.7] Le drainage des connexions doit être activé pour les équilibreurs de charge classiques	Security Hub CSPM a modifié la sévérité de ce contrôle de à`MEDIUM`. `LOW` Dans les déploiements multi-instances, d'autres instances saines peuvent gérer les sessions utilisateur lorsqu'une instance est arrêtée sans épuiser la connexion, ce qui réduit l'impact opérationnel et les risques de disponibilité.

Date du changement	ID et titre du contrôle	Description du changement
13 novembre 2025	[RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut	Security Hub CSPM a mis à jour ce contrôle pour supprimer le paramètre facultati `fvalidAdmi nUserNames` .
23 octobre 2025	[ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées	Security Hub CSPM a annulé les modificat ions apportées au titre, à la description et à la règle de ce contrôle le 14 octobre 2025.
22 octobre 2025	[CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut	Security Hub CSPM a mis à jour ce contrôle afin de ne pas générer de résultats pour les CloudFront distribut ions Amazon qui utilisent des origines personnalisées.

Date du changement	ID et titre du contrôle	Description du changement
16 octobre 2025	[CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée	Ce contrôle vérifie si une CloudFront distribution Amazon est configurée pour utiliser une politique de sécurité TLS recommandée. Security Hub CSPM prend désormais en charge `TLSv1.2_2025` et en `TLSv1.3_2025` tant que valeurs de paramètre pour ce contrôle.

Date du changement	ID et titre du contrôle	Description du changement
14 octobre 2025	[ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées	Security Hub CSPM a modifié le titre, la description et la règle de ce contrôle. Auparavant, le contrôle vérifiait les clusters Redis OSS et tous les groupes de réplication à l'aide de la règle https://docs.aws.amazon.com/config/latest/developerguide/elasticache-redis-cluster-automatic-backup-check.html elasticache-redis-cluster-automatic-backup-check. Le titre du contrôle était le suivant : ElastiCache (Redis OSS) les sauvegardes automatiques devraient être activées pour les clusters. Ce contrôle vérifie désormais les clusters Valkey en plus des clusters Redis OSS et de tous les groupes de réplication, à

Date du changement	ID et titre du contrôle	Description du changement
		l'aide de la règle https://docs.aws.amazon.com/config/latest/developerguide/elasticache-automatic-backup-check-enabled.html elasticache-automatic-backup-check-enabled. Le nouveau titre et la nouvelle description indiquent que le contrôle vérifie les deux types de clusters.

Date du changement	ID et titre du contrôle	Description du changement
5 octobre 2025	[Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée	La règle de ce contrôle a été mise à jour afin de générer également une détection si `PASSED` aucune mise à jour logicielle n'est disponible pour un domaine Amazon OpenSearch Service et si le statut de mise à jour n'est pas éligible. Auparavant, ce contrôle générait un `PASSED` résultat uniquement si aucune mise à jour logiciell e n'était disponible pour un OpenSearc h domaine et si l'état de la mise à jour était terminé.

Date du changement	ID et titre du contrôle	Description du changement
24 septembre 2025	[Redshift.9] Les clusters Redshift ne doivent pas utiliser le nom de base de données par défaut [RedshiftServerless.7] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom de base de données par défaut	Security Hub CSPM a retiré ces contrôles et les a retirés de toutes les normes applicables. Security Hub CSPM a retiré ces contrôles en raison des limites inhérentes à Amazon Redshift qui empêchaient de corriger efficacement les `FAILED` résultats des contrôles. Auparavant, les contrôles s'appliquaient à la norme FSBP (AWS Foundational Security Best Practices) et à la norme NIST SP 800-53 Rev. 5. Le Redshift.9 contrôle s'appliquait également à la norme de AWS Control Tower gestion des services.

Date du changement	ID et titre du contrôle	Description du changement
9 septembre 2025	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM ne prend plus en charge `nodejs18.x` la valeur de paramètre pour ce contrôle. AWS Lambda ne prend plus en charge Node.js 18 temps d'exécution.

Date du changement	ID et titre du contrôle	Description du changement
13 août 2025	[SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée	Security Hub CSPM a modifié le titre et la description de ce contrôle. Le nouveau titre et la nouvelle description reflètent plus précisément le fait que le contrôle vérifie le réglage du `EnableNetworkIsolation` paramètre des modèles hébergés par Amazon SageMaker AI. Auparavant, le titre de ce contrôle était : SageMaker models should block inbound traffic

Date du changement	ID et titre du contrôle	Description du changement
13 août 2025	[EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement	Security Hub CSPM a modifié le titre et la description de ce contrôle. Le nouveau titre et la nouvelle description reflètent plus précisément l'étendue et la nature de la vérification effectuée par le contrôle. Auparavant, le titre de ce contrôle était : EFS mount targets should not be associated with a public subnet
24 juillet 2025	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon EKS s'exécute sur une version de Kubernetes prise en charge. Security Hub CSPM a modifié la valeur du paramètre pour ce contrôle, la faisant passer de à`1.30`. `1.31` Le support standard pour la version 1.30 de Kubernetes dans Amazon EKS a pris fin le 23 juillet 2025.

Date du changement	ID et titre du contrôle	Description du changement
23 juillet 2025	[EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés	Security Hub CSPM a modifié le titre de ce contrôle. Le nouveau titre reflète plus préciséme nt le fait que le contrôle ne vérifie que les demandes Amazon EC2 Spot Fleet qui spécifien t des paramètre s de lancement . Auparavant, le titre de ce contrôle était : EC2 Spot Fleet requests should enable encryption for attached EBS volumes
30 juin 2025	[IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole	Security Hub CSPM a supprimé ce contrôle de la norme PCI DSS v4.0.1. La norme PCI DSS v4.0.1 n'exige pas explicite ment l'utilisation de symboles dans les mots de passe.

Date du changement	ID et titre du contrôle	Description du changement
30 juin 2025	[IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins	Security Hub CSPM a supprimé ce contrôle de la norme NIST SP 800-171 Revision 2. Le NIST SP 800-171 Revision 2 n'exige pas explicitement une période d'expiration des mots de passe de 90 jours ou moins.
30 juin 2025	[RDS.16] Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données	Security Hub CSPM a modifié le titre de ce contrôle. Le nouveau titre reflète plus précisément le fait que le contrôle vérifie uniquement les clusters de bases de données Amazon Aurora. Auparavant, le titre de ce contrôle était : RDS DB clusters should be configured to copy tags to snapshots

Date du changement	ID et titre du contrôle	Description du changement
30 juin 2025	[SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge	Ce contrôle vérifie si une instance de bloc-notes Amazon SageMaker AI est configurée pour s'exécuter sur une plate-forme prise en charge, en fonction de l'identifiant de plate-forme spécifié pour l'instance de bloc-notes. Security Hub CSPM ne prend plus en charge `notebook-al2-v1` et en `notebook-al2-v2` tant que valeurs de paramètre pour ce contrôle. Le support des instances Notebook qui s'exécutent sur ces plateformes a pris fin le 30 juin 2025.

Date du changement	ID et titre du contrôle	Description du changement
30 mai 2025	[IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes	Security Hub CSPM a supprimé ce contrôle de la norme PCI DSS v4.0.1. Ce contrôle vérifie si les politiques relatives aux mots de passe des comptes pour les utilisateurs IAM répondent aux exigences minimales, notamment une longueur de mot de passe minimale de 7 caractères. La norme PCI DSS v4.0.1 exige désormais que les mots de passe comportent au moins 8 caractères. Le contrôle continue de s'appliquer à la norme PCI DSS v3.2.1, qui impose des exigences de mot de passe différentes. Pour évaluer les politiques de mot de passe des comptes par rapport aux exigences de la norme PCI DSS v4.0.1, vous pouvez utiliser le contrôle.

Date du changement	ID et titre du contrôle	Description du changement
		IAM.7 Ce contrôle nécessite que les mots de passe comportent au moins 8 caractères. Il prend également en charge les valeurs personnalisées pour la longueur du mot de passe et d'autres paramètres. Le IAM.7 contrôle fait partie de la norme PCI DSS v4.0.1 de Security Hub CSPM.
8 mai 2025	[RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet	Security Hub CSPM a annulé la publication du RDS.46 contrôle dans son ensemble. Régions AWS Auparavant, ce contrôle était compatible avec la norme FSBP (AWS Foundational Security Best Practices).

Date du changement	ID et titre du contrôle	Description du changement
7 avril 2025	[ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées	Ce contrôle vérifie si l'écouteur HTTPS d'un équilibreur de charge d'application ou l'écouteur TLS d'un équilibreur de charge réseau est configuré pour chiffrer les données en transit à l'aide d'une politique de sécurité recommandée. Security Hub CSPM prend désormais en charge deux valeurs de paramètres supplémentaires pour ce contrôle : `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` et. `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`

Date du changement	ID et titre du contrôle	Description du changement
27 mars 2025	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `ruby3.4` comme valeur de paramètre pour ce contrôle. AWS Lambda ajout du support pour ce runtime.

Date du changement	ID et titre du contrôle	Description du changement
26 mars 2025	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon Elastic Kubernetes Service (Amazon EKS) s'exécute sur une version de Kubernetes prise en charge. Pour le `oldestVersionSupported` paramètre, Security Hub CSPM a modifié la valeur de à`1.29`. `1.30` La version la plus ancienne de Kubernetes prise en charge existe désormais. `1.30`

Date du changement	ID et titre du contrôle	Description du changement
10 mars 2025	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Ce contrôle vérifie si les paramètres d'exécution d'une AWS Lambda fonction correspondent aux valeurs attendues pour les temps d'exécution pris en charge dans chaque langue. Security Hub CSPM ne prend plus en charge `dotnet6` et en `python3.8` tant que valeurs de paramètre pour ce contrôle. AWS Lambda ne prend plus en charge ces environnements d'exécution.

Date du changement	ID et titre du contrôle	Description du changement
07 mars 2025	[RDS.18] Les instances RDS doivent être déployées dans un VPC	Security Hub CSPM a supprimé ce contrôle de la norme des meilleures pratiques de sécurité AWS fondamentales et a automatisé les vérifications pour les exigences du NIST SP 800-53 Rev. 5. Depuis le retrait du EC2-Class ic réseau Amazon, les instances Amazon Relational Database Service (Amazon RDS) ne peuvent plus être déployées en dehors d'un VPC.
10 janvier 2025	[Glue.2] AWS La journalisation des tâches Glue doit être activée	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes.
20 décembre 2024	EC2.61 à travers EC2.169	Security Hub CSPM a annulé la publication des contrôles directs EC2.61 . EC2.169

Date du changement	ID et titre du contrôle	Description du changement
12 décembre 2024	[RDS.23] Les instances RDS ne doivent pas utiliser le port par défaut d'un moteur de base de données	RDS.23 vérifie si un cluster ou une instance Amazon Relational Database Service (Amazon RDS) utilise un port autre que le port par défaut du moteur de base de données. Nous avons mis à jour le contrôle afin que la AWS Config règle sous-jacente renvoie un résultat de `NOT_APPLICABLE` pour les instances RDS qui font partie d'un cluster.

Date du changement	ID et titre du contrôle	Description du changement
2 décembre 2024	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `nodejs22.x` tant que paramètre.
26 novembre 2024	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon Elastic Kubernetes Service (Amazon EKS) s'exécute sur une version de Kubernetes prise en charge. La version la plus ancienne prise en charge existe désormais `1.29`.

Date du changement	ID et titre du contrôle	Description du changement
20 novembre 2024	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources	Config.1 vérifie si elle AWS Config est activée, utilise le rôle lié au service et enregistre les ressources pour les contrôles activés. Security Hub CSPM a augmenté la sévérité de ce contrôle de à`MEDIUM`. `CRITICAL` Security Hub CSPM a également ajouté de nouveaux codes d'état et des raisons d'état pour les erreurs de détection . Config.1 Ces modifications reflètent l'importance des contrôles CSPM de Security Hub Config.1 pour le fonctionn ement. Si l'enregis trement AWS Config des ressources est désactivé, vous pouvez recevoir des résultats de contrôle inexacts. Pour recevoir un `PASSED` résultat pour Config.1, activez

Date du changement	ID et titre du contrôle	Description du changement
		l'enregistrement des ressources correspondant aux contrôles CSPM de Security Hub activés et désactivez les contrôles qui ne sont pas requis dans votre organisation. Pour obtenir des instructions sur la configuration AWS Config de Security Hub CSPM, consultez. Activation et configuration AWS Config pour Security Hub CSPM Pour obtenir la liste des contrôles CSPM de Security Hub et de leurs ressources correspondantes, consultez . ObligatoireAWS Configressources pour les résultats des contrôles

Date du changement	ID et titre du contrôle	Description du changement
12 novembre 2024	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `python3.13` tant que paramètre.
11 octobre 2024	ElastiCache contrôles	Les titres de contrôle ont été modifiés pour ElastiCac he.3 ElastiCac he.4 ElastiCac he.5,, et ElastiCac he.7. Les titres ne mentionnent plus Redis OSS car les commandes s'appliqu ent également ElastiCache à Valkey.

Date du changement	ID et titre du contrôle	Description du changement
27 septembre 2024	[ELB.4] L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP non valides	Le titre de contrôle modifié depuis Application Load Balancer doit être configuré pour supprimer les en-têtes HTTP alors que Application Load Balancer doit être configuré pour supprimer les en-têtes HTTP non valides.
19 août 2024	Changements de titre DMS.12 et ElastiCache contrôles	Les titres de contrôle ont été modifiés pour DMS.12 et ElastiCache.1 jusqu'à ElastiCache.7. Nous avons modifié ces titres pour refléter le changement de nom du service Amazon ElastiCache (Redis OSS).

Date du changement	ID et titre du contrôle	Description du changement
15 août 2024	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources	Config.1 vérifie si elle AWS Config est activée, utilise le rôle lié au service et enregistre les ressources pour les contrôles activés. Security Hub CSPM a ajouté un paramètre de contrôle personnalisé nommé. `includeConfigServiceLinkedRoleCheck` En définissant ce paramètre sur`false`, vous pouvez choisir de ne pas vérifier s'il AWS Config utilise le rôle lié à un service.
31 juillet 2024	[IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés	Le titre de contrôle modifié dans les profils de AWS IoT Core sécurité doit être associé aux profils AWS IoT Device Defender de sécurité qui doivent être balisés.

Date du changement	ID et titre du contrôle	Description du changement
29 juillet 2024	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM n'est plus pris en charge en `nodejs16.x` tant que paramètre.
29 juillet 2024	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon Elastic Kubernetes Service (Amazon EKS) s'exécute sur une version de Kubernetes prise en charge. La version la plus ancienne prise en charge est`1.28`.

Date du changement	ID et titre du contrôle	Description du changement
25 juin 2024	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources	Ce contrôle vérifie s'il AWS Config est activé, utilise le rôle lié au service et enregistre les ressources pour les contrôles activés. Security Hub CSPM a mis à jour le titre du contrôle pour refléter ce que le contrôle évalue.
14 juin 2024	[RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs	Ce contrôle vérifie si un cluster de base de données Amazon Aurora MySQL est configuré pour publier des journaux d'audit sur Amazon CloudWatch Logs. Security Hub CSPM a mis à jour le contrôle afin qu'il ne génère pas de résultats pour les clusters de bases de données Aurora Serverless v1.

Date du changement	ID et titre du contrôle	Description du changement
11 juin 2024	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Ce contrôle vérifie si un cluster Amazon Elastic Kubernetes Service (Amazon EKS) s'exécute sur une version de Kubernetes prise en charge. La version la plus ancienne prise en charge est `1.27`.

Date du changement	ID et titre du contrôle	Description du changement
10 juin 2024	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources	Cette commande vérifie si elle AWS Config est activée et si l'enregistrement AWS Config des ressources est activé. Auparavant, le contrôle ne produisait un `PASSED` résultat que si vous configuriez l'enregistrement pour toutes les ressources. Security Hub CSPM a mis à jour le contrôle pour générer `PASSED` une détection lorsque l'enregistrement est activé pour les ressources requises pour les contrôles activés. Le contrôle a également été mis à jour pour vérifier si le rôle AWS Config lié à un service est utilisé, qui fournit des autorisations pour enregistrer les ressources nécessaires.

Date du changement	ID et titre du contrôle	Description du changement
8 mai 2024	[S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général	Ce contrôle vérifie si la suppressi on de l'authent ification multifacteur (MFA) est activée pour un bucket versionné à usage général Amazon S3. Auparavant, le contrôle produisai t une `FAILED` recherche pour les buckets dotés d'une configuration Lifecycle . Cependant, la suppression MFA avec gestion des versions ne peut pas être activée sur un bucket doté d'une configuration Lifecycle. Security Hub CSPM a mis à jour le contrôle afin de ne produire aucun résultat pour les buckets dotés d'une configuration Lifecycle . La description du contrôle a été mise à jour pour refléter le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
2 mai 2024	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Security Hub CSPM a mis à jour la plus ancienne version prise en charge de Kubernetes sur laquelle le cluster Amazon EKS peut s'exécuter afin de générer un résultat positif. La version la plus ancienne actuellement prise en charge est Kubernetes1.26.
30 avril 2024	[CloudTrail.3] Au moins une CloudTrail piste doit être activée	Le titre du contrôle a été modifié, passant de « CloudTrail Doit être activé » à « Au moins une CloudTrail piste doit être activée ». Ce contrôle produit actuellement un PASSED résultat si au moins Compte AWS une CloudTrail piste est activée. Le titre et la description ont été modifiés pour refléter fidèlement le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
29 avril 2024	[AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB	Le titre de contrôle modifié, passant des groupes Auto Scaling associés à un équilibreur de charge classique doivent utiliser des bilans de santé de l'équilibreur de charge au lieu des groupes Auto Scaling associés à un équilibreur de charge doivent utiliser des bilans de santé ELB. Ce contrôle évalue actuellement les équilibreurs de charge d'application, de passerelle, de réseau et classiques. Le titre et la description ont été modifiés pour refléter fidèlement le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
19 avril 2024	[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture	Le contrôle vérifie s'il AWS CloudTrail est activé et configuré avec au moins une piste multirégionale qui inclut des événements de gestion de lecture et d'écriture. Auparavant, le contrôle générait des `PASSED` résultats de manière incorrecte lorsqu'un compte avait été CloudTrail activé et configuré avec au moins un suivi multirégional, même si aucun suivi ne capturait les événements de gestion de lecture et d'écriture. Le contrôle génère désormais une `PASSED` recherche uniquement lorsqu'il CloudTrail est activé et configuré avec au moins une piste multirégionale qui capture les événements de gestion de lecture et d'écriture.

Date du changement	ID et titre du contrôle	Description du changement
10 avril 2024	[Athena.1] Les groupes de travail Athena doivent être chiffrés au repos	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. Les groupes de travail Athena envoient des journaux vers des compartiments Amazon Simple Storage Service (Amazon S3). Amazon S3 fournit désormais un chiffrement par défaut avec des clés gérées S3 (SS3-S3) sur les compartiments S3 nouveaux et existants.
10 avril 2024	[AutoScaling.4] La configuration de lancement du groupe Auto Scaling ne doit pas avoir de limite de sauts de réponse aux métadonnées supérieure à 1	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. Les limites de saut de réponse aux métadonnées pour les instances Amazon Elastic Compute Cloud (Amazon EC2) dépendent de la charge de travail.

Date du changement	ID et titre du contrôle	Description du changement
10 avril 2024	[CloudFormation.1] les CloudFormation piles doivent être intégrées au Service de notification simple (SNS)	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. L'intégration de AWS CloudFormation piles aux rubriques Amazon SNS ne constitue plus une bonne pratique en matière de sécurité. Bien que l'intégration de CloudFormation piles importantes aux rubriques SNS puisse être utile, elle n'est pas obligatoire pour toutes les piles.
10 avril 2024	[CodeBuild.5] les environnements de CodeBuild projet ne doivent pas avoir le mode privilégié activé	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. L'activation du mode privilégié dans un CodeBuild projet n'impose aucun risque supplémentaire à l'environnement du client.

Date du changement	ID et titre du contrôle	Description du changement
10 avril 2024	[IAM.20] Évitez d'utiliser l'utilisateur root	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. L'objectif de ce contrôle est couvert par un autre contrôle,[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root ».
10 avril 2024	[SNS.2] L'enregistrement de l'état de livraison doit être activé pour les messages de notification envoyés à un sujet	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. L'enregistrement de l'état de diffusion des sujets SNS n'est plus une bonne pratique en matière de sécurité. Bien que l'enregistrement de l'état de diffusion pour les sujets SNS importants puisse être utile, il n'est pas obligatoire pour tous les sujets.

Date du changement	ID et titre du contrôle	Description du changement
10 avril 2024	[S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie	Security Hub CSPM a supprimé ce contrôle des meilleures pratiques et AWS Service-Managed normes de sécurité fondamentales :. AWS Control Tower L'objectif de ce contrôle est couvert par deux autres contrôles : [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie et[S3.14] Les compartiments S3 à usage général doivent avoir le contrôle de version activé. Ce contrôle fait toujours partie du NIST SP 800-53 Rev. 5.

Date du changement	ID et titre du contrôle	Description du changement
10 avril 2024	[S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général	Security Hub CSPM a supprimé ce contrôle des meilleures pratiques et AWS Service-Managed normes de sécurité fondamentales :. AWS Control Tower Bien que les notifications d'événements soient utiles dans certains cas pour les compartiments S3, il ne s'agit pas d'une bonne pratique de sécurité universelle. Ce contrôle fait toujours partie du NIST SP 800-53 Rev. 5.

Date du changement	ID et titre du contrôle	Description du changement
10 avril 2024	[SNS.1] Les sujets SNS doivent être chiffrés au repos à l'aide deAWS KMS	Security Hub CSPM a supprimé ce contrôle des meilleures pratiques et AWS Service-Managed normes de sécurité fondamentales :. AWS Control Tower Par défaut, SNS chiffre les sujets au repos à l'aide du chiffrement de disque. Pour en savoir plus, consultez Chiffrement des données. L'utilisation AWS KMS du chiffrement des sujets n'est plus recommandée en tant que meilleure pratique de sécurité. Ce contrôle fait toujours partie du NIST SP 800-53 Rev. 5.

Date du changement	ID et titre du contrôle	Description du changement
8 avril 2024	[ELB.6] La protection contre la suppression doit être activée pour les équilibreurs de charge des applications, des passerelles et du réseau	Le titre de contrôle modifié de la protection contre la suppression de l'équilibreur de charge des applications doit être activé à celui des équilibreurs de charge des applications, des passerelles et du réseau. Ce contrôle évalue actuellement les équilibreurs de charge des applications, des passerelles et du réseau. Le titre et la description ont été modifiés pour refléter fidèlement le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
22 mars 2024	[Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS	Le titre de contrôle modifié, passant de Connexions aux OpenSearch domaines doit être chiffré à l'aide de TLS 1.2 à Les connexions aux OpenSearch domaines doivent être chiffrées à l'aide de la politique de sécurité TLS la plus récente. Auparavant, le contrôle vérifiait uniquement si les connexions aux OpenSearch domaines utilisaient le protocole TLS 1.2. Le contrôle permet désormais de déterminer si `PASSED` les OpenSearch domaines sont chiffrés à l'aide de la dernière politique de sécurité TLS. Le titre et la description du contrôle ont été mis à jour pour refléter le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
22 mars 2024	[ES.8] Les connexions aux domaines Elasticsearch doivent être chiffrées conformément à la dernière politique de sécurité TLS	Le titre de contrôle modifié de Connections aux domaines Elasticsearch doit être chiffré à l'aide de TLS 1.2 à Les connexions aux domaines Elasticsearch doivent être chiffrées à l'aide de la dernière politique de sécurité TLS. Auparavant, le contrôle vérifiait uniquement si les connexions aux domaines Elasticsearch utilisaient le protocole TLS 1.2. Le contrôle permet désormais de déterminer si les domaines Elasticsearch sont chiffrés à l'aide de la dernière politique de sécurité TLS. PASSED Le titre et la description du contrôle ont été mis à jour pour refléter le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés	Le titre modifié du paramètre S3 Block Public Access doit être activé à S3 Les compartiments à usage général S3 doivent avoir les paramètres d'accès public bloqué activés. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.2] Les compartiments S3 à usage général devraient bloquer l'accès public en lecture	Le titre modifié des compartiments S3 devrait interdire l'accès public en lecture aux compartiments S3 à usage général devrait bloquer l'accès public en lecture. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.3] Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture	Le titre modifié des compartiments S3 devrait interdire l'accès public en écriture aux compartiments S3 à usage général devrait bloquer l'accès public en écriture. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS	Le titre modifié des compartiments S3 devrait nécessiter des demandes d'utilisation de Secure Socket Layer alors que les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole SSL. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.6] Les politiques de bucket à usage général S3 devraient restreindre l'accès aux autres Comptes AWS	Titre modifié des autorisations S3 accordées à d'autres Comptes AWS politiques du compartiment doivent être limitées aux politiques de compartiment à usage général S3. Les politiques de compartiment à usage général devraient restreindre l'accès aux autres Comptes AWS. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions	Le titre modifié des compartiments S3 doit avoir la réplication interrégionale activée. Les compartiments S3 à usage général doivent utiliser la réplication interrégionale. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions	Le titre modifié des compartiments S3 doit avoir la réplication interrégionale activée. Les compartiments S3 à usage général doivent utiliser la réplication interrégionale. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public	Le titre modifié du paramètre S3 Block Public Access doit être activé au niveau du bucket pour que les compartiments à usage général S3 bloquent l'accès public. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.9] Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée	Le titre modifié de la journalisation de l'accès au serveur de compartiment S3 doit être activé à La journalisation de l'accès au serveur doit être activée pour les compartiments S3 à usage général. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie	Le titre modifié des compartiments S3 avec le contrôle de version activé doit avoir des politiques de cycle de vie configurées. Les compartiments S3 à usage général avec le contrôle de version activé doivent avoir des configurations de cycle de vie. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général	Le titre modifié des compartiments S3 doit avoir les notifications d'événements activées. Les notifications d'événements doivent être activées pour les compartiments S3 à usage général. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3	Le titre modifié des listes de contrôle d'accès (ACL) S3 ne doit pas être utilisé pour gérer l'accès des utilisateurs aux compartiments. Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie	Le titre modifié des compartiments S3 doit avoir des politiques de cycle de vie configurées. Les compartiments à usage général S3 doivent avoir des configurations de cycle de vie. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.14] Les compartiments S3 à usage général doivent avoir le contrôle de version activé	Le titre modifié des compartiments S3 doit utiliser le contrôle de version alors que les compartiments S3 à usage général doivent avoir la gestion des versions activée. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
12 mars 2024	[S3.15] Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé	Le titre modifié des compartiments S3 doit être configuré pour utiliser Object Lock. Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé. Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.
12 mars 2024	[S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys	Le titre modifié des compartiments S3 doit être chiffré au repos alors que les compartiments AWS KMS keys à usage général S3 doivent être chiffrés au repos avec. AWS KMS keys Security Hub CSPM a modifié le titre pour tenir compte d'un nouveau type de compartiment S3.

Date du changement	ID et titre du contrôle	Description du changement
07 mars 2024	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `nodejs20.x` et en `ruby3.3` tant que paramètres.

Date du changement	ID et titre du contrôle	Description du changement
22 février 2024	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `dotnet8` tant que paramètre.
5 février 2024	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Security Hub CSPM a mis à jour la plus ancienne version prise en charge de Kubernetes sur laquelle le cluster Amazon EKS peut s'exécuter afin de générer un résultat positif. La version la plus ancienne actuellement prise en charge est Kubernetes `1.25`.

Date du changement	ID et titre du contrôle	Description du changement
10 janvier 2024	[CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles	Le titre modifié depuis CodeBuild GitHub ou les URL du référenti el source Bitbucket doivent utiliser OAuth. Les URL du référenti el source CodeBuild Bitbucket ne doivent pas contenir d'informa tions d'identif ication sensibles . Security Hub CSPM a supprimé la mention d'OAuth car d'autres méthodes de connexion peuvent également être sécurisées. Security Hub CSPM a supprimé la mention de, GitHub car il n'est plus possible d'avoir un jeton d'accès personnel ou un nom d'utilisateur et un mot de passe dans les URL du référentiel GitHub source.

Date du changement	ID et titre du contrôle	Description du changement
8 janvier 2024	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM ne prend plus en charge `go1.x` et en `java8` tant que paramètres car ce sont des environnements d'exécution retirés.

Date du changement	ID et titre du contrôle	Description du changement
29 décembre 2023	[RDS.8] La protection contre la suppression des instances de base de données RDS doit être activée	RDS.8 vérifie si la protection contre la suppression est activée sur une instance de base de données Amazon RDS qui utilise l'un des moteurs de base de données pris en charge. Security Hub CSPM prend désormais en charge `custom-oracle-eeoracle-ee-cdb` , et en `oracle-se2-cdb` tant que moteurs de base de données.

Date du changement	ID et titre du contrôle	Description du changement
22 décembre 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM prend désormais en charge `java21` et en `python3.12` tant que paramètres. Security Hub CSPM n'est plus pris en charge en `ruby2.7` tant que paramètre.

Date du changement	ID et titre du contrôle	Description du changement
15 décembre 2023	[CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut	CloudFront.1 vérifie si un objet racine par défaut est configuré pour une CloudFront distribution Amazon. Security Hub CSPM a réduit la sévérité de ce contrôle de CRITIQUE à ÉLEVÉE, car l'ajout de l'objet racine par défaut est une recommandation qui dépend de l'application de l'utilisateur et de ses exigences spécifiques.
5 décembre 2023	[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22	Le titre de contrôle modifié dans les groupes de sécurité ne devrait pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers le port 22 vers les groupes de sécurité ne devraient pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 sur le port 22.

Date du changement	ID et titre du contrôle	Description du changement
5 décembre 2023	[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389	Titre du contrôle modifié : Assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée à partir de la version 0.0.0. 0/0 le port 3389 vers les groupes de sécurité ne devrait pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 sur le port 3389.

Date du changement	ID et titre du contrôle	Description du changement
5 décembre 2023	[RDS.9] Les instances de base de données RDS doivent publier des CloudWatch journaux dans Logs	Le titre de contrôle modifié depuis la journalisation de la base de données doit être activé pour que les instances de base de données RDS publient des CloudWatch journaux dans Logs. Security Hub CSPM a identifié que ce contrôle vérifie uniquement si les journaux sont publiés sur Amazon CloudWatch Logs et ne vérifie pas si les journaux RDS sont activés. Le contrôle permet de déterminer si `PASSED` les instances de base de données RDS sont configuré es pour publier des CloudWatch journaux dans Logs. Le titre du contrôle a été mis à jour pour refléter le comportement actuel.

Date du changement	ID et titre du contrôle	Description du changement
5 décembre 2023	[EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée	Ce contrôle vérifie si la journalisation des audits est activée pour les clusters Amazon EKS. La AWS Config règle utilisée par Security Hub CSPM pour évaluer ce contrôle est passée de à`eks-cluster-logging-enabled` . `eks-cluster-log-enabled`

Date du changement	ID et titre du contrôle	Description du changement
17 novembre 2023	[EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé	EC2.19 vérifie si le trafic entrant sans restriction pour un groupe de sécurité est accessible aux ports spécifiés considéré s comme présentan t un risque élevé. Security Hub CSPM a mis à jour ce contrôle pour tenir compte des listes de préfixes gérées lorsqu'elles sont fournies comme source pour une règle de groupe de sécurité. Le contrôle produit un `FAILED` résultat si les listes de préfixes contiennent les chaînes « 0.0.0 ». 0/0' ou ': :/0'.

Date du changement	ID et titre du contrôle	Description du changement
16 novembre 2023	[CloudWatch.15] CloudWatch les actions spécifiées doivent être configurées pour les alarmes	Le titre de contrôle modifié depuis CloudWatch les alarmes doit comporter une action configurée pour l'état ALARME alors que les CloudWatch alarmes doivent avoir des actions spécifiées configurées.
16 novembre 2023	[CloudWatch.16] les groupes de CloudWatch journaux doivent être conservés pendant une période spécifiée	Le titre de contrôle modifié depuis les groupes de CloudWatch journaux doit être conservé pendant au moins un an, tandis que les groupes de CloudWatch journaux doivent être conservés pendant une période spécifiée.

Date du changement	ID et titre du contrôle	Description du changement
16 novembre 2023	[Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité	Titre de contrôle modifié : les fonctions Lambda du VPC doivent fonctionner dans plus d'une zone de disponibilité, tandis que les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité.
16 novembre 2023	[AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée	Titre du AWS AppSync contrôle modifié : la journalisation au niveau de la demande et au niveau du champ AWS AppSync devrait être activée à la journalisation au niveau du champ.

Date du changement	ID et titre du contrôle	Description du changement
16 novembre 2023	[EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques	Titre de contrôle modifié : les nœuds principaux du MapReduce cluster Amazon Elastic ne devraient pas avoir d'adresses IP publiques par rapport aux nœuds principau x du cluster Amazon EMR ne devraient pas avoir d'adresses IP publiques.
16 novembre 2023	[Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public	Le titre de contrôle modifié des OpenSearch domaines doit se trouver dans un VPC et les OpenSearch domaines ne doivent pas être accessibles au public.
16 novembre 2023	[ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public	Le titre de contrôle modifié des domaines Elasticsearch doit se trouver dans un VPC. Les domaines Elasticsearch ne doivent pas être accessibles au public.

Date du changement	ID et titre du contrôle	Description du changement
31 octobre 2023	[ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée	ES.4 vérifie si les domaines Elasticsearch sont configurés pour envoyer des journaux d'erreurs à Amazon CloudWatch Logs. Le contrôle avait précédemment généré une détection PASSED pour un domaine Elasticsearch dont tous les journaux étaient configurés pour être envoyés à CloudWatch Logs. Security Hub CSPM a mis à jour le contrôle afin de générer une PASSED recherche uniquement pour un domaine Elasticsearch configuré pour envoyer des journaux d'erreurs à Logs. CloudWatch Le contrôle a également été mis à jour pour exclure de l'évaluation les versions d'Elasticsearch qui ne prennent pas en

Date du changement	ID et titre du contrôle	Description du changement
		charge les journaux d'erreurs.
16 octobre 2023	[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0.0/0 ou : :/0 vers le port 22	EC2.13 vérifie si les groupes de sécurité autorisent un accès d'entrée illimité au port 22. Security Hub CSPM a mis à jour ce contrôle pour tenir compte des listes de préfixes gérées lorsqu'elles sont fournies comme source pour une règle de groupe de sécurité. Le contrôle produit un `FAILED` résultat si les listes de préfixes contiennent les chaînes « 0.0.0 ». 0/0' ou ': :/0'.

Date du changement	ID et titre du contrôle	Description du changement
16 octobre 2023	[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0.0/0 ou : :/0 vers le port 3389	EC2.14 vérifie si les groupes de sécurité autorisent un accès d'entrée illimité au port 3389. Security Hub CSPM a mis à jour ce contrôle pour tenir compte des listes de préfixes gérées lorsqu'elles sont fournies comme source pour une règle de groupe de sécurité. Le contrôle produit un `FAILED` résultat si les listes de préfixes contiennent les chaînes « 0.0.0 ». 0/0' ou ': :/0'.

Date du changement	ID et titre du contrôle	Description du changement
16 octobre 2023	[EC2.18] Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés	EC2.18 vérifie si les groupes de sécurité utilisés autorisent un trafic entrant illimité. Security Hub CSPM a mis à jour ce contrôle pour tenir compte des listes de préfixes gérées lorsqu'elles sont fournies comme source pour une règle de groupe de sécurité. Le contrôle produit un `FAILED` résultat si les listes de préfixes contiennent les chaînes « 0.0.0 ». 0/0' ou ': :/0'.

Date du changement	ID et titre du contrôle	Description du changement
16 octobre 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `python3.11` tant que paramètre.
4 octobre 2023	[S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions	Security Hub CSPM a ajouté le paramètre `ReplicationType` dont la valeur est de `CROSS-REGION` pour s'assurer que la réplication entre régions est activée pour les compartiments S3 plutôt que la réplication entre régions.

Date du changement	ID et titre du contrôle	Description du changement
27 septembre 2023	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	Security Hub CSPM a mis à jour la plus ancienne version prise en charge de Kubernetes sur laquelle le cluster Amazon EKS peut s'exécuter afin de générer un résultat positif. La version la plus ancienne actuellement prise en charge est Kubernetes `1.24`.
20 septembre 2023	[CloudFront.2] CloudFront les distributions doivent avoir l'identité d'accès à l'origine activée	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. Reportez-vous plutôt à la section [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine. Le contrôle d'accès Origin est la meilleure pratique de sécurité actuelle. Ce contrôle sera supprimé de la documentation dans 90 jours.

Date du changement	ID et titre du contrôle	Description du changement
20 septembre 2023	[EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés	Security Hub CSPM a supprimé ce contrôle des meilleures pratiques de sécurité AWS fondamentales (FSBP) et du National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Il fait toujours partie de Service-Managed Standard : AWS Control Tower. Ce contrôle produit une détection réussie si des groupes de sécurité sont attachés à des instances EC2 ou à une interface réseau élastique . Toutefois, dans certains cas d'utilisation, les groupes de sécurité indépendants ne présentent aucun risque de sécurité. Vous pouvez utiliser d'autres contrôles EC2 EC2.2, tels que,, et EC2.13 EC2.14 EC2.18, EC2.19 pour surveiller vos groupes de sécurité.

Date du changement	ID et titre du contrôle	Description du changement
20 septembre 2023	[EC2.29] Les instances EC2 doivent être lancées dans un VPC	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. Amazon EC2 a migré des EC2-Classic instances vers un VPC. Ce contrôle sera supprimé de la documentation dans 90 jours.
20 septembre 2023	[S3.4] Le chiffrement côté serveur doit être activé pour les compartiments S3	Security Hub CSPM a retiré ce contrôle et l'a retiré de toutes les normes. Amazon S3 fournit désormais un chiffrement par défaut avec des clés gérées S3 (SS3-S3) sur les compartiments S3 nouveaux et existants . Les paramètre s de chiffrement restent inchangés pour les compartim ents existants qui sont chiffrés SS3-S3 ou chiffrés SS3-KMS côté serveur. Ce contrôle sera supprimé de la documentation dans 90 jours.

Date du changement	ID et titre du contrôle	Description du changement
14 septembre 2023	[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant	Titre de contrôle modifié : Le groupe de sécurité par défaut du VPC ne doit pas autoriser le trafic entrant et sortant vers le VPC. Les groupes de sécurité par défaut ne doivent pas autoriser le trafic entrant ou sortant.
14 septembre 2023	[IAM.9] La MFA doit être activée pour l'utilisateur root	Le titre de contrôle modifié de Virtual MFA doit être activé pour l'utilisateur root à MFA doit être activé pour l'utilisateur root.
14 septembre 2023	[RDS.19] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements de cluster critiques	Titre du contrôle modifié, passant de Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de cluster critiques à Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements de cluster critiques.

Date du changement	ID et titre du contrôle	Description du changement
14 septembre 2023	[RDS.20] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques	Titre du contrôle modifié, passant de Un abonnement aux notifications d'événements RDS doit être configuré pour les événements d'instance de base de données critiques à Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques.
14 septembre 2023	[WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition	Titre de contrôle modifié, passant de Une règle WAF régionale doit avoir au moins une condition à Les règles régionales AWS WAF classiques doivent avoir au moins une condition.

Date du changement	ID et titre du contrôle	Description du changement
14 septembre 2023	[WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle	Titre de contrôle modifié, passant de Un groupe de règles régional WAF doit avoir au moins une règle à un groupe de règles régional AWS WAF classique Les groupes de règles régionaux doivent avoir au moins une règle.
14 septembre 2023	[WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles	Titre de contrôle modifié, passant de A WAF Regional Web ACL doit avoir au moins une règle ou un groupe de règles à AWS WAF Classic Regional Web ACL doit avoir au moins une règle ou un groupe de règles.
14 septembre 2023	[WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition	Titre de contrôle modifié, passant de Une règle globale WAF doit avoir au moins une condition à Les règles globales AWS WAF class iques doivent avoir au moins une condition.

Date du changement	ID et titre du contrôle	Description du changement
14 septembre 2023	[WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle	Titre de contrôle modifié, passant de Un groupe de règles global WAF doit avoir au moins une règle à Les groupes de règles globales AWS WAF classiques doivent avoir au moins une règle.
14 septembre 2023	[WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles	Titre de contrôle modifié, passant de Une liste ACL Web globale WAF doit avoir au moins une règle ou un groupe de règles à une liste ACL Web globale AWS WAF classique doit avoir au moins une règle ou un groupe de règles.
14 septembre 2023	[WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles	Titre de contrôle modifié, passant de Une ACL Web WAFv2 doit avoir au moins une règle ou un groupe de règles à une liste ACL AWS WAF Web doit avoir au moins une règle ou un groupe de règles.

Date du changement	ID et titre du contrôle	Description du changement
14 septembre 2023	[WAF.11]AWS WAFla journalisation des ACL Web doit être activée	Le titre de contrôle modifié de la journalisation des ACL web AWS WAF v2 doit être activé à AWS WAF celui de la journalisation des ACL web.
20 juillet 2023	[S3.4] Le chiffrement côté serveur doit être activé pour les compartiments S3	S3.4 vérifie si le chiffrement côté serveur est activé sur un compartiment Amazon S3 ou si la politique du compartiment S3 refuse explicitement les `PutObject` demandes sans chiffrement côté serveur. Security Hub CSPM a mis à jour ce contrôle pour inclure un chiffrement double couche côté serveur avec des clés KMS (). DSSE-KMS Le contrôle produit une découverte réussie lorsqu'un compartiment S3 est chiffré avec SSE-S3 SSE-KMS, ou DSSE-KMS.

Date du changement	ID et titre du contrôle	Description du changement
17 juillet 2023	[S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys	S3.17 vérifie si un compartiment Amazon S3 est chiffré avec un AWS KMS key. Security Hub CSPM a mis à jour ce contrôle pour inclure un chiffrement double couche côté serveur avec des clés KMS (). DSSE-KMS Le contrôle produit une découverte réussie lorsqu'un compartiment S3 est chiffré avec SSE-KMS ou DSSE-KMS.
9 juin 2023	[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge	EKS.2 vérifie si un cluster Amazon EKS s'exécute sur une version de Kubernetes prise en charge. La version la plus ancienne prise en charge est désormais `1.23`.

Date du changement	ID et titre du contrôle	Description du changement
9 juin 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `ruby3.2` tant que paramètre.
5 juin 2023	[APIGateway.5] Les données du cache de l'API REST API Gateway doivent être chiffrées au repos	APIGateway.5.checks si toutes les méthodes des étapes de l'API REST Amazon API Gateway sont chiffrées au repos. Security Hub CSPM a mis à jour le contrôle pour évaluer le chiffrement d'une méthode particulière uniquement lorsque la mise en cache est activée pour cette méthode.

Date du changement	ID et titre du contrôle	Description du changement
18 mai 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `java17` tant que paramètre.
18 mai 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM n'est plus pris en charge en `nodejs12.x` tant que paramètre.

Date du changement	ID et titre du contrôle	Description du changement
23 avril 2023	[ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate	ECS.10 vérifie si les services Amazon ECS Fargate exécutent la dernière version de la plateforme Fargate. Les clients peuvent déployer Amazon ECS via ECS directement ou en utilisant CodeDeploy. Security Hub CSPM a mis à jour ce contrôle pour générer des résultats positifs lorsque vous l'utilise z CodeDeploy pour déployer les services ECS Fargate.

Date du changement	ID et titre du contrôle	Description du changement
20 avril 2023	[S3.6] Les politiques de bucket à usage général S3 devraient restreindre l'accès aux autres Comptes AWS	S3.6 vérifie si une politique de compartiment Amazon Simple Storage Service (Amazon S3) empêche les principaux d' Comptes AWS effectuer des actions refusées sur les ressources du compartiment S3. Security Hub CSPM a mis à jour le contrôle pour tenir compte des conditions dans une politique de bucket.

Date du changement	ID et titre du contrôle	Description du changement
18 avril 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM est désormais pris en charge en `python3.10` tant que paramètre.
18 avril 2023	[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge	Lambda.2 vérifie si les paramètres des AWS Lambda fonctions pour les environnements d'exécution correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Security Hub CSPM n'est plus pris en charge en `dotnetcore3.1` tant que paramètre.

Date du changement	ID et titre du contrôle	Description du changement
17 avril 2023	[RDS.11] Les sauvegardes automatiques doivent être activées sur les instances RDS	RDS.11 vérifie si les sauvegardes automatiques sont activées sur les instances Amazon RDS, avec une période de conservation des sauvegardes supérieure ou égale à sept jours. Security Hub CSPM a mis à jour ce contrôle pour exclure les répliques en lecture de l'évaluation, car tous les moteurs ne prennent pas en charge les sauvegardes automatisées sur les répliques en lecture. En outre, RDS ne fournit pas la possibilité de spécifier une période de conservation des sauvegardes lors de la création de répliques en lecture. Les répliques en lecture sont créées avec une période de conservation des

Date du changement	ID et titre du contrôle	Description du changement
		sauvegardes `0` par défaut.

Contrôles Security Hub CSPM pourComptes AWS

Ces contrôles Security Hub CSPM évaluent. Comptes AWS

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/12, 2 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `security-account-information-provided`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un compte Amazon Web Services (AWS) possède des informations de contact de sécurité. Le contrôle échoue si les coordonnées de sécurité ne sont pas fournies pour le compte.

Les contacts de sécurité alternatifs permettent AWS de contacter une autre personne à propos de problèmes liés à votre compte au cas où vous ne seriez pas disponible. Les notifications peuvent provenir d'Supportéquipes ou d'autres Service AWS équipes concernant des sujets liés à la sécurité associés à votre Compte AWS utilisation.

Correction

Pour ajouter un autre contact en tant que contact de sécurité à votre compteCompte AWS, voir Mettre à jour les contacts alternatifs pour vous Compte AWS dans le Guide de référence de gestion de AWS compte.

[Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization

Catégorie : Protéger > Gestion des accès sécurisés > Contrôle d'accès

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : `account-part-of-organizations`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un Compte AWS fait partie d'une organisation gérée viaAWS Organizations. Le contrôle échoue si le compte ne fait pas partie d'une organisation.

Organizations vous aide à gérer votre environnement de manière centralisée à mesure que vous adaptez vos charges de travail. AWS Vous pouvez en utiliser plusieurs Comptes AWS pour isoler les charges de travail soumises à des exigences de sécurité spécifiques ou pour vous conformer à des frameworks tels que HIPAA ou PCI. En créant une organisation, vous pouvez administrer plusieurs comptes en tant qu'unité unique et gérer de manière centralisée leur accèsServices AWS, leurs ressources et leurs régions.

Correction

Pour créer une nouvelle organisation et y ajouter automatiquement des informationsComptes AWS, consultez la section Création d'une organisation dans le Guide de AWS Organizations l'utilisateur. Pour ajouter des comptes à une organisation existante, voir Inviter un homme Compte AWS à rejoindre votre organisation dans le Guide de AWS Organizations l'utilisateur.

Contrôles Security Hub CSPM pourAWS Amplify

Ces contrôles CSPM du Security Hub évaluent le AWS Amplify service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Amplify.1] Les applications Amplify doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Amplify::App`

Règle AWS Config : amplify-app-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « 2 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS Amplify application possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si l'application ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'application n'en possède aucune. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à une AWS Amplify application, consultez la section Assistance au balisage des ressources dans le guide de l'utilisateur de l'AWS Amplifyhébergement.

[Amplify.2] Les branches Amplify doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Amplify::Branch`

Règle AWS Config : amplify-branch-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « 2 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS Amplify branche possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si la branche ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la branche ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à une AWS Amplify branche, consultez la section Support du balisage des ressources dans le Guide de l'utilisateur de l'AWS Amplifyhébergement.

Contrôles CSPM Security Hub pour Amazon API Gateway

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon API Gateway. Il se peut que les commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[APIGateway.1] API Gateway REST et la journalisation de l'exécution des WebSocket API doivent être activés

Exigences connexes : NIST.800-53.r5 AC-4 (26) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

Règle AWS Config : api-gw-execution-logging-enabled

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`loggingLevel`	Logging level (Niveau de journalisation)	Enum	`ERROR`, `INFO`	`No default value`

Ce contrôle vérifie si la journalisation est activée pour toutes les étapes d'un REST ou d'une WebSocket API Amazon API Gateway. Le contrôle échoue si `loggingLevel` ce n'est pas le cas

ERROR ou INFO pour toutes les étapes de l'API. À moins que vous ne fournissiez des valeurs de paramètres personnalisées pour indiquer qu'un type de journal spécifique doit être activé, Security Hub CSPM génère un résultat positif si le niveau de journalisation est égal ou ERROR égal à. INFO

Les journaux pertinents doivent être activés dans les étapes WebSocket REST ou API Gateway REST ou API Gateway. La journalisation des exécutions WebSocket REST et API Gateway fournit des enregistrements détaillés des demandes adressées aux étapes REST et WebSocket API Gateway. Les étapes incluent les réponses du backend d'intégration des API, les réponses de l'autorisateur Lambda et les points de terminaison d'requestIdintégration. AWS

Correction

Pour activer la journalisation des opérations WebSocket REST et API, voir Configuration de la journalisation des CloudWatch API à l'aide de la console API Gateway dans le Guide du développeur d'API Gateway.

[APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend

Exigences connexes : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : AWS::ApiGateway::Stage

Règle AWS Config : api-gw-ssl-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les étapes de l'API REST Amazon API Gateway disposent de certificats SSL configurés. Les systèmes principaux utilisent ces certificats pour authentifier que les demandes entrantes proviennent d'API Gateway.

Les étapes de l'API REST API Gateway doivent être configurées avec des certificats SSL pour permettre aux systèmes principaux d'authentifier que les demandes proviennent d'API Gateway.

Correction

Pour obtenir des instructions détaillées sur la façon de générer et de configurer des certificats SSL API REST API Gateway, voir Générer et configurer un certificat SSL pour l'authentification du backend dans le guide du développeur API Gateway.

[APIGateway.3] Les étapes de l'API REST API Gateway doivent avoir AWS X-Ray traçage activé

Exigences connexes : NIST.800-53.r5 CA-7

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::ApiGateway::Stage`

Règle AWS Config : api-gw-xray-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le suivi AWS X-Ray actif est activé pour vos étapes d'API REST Amazon API Gateway.

X-Ray le traçage actif permet de réagir plus rapidement à l'évolution des performances de l'infrastructure sous-jacente. Les changements de performances peuvent entraîner une indisponibilité de l'API. X-RayActive Tracing fournit des mesures en temps réel des demandes des utilisateurs qui transitent par les opérations de l'API REST API Gateway et les services connectés.

Correction

Pour obtenir des instructions détaillées sur la façon d'activer le suivi X-Ray actif pour les opérations de l'API REST API Gateway, consultez la section relative à la prise en charge du suivi actif d'Amazon API Gateway AWS X-Ray dans le Guide du AWS X-Ray développeur.

[APIGateway.4] API Gateway doit être associée à une ACL Web WAF

Exigences connexes : NIST.800-53.r5 AC-4 (21)

Catégorie : Protéger > Services de protection

Gravité : Moyenne

Type de ressource : `AWS::ApiGateway::Stage`

Règle AWS Config : api-gw-associated-with-waf

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un stage API Gateway utilise une liste de contrôle d'accès AWS WAF Web (ACL). Ce contrôle échoue si aucune ACL AWS WAF Web n'est attachée à un stage REST API Gateway.

AWS WAF est un pare-feu d'applications Web qui permet de protéger les applications Web et les API contre les attaques. Il vous permet de configurer une ACL, qui est un ensemble de règles qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre stage API Gateway est associé à une ACL AWS WAF Web afin de le protéger contre les attaques malveillantes.

Correction

Pour plus d'informations sur l'utilisation de la console API Gateway pour associer une ACL Web AWS WAF régionale à un stage d'API API Gateway existant, consultez la section Utilisation AWS WAF pour protéger vos API dans le guide du développeur d'API Gateway.

[APIGateway.5] Les données du cache de l'API REST API Gateway doivent être chiffrées au repos

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::ApiGateway::Stage`

AWS Config règle : `api-gw-cache-encrypted` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si toutes les méthodes des étapes de l'API REST API Gateway pour lesquelles le cache est activé sont chiffrées. Le contrôle échoue si l'une des méthodes d'un stage d'API REST API

Gateway est configurée pour mettre en cache et que le cache n'est pas chiffré. Security Hub CSPM évalue le chiffrement d'une méthode particulière uniquement lorsque la mise en cache est activée pour cette méthode.

Le chiffrement des données au repos réduit le risque qu'un utilisateur non authentifié accède aux données stockées sur le disque. AWS Il ajoute un autre ensemble de contrôles d'accès pour limiter la capacité des utilisateurs non autorisés à accéder aux données. Par exemple, des autorisations d'API sont requises pour déchiffrer les données avant qu'elles ne puissent être lues.

Les caches d'API REST d'API Gateway doivent être chiffrés au repos pour renforcer la sécurité.

Correction

Pour configurer la mise en cache des API pour une étape, consultez la section Activer la mise en cache d'Amazon API Gateway dans le guide du développeur d'API Gateway. Dans Paramètres du cache, choisissez Chiffrer les données du cache.

[APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation

Exigences connexes : NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Protéger > Gestion sécurisée des accès

Gravité : Moyenne

Type de ressource : `AWS::ApiGatewayV2::Route`

Règle AWS Config : api-gwv2-authorization-type-configured

Type de programme : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`authorizationType`	Type d'autorisation des routes API	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Aucune valeur par défaut

Ce contrôle vérifie si les routes Amazon API Gateway possèdent un type d'autorisation. Le contrôle échoue si la route API Gateway ne possède aucun type d'autorisation. Vous pouvez éventuellement fournir une valeur de paramètre personnalisée si vous souhaitez que le contrôle passe uniquement si l'itinéraire utilise le type d'autorisation spécifié dans le `authorizationType` paramètre.

API Gateway prend en charge plusieurs mécanismes pour contrôler et gérer l'accès à votre API. En spécifiant un type d'autorisation, vous pouvez limiter l'accès à votre API aux seuls utilisateurs ou processus autorisés.

Correction

Pour définir un type d'autorisation pour les API HTTP, consultez la section Contrôle et gestion de l'accès à une API HTTP dans API Gateway dans le Guide du développeur d'API Gateway. Pour définir un type d'autorisation pour les WebSocket API, consultez la section Contrôle et gestion de l'accès à une WebSocket API dans API Gateway dans le Guide du développeur d'API Gateway.

[APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2

Exigences associées : NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104,2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::ApiGatewayV2::Stage`

Règle AWS Config : api-gwv2-access-logs-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des accès est configurée pour les stages Amazon API Gateway V2. Ce contrôle échoue si les paramètres du journal d'accès ne sont pas définis.

Les journaux d'accès à API Gateway fournissent des informations détaillées sur les personnes qui ont accédé à votre API et sur la manière dont l'appelant a accédé à l'API. Ces journaux sont utiles pour des applications telles que les audits de sécurité et d'accès et les enquêtes judiciaires. Activez ces journaux d'accès pour analyser les modèles de trafic et résoudre les problèmes.

Pour en savoir plus sur les meilleures pratiques, consultez la section Surveillance des API REST dans le guide du développeur d'API Gateway.

Correction

Pour configurer la journalisation des accès, voir Configuration de la journalisation des CloudWatch API à l'aide de la console API Gateway dans le Guide du développeur API Gateway.

[APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ApiGatewayV2::Integration`

Règle AWS Config : apigatewayv2-integration-private-https-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le protocole HTTPS est activé pour les connexions privées dans le cadre d'une intégration API Gateway V2. Le contrôle échoue si le protocole TLS n'est pas configuré pour une connexion privée.

Les liens VPC connectent API Gateway à des ressources privées. Bien que les liens VPC créent une connectivité privée, ils ne chiffrent pas les données de manière intrinsèque. La configuration de TLS garantit l'utilisation du protocole HTTPS pour le chiffrement de bout en bout, du client au backend via API Gateway. Sans TLS, le trafic d'API sensible circule en clair sur les connexions privées. Le cryptage HTTPS protège le trafic via les connexions privées contre l'interception des données, les attaques de type « man-in-the-middle » et l'exposition aux informations d'identification.

Correction

Pour activer le chiffrement en transit pour les connexions privées dans le cadre d'une intégration API Gateway v2, consultez la section Mettre à jour une intégration privée dans le guide du développeur Amazon API Gateway. Configurez la configuration TLS de sorte que l'intégration privée utilise le protocole HTTPS.

[APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées

Catégorie : Protéger > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ApiGateway::DomainName`

Règle AWS Config : apigateway-domain-name-tls-check

Type de calendrier : Déclenché par un changement

Paramètres :

- `allowedSecurityPolicies`: `SecurityPolicy_TLS13_1_3_2025_09`, `SecurityPolicy_TLS13_1_3_FIPS_2025_09`, `SecurityPolicy_TLS13_1_2_PFS_PQ_2025_09`, `SecurityPolicy_TLS13_2025_EDGE`, `SecurityPolicy_TLS12_PFS_2025_EDGE` (non personnalisable)

Ce contrôle vérifie si un nom de domaine API Gateway est configuré pour chiffrer les données en transit à l'aide d'une politique de sécurité recommandée. Le contrôle échoue si le nom de domaine API Gateway n'est pas configuré pour utiliser une politique de sécurité recommandée.

Ce contrôle génère une `FAILED` recherche pour les noms de domaine personnalisés qui sont attachés aux API HTTP. Si vous avez un cas d'utilisation légitime des API HTTP, vous pouvez supprimer cette découverte.

Une politique de sécurité est une combinaison prédéfinie d'une version minimale du protocole TLS et de suites de chiffrement offertes par API Gateway. Lorsque vos clients établissent une liaison TLS vers votre API ou nom de domaine personnalisé, la politique de sécurité applique la version TLS et la suite de chiffrement acceptées par API Gateway. Les politiques de sécurité protègent vos API et vos noms de domaine personnalisés contre les problèmes de sécurité réseau tels que la falsification et l'écoute clandestine entre un client et un serveur. L'utilisation d'une politique de sécurité recommandée permet de garantir que les noms de domaine API Gateway utilisent des configurations TLS modernes et sécurisées qui protègent les données en transit entre les clients et votre API.

Correction

Pour mettre à jour la politique de sécurité TLS pour un nom de domaine API Gateway, consultez Comment modifier une politique de sécurité dans le guide du développeur Amazon API Gateway.

Contrôles Security Hub CSPM pourAWS AppConfig

Ces contrôles CSPM du Security Hub évaluent le AWS AppConfig service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[AppConfig.1]AWS AppConfigles applications doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppConfig::Application`

Règle AWS Config : `appconfig-application-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS AppConfig application possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'application

ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'application n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une AWS AppConfig application, reportez-vous TagResourceà la référence des AWS AppConfig API.

[AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppConfig::ConfigurationProfile`

Règle AWS Config : `appconfig-configuration-profile-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un profil AWS AppConfig de configuration comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le profil de configuration ne possède aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le profil de configuration n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du

principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un profil de AWS AppConfig configuration, consultez TagResourcela référence de l'AWS AppConfigAPI.

[AppConfig.3]AWS AppConfigles environnements doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppConfig::Environment`

Règle AWS Config : `appconfig-environment-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		aux AWSexigences.	

Ce contrôle vérifie si un AWS AppConfig environnement possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'environnement ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'environnement n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures

pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un AWS AppConfig environnement, reportez-vous TagResourceà la référence des AWS AppConfig API.

[AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppConfig::ExtensionAssociation`

Règle AWS Config : `appconfig-extension-association-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une association d'AWS AppConfigextensions possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'association d'extensions ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées

dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'association d'extension n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une association d'AWS AppConfigextensions, consultez TagResourcela référence de l'AWS AppConfigAPI.

Contrôles Security Hub CSPM pour Amazon AppFlow

Ces contrôles CSPM du Security Hub évaluent le AppFlow service et les ressources Amazon.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[AppFlow.1] AppFlow Les flux Amazon doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppFlow::Flow`

Règle AWS Config : `appflow-flow-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AppFlow flux Amazon possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le flux ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le flux n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque

vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un AppFlow flux Amazon, consultez la section Création de flux dans Amazon AppFlow dans le guide de AppFlow l'utilisateur Amazon.

Contrôles Security Hub CSPM pourAWS App Runner

Ces AWS Security Hub CSPM contrôles évaluent le AWS App Runner service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[AppRunner.1] Les services App Runner doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppRunner::Service`

Règle AWS Config : apprunner-service-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS App Runner service possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le service App Runner ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le service App Runner n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour plus d'informations sur l'ajout de balises à un AWS App Runner service, consultez TagResourcela référence des AWS App Runner API.

[AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppRunner::VpcConnector`

Règle AWS Config : apprunner-vpc-connector-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un connecteur AWS App Runner VPC possède des balises avec les clés spécifiques définies dans le paramètre. `requiredKeyTags` Le contrôle échoue si le connecteur VPC ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre. `requiredKeyTags` Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le connecteur VPC n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour plus d'informations sur l'ajout de balises à un connecteur AWS App Runner VPC, consultez la TagResourceréférence des AWS App RunnerAPI.

Contrôles Security Hub CSPM pourAWS AppSync

Ces contrôles CSPM du Security Hub évaluent le AWS AppSync service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos

> **Important**
>
> Security Hub CSPM a retiré ce contrôle le 9 mars 2026. Pour plus d'informations, consultezJournal des modifications pour les contrôles CSPM de Security Hub. AWS AppSyncfournit désormais un chiffrement par défaut sur tous les caches d'API actuels et futurs.

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::AppSync::GraphQLApi`

Règle AWS Config : appsync-cache-ct-encryption-at-rest

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le cache d'une AWS AppSync API est chiffré au repos. Le contrôle échoue si le cache de l'API n'est pas chiffré au repos.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Vous ne pouvez pas modifier les paramètres de chiffrement après avoir activé la mise en cache pour votre AWS AppSync API. Vous devez plutôt supprimer le cache et le recréer avec le chiffrement activé. Pour plus d'informations, consultez la section Chiffrement du cache dans le Guide du AWS AppSync développeur.

[AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée

Exigences associées : PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::AppSync::GraphQLApi`

Règle AWS Config : `appsync-logging-enabled`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM	
`fieldLoggingLevel`	Niveau de journalisation sur le terrain	Enum	`ERROR`, `ALL`, `INFO`, `DEBUG`	No `default value`	

Ce contrôle vérifie si la journalisation au niveau du champ est activée pour une AWS AppSync API. Le contrôle échoue si le niveau de journalisation du résolveur de champs est défini sur Aucun. À moins que vous ne fournissiez des valeurs de paramètres personnalisées pour indiquer qu'un type de journal spécifique doit être activé, Security Hub CSPM produit un résultat positif si le niveau de journal du résolveur de champs est l'un ou l'autre. `ERROR` `ALL`

Vous pouvez utiliser la journalisation et les métriques pour identifier, dépanner et optimiser vos requêtes GraphQL. L'activation de la journalisation pour AWS AppSync GraphQL vous permet d'obtenir des informations détaillées sur les demandes et réponses des API, d'identifier les problèmes et d'y répondre, et de vous conformer aux exigences réglementaires.

Correction

Pour activer la journalisationAWS AppSync, reportez-vous à la section Configuration et configuration du Guide du AWS AppSync développeur.

[AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AppSync::GraphQLApi`

AWS Configrègle : `tagged-appsync-graphqlapi` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une API AWS AppSync GraphQL possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si l'API GraphQL ne possède aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre. `requiredTagKeys` Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'API GraphQL n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous

pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une API AWS AppSync GraphQL, consultez la TagResourceréférence des AWS AppSyncAPI.

[AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API

Exigences connexes : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Catégorie : Protéger > Gestion des accès sécurisés > Authentification sans mot de passe

Gravité : Élevée

Type de ressource : `AWS::AppSync::GraphQLApi`

Règle AWS Config : `appsync-authorization-check`

Type de calendrier : changement déclenché

Paramètres :

- `AllowedAuthorizationTypes: AWS_LAMBDA,AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (non personnalisable)

Ce contrôle vérifie si votre application utilise une clé d'API pour interagir avec une API AWS AppSync GraphQL. Le contrôle échoue si une API AWS AppSync GraphQL est authentifiée à l'aide d'une clé d'API.

Une clé d'API est une valeur codée en dur dans votre application qui est générée par le AWS AppSync service lorsque vous créez un point de terminaison GraphQL non authentifié. Si cette clé d'API est compromise, votre terminal est vulnérable à un accès involontaire. À moins que vous ne souteniez une application ou un site Web accessible au public, nous vous déconseillons d'utiliser une clé d'API pour l'authentification.

Correction

Pour définir une option d'autorisation pour votre API AWS AppSync GraphQL, consultez la section Autorisation et authentification dans le Guide du AWS AppSyncdéveloppeur.

[AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport

> **Important**
>
> Security Hub CSPM a retiré ce contrôle le 9 mars 2026. Pour plus d'informations, consultezJournal des modifications pour les contrôles CSPM de Security Hub. AWS AppSyncfournit désormais un chiffrement par défaut sur tous les caches d'API actuels et futurs.

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::AppSync::ApiCache`

Règle AWS Config : appsync-cache-ct-encryption-in-transit

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le cache d'une AWS AppSync API est chiffré en transit. Le contrôle échoue si le cache de l'API n'est pas chiffré pendant le transfert.

Les données en transit font référence aux données qui se déplacent d'un emplacement à un autre, par exemple entre les nœuds de votre cluster ou entre votre cluster et votre application. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque qu'un utilisateur non autorisé puisse espionner le trafic réseau.

Correction

Vous ne pouvez pas modifier les paramètres de chiffrement après avoir activé la mise en cache pour votre AWS AppSync API. Vous devez plutôt supprimer le cache et le recréer avec le chiffrement activé. Pour plus d'informations, consultez la section Chiffrement du cache dans le Guide du AWS AppSync développeur.

Contrôles Security Hub CSPM pour Amazon Athena

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Athena. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Athena.1] Les groupes de travail Athena doivent être chiffrés au repos

> **Important**
>
> Security Hub CSPM a retiré ce contrôle en avril 2024. Pour de plus amples informations, veuillez consulter Journal des modifications pour les contrôles CSPM de Security Hub.

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Gravité : Moyenne

Type de ressource : `AWS::Athena::WorkGroup`

Règle AWS Config : athena-workgroup-encrypted-at-rest

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe de travail Athena est chiffré au repos. Le contrôle échoue si un groupe de travail Athena n'est pas chiffré au repos.

Dans Athena, vous pouvez créer des groupes de travail pour exécuter des requêtes pour des équipes, des applications ou différentes charges de travail. Chaque groupe de travail dispose d'un

paramètre permettant d'activer le chiffrement de toutes les requêtes. Vous avez la possibilité d'utiliser le chiffrement côté serveur avec les clés gérées par Amazon Simple Storage Service (Amazon S3), le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) ou le chiffrement côté client avec des clés KMS gérées par le client. Les données au repos désignent toutes les données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement vous aide à protéger la confidentialité de ces données, réduisant ainsi le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour activer le chiffrement au repos pour les groupes de travail Athena, consultez la section Modifier un groupe de travail dans le guide de l'utilisateur d'Amazon Athena. Dans la section Configuration des résultats de requête, sélectionnez Chiffrer les résultats de la requête.

[Athena.2] Les catalogues de données Athena doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Athena::DataCatalog`

AWS Configrègle : `tagged-athena-datacatalog` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un catalogue de données Amazon Athena comporte des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le catalogue de données ne possède aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le catalogue de données n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un catalogue de données Athena, consultez la section Marquage des ressources Athena dans le guide de l'utilisateur d'Amazon Athena.

[Athena.3] Les groupes de travail Athena doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Athena::WorkGroup`

AWS Configrègle : `tagged-athena-workgroup` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un groupe de travail Amazon Athena possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le groupe de travail ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de travail n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe de travail Athena, consultez la section Ajouter et supprimer des balises sur un groupe de travail individuel dans le guide de l'utilisateur d'Amazon Athena.

[Athena.4] La journalisation des groupes de travail Athena doit être activée

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Athena::WorkGroup`

Règle AWS Config : athena-workgroup-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée dans un groupe de travail Amazon Athena. Le contrôle échoue si la journalisation n'est pas activée dans le groupe de travail.

Les journaux d'audit suivent et surveillent les activités du système. Ils fournissent un enregistrement des événements qui peut vous aider à détecter les failles de sécurité, à enquêter sur les incidents et à vous conformer aux réglementations. Les journaux d'audit améliorent également la responsabilité globale et la transparence de votre organisation.

Correction

Pour plus d'informations sur l'activation de la journalisation pour un groupe de travail Athena, consultez la section Activer les métriques de CloudWatch requête dans Athena dans le guide de l'utilisateur d'Amazon Athena.

Contrôles Security Hub CSPM pourAWS Backup

Ces contrôles CSPM du Security Hub évaluent le AWS Backup service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos

Exigences connexes : NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::Backup::RecoveryPoint`

Règle AWS Config : `backup-recovery-point-encrypted`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un point AWS Backup de restauration est chiffré au repos. Le contrôle échoue si le point de restauration n'est pas chiffré au repos.

Un point de AWS Backup restauration fait référence à une copie ou à un instantané spécifique des données créé dans le cadre d'un processus de sauvegarde. Il représente un moment précis où les données ont été sauvegardées et sert de point de restauration au cas où les données d'origine seraient perdues, corrompues ou inaccessibles. Le chiffrement des points de restauration des sauvegardes ajoute une couche de protection supplémentaire contre les accès non autorisés. Le chiffrement est une bonne pratique pour protéger la confidentialité, l'intégrité et la sécurité des données de sauvegarde.

Correction

Pour chiffrer un point de AWS Backup restauration, consultez la section Chiffrement des sauvegardes AWS Backup dans le Guide du AWS Backup développeur.

[Backup.2]AWS Backuples points de récupération doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Backup::RecoveryPoint`

AWS Configrègle : `tagged-backup-recoverypoint` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un point AWS Backup de récupération possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le point de récupération ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le point de récupération n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque

vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour copier des balises depuis des ressources sources au moment de la création de la sauvegarde, voir Copier des balises dans les sauvegardes AWS Backup du Guide du développeur.

Les balises ne sont pas copiées au moment de la création pour les points parent/composite de récupération. Pour ajouter des balises sur des points de récupération existants, y compris des points de parent/composite récupération, voir Ajouter ou supprimer des balises sur des points de récupération existants dans le Guide AWS Backup du développeur.

[Backup.3]AWS Backuples coffres-forts doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Backup::BackupVault`

AWS Configrègle : `tagged-backup-backupvault` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS Backup coffre possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le point de récupération ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le point de récupération n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à unAWS Backupcoffre-fort

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Sélectionnez un coffre-fort de sauvegarde dans la liste.
4. Dans la section Backup vault tags, sélectionnez Manage tags.
5. Entrez la clé et la valeur de la balise. Choisissez Ajouter une nouvelle balise pour des paires clé-valeur supplémentaires.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

[Backup.4]AWS Backuples plans de rapport doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Backup::ReportPlan`

AWS Configrègle : `tagged-backup-reportplan` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un plan de AWS Backup rapport comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le plan de rapport ne comporte aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le plan de rapport n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à unAWS Backupplan de rapport

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Sélectionnez un coffre-fort de sauvegarde dans la liste.
4. Dans la section Backup vault tags, sélectionnez Manage tags.
5. Sélectionnez Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Répétez l'opération pour d'autres paires clé-valeur.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

[Backup.5]AWS Backuples plans de sauvegarde doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Backup::BackupPlan`

AWS Configrègle : `tagged-backup-backupplan` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un plan AWS Backup de sauvegarde comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le plan de sauvegarde ne comporte aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le plan de sauvegarde n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à unAWS Backupplan de sauvegarde

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Sélectionnez un coffre-fort de sauvegarde dans la liste.
4. Dans la section Backup vault tags, sélectionnez Manage tags.
5. Sélectionnez Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Répétez l'opération pour d'autres paires clé-valeur.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

Contrôles Security Hub CSPM pourAWS Batch

Ces contrôles CSPM du Security Hub évaluent le AWS Batch service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Batch.1] Les files d'attente de tâches par lots doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Batch::JobQueue`

Règle AWS Config : batch-job-queue-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une file d'attente de AWS Batch tâches comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la file d'attente de tâches ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la file d'attente de tâches n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une file d'attente de tâches Batch, consultez la section Marquer vos ressources dans le guide de AWS Batch l'utilisateur.

[Batch.2] Les politiques de planification par lots doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Batch::SchedulingPolicy`

Règle AWS Config : batch-scheduling-policy-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une politique de AWS Batch planification comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la politique de planification ne comporte aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la politique de planification n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une politique de planification par lots, consultez la section Marquer vos ressources dans le guide de AWS Batch l'utilisateur.

[Batch.3] Les environnements de calcul par lots doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Batch::ComputeEnvironment`

Règle AWS Config : batch-compute-environment-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un environnement AWS Batch informatique possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'environnement de calcul ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'environnement de calcul n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un environnement de calcul Batch, consultez la section Marquer vos ressources dans le guide de AWS Batch l'utilisateur.

[Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Batch::ComputeEnvironment`

Règle AWS Config : batch-managed-compute-env-compute-resources-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « 2 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si la propriété des ressources de calcul dans un environnement AWS Batch informatique géré possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si la propriété des ressources de calcul ne possède aucune clé de balise ou si toutes les clés spécifiées par le `requiredKeyTags` paramètre ne sont pas présentes. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si une propriété de ressources de calcul ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe. Ce contrôle n'évalue pas les environnements informatiques non gérés ni les environnements gérés qui utilisent des AWS Fargate ressources.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises aux ressources de calcul dans un environnement AWS Batch informatique géré, consultez la section Marquer vos ressources dans le guide de AWS Batch l'utilisateur.

Contrôles Security Hub CSPM pour Amazon Bedrock

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Bedrock. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Bedrock.1] Les sources de données Amazon Bedrock doivent être cryptées et gérées par le clientAWS KMSclés

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::Bedrock::DataSource`

Règle AWS Config : bedrock-data-source-encryption-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une source de données Amazon Bedrock est chiffrée au repos avec une AWS KMS clé gérée par le client. Le contrôle échoue si la source de données n'est pas chiffrée à l'aide d'une clé KMS gérée par le client.

Par défaut, Amazon Bedrock chiffre le contenu de la source de données à l'aide de clés AWS gérées. L'utilisation d'une clé KMS gérée par le client vous permet de contrôler totalement le cycle de vie

de la clé de chiffrement, y compris la rotation, les politiques d'accès et les audits completsAWS CloudTrail. Cela permet de répondre aux exigences de conformité qui imposent un chiffrement contrôlé par le client pour les données sensibles ingérées dans les bases de connaissances.

Correction

Pour chiffrer votre source de données Amazon Bedrock à l'aide d'une clé KMS gérée par le client, consultez Modifier une source de données pour votre base de connaissances Amazon Bedrock dans le guide de l'utilisateur d'Amazon Bedrock.

Contrôles Security Hub CSPM pour Amazon Bedrock AgentCore

Ces AWS Security Hub CSPM contrôles évaluent le AgentCore service et les ressources Amazon Bedrock. Les commandes ne sont peut-être pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC

Catégorie : Protéger > Gestion des accès sécurisés > Ressource non accessible au public

Gravité : Élevée

Type de ressource : `AWS::BedrockAgentCore::Runtime`

Règle AWS Config : bedrockagentcore-runtime-private-network-required

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un environnement d' AgentCore exécution Amazon Bedrock est configuré en mode réseau VPC. Le contrôle échoue si le mode réseau du moteur d'exécution est défini sur PUBLIC.

L'utilisation du mode réseau public pour les environnements d' AgentCore exécution d'Amazon Bedrock expose le moteur d'exécution directement à Internet, ce qui augmente la surface d'attaque et le risque d'accès non autorisé. La configuration des environnements d'exécution en mode réseau VPC garantit que le trafic d'exécution est confiné au sein de votre réseau privé, ce qui vous permet d'appliquer des contrôles de sécurité au niveau du réseau tels que les groupes de sécurité, les ACL réseau et les journaux de flux VPC.

Correction

Pour remédier à ce problème, mettez à jour le AgentCore moteur d'exécution Bedrock non conforme et configurez-le en mode réseau VPC. Pour obtenir des instructions, consultez la section Configurer Amazon Bedrock AgentCore Runtime et les outils pour VPC dans le guide du développeur Amazon AgentCore Bedrock.

[BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Élevée

Type de ressource : `AWS::BedrockAgentCore::Gateway`

Règle AWS Config : bedrockagentcore-gateway-authorizer-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une AgentCore passerelle Amazon Bedrock nécessite une autorisation pour les demandes entrantes. Le contrôle échoue si l'autorisation entrante n'est pas configurée sur la AgentCore passerelle Bedrock.

La configuration de l'authentification sur les AgentCore passerelles Amazon Bedrock garantit que seuls les clients autorisés peuvent envoyer des demandes à vos agents d'intelligence artificielle. Sans autorisation, toute entité disposant d'un accès réseau au point de terminaison de la passerelle peut appeler vos agents, ce qui peut entraîner un accès non autorisé aux données, une utilisation abusive des ressources ou des coûts imprévus. L'autorisation entrante valide les utilisateurs qui tentent d'accéder aux cibles via votre AgentCore passerelle.

Correction

Pour configurer l'autorisation entrante pour une AgentCore passerelle Amazon Bedrock, consultez la section Configurer l'autorisation entrante pour votre passerelle dans le guide du développeur Amazon AgentCore Bedrock.

[BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés

Exigences associées : NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::BedrockAgentCore::Memory`

Règle AWS Config : bedrock-agentcore-memory-encryption-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une AgentCore mémoire Amazon Bedrock est chiffrée au repos avec une AWS KMS clé gérée par le client. Le contrôle échoue si la AgentCore mémoire Bedrock n'est pas chiffrée avec une clé KMS gérée par le client.

L'utilisation d'une clé KMS gérée par le client pour le chiffrement de la AgentCore mémoire Amazon Bedrock renforce la sécurité par rapport à la clé gérée par le service par défaut. Les clés KMS gérées par le client vous permettent de contrôler totalement le cycle de vie des clés de chiffrement et les politiques d'accès. De plus, toutes les utilisations des clés de chiffrement peuvent être enregistrées et surveillées à des AWS CloudTrail fins d'auditabilité.

Correction

Pour chiffrer votre AgentCore mémoire Amazon Bedrock à l'aide d'une clé KMS gérée par le client, consultez la section Chiffrer votre mémoire Amazon Bedrock AgentCore dans le guide du développeur Amazon Bedrock. AgentCore

[BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés

Exigences associées : NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::BedrockAgentCore::Gateway`

Règle AWS Config : bedrockagentcore-gateway-encryption-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une AgentCore passerelle Amazon Bedrock est chiffrée au repos avec une AWS KMS clé gérée par le client. Le contrôle échoue si la AgentCore passerelle Bedrock n'est pas chiffrée avec une clé KMS gérée par le client.

Par défaut, Amazon Bedrock AgentCore chiffre les données de passerelle à l'aide de clés AWS gérées. L'utilisation d'une clé KMS gérée par le client vous permet de contrôler totalement le cycle de vie de la clé de chiffrement, y compris la rotation, les politiques d'accès et les auditsAWS CloudTrail. Cela permet de répondre aux exigences de conformité qui imposent un chiffrement contrôlé par le client pour les charges de travail sensibles liées à l'IA.

Correction

Pour chiffrer votre AgentCore passerelle Bedrock avec une clé KMS gérée par le client, consultez la section Chiffrer votre AgentCore passerelle avec une clé KMS gérée par le client dans le guide du développeur Amazon Bedrock. AgentCore

[BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public

Catégorie : Protection > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Élevée

Type de ressource : `AWS::BedrockAgentCore::BrowserCustom`

Règle AWS Config : bedrockagentcore-browsercustom-network-mode-not-public

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un navigateur AgentCore personnalisé Amazon Bedrock est configuré en mode réseau public. Le contrôle échoue si le mode réseau est défini sur public.

L'utilisation du mode réseau PUBLIC pour les navigateurs AgentCore personnalisés Amazon Bedrock expose les sessions de navigation directement à Internet, ce qui augmente la surface d'attaque et le risque d'accès non autorisé. La configuration des navigateurs en mode réseau VPC garantit que le trafic du navigateur est confiné au sein de votre réseau privé, ce qui vous permet d'appliquer des contrôles de sécurité au niveau du réseau tels que les groupes de sécurité, les ACL réseau et les journaux de flux VPC.

Correction

Pour remédier à ce problème, supprimez le navigateur AgentCore personnalisé Bedrock non conforme et recréez-le en mode réseau VPC. Pour obtenir des instructions, consultez la section Configurer Amazon Bedrock AgentCore Runtime et les outils pour VPC dans le guide du développeur Amazon AgentCore Bedrock.

[BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::BedrockAgentCore::BrowserCustom`

Règle AWS Config : bedrockagentcore-browsercustom-recording-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si l'enregistrement de session est activé sur un navigateur AgentCore personnalisé Amazon Bedrock avec une destination S3 configurée. Le contrôle échoue si l'enregistrement n'est pas activé dans un navigateur personnalisé ou si aucun emplacement S3 n'est configuré pour le stockage des enregistrements.

L'enregistrement de session pour les navigateurs AgentCore personnalisés de Bedrock garantit une auditabilité complète des interactions du navigateur, permettant de détecter les accès non autorisés, l'exfiltration de données ou les activités malveillantes lors des sessions de navigation automatisées.

Correction

Pour savoir comment activer l'enregistrement de session dans le navigateur, consultez la section Enregistrement et rediffusion de session dans le manuel Amazon Bedrock AgentCore Developer Guide.

[BedrockAgentCore.7] Les interpréteurs de code AgentCore personnalisés de Bedrock doivent utiliser une configuration de réseau privé

Catégorie : Protection > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Élevée

Type de ressource : `AWS::BedrockAgentCore::CodeInterpreterCustom`

Règle AWS Config : bedrockagentcore-codeinterpreter-networkmode-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un interpréteur de code AgentCore personnalisé Amazon Bedrock est configuré en mode réseau privé. Le contrôle échoue si le mode réseau est réglé sur `PUBLIC` ou`SANDBOX`.

La configuration des interpréteurs de code AgentCore personnalisés Bedrock en mode réseau privé garantit que les environnements d'exécution du code sont isolés au sein de votre VPC. Les modes réseau public ou sandbox exposent l'interpréteur de code à Internet, ce qui augmente le risque d'accès non autorisé et d'exfiltration de données. L'utilisation du mode réseau privé restreint l'accès au réseau et contribue à protéger les données sensibles traitées lors de l'interprétation du code.

Correction

Pour remédier à ce problème, supprimez l'interpréteur de code AgentCore personnalisé Bedrock non conforme et recréez-le en mode réseau VPC. Pour obtenir des instructions, consultez la section Configuration de l'accès au VPC pour l'exécution et les outils dans le manuel Amazon Bedrock AgentCore Developer Guide.

Contrôles Security Hub CSPM pourAWS Certificate Manager

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources AWS Certificate Manager (ACM). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée

Exigences associées : NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ACM::Certificate`

Règle AWS Config : acm-certificate-expiration-check

Type de calendrier : changement déclenché et périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`daysToExpiration`	Nombre de jours pendant lesquels le certificat ACM doit être renouvelé	Entier	`14` sur `365`	`30`

Ce contrôle vérifie si un certificat AWS Certificate Manager (ACM) est renouvelé dans le délai spécifié. Il vérifie à la fois les certificats importés et les certificats fournis par ACM. Le contrôle échoue si le certificat n'est pas renouvelé dans le délai spécifié. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de renouvellement, Security Hub CSPM utilise une valeur par défaut de 30 jours.

ACM peut renouveler automatiquement les certificats qui utilisent la validation DNS. Pour les certificats qui utilisent la validation par e-mail, vous devez répondre à un e-mail de validation de domaine. ACM ne renouvelle pas automatiquement les certificats que vous importez. Vous devez renouveler manuellement les certificats importés.

Correction

ACM assure le renouvellement géré de vos SSL/TLS certificats émis par Amazon. Cela signifie qu'ACM renouvelle automatiquement vos certificats (si vous utilisez la validation DNS) ou qu'elle vous envoie des notifications par e-mail lorsque l'expiration des certificats approche. Ces services s'appliquent aux certificats ACM publics et privés.

Pour les domaines validés par e-mail

Lorsqu'un certificat arrive à expiration dans un délai de 45 jours, ACM envoie au propriétaire du domaine un e-mail pour chaque nom de domaine. Pour valider les domaines et terminer le renouvellement, vous devez répondre aux notifications par e-mail.

Pour plus d'informations, consultez la section Renouvellement pour les domaines validés par e-mail dans le guide de AWS Certificate Manager l'utilisateur.

Pour les domaines validés par DNS

ACM renouvelle automatiquement les certificats qui utilisent la validation DNS. 60 jours avant l'expiration, ACM vérifie que le certificat peut être renouvelé.

S'il ne parvient pas à valider un nom de domaine, ACM envoie une notification indiquant qu'une validation manuelle est requise. Il envoie ces notifications 45 jours, 30 jours, 7 jours et 1 jour avant l'expiration.

Pour plus d'informations, consultez la section Renouvellement pour les domaines validés par DNS dans le Guide de AWS Certificate Manager l'utilisateur.

[ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits

Exigences associées : PCI DSS v4.0. 1/4.2.1

Catégorie : Identifier > Inventaire > Services d'inventaire

Gravité : Élevée

Type de ressource : `AWS::ACM::Certificate`

Règle AWS Config : acm-certificate-rsa-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les certificats RSA gérés par AWS Certificate Manager utilisent une longueur de clé d'au moins 2 048 bits. Le contrôle échoue si la longueur de la clé est inférieure à 2 048 bits.

La puissance du chiffrement est directement liée à la taille de la clé. Nous recommandons des longueurs de clé d'au moins 2 048 bits pour protéger vos AWS ressources à mesure que la puissance de calcul diminue et que les serveurs deviennent plus avancés.

Correction

La longueur de clé minimale pour les certificats RSA émis par ACM est déjà de 2 048 bits. Pour obtenir des instructions sur l'émission de nouveaux certificats RSA avec ACM, consultez la section Émission et gestion des certificats dans le guide de l'AWS Certificate Managerutilisateur.

ACM vous permet d'importer des certificats dont la longueur de clé est plus courte, mais vous devez utiliser des clés d'au moins 2 048 bits pour passer ce contrôle. Vous ne pouvez pas modifier la longueur de la clé après avoir importé un certificat. Vous devez plutôt supprimer les certificats dont la longueur de clé est inférieure à 2 048 bits. Pour plus d'informations sur l'importation de certificats dans ACM, consultez la section Conditions préalables à l'importation de certificats dans le Guide de l'AWS Certificate Managerutilisateur.

[ACM.3] Les certificats ACM doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::ACM::Certificate`

AWS Configrègle : `tagged-acm-certificate` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un certificat AWS Certificate Manager (ACM) possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le certificat ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le certificat n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un certificat ACM, consultez la section Marquage des AWS Certificate Manager certificats dans le guide de l'AWS Certificate Managerutilisateur.

Contrôles Security Hub CSPM pourCloudFormation

Ces contrôles CSPM du Security Hub évaluent le AWS CloudFormation service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CloudFormation.1] les CloudFormation piles doivent être intégrées au Simple Notification Service (SNS)

> **Important**
>
> Security Hub CSPM a retiré ce contrôle en avril 2024. Pour de plus amples informations, veuillez consulter Journal des modifications pour les contrôles CSPM de Security Hub.

Exigences connexes : NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Catégorie : Détecter > Services de détection > Surveillance des applications

Gravité : Faible

Type de ressource : `AWS::CloudFormation::Stack`

Règle AWS Config : `cloudformation-stack-notification-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une notification Amazon Simple Notification Service est intégrée à une CloudFormation pile. Le contrôle échoue pour une CloudFormation pile si aucune notification SNS n'y est associée.

La configuration d'une notification SNS avec votre CloudFormation stack permet d'informer immédiatement les parties prenantes de tout événement ou changement survenant dans le stack.

Correction

Pour intégrer une CloudFormation pile et une rubrique SNS, consultez la section Mettre à jour les piles directement dans le guide de l'AWS CloudFormationutilisateur.

[CloudFormation.2] les CloudFormation piles doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::CloudFormation::Stack`

AWS Configrègle : `tagged-cloudformation-stack` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS CloudFormation pile possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la pile ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la pile n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous

pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une CloudFormation pile, reportez-vous CreateStackà la référence de l'AWS CloudFormationAPI.

[CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Moyenne

Type de ressource : `AWS::CloudFormation::Stack`

Règle AWS Config : cloudformation-termination-protection-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la protection de terminaison est activée sur une AWS CloudFormation pile. Le contrôle échoue si la protection de terminaison n'est pas activée sur une CloudFormation pile.

CloudFormation permet de gérer les ressources connexes en tant qu'unité unique appelée Stack. Vous pouvez empêcher la suppression accidentelle d'une pile en activant la protection contre la résiliation sur la pile. Si un utilisateur tente de supprimer une pile pour laquelle la protection contre la résiliation est activée, la suppression échoue et la pile, et son statut, restent inchangés.

Vous pouvez définir la protection contre la résiliation sur une pile ayant n'importe quel status sauf `DELETE_IN_PROGRESS` ou `DELETE_COMPLETE`.

> **Note**
>
> L'activation ou la désactivation de la protection pour résilier sur une pile transmet le même choix à toutes les piles imbriquées appartenant à cette pile. Vous ne pouvez pas activer ou désactiver la protection contre la résiliation directement sur une pile imbriquée. Vous ne pouvez pas supprimer directement une pile imbriquée appartenant à une pile pour laquelle la protection de terminaison est activée. Si NESTED s'affiche en regard du nom de la pile, cela signifie que la pile est imbriquée. Dans ce cas, vous pouvez seulement modifier la protection contre la résiliation sur la pile racine à laquelle appartient la pile imbriquée.

Correction

Pour activer la protection contre le licenciement sur une CloudFormation pile, voir Protéger les CloudFormation piles contre la suppression dans le Guide de l'AWS CloudFormationutilisateur.

[CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés

Catégorie : Détecter > Gestion des accès sécurisés

Gravité : Moyenne

Type de ressource : `AWS::CloudFormation::Stack`

Règle AWS Config : cloudformation-stack-service-role-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un rôle de service est associé à une AWS CloudFormation pile. Le contrôle échoue pour une CloudFormation pile si aucun rôle de service n'y est associé.

Service-managed StackSets utilisez des rôles d'exécution grâce à l'intégration des accès sécurisés des AWS Organizations. Le contrôle génère également un résultat d'échec pour une AWS CloudFormation pile créée par un service géré StackSets car aucun rôle de service n'y est associé. En raison de la méthode d' StackSets authentification gérée par les services, le `roleARN` champ ne peut pas être renseigné pour ces piles.

L'utilisation de rôles de service avec des CloudFormation piles permet de mettre en œuvre l'accès avec le moindre privilège en séparant les autorisations entre l'utilisateur qui creates/updates cumule les autorisations et les autorisations requises par CloudFormation les create/update ressources. Cela réduit le risque d'augmentation des privilèges et contribue à maintenir les limites de sécurité entre les différents rôles opérationnels.

> **Note**
>
> Un rôle de service attaché à une pile ne peut pas être supprimé après la création de la pile. Les autres utilisateurs disposant des autorisations nécessaires pour effectuer des opérations sur cette pile peuvent utiliser ce rôle, qu'ils disposent ou non de l'autorisation `iam:PassRole`. Si le rôle comprend des autorisations que l'utilisateur ne devrait pas avoir, vous avez peut-être remonté accidentellement ses autorisations. Vérifiez que le rôle accorde le privilège le plus faible.

Correction

Pour associer un rôle de service à une CloudFormation pile, voir rôle CloudFormation de service dans le Guide de AWS CloudFormation l'utilisateur.

Contrôles CSPM de Security Hub pour Amazon CloudFront

Ces AWS Security Hub CSPM contrôles évaluent le CloudFront service et les ressources Amazon. Les commandes ne sont peut-être pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut

Exigences associées : NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0. 1/22.6

Catégorie : Protéger > Gestion sécurisée des accès > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-default-root-object-configured

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une CloudFront distribution Amazon ayant pour origine S3 est configurée pour renvoyer un objet spécifique qui est l'objet racine par défaut. Le contrôle échoue si la CloudFront distribution utilise des origines S3 et qu'aucun objet racine par défaut n'est configuré. Ce contrôle ne s'applique pas aux CloudFront distributions qui utilisent des origines personnalisées.

Un utilisateur peut parfois demander l'URL racine de la distribution au lieu d'un objet de la distribution. Dans ce cas, la spécification d'un objet racine par défaut peut vous aider à éviter d'exposer le contenu de votre distribution web.

Correction

Pour configurer un objet racine par défaut pour une CloudFront distribution, consultez Comment spécifier un objet racine par défaut dans l'Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-viewer-policy-https

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une CloudFront distribution Amazon nécessite que les spectateurs utilisent directement le protocole HTTPS ou si elle utilise la redirection. La commande échoue si elle `ViewerProtocolPolicy` est réglée sur `allow-all` pour `defaultCacheBehavior` ou pour`cacheBehaviors`.

Vous pouvez utiliser HTTPS (TLS) pour empêcher les pirates potentiels d'espionner ou de manipuler le trafic réseau à l'aide d'attaques de l'homme du milieu au d'autres attaques similaires. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées. Le chiffrement des données en transit

peut affecter les performances. Vous devriez tester votre application à l'aide de cette fonctionnalité pour comprendre le profil de performances et l'impact du protocole TLS.

Correction

Pour chiffrer une CloudFront distribution en transit, consultez la section Exiger le protocole HTTPS pour les communications entre les spectateurs et CloudFront le guide du CloudFront développeur Amazon.

[CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Faible

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-origin-failover-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une CloudFront distribution Amazon est configurée avec un groupe d'origine qui possède deux origines ou plus.

CloudFront le basculement d'origine peut améliorer la disponibilité. Le basculement d'origine redirige automatiquement le trafic vers une origine secondaire si l'origine principale n'est pas disponible ou si elle renvoie des codes d'état de réponse HTTP spécifiques.

Correction

Pour configurer le basculement d'origine pour une CloudFront distribution, consultez la section Création d'un groupe d'origine dans l'Amazon CloudFront Developer Guide.

[CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-accesslogs-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des accès au serveur est activée sur les CloudFront distributions. Le contrôle échoue si la journalisation des accès n'est pas activée pour une distribution. Ce contrôle évalue uniquement si la journalisation standard (ancienne) est activée pour une distribution.

CloudFront les journaux d'accès fournissent des informations détaillées sur chaque demande utilisateur CloudFront reçue. Chaque journal contient des informations telles que la date et l'heure de réception de la demande, l'adresse IP de l'utilisateur qui a fait la demande, la source de la demande et le numéro de port de la demande formulée par l'utilisateur. Ces journaux sont utiles pour des applications telles que les audits de sécurité et d'accès et les enquêtes judiciaires. Pour plus d'informations sur l'analyse des journaux d'accès, consultez la section Interroger CloudFront les journaux Amazon dans le guide de l'utilisateur Amazon Athena.

Correction

Pour configurer la journalisation standard (ancienne) pour une CloudFront distribution, voir Configurer la journalisation standard (ancienne) dans l'Amazon CloudFront Developer Guide.

[CloudFront.6] CloudFront les distributions doivent avoir le WAF activé

Exigences associées : NIST.800-53.r5 AC-4 (21), PCI DSS v4.0. 1/64.2

Catégorie : Protéger > Services de protection

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-associated-with-waf

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les CloudFront distributions sont associées à des ACL AWS WAF classiques ou AWS WAF Web. Le contrôle échoue si la distribution n'est pas associée à une ACL Web.

AWS WAF est un pare-feu d'applications Web qui permet de protéger les applications Web et les API contre les attaques. Il vous permet de configurer un ensemble de règles appelé liste de contrôle d'accès web (ACL web) qui autorisent, bloquent ou comptent les requêtes web en fonction des règles et conditions de sécurité web personnalisables que vous définissez. Assurez-vous que votre CloudFront distribution est associée à une ACL AWS WAF Web pour la protéger contre les attaques malveillantes.

Correction

Pour associer une ACL AWS WAF Web à une CloudFront distribution, consultez la section Utilisation AWS WAF pour contrôler l'accès à votre contenu dans l'Amazon CloudFront Developer Guide.

[CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés

Exigences connexes : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Faible

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-custom-ssl-certificate

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les CloudFront distributions utilisent le SSL/TLS certificat CloudFront fourni par défaut. Ce contrôle passe si la CloudFront distribution utilise un SSL/TLS certificat personnalisé. Ce contrôle échoue si la CloudFront distribution utilise le SSL/TLS certificat par défaut.

Personnalisez : SSL/TLS autorisez vos utilisateurs à accéder au contenu en utilisant d'autres noms de domaine. Vous pouvez stocker des certificats personnalisés dans AWS Certificate Manager (recommandé) ou dans IAM.

Correction

Pour ajouter un autre nom de domaine pour une CloudFront distribution à l'aide d'un SSL/TLS certificat personnalisé, consultez la section Ajouter un autre nom de domaine dans l'Amazon CloudFront Developer Guide.

[CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Faible

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-sni-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les CloudFront distributions Amazon utilisent un SSL/TLS certificat personnalisé et sont configurées pour utiliser le SNI pour traiter les requêtes HTTPS. Ce contrôle échoue si un SSL/TLS certificat personnalisé est associé mais que la méthode de SSL/TLS support est une adresse IP dédiée. Le contrôle échoue également si la distribution utilise CloudFront SSL/TLS un certificat par défaut.

Server Name Indication (SNI) est une extension du protocole TLS prise en charge par les navigateurs et les clients lancés après 2010. Si vous configurez CloudFront pour traiter les requêtes HTTPS à l'aide du SNI, CloudFront associez votre nom de domaine alternatif à une adresse IP pour chaque emplacement périphérique. Lorsqu'un utilisateur envoie une demande HTTPS pour votre contenu, DNS achemine la demande vers l'adresse IP de l'emplacement périphérique correct. L'adresse IP de votre nom de domaine est déterminée lors de la négociation de la SSL/TLS poignée de main ; l'adresse IP n'est pas dédiée à votre distribution.

Correction

Pour configurer une CloudFront distribution de manière à utiliser le SNI pour traiter les requêtes HTTPS, consultez la section Utilisation du SNI pour servir les requêtes HTTPS (fonctionne pour la plupart des clients) dans le Guide du CloudFront développeur. Pour plus d'informations sur les

certificats SSL personnalisés, consultez la section Exigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront.

[CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-traffic-to-origin-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les CloudFront distributions Amazon chiffrent le trafic vers des origines personnalisées. Ce contrôle échoue pour une CloudFront distribution dont la politique de protocole d'origine autorise « HTTP uniquement ». Ce contrôle échoue également si la politique de protocole d'origine de la distribution est « match-viewer » alors que la politique de protocole de visualisation est « Allow-all ».

Le protocole HTTPS (TLS) peut être utilisé pour empêcher l'écoute ou la manipulation du trafic réseau. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées.

Correction

Pour mettre à jour la politique du protocole d'origine afin d'exiger le chiffrement d'une CloudFront connexion, consultez Exiger le protocole HTTPS pour les communications entre CloudFront et votre origine personnalisée dans l'Amazon CloudFront Developer Guide.

[CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-23,,

(1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-no-deprecated-ssl-protocols

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les CloudFront distributions Amazon utilisent des protocoles SSL obsolètes pour les communications HTTPS entre les emplacements CloudFront périphériques et vos origines personnalisées. Ce contrôle échoue si une CloudFront distribution comporte un « `CustomOriginConfig` where `OriginSslProtocols` includes `SSLv3` ».

En 2015, l'Internet Engineering Task Force (IETF) a officiellement annoncé que le protocole SSL 3.0 devait être obsolète car le protocole n'était pas suffisamment sécurisé. Il est recommandé d'utiliser TLSv1.2 ou une version ultérieure pour les communications HTTPS vers vos origines personnalisées.

Correction

Pour mettre à jour les protocoles SSL Origin pour une CloudFront distribution, consultez la section Exiger le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée dans l'Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

Exigences associées : NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), PCI DSS v4.0. 1/22.2.6

Catégorie : Identifier > Configuration des ressources

Gravité : Élevée

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-s3-origin-non-existent-bucket

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les CloudFront distributions Amazon pointent vers des origines Amazon S3 inexistantes. Le contrôle échoue pour une CloudFront distribution si l'origine est configurée pour pointer vers un bucket inexistant. Ce contrôle s'applique uniquement aux CloudFront distributions dont l'origine S3 est un compartiment S3 sans hébergement de site Web statique.

Lorsqu'une CloudFront distribution de votre compte est configurée pour pointer vers un compartiment inexistant, un tiers malveillant peut créer le compartiment référencé et diffuser son propre contenu via votre distribution. Nous vous recommandons de vérifier toutes les origines, quel que soit le comportement de routage, afin de vous assurer que vos distributions pointent vers les origines appropriées.

Correction

Pour modifier une CloudFront distribution afin qu'elle pointe vers une nouvelle origine, consultez la section Mettre à jour une distribution dans l'Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine

Catégorie : Protéger > Gestion sécurisée des accès > Ressource non accessible au public

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-s3-origin-access-control-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le contrôle d'accès à l'origine (OAC) est configuré pour une CloudFront distribution Amazon ayant une origine Amazon S3. Le contrôle échoue si l'OAC n'est pas configuré pour la CloudFront distribution.

Lorsque vous utilisez un compartiment S3 comme origine pour votre CloudFront distribution, vous pouvez activer l'OAC. Cela permet d'accéder au contenu du compartiment uniquement via la CloudFront distribution spécifiée et interdit l'accès directement depuis le compartiment ou une autre distribution. Bien que CloudFront prenant en charge Origin Access Identity (OAI), l'OAC propose des fonctionnalités supplémentaires, et les distributions utilisant OAI peuvent migrer vers OAC. Bien que l'OAI fournisse un moyen sécurisé d'accéder aux origines S3, il présente des limites, telles

que l'absence de prise en charge des configurations de politiques granulaires et des HTTP/HTTPS requêtes utilisant la méthode POST Régions AWS qui nécessitent AWS Signature Version 4 (SigV4). OAI ne prend pas non plus en charge le chiffrement avec AWS Key Management Service. L'OAC est basé sur une AWS bonne pratique consistant à utiliser les principes de service IAM pour s'authentifier auprès des origines S3.

Correction

Pour configurer l'OAC pour une CloudFront distribution ayant des origines S3, consultez la section Restreindre l'accès à une origine Amazon S3 dans l'Amazon CloudFront Developer Guide.

[CloudFront.14] les CloudFront distributions doivent être étiquetées

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::CloudFront::Distribution`

AWS Config règle : `tagged-cloudfront-distribution` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une CloudFront distribution Amazon possède des balises dont les clés spécifiques sont définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la distribution ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le

paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la distribution n'est balisée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une CloudFront distribution, consultez la section Marquage des CloudFront distributions Amazon dans l'Amazon CloudFront Developer Guide.

[CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-ssl-policy-check

Type de calendrier : Déclenché par un changement

Paramètres `securityPolicies` : `TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025` (non personnalisable)

Ce contrôle vérifie si une CloudFront distribution Amazon est configurée pour utiliser une politique de sécurité TLS recommandée. Le contrôle échoue si la CloudFront distribution n'est pas configurée pour utiliser une politique de sécurité TLS recommandée.

Si vous configurez une CloudFront distribution Amazon pour obliger les spectateurs à utiliser le protocole HTTPS pour accéder au contenu, vous devez choisir une politique de sécurité et spécifier la version minimale SSL/TLS du protocole à utiliser. Cela détermine la version du protocole CloudFront utilisée pour communiquer avec les spectateurs et les chiffrements CloudFront utilisés pour crypter les communications. Nous vous recommandons d'utiliser la politique de sécurité la plus CloudFront récente. Cela garantit qu'il CloudFront utilise les dernières suites de chiffrement pour crypter les données en transit entre un visualiseur et une CloudFront distribution.

> **Note**
>
> Ce contrôle génère des résultats uniquement pour les CloudFront distributions configurées pour utiliser des certificats SSL personnalisés et qui ne sont pas configurées pour prendre en charge les anciens clients.

Correction

Pour plus d'informations sur la configuration de la politique de sécurité d'une CloudFront distribution, voir Mettre à jour une distribution dans l'Amazon CloudFront Developer Guide. Lorsque vous configurez la politique de sécurité d'une distribution, choisissez la politique de sécurité la plus récente.

[CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda

Catégorie : Protéger > Gestion sécurisée des accès > Contrôle d'accès

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-origin-lambda-url-oac-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le contrôle d'accès à l'origine est activé pour une CloudFront distribution Amazon dont l'URL de AWS Lambda fonction est l'origine. Le contrôle échoue si la CloudFront distribution possède une URL de fonction Lambda comme origine et que l'OAC n'est pas activé.

L'URL d'une AWS Lambda fonction est un point de terminaison HTTPS dédié à une fonction Lambda. Si l'URL d'une fonction Lambda est à l'origine d'une CloudFront distribution, l'URL de la fonction doit être accessible au public. Par conséquent, pour des raisons de sécurité, vous devez créer un OAC et l'ajouter à l'URL de la fonction Lambda dans une distribution. L'OAC utilise les principes du service IAM pour authentifier les requêtes entre CloudFront et l'URL de la fonction. Il prend également en charge l'utilisation de politiques basées sur les ressources pour autoriser l'invocation d'une fonction uniquement si une demande est faite pour le compte d'une CloudFront distribution spécifiée dans la politique.

Correction

Pour plus d'informations sur la configuration de l'OAC pour une CloudFront distribution Amazon qui utilise une URL de fonction Lambda comme origine, consultez Restreindre l'accès à l'origine d'une URL de AWS Lambda fonction dans l'Amazon CloudFront Developer Guide.

[CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies

Catégorie : Protéger > Gestion sécurisée des accès > Contrôle d'accès

Gravité : Moyenne

Type de ressource : `AWS::CloudFront::Distribution`

Règle AWS Config : cloudfront-distribution-key-group-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une CloudFront distribution Amazon est configurée pour utiliser des groupes de clés fiables pour l'authentification par URL signée ou par cookie signé. Le contrôle échoue si la CloudFront distribution utilise des signataires fiables ou si aucune authentification n'est configurée pour la distribution.

Pour utiliser des URL ou des cookies signés, vous avez besoin d'un signataire. Un signataire est soit un groupe de clés de confiance dans lequel vous créez CloudFront, soit un AWS compte contenant une paire de CloudFront clés. Nous vous recommandons d'utiliser des groupes de clés approuvés, car avec les groupes de CloudFront clés, vous n'avez pas besoin d'utiliser l'utilisateur root du AWS compte pour gérer les clés publiques des URL CloudFront signées et des cookies signés.

> **Note**
>
> Ce contrôle n'évalue pas les CloudFront distributions (`connectionMode=tenant-only`) multi-locataires.

Correction

Pour plus d'informations sur l'utilisation de groupes de clés fiables avec des URL signées et des cookies, consultez la section Utilisation de groupes de clés fiables dans l'Amazon CloudFront Developer Guide.

Contrôles Security Hub CSPM pourAWS CloudTrail

Ces AWS Security Hub CSPM contrôles évaluent le AWS CloudTrail service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/31.1, CIS AWS Foundations Benchmark v1.2. 0/21.1, CIS AWS Foundations Benchmark v1.4. 0/31.1, CIS AWS Foundations Benchmark v3.0. 0/31., NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-14 (1) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SA-8 (22)

Catégorie : Identifier - Journalisation

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : multi-region-cloudtrail-enabled

Type de calendrier : Périodique

Paramètres :

- `readWriteType`: `ALL` (non personnalisable)

  `includeManagementEvents`: `true` (non personnalisable)

Ce contrôle vérifie s'il existe au moins un journal multirégional qui capture AWS CloudTrail les événements de gestion de lecture et d'écriture. Le contrôle échoue s'il CloudTrail est désactivé ou s'il n'existe pas au moins une CloudTrail trace qui capture les événements de gestion de lecture et d'écriture.

AWS CloudTrailenregistre les appels d'AWSAPI pour votre compte et vous envoie des fichiers journaux. Les informations enregistrées incluent les informations suivantes :

- Identité de l'appelant d'API
- Heure de l'appel API
- Adresse IP source de l'appelant d'API
- Paramètres de demande
- Éléments de réponse renvoyés par le Service AWS

CloudTrail fournit un historique des appels d'AWSAPI pour un compte, y compris les appels d'API effectués à partir des Console de gestion AWS AWS SDK et des outils de ligne de commande. L'historique inclut également les appels d'API provenant de niveaux supérieurs Services AWS tels que. AWS CloudFormation

L'historique des appels d'AWSAPI produit par CloudTrail permet l'analyse de la sécurité, le suivi des modifications des ressources et l'audit de conformité. Multi-Region les sentiers offrent également les avantages suivants.

- Un journal de suivi multi-régions permet de détecter les activités inattendues qui se produisent dans des régions par ailleurs inutilisées
- Un journal de suivi multi-régions garantit que la journalisation mondiale des services est activée par défaut pour un journal de suivi. L'enregistrement des événements de service mondiaux enregistre les événements générés par les services AWS mondiaux.
- Pour un parcours multirégional, les événements de gestion pour toutes les opérations de lecture et d'écriture garantissent que les opérations de gestion des CloudTrail enregistrements sur toutes les ressources d'unCompte AWS.

Par défaut, les CloudTrail sentiers créés à l'aide du Console de gestion AWS sont des sentiers multirégionaux.

Correction

Pour créer un nouveau parcours multirégional dans CloudTrail, voir Création d'un parcours dans le guide de l'AWS CloudTrailutilisateur. Utilisez les valeurs suivantes :

Champ	Value
Paramètres supplémentaires, validation du fichier journal	Activé
Choisissez les événements du journal, les événements de gestion, l'activité de l'API	Lisez et écrivez. Désactivez les cases à cocher pour les exclusions.

Pour mettre à jour un parcours existant, voir Mettre à jour un parcours dans le Guide de AWS CloudTrail l'utilisateur. Dans Événements de gestion, pour l'activité de l'API, sélectionnez Read and Write.

[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/3.5, CIS AWS Foundations Benchmark v1.2. 0/22.7, CIS AWS Foundations Benchmark v1.4. 0/32.7, CIS AWS Foundations Benchmark v3.0. 0/35 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.3.8, PCI DSS version 3.2. 1/34., PCI DSS version 4.0. 1/10.3.2

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::CloudTrail::Trail`

Règle AWS Config : cloud-trail-encryption-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement côté serveur (SSE) CloudTrail est configuré pour utiliser le chiffrement côté serveur (SSE). AWS KMS key Le contrôle échoue si le `KmsKeyId` n'est pas défini.

Pour renforcer la sécurité de vos fichiers CloudTrail journaux sensibles, vous devez utiliser le chiffrement côté serveur avec AWS KMS keys (SSE-KMS) pour vos fichiers CloudTrail journaux pour le chiffrement au repos. Notez que par défaut, les fichiers journaux envoyés par vos buckets sont chiffrés par chiffrement côté serveur Amazon CloudTrail à l'aide des clés de S3-managed chiffrement Amazon (). SSE-S3

Correction

Pour activer SSE-KMS le chiffrement des fichiers CloudTrail journaux, voir Mettre à jour un journal pour utiliser une clé KMS dans le Guide de AWS CloudTrail l'utilisateur.

[CloudTrail.3] Au moins une CloudTrail piste doit être activée

Exigences associées : NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/101.1, PCI DSS version 3.2. 1/102.2.1, PCI DSS v3.2. 1/102.2.2, PCI DSS v3.2. 1/102.2.3, PCI DSS v3.2. 1/102.2.4, PCI DSS v3.2. 1/102.2.5, PCI DSS version 3.2. 1/102.2.6, PCI DSS version 3.2. 1/102.2.7, PCI DSS version 3.2. 1/103.3.1, PCI DSS v3.2. 1/103.3.2, PCI DSS v3.2. 1/103.3.3, PCI DSS v3.2. 1/103.3.4, PCI DSS v3.2. 1/103.3.5, PCI DSS v3.2. 1/103.3.6, PCI DSS v4.0. 1/10.2.1

Catégorie : Identifier - Journalisation

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : cloudtrail-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un AWS CloudTrail parcours est activé dans votreCompte AWS. Le contrôle échoue si aucun suivi n'est activé sur votre compte. CloudTrail

Cependant, certains AWS services ne permettent pas de consigner tous les événements et API. Vous devez mettre en œuvre toute piste d'audit supplémentaire autre que CloudTrail et consulter la documentation de chaque service dans la section Services et intégrations CloudTrail pris en charge.

Correction

Pour commencer CloudTrail et créer un parcours, consultez le AWS CloudTraildidacticiel de prise en main du guide de l'AWS CloudTrailutilisateur.

[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/32.2, CIS AWS Foundations Benchmark v1.2. 0/22.2, CIS AWS Foundations Benchmark v1.4. 0/32.2, CIS AWS Foundations Benchmark v3.0. 0/32. NIST.800-53.r5 AU-9, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (1), NIST.800-53.r5 SI-7 (3), NIST.800-53.r5 SI-7 (7), NIST.800-171.r2 3.3.8, PCI DSS version 3.2. 1/105.5.2, PCI DSS v3.2. 1/105.5.5, PCI DSS v4.0. 1/10.3.2

Catégorie : Protection des données > Intégrité des données

Gravité : Faible

Type de ressource : `AWS::CloudTrail::Trail`

Règle AWS Config : cloud-trail-log-file-validation-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la validation de l'intégrité du fichier journal est activée sur un CloudTrail journal.

CloudTrail la validation du fichier journal crée un fichier condensé signé numériquement qui contient le hachage de chaque journal CloudTrail écrit sur Amazon S3. Vous pouvez utiliser ces fichiers de synthèse pour déterminer si un fichier journal a été modifié, supprimé ou inchangé après la CloudTrail livraison du journal.

Security Hub CSPM vous recommande d'activer la validation des fichiers sur tous les sentiers. La validation des fichiers journaux fournit des contrôles d'intégrité supplémentaires des CloudTrail journaux.

Correction

Pour activer la validation du fichier CloudTrail journal, voir Activation de la validation de l'intégrité du fichier journal CloudTrail dans le guide de AWS CloudTrail l'utilisateur.

[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/34., PCI DSS version 3.2. 1/105.5.3, CIS AWS Foundations Benchmark v1.2. 0/2.4, CIS AWS Foundations Benchmark v1.4. 0/34, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::CloudTrail::Trail`

Règle AWS Config : cloud-trail-cloud-watch-logs-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les CloudTrail sentiers sont configurés pour envoyer des CloudWatch journaux à Logs. Le contrôle échoue si la `CloudWatchLogsLogGroupArn` propriété de la piste est vide.

CloudTrail enregistre les appels d'AWSAPI effectués dans un compte donné. Les informations enregistrées incluent les éléments suivants :

- L'identité de l'appelant de l'API
- Heure de l'appel d'API
- Adresse IP source de l'appelant de l'API
- Les paramètres de la demande

- Les éléments de réponse renvoyés par le Service AWS

CloudTrail utilise Amazon S3 pour le stockage et la livraison des fichiers journaux. Vous pouvez capturer CloudTrail des journaux dans un compartiment S3 spécifique pour une analyse à long terme. Pour effectuer une analyse en temps réel, vous pouvez configurer CloudTrail l'envoi des CloudWatch journaux vers Logs.

Pour un suivi activé dans toutes les régions d'un compte, CloudTrail envoie les fichiers journaux de toutes ces régions à un groupe de CloudWatch journaux de journaux.

Security Hub CSPM vous recommande d'envoyer les CloudTrail journaux à CloudWatch Logs. Notez que cette recommandation vise à garantir que l'activité du compte est capturée, surveillée et déclenchée de manière appropriée. Vous pouvez utiliser CloudWatch Logs pour configurer cela avec votreServices AWS. Cette recommandation n'exclut pas l'utilisation d'une autre solution.

L'envoi de CloudTrail CloudWatch journaux à Logs facilite la journalisation en temps réel et historique des activités en fonction de l'utilisateur, de l'API, de la ressource et de l'adresse IP. Vous pouvez utiliser cette approche pour établir des alarmes et des notifications en cas d'activité anormale ou sensible du compte.

Correction

Pour intégrer CloudTrail les CloudWatch journaux, consultez la section Envoyer des événements aux CloudWatch journaux dans le guide de AWS CloudTrail l'utilisateur.

[CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/2.3, CIS AWS Foundations Benchmark v1.4. 0/33., PCI DSS version 4.0. 1/1.4.4

Catégorie : Identifier - Journalisation

Gravité : Critique

Type de ressource : `AWS::S3::Bucket`

AWS Configrègle : Aucune (règle CSPM personnalisée de Security Hub)

Type de calendrier : périodique et déclenché par des modifications

Paramètres : Aucun

CloudTrail enregistre un enregistrement de chaque appel d'API effectué sur votre compte. Ces fichiers journaux sont stockés dans un compartiment S3. Le CIS recommande que la politique de compartiment S3, ou liste de contrôle d'accès (ACL), soit appliquée au compartiment S3 qui CloudTrail enregistre afin d'empêcher l'accès public aux CloudTrail journaux. Autoriser l'accès public au contenu des CloudTrail journaux peut aider un adversaire à identifier les faiblesses liées à l'utilisation ou à la configuration du compte concerné.

Pour exécuter cette vérification, Security Hub CSPM utilise d'abord une logique personnalisée pour rechercher le compartiment S3 dans lequel vos CloudTrail journaux sont stockés. Il utilise ensuite les règles AWS Config gérées pour vérifier que le bucket est accessible au public.

Si vous regroupez vos journaux dans un seul compartiment S3 centralisé, Security Hub CSPM effectue la vérification uniquement par rapport au compte et à la région où se trouve le compartiment S3 centralisé. Pour les autres comptes et régions, le statut de contrôle est Aucune donnée.

Si le compartiment est accessible au public, la vérification génère un échec de recherche.

Correction

Pour bloquer l'accès public à votre compartiment CloudTrail S3, consultez la section Configuration des paramètres de blocage de l'accès public pour vos compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service. Sélectionnez les quatre paramètres d'accès public par bloc d'Amazon S3.

[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/22.6, CIS AWS Foundations Benchmark v1.4. 0/32.6, CIS AWS Foundations Benchmark v3.0. 0/34., PCI DSS version 4.0. 1/10.2.1

Catégorie : Identifier - Journalisation

Gravité : Faible

Type de ressource : `AWS::S3::Bucket`

AWS Configrègle : Aucune (règle CSPM personnalisée de Security Hub)

Type de calendrier : Périodique

Paramètres : Aucun

La journalisation des accès au compartiment S3 génère un journal qui contient les enregistrements d'accès pour chaque demande envoyée à votre compartiment S3. Un enregistrement du journal d'accès contient des détails sur la demande, tels que le type de demande, les ressources spécifiées dans la demande utilisée, ainsi que l'heure et la date du traitement de la demande.

Le CIS vous recommande d'activer la journalisation des accès au compartiment sur le compartiment CloudTrail S3.

En activant la journalisation des accès aux compartiments S3 cibles, vous pouvez capturer tous les événements susceptibles d'affecter les objets dans un compartiment cible. Si les journaux sont configurés pour être placés dans un compartiment distinct, il est possible d'accéder aux informations qu'ils contiennent, qui peuvent s'avérer utiles dans les flux de travail de sécurité et de réponse aux incidents.

Pour exécuter cette vérification, Security Hub CSPM utilise d'abord une logique personnalisée pour rechercher le compartiment dans lequel vos CloudTrail journaux sont stockés, puis utilise la règle AWS Config gérée pour vérifier si la journalisation est activée.

S'il CloudTrail fournit des fichiers journaux provenant de plusieurs compartiments Comptes AWS vers un seul compartiment Amazon S3 de destination, Security Hub CSPM évalue ce contrôle uniquement par rapport au compartiment de destination de la région où il se trouve. Cela rationalise vos résultats. Toutefois, vous devez l'activer CloudTrail dans tous les comptes qui fournissent des journaux au compartiment de destination. Pour tous les comptes, à l'exception de celui qui contient le compartiment de destination, le statut de contrôle est Aucune donnée.

Correction

Pour activer la journalisation de l'accès au serveur pour votre compartiment CloudTrail S3, consultez la section Activation de la journalisation de l'accès au serveur Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[CloudTrail.9] les CloudTrail sentiers doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::CloudTrail::Trail`

AWS Configrègle : `tagged-cloudtrail-trail` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS CloudTrail parcours possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le parcours ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le parcours n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un CloudTrail parcours, reportez-vous AddTagsà la référence de l'AWS CloudTrailAPI.

[CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys

Exigences associées : NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::CloudTrail::EventDataStore`

Règle AWS Config : event-data-store-cmk-encryption-enabled

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`kmsKeyArns`	Une liste des Amazon Resource	StringList (maximum de 3 articles)	1 à 3 ARN de clés KMS existantes.	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Names (ARN) AWS KMS keys à inclure dans l'évaluation. Le contrôle permet de déterminer `FAILED` si un magasin de données d'événements n'est pas chiffré avec une clé KMS dans la liste.		Par exemple : `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	

Ce contrôle vérifie si un magasin de données d'événements AWS CloudTrail Lake est chiffré au repos et qu'il est géré par un clientAWS KMS key. Le contrôle échoue si le magasin de données d'événements n'est pas chiffré à l'aide d'une clé KMS gérée par le client. Vous pouvez éventuellement spécifier une liste de clés KMS que le contrôle doit inclure dans l'évaluation.

Par défaut, AWS CloudTrail Lake chiffre les magasins de données d'événements avec des clés gérées par Amazon S3 (SSE-S3), à l'aide d'un AES-256 algorithme. Pour un contrôle supplémentaire, vous pouvez configurer CloudTrail Lake pour crypter un magasin de données d'événements avec un fichier géré par le client AWS KMS key (SSE-KMS) à la place. Une clé KMS gérée par le client est une clé AWS KMS key que vous créez, détenez et gérez dans votreCompte AWS. Vous avez un contrôle total sur ce type de clé KMS. Cela inclut la définition et le maintien de la politique des clés, la gestion des subventions, la rotation du matériel cryptographique, l'attribution de balises, la création d'alias, ainsi que l'activation et la désactivation de la clé. Vous pouvez utiliser une clé KMS gérée par le client dans le cadre des opérations de chiffrement de vos CloudTrail données et auditer l'utilisation à l'aide de CloudTrail journaux.

Correction

Pour plus d'informations sur le chiffrement d'un magasin de données d'événements AWS CloudTrail Lake avec un AWS KMS key que vous spécifiez, voir Mettre à jour un magasin de données d'événements dans le Guide de l'AWS CloudTrailutilisateur. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

Contrôles CSPM de Security Hub pour Amazon CloudWatch

Ces AWS Security Hub CSPM contrôles évaluent le CloudWatch service et les ressources Amazon. Les commandes ne sont peut-être pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/1.1, CIS AWS Foundations Benchmark v1.2. 0/3.3, CIS AWS Foundations Benchmark v1.4. 0/1.7, CIS AWS Foundations Benchmark v1.4. 0/4.3, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/72.1.1

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

L'utilisateur root dispose d'un accès illimité à tous les services et ressources d'un Compte AWS. Nous vous recommandons vivement d'éviter d'utiliser l'utilisateur root pour les tâches quotidiennes. La réduction de l'utilisation de l'utilisateur root et l'adoption du principe du moindre privilège pour la gestion des accès réduisent le risque de modifications accidentelles et de divulgation involontaire d'informations d'identification hautement privilégiées.

Il est recommandé d'utiliser vos informations d'identification d'utilisateur root uniquement lorsque cela est nécessaire pour effectuer des tâches de gestion des comptes et des services. Appliquez les

politiques Gestion des identités et des accès AWS (IAM) directement aux groupes et aux rôles, mais pas aux utilisateurs. Pour un didacticiel sur la configuration d'un administrateur pour une utilisation quotidienne, consultez la section Création de votre premier utilisateur et groupe d'administrateurs IAM dans le Guide de l'utilisateur IAM.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 1.7 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez

consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**

Champ	Value
Valeur par défaut	**0**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *your-metric-name* c'est...	Greater/Equal
que...	**1**

[CloudWatch.2] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les appels d'API non autorisés

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.1, NIST.800-171.r2 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme pour les appels d'API non autorisés. La surveillance des appels d'API non autorisés contribue à révéler les erreurs d'application et à détecter plus rapidement les opérations malveillantes.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 3.1 dans le CIS AWS Foundations Benchmark v1.2. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez

consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**

Champ	Value
Valeur par défaut	**0**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *your-metric-name* c'est...	Greater/Equal
que...	**1**

[CloudWatch.3] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la connexion à la console de gestion sans MFA

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/32.

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et des connexions à la console d'alarme qui ne sont pas protégées par l'authentification multifacteur. La surveillance des connexions à un seul facteur à la console améliore la visibilité sur les comptes qui ne sont pas protégés par un MFA.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 3.2 dans le CIS AWS Foundations Benchmark v1.2. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez

consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`

Champ	Value
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.4, indice de référence CIS AWS Foundations v1.4. 0/44, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si vous surveillez les appels d'API en temps réel en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux politiques IAM. Ceci permet de s'assurer que les contrôles d'authentification et d'autorisation restent inchangés.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Note

Le modèle de filtre que nous recommandons dans ces étapes de remédiation diffère de celui indiqué dans les directives du CIS. Nos filtres recommandés ciblent uniquement les événements provenant d'appels d'API IAM.

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventN`

Champ	Value
	`ame=DeleteRolePolicy) || ($.eventName=DeleteUserPolicy) \|\| ($.eventName=PutGroupPolicy) || ($.eventName=PutRo lePolicy) \|\| ($.eventName=PutUs erPolicy) || ($.eventName=Creat ePolicy) \|\| ($.eventName=Delet ePolicy) || ($.eventName=Creat ePolicyVersion) \|\| ($.eventN ame=DeletePolicyVersion) || ($.eventName=AttachRolePoli cy) \|\| ($.eventName=Detac hRolePolicy) || ($.eventN ame=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPol icy) \|\| ($.eventName=Detac hGroupPolicy))}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal

Champ	Value
que...	**1**

[CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.5, CIS AWS Foundations Benchmark v1.4. 0/4.5, NIST.800-171.r2 3.3.8, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux paramètres CloudTrail de configuration. Ceci permet de garantir une visibilité constante sur les activités du compte.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.5 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

> **Note**
>
> Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à

un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal

Champ	Value
que...	**1**

[CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.6, CIS AWS Foundations Benchmark v1.4. 0/4.6, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme en cas d'échec des tentatives d'authentification de la console. La surveillance des échecs de connexion à la console peut contribuer à réduire les délais de détection d'une tentative de connexion en force, ce qui peut fournir un indicateur, telle une adresse IP source, qui pourra servir dans d'autres corrélations d'événements.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.6 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

> **Note**
>
> Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à

un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.7, CIS AWS Foundations Benchmark v1.4. 0/4.7, NIST.800-171.r2 3.13.10, 3.13.16, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme pour les clés gérées par le client qui ont changé d'état pour devenir désactivées ou dont la suppression est programmée. Les données chiffrées avec des clés désactivées ou supprimées ne sont plus accessibles.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.7 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique. Le contrôle échoue également s'il `ExcludeManagementEventSources` contient`kms.amazonaws.com`.

> **Note**
>
> Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
> Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service.

Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.

2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.

3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.8, CIS AWS Foundations Benchmark v1.4. 0/4.8, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux politiques des compartiments S3. La surveillance de ces modifications peut contribuer à réduire les délais de détection et de correction des stratégies permissives associées aux compartiments S3 sensibles.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.8 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

> **Note**
>
> Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
> Le contrôle donne des `FAILED` résultats dans les cas suivants :
>
> - Aucune piste n'est configurée.

- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.

2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.

3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *your-metric-name* c'est...	Greater/Equal
que...	**1**

[CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.9, CIS AWS Foundations Benchmark v1.4. 0/4.9, NIST.800-171.r2 3.3.8, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux paramètres AWS Config de configuration. La surveillance de ces modifications permet de garantir une visibilité constante sur les éléments de configuration du compte.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.9 dans le CIS AWS Foundations Benchmark

v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant.

`ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, voir Créer un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *your-metric-name* c'est...	Greater/Equal
que...	**1**

[CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.10, CIS AWS Foundations Benchmark v1.4. 0/41.0, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants. Les groupes de sécurité constituent un filtre de paquet avec état qui contrôle le trafic entrant et sortant dans un VPC.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux groupes de sécurité. La surveillance de ces modifications permet de s'assurer que les ressources et les services ne sont pas involontairement exposés.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.10 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez

consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) ||`

Champ	Value
	`($.eventName=DeleteSecurity Group)}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/31.1, CIS AWS Foundations Benchmark v1.4. 0/41.1, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants. Les ACL réseau sont utilisées comme un filtre de paquet sans état pour contrôler le trafic entrant et sortant des sous-réseaux dans un VPC.

Le CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux NACL. La surveillance de ces modifications permet de s'assurer que AWS les ressources et les services ne sont pas exposés involontairement.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.11 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué.

L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventN`

Champ	Value
	`ame=DeleteNetworkAcl) || ($.eventName=DeleteNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclEntry) || ($.eventName=ReplaceNetworkAclAssociation)}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/31.2, CIS AWS Foundations Benchmark v1.4. 0/41.2, NIST.800-171.r2 3.3.1, 3.13.1 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants. Les passerelles réseau permettent d'envoyer et de recevoir le trafic vers une destination en dehors d'un VPC.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux passerelles réseau. La surveillance de ces modifications permet de s'assurer que tout le trafic entrant et sortant traverse le VPC par un chemin d'accès contrôlé.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.12 dans le CIS AWS Foundations Benchmark v1.2. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

> **Note**
>
> Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
> Le contrôle donne des `FAILED` résultats dans les cas suivants :
>
> - Aucune piste n'est configurée.
> - Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.
>
> La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :
>
> - Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.

- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.

3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/3.13, CIS AWS Foundations Benchmark v1.4. 0/4.13, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si vous surveillez les appels d'API en temps réel en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants. Les tables de routage acheminent le trafic réseau entre les sous-réseaux et vers les passerelles réseau.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux tables de routage. La surveillance de ces modifications permet de s'assurer que l'ensemble du trafic du VPC passe par un chemin d'accès attendu.

> **Note**
>
> Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
> Le contrôle donne des `FAILED` résultats dans les cas suivants :
>
> - Aucune piste n'est configurée.
> - Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Note

Le modèle de filtre que nous recommandons dans ces étapes de remédiation diffère de celui indiqué dans les directives du CIS. Nos filtres recommandés ciblent uniquement les événements provenant des appels d'API Amazon Elastic Compute Cloud (EC2).

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *your-metric-name* c'est...	Greater/Equal
que...	**1**

[CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/31.4, CIS AWS Foundations Benchmark v1.4. 0/41.4, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres : Aucun

Vous pouvez surveiller en temps réel les appels d'API en dirigeant CloudTrail les journaux vers les CloudWatch journaux et en établissant des filtres métriques et des alarmes correspondants. Un compte peut comprendre plusieurs VPC et vous pouvez créer une connexion d'appairage entre deux VPC, ce qui permet au trafic réseau de s'acheminer entre eux.

CIS vous recommande de créer un filtre métrique et une alarme pour les modifications apportées aux VPC. Ceci permet de s'assurer que les contrôles d'authentification et d'autorisation restent inchangés.

Pour exécuter cette vérification, Security Hub CSPM utilise une logique personnalisée pour effectuer les étapes d'audit exactes prescrites pour le contrôle 4.14 dans le CIS AWS Foundations Benchmark v1.4.0. Ce contrôle échoue si les filtres de métrique exacts prescrits par CIS ne sont pas utilisés. Des champs ou des termes supplémentaires ne peuvent pas être ajoutés aux filtres de métrique.

Note

Lorsque Security Hub CSPM vérifie ce contrôle, il recherche les CloudTrail traces utilisées par le compte actuel. Ces parcours peuvent être des parcours d'organisation appartenant à un autre compte. Multi-Region les sentiers peuvent également être basés dans une région différente.
Le contrôle donne des `FAILED` résultats dans les cas suivants :

- Aucune piste n'est configurée.
- Les sentiers disponibles qui se trouvent dans la région actuelle et qui sont détenus par un compte courant ne répondent pas aux exigences de contrôle.

La vérification aboutit à un état de contrôle `NO_DATA` dans les cas suivants :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un autre compte. Security Hub CSPM ne peut générer des résultats que pour le compte propriétaire du trail.

  Il est recommandé d'utiliser les journaux d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les pistes d'organisation sont des pistes multirégionales par défaut et ne peuvent être gérées que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation d'un journal d'organisation permet d'obtenir un statut de contrôle égal à `NO_DATA` celui des contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes des membres, Security Hub CSPM génère des résultats uniquement pour les ressources appartenant aux membres. Les résultats relatifs aux pistes d'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué CSPM Security Hub à l'aide de l'agrégation interrégionale.

Pour déclencher l'alarme, le compte actuel doit soit être propriétaire de la rubrique Amazon SNS référencée, soit accéder à la rubrique Amazon SNS en appelant. `ListSubscriptionsByTopic` Sinon, Security Hub CSPM génère des `WARNING` résultats pour le contrôle.

Correction

Pour passer ce contrôle, procédez comme suit pour créer une rubrique Amazon SNS, un AWS CloudTrail journal, un filtre métrique et une alarme pour le filtre métrique.

1. Créer une rubrique Amazon SNS. Pour obtenir des instructions, consultez la section Premiers pas avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service. Créez une rubrique qui reçoit toutes les alarmes CIS et créez au moins un abonnement à cette rubrique.
2. Créez un CloudTrail parcours qui s'applique à tous Régions AWS. Pour obtenir des instructions, consultez la section Création d'un parcours dans le Guide de AWS CloudTrail l'utilisateur.

   Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail trail. Vous créez le filtre métrique pour ce groupe de journaux à l'étape suivante.
3. Créez un filtre de métrique. Pour obtenir des instructions, consultez la section Création d'un filtre métrique pour un groupe de journaux dans le Guide de CloudWatch l'utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Définir le modèle, Filtrer le modèle	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) ||`

Champ	Value
	`($.eventName=AttachClassicLinkVpc) \|\| ($.eventName=DetachClassicLinkVpc) || ($.eventName=DisableVpcClassicLink) \|\| ($.eventName=EnableVpcClassicLink)}`
Espace de noms métrique	**`LogMetrics`**
Valeur de la métrique	**`1`**
Valeur par défaut	**`0`**

4. Créez une alarme en fonction du filtre. Pour obtenir des instructions, voir Créer une CloudWatch alarme basée sur un filtre métrique de groupe de journaux dans le Guide de l' CloudWatch utilisateur Amazon. Utilisez les valeurs suivantes :

Champ	Value
Conditions, type de seuil	Statique
Chaque fois que *`your-metric-name`* c'est...	Greater/Equal
que...	**`1`**

[CloudWatch.15] CloudWatch les actions spécifiées doivent être configurées pour les alarmes

Exigences connexes : NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (1), NIST.800-53.r5 IR-4 (5),, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.3.4, NIST.800-171.r2 3.14.6

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::CloudWatch::Alarm`

AWS Config règle : `cloudwatch-alarm-action-check`

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`alarmActionRequired`	La commande détermine si `PASSED` le paramètre est réglé sur `true` et si l'alarme agit lorsque l'état de l'alarme passe à`ALARM`.	Booléen	Non personnalisable	`true`
`insufficientDataActionRequired`	La commande détermine si `PASSED` le paramètre est réglé sur `true` et si l'alarme agit lorsque l'état de l'alarme passe à`INSUFFICIENT_DATA` .	Booléen	`true` ou `false`	`false`
`okActionRequired`	La commande détermine si `PASSED` le paramètre est réglé sur `true` et si l'alarme agit lorsque l'état de l'alarme passe à`OK`.	Booléen	`true` ou `false`	`false`

Ce contrôle vérifie si au moins une action est configurée pour l'`ALARM`état d'une CloudWatch alarme Amazon. Le contrôle échoue si aucune action de l'alarme n'est configurée pour `ALARM` cet état. Vous pouvez éventuellement inclure des valeurs de paramètres personnalisées pour exiger également des actions d'alarme pour les `OK` états `INSUFFICIENT_DATA` ou.

> **Note**
>
> Security Hub CSPM évalue ce contrôle sur CloudWatch la base d'alarmes métriques. Les alarmes métriques peuvent faire partie d'alarmes composites pour lesquelles les actions spécifiées sont configurées. Le contrôle génère `FAILED` des résultats dans les cas suivants :
>
> - Les actions spécifiées ne sont pas configurées pour une alarme métrique.
> - L'alarme métrique fait partie d'une alarme composite dont les actions spécifiées sont configurées.

Ce contrôle permet de déterminer si une action CloudWatch d'alarme est configurée pour une alarme, tout en CloudWatch.17 se concentrant sur l'état d'activation d'une action CloudWatch d'alarme.

Nous recommandons des actions CloudWatch d'alarme pour vous avertir automatiquement lorsqu'une métrique surveillée dépasse le seuil défini. Les alarmes de surveillance vous aident à identifier les activités inhabituelles et à réagir rapidement aux problèmes de sécurité et de fonctionnement lorsqu'une alarme passe dans un état spécifique. Le type d'action d'alarme le plus courant consiste à avertir un ou plusieurs utilisateurs en envoyant un message à une rubrique Amazon Simple Notification Service (Amazon SNS).

Correction

Pour plus d'informations sur les actions prises en charge par CloudWatch les alarmes, consultez la section Actions d'alarme dans le Guide de CloudWatch l'utilisateur Amazon.

[CloudWatch.16] les groupes de CloudWatch journaux doivent être conservés pendant une période spécifiée

Catégorie : Identifier - Journalisation

Exigences connexes : NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Gravité : Moyenne

Type de ressource : `AWS::Logs::LogGroup`

AWS Config règle : `cw-loggroup-retention-period-check`

Type de programme : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM	
`minRetentionTime`	Durée de conservation minimale en jours pour les groupes de CloudWatch journaux	Enum	`365, 400, 545, 731, 1827, 3653`	`365`	

Ce contrôle vérifie si la période de conservation d'un groupe de CloudWatch journaux Amazon est d'au moins le nombre de jours spécifié. Le contrôle échoue si la durée de conservation est inférieure au nombre spécifié. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de rétention, Security Hub CSPM utilise une valeur par défaut de 365 jours.

CloudWatch Les journaux centralisent les journaux de tous vos systèmes et applications Services AWS au sein d'un service unique et hautement évolutif. Vous pouvez utiliser CloudWatch Logs pour surveiller, stocker et accéder à vos fichiers journaux à partir d'instances Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, d'Amazon Route 53 et d'autres sources. La conservation de vos journaux pendant au moins un an peut vous aider à vous conformer aux normes de conservation des journaux.

Correction

Pour configurer les paramètres de conservation des journaux, voir Modifier la conservation des données des CloudWatch journaux dans Logs in the Amazon CloudWatch User Guide.

[CloudWatch.17] les actions CloudWatch d'alarme doivent être activées

Catégorie : Détecter - Services de détection

Exigences connexes : NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12)

Gravité : Élevée

Type de ressource : `AWS::CloudWatch::Alarm`

AWS Config règle : `cloudwatch-alarm-action-enabled-check`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Cette commande vérifie si les actions CloudWatch d'alarme sont activées (`ActionEnabled`doit être réglée sur true). La commande échoue si l'action d'alarme associée à une CloudWatch alarme est désactivée.

> **Note**
>
> Security Hub CSPM évalue ce contrôle sur CloudWatch la base d'alarmes métriques. Les alarmes métriques peuvent faire partie d'alarmes composites dont les actions d'alarme sont activées. Le contrôle génère `FAILED` des résultats dans les cas suivants :
>
> - Les actions spécifiées ne sont pas configurées pour une alarme métrique.
> - L'alarme métrique fait partie d'une alarme composite dont les actions d'alarme sont activées.

Ce contrôle se concentre sur l'état d'activation d'une action CloudWatch d'alarme, tout en se CloudWatch.15 concentrant sur la question de savoir si une `ALARM` action est configurée dans une CloudWatch alarme.

Les actions d'alarme vous alertent automatiquement lorsqu'une métrique surveillée dépasse le seuil défini. Si l'action d'alarme est désactivée, aucune action n'est exécutée lorsque l'alarme change d'état et vous ne serez pas alerté des modifications des mesures surveillées. Nous vous recommandons CloudWatch d'activer les actions d'alarme pour vous aider à réagir rapidement aux problèmes de sécurité et de fonctionnement.

Correction

Pour activer une action CloudWatch d'alarme (console)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, sous Alarmes, sélectionnez Toutes les alarmes.

3. Sélectionnez l'alarme pour laquelle vous souhaitez activer des actions.
4. Pour Actions, choisissez Actions d'alarme : nouvelles, puis choisissez Activer.

Pour plus d'informations sur l'activation des actions CloudWatch d'alarme, consultez la section Actions d'alarme dans le Guide de CloudWatch l'utilisateur Amazon.

Contrôles Security Hub CSPM pour CodeArtifact

Ces contrôles CSPM du Security Hub évaluent le AWS CodeArtifact service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CodeArtifact.1] les CodeArtifact référentiels doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::CodeArtifact::Repository`

AWS Configrègle : `tagged-codeartifact-repository` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS CodeArtifact dépôt possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le référentiel ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le référentiel n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un CodeArtifact référentiel, voir Marquer un référentiel CodeArtifact dans le Guide de AWS CodeArtifact l'utilisateur.

Contrôles Security Hub CSPM pour CodeBuild

Ces contrôles CSPM du Security Hub évaluent le AWS CodeBuild service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles

Exigences associées : NIST.800-53.r5 SA-3 PCI DSS v3.2. 1/82.2.1, PCI DSS v4.0. 1/8.3.2

Catégorie : Protéger - Développement sécurisé

Gravité : Critique

Type de ressource : `AWS::CodeBuild::Project`

Règle AWS Config : `codebuild-project-source-repo-url-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si l'URL du référentiel source Bitbucket d'un AWS CodeBuild projet contient des jetons d'accès personnels ou un nom d'utilisateur et un mot de passe. Le contrôle échoue si l'URL du référentiel source de Bitbucket contient des jetons d'accès personnels ou un nom d'utilisateur et un mot de passe.

> **Note**
>
> Ce contrôle évalue à la fois la source principale et les sources secondaires d'un projet de CodeBuild construction. Pour plus d'informations sur les sources de projet, consultez l'exemple de sources d'entrée multiples et d'artefacts de sortie dans le guide de AWS CodeBuild l'utilisateur.

Sign-in les informations d'identification ne doivent pas être stockées ou transmises en texte clair ni apparaître dans l'URL du référentiel source. Au lieu d'utiliser des jetons d'accès personnels ou des identifiants de connexion, vous devez accéder à votre fournisseur source et modifier l'URL de votre dépôt source pour qu'elle ne contienne que le chemin d'accès à l'emplacement du référentiel Bitbucket. CodeBuild L'utilisation de jetons d'accès personnels ou d'identifiants de connexion peut entraîner une exposition involontaire aux données ou un accès non autorisé.

Correction

Vous pouvez mettre à jour votre CodeBuild projet pour utiliser OAuth.

Pour supprimer le jeton d'accès personnel/(GitHub) d'authentification de base de la source du CodeBuild projet

1. Ouvrez la CodeBuild console à l'adresse https://console.aws.amazon.com/codebuild/.
2. Sélectionnez votre projet de génération qui contient des jetons d'accès personnels ou un nom d'utilisateur et un mot de passe
3. Dans Edit (Modifier), choisissez Source.
4. Choisissez Déconnecter de GitHub /Bitbucket.
5. Choisissez Connect using OAuth, puis Connect to GitHub/Bitbucket.
6. Lorsque vous y êtes invité, choisissez authorize as appropriate (autoriser le cas échéant).
7. Reconfigurez l'URL du référentiel et les paramètres de configuration supplémentaire si nécessaire.
8. Choisissez Mettre à jour la source.

Pour plus d'informations, reportez-vous aux exemples d'CodeBuild utilisation basés sur des cas dans le Guide de l'AWS CodeBuildutilisateur.

[CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair

Exigences associées : NIST.800-53.r5 IA-5 (7) NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/82.2.1, PCI DSS v4.0. 1/8.3.2

Catégorie : Protéger - Développement sécurisé

Gravité : Critique

Type de ressource : `AWS::CodeBuild::Project`

Règle AWS Config : `codebuild-project-envvar-awscred-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le projet contient des variables d'environnement `AWS_ACCESS_KEY_ID` et `AWS_SECRET_ACCESS_KEY`.

Les informations d'identification `AWS_ACCESS_KEY_ID` et `AWS_SECRET_ACCESS_KEY` ne doivent jamais être stockées en texte clair, car cela pourrait conduire à une exposition involontaire des données et un accès non autorisé.

Correction

Pour supprimer des variables d'environnement d'un CodeBuild projet, voir Modifier les paramètres d'un projet de construction AWS CodeBuild dans le Guide de AWS CodeBuild l'utilisateur. Assurez-vous que rien n'est sélectionné pour les variables d'environnement.

Vous pouvez stocker des variables d'environnement contenant des valeurs sensibles dans le magasin de AWS Systems Manager paramètres ou AWS Secrets Manager les récupérer à partir de vos spécifications de construction. Pour obtenir des instructions, reportez-vous à la case intitulée Important dans la section Environnement du guide de AWS CodeBuild l'utilisateur.

[CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/10.3.2

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Faible

Type de ressource : `AWS::CodeBuild::Project`

Règle AWS Config : `codebuild-project-s3-logs-encrypted`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les journaux Amazon S3 d'un AWS CodeBuild projet sont chiffrés. Le contrôle échoue si le chiffrement est désactivé pour les journaux S3 d'un CodeBuild projet.

Le chiffrement des données au repos est une bonne pratique recommandée pour ajouter une couche de gestion des accès à vos données. Le chiffrement des journaux au repos réduit le risque qu'un utilisateur non authentifié AWS accède aux données stockées sur le disque. Il ajoute un autre ensemble de contrôles d'accès pour limiter la capacité des utilisateurs non autorisés à accéder aux données.

Correction

Pour modifier les paramètres de chiffrement des journaux CodeBuild du projet S3, voir Modifier les paramètres d'un projet de génération AWS CodeBuild dans le Guide de AWS CodeBuild l'utilisateur.

[CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée

Exigences connexes : NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::CodeBuild::Project`

Règle AWS Config : `codebuild-project-logging-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un environnement de CodeBuild projet dispose d'au moins une option de journalisation, soit vers S3, soit avec CloudWatch les journaux activés. Ce contrôle échoue si au moins une option de journalisation n'est pas activée dans un environnement de CodeBuild projet.

Du point de vue de la sécurité, la journalisation est une fonctionnalité importante pour permettre les futurs efforts de criminalistique en cas d'incident de sécurité. La corrélation entre les anomalies des CodeBuild projets et les détections de menaces peut accroître la confiance dans la précision de ces détections de menaces.

Correction

Pour plus d'informations sur la configuration des paramètres CodeBuild du journal de projet, voir Créer un projet de génération (console) dans le guide de CodeBuild l'utilisateur.

[CodeBuild.5] le mode privilégié ne doit pas être activé dans les environnements de CodeBuild projet

> **Important**
>
> Security Hub CSPM a retiré ce contrôle en avril 2024. Pour de plus amples informations, veuillez consulter Journal des modifications pour les contrôles CSPM de Security Hub.

Exigences associées : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Catégorie : Protéger > Gestion des accès sécurisés

Gravité : Élevée

Type de ressource : `AWS::CodeBuild::Project`

Règle AWS Config : `codebuild-project-environment-privileged-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le mode privilégié est activé ou désactivé dans un environnement de AWS CodeBuild projet. Le contrôle échoue si le mode privilégié est activé dans un environnement de CodeBuild projet.

Par défaut, les conteneurs Docker n'autorisent l'accès à aucun périphérique. Le mode privilégié accorde un accès au conteneur Docker d'un projet de génération à tous les périphériques. Le réglage `privilegedMode` avec une valeur `true` permet au démon Docker de s'exécuter dans un conteneur Docker. Le démon Docker écoute les demandes d'API Docker et gère les objets Docker tels que les images, les conteneurs, les réseaux et les volumes. Ce paramètre ne doit être défini sur true que si le projet de génération est utilisé pour créer des images Docker. Dans le cas contraire, ce paramètre doit être désactivé pour empêcher tout accès involontaire aux API Docker ainsi qu'au matériel sous-jacent du conteneur. Le réglage `privilegedMode` sur `false` permet de protéger les ressources critiques contre la falsification et la suppression.

Correction

Pour configurer les paramètres d'environnement CodeBuild du projet, voir Création d'un projet de génération (console) dans le guide de CodeBuild l'utilisateur. Dans la section Environnement, ne sélectionnez pas le paramètre Privileged.

[CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::CodeBuild::ReportGroup`

Règle AWS Config : `codebuild-report-group-encrypted-at-rest`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les résultats des tests d'un groupe de AWS CodeBuild rapports exportés vers un bucket Amazon Simple Storage Service (Amazon S3) sont chiffrés au repos. Le contrôle échoue si l'exportation du groupe de rapports n'est pas cryptée au repos.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour chiffrer l'exportation du groupe de rapports vers S3, voir Mettre à jour un groupe de rapports dans le Guide de l'AWS CodeBuildutilisateur.

Contrôles Security Hub CSPM pour Amazon Profiler CodeGuru

Ces contrôles Security Hub CSPM évaluent le service et les ressources Amazon CodeGuru Profiler.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::CodeGuruProfiler::ProfilingGroup`

Règle AWS Config : `codeguruprofiler-profiling-group-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de CodeGuru profilage Amazon Profiler possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le groupe de profilage ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de profilage n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond

à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un groupe de profilage CodeGuru Profiler, consultez la section Marquage des groupes de profilage dans le guide de l'utilisateur d'Amazon CodeGuru Profiler.

Contrôles CSPM du Security Hub pour Amazon Reviewer CodeGuru

Ces contrôles Security Hub CSPM évaluent le service et les ressources Amazon CodeGuru Reviewer.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::CodeGuruReviewer::RepositoryAssociation`

Règle AWS Config : `codegurureviewer-repository-association-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une association de référentiel Amazon CodeGuru Reviewer possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'association du référentiel ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'association du référentiel n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une association de référentiel CodeGuru Reviewer, consultez la section Marquage d'une association de référentiel dans le guide de l'utilisateur Amazon CodeGuru Reviewer.

Contrôles CSPM de Security Hub pour Amazon Cognito

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Cognito. Les commandes ne sont peut-être pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::Cognito::UserPool`

Règle AWS Config : cognito-user-pool-advanced-security-enabled

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`SecurityMode`	Mode d'application de la protection contre les menaces que le contrôle vérifie.	Chaîne	`AUDIT`, `ENFORCED`	`ENFORCED`

Ce contrôle vérifie si la protection contre les menaces d'un groupe d'utilisateurs Amazon Cognito est activée avec le mode d'application réglé sur Fonctionnalité complète pour l'authentification standard. Le contrôle échoue si la protection contre les menaces du pool d'utilisateurs est désactivée ou si le mode d'application n'est pas réglé sur une fonction complète pour l'authentification standard. À moins que vous ne fournissiez des valeurs de paramètres personnalisées, Security Hub CSPM utilise la valeur par défaut de `ENFORCED` for enforcement mode réglé sur Full function pour l'authentification standard.

Après avoir créé un groupe d'utilisateurs Amazon Cognito, vous pouvez activer la protection contre les menaces et personnaliser les actions entreprises en réponse aux différents risques. Vous pouvez également utiliser le mode audit pour recueillir des mesures sur les risques détectés sans appliquer de mesures d'atténuation de sécurité. En mode audit, la protection contre les menaces publie des métriques sur Amazon CloudWatch. Vous pouvez consulter les statistiques une fois qu'Amazon Cognito a généré son premier événement.

Correction

Pour plus d'informations sur l'activation de la protection contre les menaces pour un groupe d'utilisateurs Amazon Cognito, consultez la section Sécurité avancée avec protection contre les menaces dans le guide du développeur Amazon Cognito.

[Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées

Catégorie : Protéger > Gestion sécurisée des accès > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::Cognito::IdentityPool`

Règle AWS Config : cognito-identity-pool-unauth-access-check

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un pool d'identités Amazon Cognito est configuré pour autoriser les identités non authentifiées. Le contrôle échoue si l'accès invité est activé (le `AllowUnauthenticatedIdentities` paramètre est défini sur`true`) pour le pool d'identités.

Si un pool d'identités Amazon Cognito autorise des identités non authentifiées, il fournit des informations d' AWS identification temporaires aux utilisateurs qui ne se sont pas authentifiés via un fournisseur d'identité (invités). Cela crée des risques de sécurité car cela permet un accès anonyme aux AWS ressources. Si vous désactivez l'accès invité, vous pouvez vous assurer que seuls les utilisateurs correctement authentifiés peuvent accéder à vos AWS ressources, ce qui réduit le risque d'accès non autorisé et de failles de sécurité potentielles. Il est recommandé qu'un pool d'identités nécessite une authentification par le biais de fournisseurs d'identité pris en charge. Si un accès non authentifié est nécessaire, il est important de restreindre soigneusement les autorisations pour les identités non authentifiées et de vérifier et surveiller régulièrement leur utilisation.

Correction

Pour plus d'informations sur la désactivation de l'accès invité pour un pool d'identités Amazon Cognito, consultez la section Activer ou désactiver l'accès invité dans le manuel Amazon Cognito Developer Guide.

[Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::Cognito::UserPool`

Règle AWS Config : cognito-user-pool-password-policy-check

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`minLength`	Le nombre minimum de caractères qu'un mot de passe doit contenir.	Entier	8 sur 99	8
`requireLowercase`	Le mot de passe doit contenir au moins une minuscule.	Booléen	`True`, `False`	`True`
`requireUppercase`	Le mot de passe doit contenir au moins une majuscule.	Booléen	`True`, `False`	`True`
`requireNumbers`	Exiger au moins un chiffre dans le mot de passe.	Booléen	`True`, `False`	`True`
`requireSymbols`	Exiger au moins un symbole dans le mot de passe.	Booléen	`True`, `False`	`True`
`temporaryPasswordValidity`	Le nombre maximum de jours pendant lesquels un mot de passe peut exister avant son expiration.	Entier	1 sur 365	7

Ce contrôle vérifie si la politique de mot de passe d'un groupe d'utilisateurs Amazon Cognito nécessite l'utilisation de mots de passe complexes, en fonction des paramètres recommandés pour les politiques de mot de passe. Le contrôle échoue si la politique de mot de passe pour le groupe d'utilisateurs ne nécessite pas de mots de passe complexes. Vous pouvez éventuellement spécifier des valeurs personnalisées pour les paramètres de politique vérifiés par le contrôle.

Les mots de passe complexes constituent une bonne pratique en matière de sécurité pour les groupes d'utilisateurs Amazon Cognito. Les mots de passe faibles peuvent exposer les informations d'identification des utilisateurs à des systèmes qui devinent les mots de passe et tentent d'accéder aux données. C'est notamment le cas pour les applications ouvertes sur Internet. Les politiques relatives aux mots de passe constituent un élément central de la sécurité des annuaires d'utilisateurs.

À l'aide d'une politique de mot de passe, vous pouvez configurer un groupe d'utilisateurs pour exiger la complexité des mots de passe et d'autres paramètres conformes à vos normes et exigences de sécurité.

Correction

Pour plus d'informations sur la création ou la mise à jour de la politique de mot de passe pour un groupe d'utilisateurs Amazon Cognito, consultez la section Ajouter des exigences de mot de passe à un groupe d'utilisateurs dans le guide du développeur Amazon Cognito.

[Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::Cognito::UserPool`

Règle AWS Config : cognito-userpool-cust-auth-threat-full-check

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la protection contre les menaces est activée pour un groupe d'utilisateurs Amazon Cognito et si le mode d'application est réglé sur Fonction complète pour une authentification personnalisée. Le contrôle échoue si la protection contre les menaces est désactivée pour le groupe d'utilisateurs ou si le mode d'application n'est pas configuré pour fonctionner pleinement pour l'authentification personnalisée.

La protection contre les menaces, anciennement appelée fonctionnalités de sécurité avancées, est un ensemble d'outils de surveillance des activités indésirables au sein de votre groupe d'utilisateurs, ainsi que des outils de configuration pour arrêter automatiquement les activités potentiellement malveillantes. Après avoir créé un groupe d'utilisateurs Amazon Cognito, vous pouvez activer la protection contre les menaces avec le mode d'application complète des fonctions pour une authentification personnalisée et personnaliser les actions entreprises en réponse aux différents risques. Full-function Le mode inclut un ensemble de réactions automatiques pour détecter les activités indésirables et les mots de passe compromis.

Correction

Pour plus d'informations sur l'activation de la protection contre les menaces pour un groupe d'utilisateurs Amazon Cognito, consultez la section Sécurité avancée avec protection contre les menaces dans le guide du développeur Amazon Cognito.

[Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito

Catégorie : Protéger > Gestion sécurisée des accès > Multi-factor Authentification

Gravité : Moyenne

Type de ressource : `AWS::Cognito::UserPool`

Règle AWS Config : cognito-user-pool-mfa-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'authentification multifacteur (MFA) est activée pour un groupe d'utilisateurs Amazon Cognito configuré avec une politique de connexion par mot de passe uniquement. Le contrôle échoue si le groupe d'utilisateurs configuré avec une politique de connexion par mot de passe uniquement n'a pas activé l'authentification multifacteur.

Multi-factor L'authentification (MFA) ajoute un facteur d'authentification « quelque chose que vous avez » au facteur « quelque chose que vous connaissez » (généralement un nom d'utilisateur et un mot de passe). Pour les utilisateurs fédérés, Amazon Cognito délègue l'authentification au fournisseur d'identité (IdP) et ne propose pas de facteurs d'authentification supplémentaires. Toutefois, si vous avez des utilisateurs locaux dotés d'une authentification par mot de passe, la configuration de l'authentification multifacteur pour le groupe d'utilisateurs renforce leur sécurité.

> **Note**
>
> Ce contrôle ne s'applique pas aux utilisateurs fédérés et aux utilisateurs qui se connectent avec des facteurs sans mot de passe.

Correction

Pour plus d'informations sur la configuration de l'authentification multifacteur pour un groupe d'utilisateurs Amazon Cognito, consultez la section Ajouter l'authentification multifacteur à un groupe d'utilisateurs dans le guide du développeur Amazon Cognito.

[Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Moyenne

Type de ressource : `AWS::Cognito::UserPool`

Règle AWS Config : cognito-user-pool-deletion-protection-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la protection contre la suppression est activée pour un groupe d'utilisateurs Amazon Cognito. Le contrôle échoue si la protection contre la suppression est désactivée pour le groupe d'utilisateurs.

La protection contre la suppression permet de s'assurer que votre groupe d'utilisateurs n'est pas supprimé accidentellement. Lorsque vous configurez un groupe d'utilisateurs avec protection contre la suppression, aucun utilisateur ne peut le supprimer. La protection contre la suppression vous empêche de demander la suppression d'un groupe d'utilisateurs à moins que vous ne le modifiiez au préalable et que vous ne désactiviez la protection contre la suppression.

Correction

Pour configurer la protection contre la suppression pour un groupe d'utilisateurs Amazon Cognito, consultez la section Protection contre la suppression du groupe d'utilisateurs dans le guide du développeur Amazon Cognito.

Contrôles CSPM Security Hub pour AWS Config

Ces contrôles CSPM de Security Hub évaluent le AWS Config service et les ressources.

Il se peut que ces commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

> **Note**
>
> Lorsque Security Hub CSPM et Security Hub sont activés, la Config.1 règle aura toujours le statut PASSED. En effet, Security Hub CSPM dispose d'un accès direct aux éléments de configuration via un enregistreur de configuration lié à un service. Le paramètre de ce contrôle n'est pas applicable car l'enregistreur de configuration interne lié à un service est automatiquement créé avec le rôle lié à un AWS Config service. Pour de plus amples informations, veuillez consulter Utilisation de l'enregistreur de configuration lié au service. Les contrôles multicloud (tels que les contrôles Azure) et l'enregistrement des ressources qui leur est associé ne sont pas pris en compte dans les évaluations. Config.1 Les normes multicloud utilisent toujours un enregistreur de configuration interne lié à un service que le connecteur multicloud CSPM configure automatiquement, quel que soit l'état d'activation de Security Hub. L'enregistrement multicloud étant entièrement géré par le connecteur, il n'affecte pas l'état de Config.1 conformité. Config.1 évalue uniquement la configuration d'enregistrement AWS des ressources.

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/3.3, CIS AWS Foundations Benchmark v1.2. 0/2.5, CIS AWS Foundations Benchmark v1.4. 0/3.5, CIS AWS Foundations Benchmark v3.0. 0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1) NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (2), PCI DSS v3.2. 1/102.5.2, PCI DSS v3.2. 1/115.

Catégorie : Identifier - Inventaire

Gravité : Critique

Type de ressource : `AWS:::::Account`

AWS Config règle : Aucune (règle CSPM Security Hub personnalisée)

Type de programme : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`includeConfigServiceLinkedRoleCheck`	Le contrôle n'évalue pas si le rôle lié au service est AWS Config utilisé si le paramètre est défini sur. `false`	Booléen	`true` ou `false`	`true`

Ce contrôle vérifie s'il AWS Config est activé dans votre compte actuellement Région AWS, enregistre toutes les ressources correspondant aux contrôles activés dans la région actuelle et utilise le rôle lié à un service AWS Config . Le nom du rôle lié à un service est. AWSServiceRoleForConfig Si vous n'utilisez pas le rôle lié à un service et que vous ne définissez pas le `includeConfigServiceLinkedRoleCheck` paramètre sur`false`, le contrôle échoue car les autres rôles ne disposent peut-être pas des autorisations nécessaires AWS Config pour enregistrer correctement vos ressources.

Le AWS Config service gère la configuration des AWS ressources prises en charge dans votre compte et vous fournit des fichiers journaux. Les informations enregistrées incluent l'élément de configuration (AWS ressource), les relations entre les éléments de configuration et tout changement de configuration au sein des ressources. Les ressources mondiales sont des ressources disponibles dans n'importe quelle région.

Le contrôle est évalué comme suit :

- Si la région actuelle est définie comme votre région d'agrégation, le contrôle produit des `PASSED` résultats uniquement si les ressources globales Gestion des identités et des accès AWS (IAM) sont enregistrées (si vous avez activé les contrôles qui les nécessitent).
- Si la région actuelle est définie comme région liée, le contrôle n'évalue pas si les ressources globales IAM sont enregistrées.
- Si la région actuelle ne figure pas dans votre agrégateur, ou si l'agrégation interrégionale n'est pas configurée dans votre compte, le contrôle produit des `PASSED` résultats uniquement si les ressources globales IAM sont enregistrées (si vous avez activé les contrôles qui les nécessitent).

Les résultats du contrôle ne sont pas affectés par le fait que vous choisissiez l'enregistrement quotidien ou continu des modifications de l'état des ressources dans AWS Config. Toutefois, les résultats de ce contrôle peuvent changer lorsque de nouveaux contrôles sont publiés si vous avez configuré l'activation automatique de nouveaux contrôles ou si vous disposez d'une politique de configuration centrale qui active automatiquement les nouveaux contrôles. Dans ces cas, si vous n'enregistrez pas toutes les ressources, vous devez configurer l'enregistrement pour les ressources associées à de nouveaux contrôles afin de recevoir un `PASSED` résultat.

Les contrôles de sécurité CSPM de Security Hub ne fonctionnent comme prévu que si vous les activez AWS Config dans toutes les régions et si vous configurez l'enregistrement des ressources pour les contrôles qui l'exigent.

> **Note**
>
> Config.1 nécessite qu'elle AWS Config soit activée dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM.
> Security Hub CSPM étant un service régional, la vérification effectuée pour ce contrôle évalue uniquement la région actuelle du compte.
> Pour autoriser les contrôles de sécurité relatifs aux ressources globales IAM d'une région, vous devez enregistrer les ressources globales IAM de cette région. Les régions pour lesquelles aucune ressource globale IAM n'est enregistrée recevront un `PASSED` résultat par défaut pour les contrôles qui vérifient les ressources globales IAM. Les ressources globales IAM étant identiques d'une région à l'autre Régions AWS, nous vous recommandons d'enregistrer les ressources globales IAM uniquement dans la région d'origine (si l'agrégation interrégionale est activée dans votre compte). Les ressources IAM ne seront enregistrées que dans la région dans laquelle l'enregistrement des ressources globales est activé.
> Les types de ressources IAM enregistrés dans le monde entier qui sont pris AWS Config en charge sont les utilisateurs, les groupes, les rôles et les politiques IAM gérées par le client. Vous pouvez envisager de désactiver les contrôles CSPM de Security Hub qui vérifient ces types de ressources dans les régions où l'enregistrement global des ressources est désactivé. Pour de plus amples informations, veuillez consulter Contrôles suggérés à désactiver dans Security Hub CSPM.

Correction

Dans la région d'origine et les régions qui ne font pas partie d'un agrégateur, enregistrez toutes les ressources requises pour les contrôles activés dans la région actuelle, y compris les ressources globales IAM si vous avez activé des contrôles qui nécessitent des ressources globales IAM.

Dans les régions liées, vous pouvez utiliser n'importe quel AWS Config mode d'enregistrement, à condition d'enregistrer toutes les ressources correspondant aux commandes activées dans la région actuelle. Dans les régions liées, si vous avez activé des contrôles qui nécessitent l'enregistrement des ressources globales IAM, vous ne recevrez aucun `FAILED` résultat (votre enregistrement des autres ressources est suffisant).

Le `StatusReasons` champ situé dans l'`Compliance`objet de votre recherche peut vous aider à déterminer pourquoi cette commande n'a pas été détectée. Pour de plus amples informations, veuillez consulter Détails de conformité pour les résultats des contrôles.

Pour une liste des ressources qui doivent être enregistrées pour chaque contrôle, consultezObligatoireAWS Configressources pour les résultats des contrôles. Pour des informations générales sur l'activation AWS Config et la configuration de l'enregistrement des ressources, consultezActivation et configuration AWS Config pour Security Hub CSPM.

Contrôles Security Hub CSPM pour Amazon Connect

Ces contrôles Security Hub CSPM évaluent le service et les ressources Amazon Connect.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::CustomerProfiles::ObjectType`

Règle AWS Config : `customerprofiles-object-type-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un type d'objet Amazon Connect Customer Profiles possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le type d'objet ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le type d'objet n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un type d'objet Customer Profiles, consultez la section Ajouter des balises aux ressources dans Amazon Connect Customer dans le guide de l'administrateur de Connect Customer.

[Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Connect::Instance`

AWS Configrègle : connect-instance-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une instance Connect Customer est configurée pour générer et stocker des journaux de flux dans un groupe de CloudWatch journaux Amazon. Le contrôle échoue si l'instance Connect Customer n'est pas configurée pour générer et stocker des journaux de flux dans un groupe de CloudWatch journaux.

Les journaux des flux clients Amazon Connect fournissent des informations en temps réel sur les événements liés aux flux clients Amazon Connect. Un flux définit l'expérience client avec un centre de contact client Amazon Connect du début à la fin. Par défaut, lorsque vous créez une nouvelle instance Amazon Connect Customer, un groupe de CloudWatch journaux Amazon est créé automatiquement pour stocker les journaux de flux de l'instance. Les journaux de flux peuvent vous aider à analyser les flux, à détecter les erreurs et à surveiller les indicateurs opérationnels.

Vous pouvez également configurer des alertes pour des événements spécifiques susceptibles de se produire dans un flux.

Correction

Pour plus d'informations sur l'activation des journaux de flux pour une instance client Amazon Connect, consultez la section Activer les journaux de flux client Amazon Connect dans un groupe de CloudWatch journaux Amazon dans le guide de l'administrateur du client Connect.

Contrôles Security Hub CSPM pour Amazon Data Firehose

Ces contrôles Security Hub CSPM évaluent le service et les ressources Amazon Data Firehose.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos

Exigences connexes : NIST.800-53.r5 AC-3 NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::KinesisFirehose::DeliveryStream`

Règle AWS Config : `kinesis-firehose-delivery-stream-encrypted`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un flux de diffusion Amazon Data Firehose est chiffré au repos avec un chiffrement côté serveur. Ce contrôle échoue si un flux de diffusion Firehose n'est pas chiffré au repos avec un chiffrement côté serveur.

Server-side le chiffrement est une fonctionnalité des flux de diffusion d'Amazon Data Firehose qui chiffre automatiquement les données avant qu'elles ne soient inactives à l'aide d'une clé créée dans AWS Key Management Service (). AWS KMS Les données sont chiffrées avant d'être écrites dans la couche de stockage du flux Data Firehose, et déchiffrées une fois extraites du stockage. Cela vous permet de respecter les exigences réglementaires et de renforcer la sécurité de vos données.

Correction

Pour activer le chiffrement côté serveur sur les flux de diffusion Firehose, consultez la section Protection des données dans Amazon Data Firehose dans le manuel Amazon Data Firehose Developer Guide.

Contrôles Security Hub CSPM pourAWS Database Migration Service

Ces AWS Security Hub CSPM contrôles évaluent le AWS Database Migration Service (AWS DMS) et les AWS DMS ressources. Les commandes ne sont peut-être pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.6, PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::DMS::ReplicationInstance`

Règle AWS Config : dms-replication-not-public

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les instances de AWS DMS réplication sont publiques. Pour ce faire, il examine la valeur du `PubliclyAccessible` champ.

Une instance de réplication privée possède une adresse IP privée à laquelle vous ne pouvez pas accéder en dehors du réseau de réplication. Une instance de réplication doit avoir une adresse IP privée lorsque les bases de données source et cible se trouvent sur le même réseau. Le réseau doit également être connecté au VPC de l'instance de réplication à l'aide d'un VPN ou d'un Direct Connect peering VPC. Pour en savoir plus sur les instances de réplication publiques

et privées, consultez la section Instances de réplication publiques et privées dans le Guide de AWS Database Migration Service l'utilisateur.

Vous devez également vous assurer que l'accès à la configuration de votre AWS DMS instance est limité aux seuls utilisateurs autorisés. Pour ce faire, limitez les autorisations IAM des utilisateurs afin de modifier AWS DMS les paramètres et les ressources.

Correction

Vous ne pouvez pas modifier le paramètre d'accès public d'une instance de réplication DMS après l'avoir créée. Pour modifier le paramètre d'accès public, supprimez votre instance actuelle, puis recréez-la. Ne sélectionnez pas l'option Accessible au public.

[DMS.2] Les certificats DMS doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::DMS::Certificate`

AWS Configrègle : `tagged-dms-certificate` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS DMS certificat comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le certificat ne possède aucune clé de

balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le certificat n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un certificat DMS, consultez la section Ressources relatives au balisage AWS Database Migration Service dans le Guide de l'AWS Database Migration Serviceutilisateur.

[DMS.3] Les abonnements aux événements DMS doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::DMS::EventSubscription`

AWS Configrègle : `tagged-dms-eventsubscription` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un abonnement à un AWS DMS événement comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'abonnement à l'événement ne comporte aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'abonnement à l'événement n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un abonnement à un événement DMS, consultez les ressources de balisage AWS Database Migration Service dans le guide de l'AWS Database Migration Serviceutilisateur.

[DMS.4] Les instances de réplication DMS doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::DMS::ReplicationInstance`

AWS Configrègle : `tagged-dms-replicationinstance` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant	`No default value`

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		aux AWSexigences.	

Ce contrôle vérifie si une instance de AWS DMS réplication possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'instance de réplication ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'instance de réplication n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures

pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une instance de réplication DMS, consultez la section Ressources de balisage AWS Database Migration Service dans le Guide de l'AWS Database Migration Serviceutilisateur.

[DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::DMS::ReplicationSubnetGroup`

AWS Configrègle : `tagged-dms-replicationsubnetgroup` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un groupe de sous-réseaux de AWS DMS réplication possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si

le groupe de sous-réseaux de réplication ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de sous-réseaux de réplication n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe de sous-réseaux de réplication DMS, consultez la section Marquage des ressources AWS Database Migration Service dans le Guide de l'AWS Database Migration Serviceutilisateur.

[DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée

Exigences associées : NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::DMS::ReplicationInstance`

Règle AWS Config : dms-auto-minor-version-upgrade-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la mise à niveau automatique des versions mineures est activée pour une instance de AWS DMS réplication. Le contrôle échoue si la mise à niveau automatique des versions mineures n'est pas activée pour une instance de réplication DMS.

DMS fournit une mise à niveau automatique des versions mineures de chaque moteur de réplication pris en charge afin que vous puissiez maintenir votre instance de réplication à jour. Les versions mineures peuvent introduire de nouvelles fonctionnalités logicielles, des corrections de bogues, des correctifs de sécurité et des améliorations de performances. En activant la mise à niveau automatique des versions mineures sur les instances de réplication DMS, les mises à niveau mineures sont appliquées automatiquement pendant la période de maintenance ou immédiatement si l'option Appliquer les modifications immédiatement est sélectionnée.

Correction

Pour activer la mise à niveau automatique des versions mineures sur les instances de réplication DMS, reportez-vous à la section Modification d'une instance de réplication dans le Guide de AWS Database Migration Service l'utilisateur.

[DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::DMS::ReplicationTask`

Règle AWS Config : dms-replication-task-targetdb-logging

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée avec le niveau de gravité minimum de `LOGGER_SEVERITY_DEFAULT` pour les tâches de réplication DMS `TARGET_APPLY` et`TARGET_LOAD`. Le contrôle échoue si la journalisation n'est pas activée pour ces tâches ou si le niveau de gravité minimal est inférieur à`LOGGER_SEVERITY_DEFAULT`.

DMS utilise Amazon CloudWatch pour enregistrer les informations pendant le processus de migration. À l'aide des paramètres des tâches de journalisation, vous pouvez spécifier les activités des composants qui sont enregistrées et la quantité d'informations enregistrées. Vous devez spécifier la journalisation pour les tâches suivantes :

- `TARGET_APPLY` : les données et les instructions DDL sont appliquées à la base de données cible.
- `TARGET_LOAD` : les données sont chargées dans la base de données cible.

La journalisation joue un rôle essentiel dans les tâches de réplication DMS en permettant la surveillance, le dépannage, l'audit, l'analyse des performances, la détection des erreurs et la restauration, ainsi que l'analyse historique et les rapports. Il permet de garantir la réplication réussie des données entre les bases de données tout en préservant l'intégrité des données et en respectant les exigences réglementaires. Les niveaux de journalisation autres que `DEFAULT` sont rarement nécessaires pour ces composants lors du dépannage. Nous vous recommandons de conserver le même niveau de journalisation que `DEFAULT` pour ces composants, sauf demande spécifique de le modifier parSupport. Un niveau de journalisation minimal de `DEFAULT` garantit que les messages d'information, les avertissements et les messages d'erreur sont écrits dans les journaux. Ce contrôle vérifie si le niveau de journalisation est au moins l'un des suivants pour les tâches de réplication précédentes : `LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG`, ou`LOGGER_SEVERITY_DETAILED_DEBUG`.

Correction

Pour activer la journalisation des tâches de réplication DMS de la base de données cible, reportez-vous à la section Affichage et gestion des journaux des AWS DMS tâches dans le Guide de AWS Database Migration Service l'utilisateur.

[DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::DMS::ReplicationTask`

Règle AWS Config : dms-replication-task-sourcedb-logging

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée avec le niveau de gravité minimum de `LOGGER_SEVERITY_DEFAULT` pour les tâches de réplication DMS `SOURCE_CAPTURE` et`SOURCE_UNLOAD`. Le contrôle échoue si la journalisation n'est pas activée pour ces tâches ou si le niveau de gravité minimal est inférieur à`LOGGER_SEVERITY_DEFAULT`.

DMS utilise Amazon CloudWatch pour enregistrer les informations pendant le processus de migration. À l'aide des paramètres des tâches de journalisation, vous pouvez spécifier les activités des composants qui sont enregistrées et la quantité d'informations enregistrées. Vous devez spécifier la journalisation pour les tâches suivantes :

- `SOURCE_CAPTURE`— Les données de réplication ou de capture des données de modification (CDC) en cours sont capturées à partir de la base de données ou du service source et transmises au composant de `SORTER` service.
- `SOURCE_UNLOAD`— Les données sont déchargées de la base de données ou du service source pendant le chargement complet.

La journalisation joue un rôle essentiel dans les tâches de réplication DMS en permettant la surveillance, le dépannage, l'audit, l'analyse des performances, la détection des erreurs et la restauration, ainsi que l'analyse historique et les rapports. Il permet de garantir la réplication réussie des données entre les bases de données tout en préservant l'intégrité des données et en

respectant les exigences réglementaires. Les niveaux de journalisation autres que `DEFAULT` sont rarement nécessaires pour ces composants lors du dépannage. Nous vous recommandons de conserver le même niveau de journalisation que `DEFAULT` pour ces composants, sauf demande spécifique de le modifier parSupport. Un niveau de journalisation minimal de `DEFAULT` garantit que les messages d'information, les avertissements et les messages d'erreur sont écrits dans les journaux. Ce contrôle vérifie si le niveau de journalisation est au moins l'un des suivants pour les tâches de réplication précédentes : `LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG`, ou`LOGGER_SEVERITY_DETAILED_DEBUG`.

Correction

Pour activer la journalisation des tâches de réplication DMS de la base de données source, reportez-vous à la section Affichage et gestion des journaux des AWS DMS tâches dans le Guide de AWS Database Migration Service l'utilisateur.

[DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL

Exigences associées : NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::DMS::Endpoint`

Règle AWS Config : dms-endpoint-ssl-configured

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un AWS DMS terminal utilise une connexion SSL. Le contrôle échoue si le terminal n'utilise pas le protocole SSL.

SSL/TLS les connexions fournissent une couche de sécurité en chiffrant les connexions entre les instances de réplication DMS et votre base de données. L'utilisation de certificats fournit un niveau de sécurité supplémentaire en validant que la connexion est établie avec la base de données attendue. Pour ce faire, il vérifie le certificat de serveur qui est automatiquement installé sur toutes les instances de base de données que vous provisionnez. En activant la connexion SSL sur vos terminaux DMS, vous protégez la confidentialité des données pendant la migration.

Correction

Pour ajouter une connexion SSL à un point de terminaison DMS nouveau ou existant, consultez la section Utilisation du protocole SSL AWS Database Migration Service dans le guide de l'AWS Database Migration Serviceutilisateur.

[DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune

Exigences associées : NIST.800-53.r5 AC-2,, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-17, NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0. 1/7.3.1

Catégorie : Protéger > Gestion des accès sécurisés > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::DMS::Endpoint`

Règle AWS Config : dms-neptune-iam-authorization-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un AWS DMS point de terminaison pour une base de données Amazon Neptune est configuré avec l'autorisation IAM. Le contrôle échoue si l'autorisation IAM n'est pas activée sur le point de terminaison DMS.

Gestion des identités et des accès AWS(IAM) fournit un contrôle d'accès précis sur l'ensemble du site. AWS Avec IAM, vous pouvez spécifier qui peut accéder à quels services et ressources, et dans quelles conditions. Avec les politiques IAM, vous gérez les autorisations accordées à votre personnel et à vos systèmes afin de garantir les autorisations du moindre privilège. En activant l'autorisation IAM sur les AWS DMS points de terminaison des bases de données Neptune, vous pouvez accorder des privilèges d'autorisation aux utilisateurs IAM en utilisant un rôle de service spécifié par le paramètre. `ServiceAccessRoleARN`

Correction

Pour activer l'autorisation IAM sur les points de terminaison DMS pour les bases de données Neptune, consultez la section Utilisation d'Amazon Neptune comme cible dans le guide de l'utilisateur. AWS Database Migration Service AWS Database Migration Service

[DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé

Exigences associées : NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-6, NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0. 1/7.3.1

Catégorie : Protéger > Gestion des accès sécurisés > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::DMS::Endpoint`

Règle AWS Config : dms-mongo-db-authentication-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un AWS DMS point de terminaison pour MongoDB est configuré avec un mécanisme d'authentification. Le contrôle échoue si aucun type d'authentification n'est défini pour le point de terminaison.

AWS Database Migration Serviceprend en charge deux méthodes d'authentification pour MongoDB : MONGODB-CRpour MongoDB version 2.x SCRAM-SHA-1et pour MongoDB version 3.x ou ultérieure. Ces méthodes d'authentification sont utilisées pour authentifier et chiffrer les mots de passe MongoDB si les utilisateurs souhaitent utiliser les mots de passe pour accéder aux bases de données. L'authentification sur les AWS DMS terminaux garantit que seuls les utilisateurs autorisés peuvent accéder aux données migrées entre les bases de données et les modifier. Sans authentification appropriée, les utilisateurs non autorisés peuvent accéder à des données sensibles pendant le processus de migration. Cela peut entraîner des violations de données, des pertes de données ou d'autres incidents de sécurité.

Correction

Pour activer un mécanisme d'authentification sur les points de terminaison DMS pour MongoDB, consultez la section Utilisation de MongoDB comme source dans le guide de l'utilisateur. AWS DMS AWS Database Migration Service

[DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS

Exigences associées : NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-13, PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::DMS::Endpoint`

Règle AWS Config : dms-redis-tls-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un AWS DMS point de terminaison pour Redis OSS est configuré avec une connexion TLS. Le contrôle échoue si le protocole TLS n'est pas activé sur le terminal.

Le protocole TLS assure une sécurité de bout en bout lorsque des données sont envoyées entre des applications ou des bases de données via Internet. Lorsque vous configurez le chiffrement SSL pour votre point de terminaison DMS, il permet une communication cryptée entre les bases de données source et cible pendant le processus de migration. Cela permet d'empêcher l'écoute et l'interception de données sensibles par des acteurs malveillants. Sans cryptage SSL, il est possible d'accéder à des données sensibles, ce qui peut entraîner des violations de données, des pertes de données ou d'autres incidents de sécurité.

Correction

Pour activer une connexion TLS sur les points de terminaison DMS pour Redis, consultez la section Utilisation de Redis comme cible dans le guide de l'utilisateur AWS Database Migration Service.
AWS Database Migration Service

[DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::DMS::ReplicationInstance`

Règle AWS Config : dms-replication-instance-multi-az-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une instance de réplication AWS Database Migration Service (AWS DMS) est configurée pour utiliser plusieurs zones de disponibilité (Multi-AZ déploiement). Le contrôle échoue si l'instance de AWS DMS réplication n'est pas configurée pour utiliser un Multi-AZ déploiement.

Lors d'un Multi-AZ déploiement, AWS DMS provisionne et gère automatiquement une réplique de secours d'une instance de réplication dans une autre zone de disponibilité (AZ). L'instance de réplication principale est ensuite répliquée de manière synchrone sur la réplique de secours. Si l'instance de réplication principale échoue ou ne répond plus, l'instance de secours reprend toutes les tâches en cours avec une interruption minimale. Pour plus d'informations, consultez la section Utilisation d'une instance de réplication dans le Guide de AWS Database Migration Service l'utilisateur.

Correction

Après avoir créé une instance de AWS DMS réplication, vous pouvez modifier Multi-AZ ses paramètres de déploiement. Pour plus d'informations sur la modification de ce paramètre et d'autres paramètres pour une instance de réplication existante, consultez la section Modification d'une instance de réplication dans le Guide de AWS Database Migration Service l'utilisateur.

Contrôles Security Hub CSPM pourAWS DataSync

Ces contrôles CSPM du Security Hub évaluent le AWS DataSync service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[DataSync.1] la journalisation des DataSync tâches doit être activée

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::DataSync::Task`

Règle AWS Config : datasync-task-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée pour une AWS DataSync tâche. Le contrôle échoue si la journalisation n'est pas activée pour la tâche.

Les journaux d'audit suivent et surveillent les activités du système. Ils fournissent un enregistrement des événements qui peut vous aider à détecter les failles de sécurité, à enquêter sur les incidents et à vous conformer aux réglementations. Les journaux d'audit améliorent également la responsabilité globale et la transparence de votre organisation.

Correction

Pour plus d'informations sur la configuration de la journalisation AWS DataSync des tâches, consultez la section Surveillance des transferts de données avec Amazon CloudWatch Logs dans le guide de AWS DataSync l'utilisateur.

[DataSync.2] DataSync les tâches doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::DataSync::Task`

Règle AWS Config : datasync-task-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « 4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS DataSync tâche possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si la tâche ne possède aucune clé de balise

ou si elle ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la tâche n'en possède aucune. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à une AWS DataSync tâche, consultez la section Marquage de vos AWS DataSync tâches dans le guide de l'AWS DataSyncutilisateur.

Contrôles Security Hub CSPM pour Amazon Detective

Ce AWS Security Hub CSPM contrôle évalue le service et les ressources d'Amazon Detective. Il se peut que le contrôle ne soit pas disponible du toutRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Detective.1] Les graphes de comportement des détectives doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Detective::Graph`

AWS Configrègle : `tagged-detective-graph` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un graphe de comportement d'Amazon Detective possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le graphe de comportement ne possède aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le graphe de comportement n'est marqué d'aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un graphe de comportement de Detective, consultez la section Ajouter des balises à un graphe de comportement dans le guide d'administration d'Amazon Detective.

Contrôles CSPM de Security Hub pour Amazon DocumentDB

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon DocumentDB (compatible avec MongoDB). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : docdb-cluster-encrypted

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon DocumentDB est chiffré au repos. Le contrôle échoue si un cluster Amazon DocumentDB n'est pas chiffré au repos.

Les données au repos désignent toutes les données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement vous aide à protéger la confidentialité de ces données, réduisant ainsi le risque qu'un utilisateur non autorisé y accède. Les données des clusters Amazon DocumentDB doivent être chiffrées au repos pour renforcer la sécurité. Amazon DocumentDB utilise la norme de chiffrement avancée 256 bits (AES-256) pour chiffrer vos données à l'aide des clés de chiffrement stockées dans (). AWS Key Management Service AWS KMS

Correction

Vous pouvez activer le chiffrement au repos lorsque vous créez un cluster Amazon DocumentDB. Vous ne pouvez pas modifier les paramètres de chiffrement après avoir créé un cluster. Pour plus d'informations, consultez la section Activation du chiffrement au repos pour un cluster Amazon DocumentDB dans le manuel du développeur Amazon DocumentDB.

[DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

Exigences associées : NIST.800-53.r5 SI-12 PCI DSS v4.0. 1/3.2.1

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : docdb-cluster-backup-retention-check

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM	
`minimumBackupReten`	Durée minimale de conservation des sauvegardes en jours	Entier	7 sur 35	7	

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM	
`tionPeriod`					

Ce contrôle vérifie si la période de rétention des sauvegardes d'un cluster Amazon DocumentDB est supérieure ou égale à la période spécifiée. Le contrôle échoue si la période de conservation des sauvegardes est inférieure à la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de conservation des sauvegardes, Security Hub CSPM utilise une valeur par défaut de 7 jours.

Les sauvegardes vous aident à vous remettre plus rapidement en cas d'incident de sécurité et à renforcer la résilience de vos systèmes. En automatisant les sauvegardes de vos clusters Amazon DocumentDB, vous serez en mesure de restaurer vos systèmes à un moment précis et de minimiser les temps d'arrêt et les pertes de données. Dans Amazon DocumentDB, la période de conservation des sauvegardes par défaut des clusters est d'un jour. Ce délai doit être porté à une valeur comprise entre 7 et 35 jours pour passer ce contrôle.

Correction

Pour modifier la période de conservation des sauvegardes pour vos clusters Amazon DocumentDB, consultez la section Modification d'un cluster Amazon DocumentDB dans le manuel du développeur Amazon DocumentDB. Pour Backup, choisissez la période de conservation des sauvegardes.

[DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::RDS::DBClusterSnapshot`

Règle AWS Config : docdb-cluster-snapshot-public-prohibited

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un instantané de cluster manuel Amazon DocumentDB est public. Le contrôle échoue si l'instantané manuel du cluster est public.

Un instantané de cluster manuel Amazon DocumentDB ne doit pas être public, sauf indication contraire. Si vous partagez un instantané manuel non chiffré en tant que public, l'instantané est accessible à tousComptes AWS. Les instantanés publics peuvent entraîner une exposition involontaire des données.

> **Note**
>
> Ce contrôle évalue les instantanés manuels du cluster. Vous ne pouvez pas partager un instantané de cluster automatisé Amazon DocumentDB. Toutefois, vous pouvez créer un instantané manuel en copiant le cliché automatique, puis en partageant la copie.

Correction

Pour supprimer l'accès public aux instantanés de cluster manuels Amazon DocumentDB, consultez la section Partage d'un instantané dans le manuel Amazon DocumentDB Developer Guide. Par programmation, vous pouvez utiliser l'opération Amazon DocumentDB. `modify-db-snapshot-attribute` Définissez `attribute-name` comme `restore` et `values-to-remove` comme`all`.

[DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.3.3

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : docdb-cluster-audit-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon DocumentDB publie des journaux d'audit sur Amazon CloudWatch Logs. Le contrôle échoue si le cluster ne publie pas les journaux d'audit dans CloudWatch Logs.

Amazon DocumentDB (compatible avec MongoDB) vous permet d'auditer les événements qui ont été effectués dans votre cluster. Les exemples d'événements enregistrés incluent les tentatives d'authentification réussies et celles ayant échoué, la suppression d'une collection dans une base de données ou la création d'un index. Par défaut, l'audit est désactivé dans Amazon DocumentDB et nécessite que vous preniez des mesures pour l'activer.

Correction

Pour publier les journaux d'audit Amazon DocumentDB dans Logs, consultez la CloudWatch section Activation de l'audit dans le manuel Amazon DocumentDB Developer Guide.

[DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : docdb-cluster-deletion-protection-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la protection contre la suppression est activée sur un cluster Amazon DocumentDB. Le contrôle échoue si la protection contre la suppression n'est pas activée sur le cluster.

L'activation de la protection contre la suppression de clusters offre un niveau de protection supplémentaire contre la suppression accidentelle de la base de données ou la suppression par un utilisateur non autorisé. Un cluster Amazon DocumentDB ne peut pas être supprimé tant que la protection contre la suppression est activée. Vous devez d'abord désactiver la protection contre la suppression pour qu'une demande de suppression puisse aboutir. La protection contre la suppression est activée par défaut lorsque vous créez un cluster dans la console Amazon DocumentDB.

Correction

Pour activer la protection contre la suppression pour un cluster Amazon DocumentDB existant, consultez la section Modification d'un cluster Amazon DocumentDB dans le manuel du développeur Amazon DocumentDB. Dans la section Modifier le cluster, choisissez Activer la protection contre la suppression.

[DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : docdb-cluster-encrypted-in-transit

Type de calendrier : Périodique

Paramètres : `excludeTlsParameters` :`disabled`, `enabled` (non personnalisable)

Cela permet de vérifier si un cluster Amazon DocumentDB nécessite le protocole TLS pour les connexions au cluster. Le contrôle échoue si le groupe de paramètres de cluster associé au cluster n'est pas synchronisé ou si le paramètre de cluster TLS est défini sur `disabled` ou`enabled`.

Vous pouvez utiliser le protocole TLS pour chiffrer la connexion entre une application et un cluster Amazon DocumentDB. L'utilisation du protocole TLS peut aider à protéger les données contre toute interception lorsqu'elles sont en transit entre une application et un cluster Amazon DocumentDB. Le chiffrement en transit pour un cluster Amazon DocumentDB est géré à l'aide du paramètre TLS dans le groupe de paramètres du cluster associé au cluster. Lorsque le chiffrement en transit est activé, des connexions sécurisées à l'aide de TLS sont nécessaires pour se connecter au cluster. Nous vous recommandons d'utiliser les paramètres TLS suivants : `tls1.2+tls1.3+`, et`fips-140-3`.

Correction

Pour plus d'informations sur la modification des paramètres TLS d'un cluster Amazon DocumentDB, consultez la section Chiffrement des données en transit dans le manuel Amazon DocumentDB Developer Guide.

Contrôles Security Hub CSPM pour DynamoDB

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon DynamoDB. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[DynamoDB.1] Les tables DynamoDB doivent automatiquement adapter la capacité à la demande

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::DynamoDB::Table`

Règle AWS Config : `dynamodb-autoscaling-enabled`

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées valides	Valeur par défaut du Security Hub CSPM
`minProvisionedReadCapacity`	Nombre minimal d'unités de capacité de lecture allouées pour le dimensionnement automatique de DynamoDB	Entier	1 sur `40000`	Aucune valeur par défaut
`targetReadUtilization`	Pourcentage d'utilisation cible de la capacité de lecture	Entier	`20` sur `90`	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées valides	Valeur par défaut du Security Hub CSPM
`minProvisionedWriteCapacity`	Nombre minimal d'unités de capacité d'écriture allouées pour le dimensionnement automatique de DynamoDB	Entier	1 sur `40000`	Aucune valeur par défaut
`targetWriteUtilization`	Pourcentage d'utilisation cible de la capacité d'écriture	Entier	`20` sur `90`	Aucune valeur par défaut

Ce contrôle vérifie si une table Amazon DynamoDB peut adapter sa capacité de lecture et d'écriture selon les besoins. Le contrôle échoue si la table n'utilise pas le mode capacité à la demande ou le mode provisionné avec mise à l'échelle automatique configurée. Par défaut, ce contrôle nécessite uniquement la configuration de l'un de ces modes, sans tenir compte des niveaux spécifiques de capacité de lecture ou d'écriture. Vous pouvez éventuellement fournir des valeurs de paramètres personnalisées pour exiger des niveaux spécifiques de capacité de lecture et d'écriture ou un taux d'utilisation cible.

L'adaptation de la capacité à la demande permet d'éviter de limiter les exceptions, ce qui permet de maintenir la disponibilité de vos applications. Les tables DynamoDB qui utilisent le mode de capacité à la demande sont limitées uniquement par les quotas de table par défaut du débit DynamoDB. Pour augmenter ces quotas, vous pouvez déposer un ticket d'assistance auprès deSupport. Les tables DynamoDB qui utilisent le mode provisionné avec mise à l'échelle automatique ajustent dynamiquement la capacité de débit allouée en fonction des modèles de trafic. Pour plus d'informations sur la limitation des demandes DynamoDB, consultez la section Limitation des demandes et capacité de rafale dans le manuel du développeur Amazon DynamoDB.

Correction

Pour activer le dimensionnement automatique de DynamoDB sur des tables existantes en mode capacité, consultez la section Activation du dimensionnement automatique de DynamoDB sur des tables existantes dans le manuel Amazon DynamoDB Developer Guide.

[DynamoDB.2] La restauration instantanée des tables DynamoDB doit être activée

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::DynamoDB::Table`

Règle AWS Config : `dynamodb-pitr-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la restauration instantanée (PITR) est activée pour une table Amazon DynamoDB.

Les sauvegardes vous aident à récupérer plus rapidement après un incident de sécurité. Ils renforcent également la résilience de vos systèmes. La restauration instantanée de DynamoDB automatise les sauvegardes des tables DynamoDB. Cela réduit le temps de restauration suite à des opérations de suppression ou d'écriture accidentelles. Les tables DynamoDB sur lesquelles le PITR est activé peuvent être restaurées à tout moment au cours des 35 derniers jours.

Correction

Pour restaurer une table DynamoDB à un point dans le temps, consultez la section Restauration d'une table DynamoDB à un moment donné dans le manuel Amazon DynamoDB Developer Guide.

[DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::DAX::Cluster`

Règle AWS Config : `dax-encryption-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon DynamoDB Accelerator (DAX) est chiffré au repos. Le contrôle échoue si le cluster DAX n'est pas chiffré au repos.

Le chiffrement des données au repos réduit le risque qu'un utilisateur non authentifié accède aux données stockées sur disque. AWS Le chiffrement ajoute un autre ensemble de contrôles d'accès pour limiter la capacité des utilisateurs non autorisés à accéder aux données. Par exemple, les autorisations d'API sont nécessaires pour déchiffrer les données avant qu'elles puissent être lues.

Correction

Vous ne pouvez pas activer ou désactiver le chiffrement au repos après la création d'un cluster. Vous devez recréer le cluster afin d'activer le chiffrement au repos. Pour obtenir des instructions détaillées sur la création d'un cluster DAX avec le chiffrement au repos activé, consultez la section Activation du chiffrement au repos à l'aide du Console de gestion AWS manuel du développeur Amazon DynamoDB.

[DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::DynamoDB::Table`

AWS Configrègle : **`dynamodb-resources-protected-by-backup-plan`**

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`backupVaultLockCheck`	Le contrôle produit un `PASSED` résultat si le paramètre est défini sur Vault Lock `true` et si la ressource utilise AWS Backup Vault Lock.	Booléen	`true` ou `false`	Aucune valeur par défaut

Ce contrôle évalue si une `ACTIVE` table Amazon DynamoDB en cours est couverte par un plan de sauvegarde. Le contrôle échoue si la table DynamoDB n'est pas couverte par un plan de sauvegarde. Si vous définissez le `backupVaultLockCheck` paramètre égal à`true`, le contrôle est transmis uniquement si la table DynamoDB est sauvegardée dans AWS Backup un coffre verrouillé.

AWS Backupest un service de sauvegarde entièrement géré qui vous aide à centraliser et à automatiser la sauvegarde des données entre tousServices AWS. Vous pouvez ainsi créer des plans de sauvegarde qui définissent vos besoins en matière de sauvegarde, tels que la fréquence de sauvegarde de vos données et la durée de conservation de ces sauvegardes. AWS Backup L'inclusion de tables DynamoDB dans vos plans de sauvegarde vous permet de protéger vos données contre toute perte ou suppression involontaire.

Correction

Pour ajouter une table DynamoDB à AWS Backup un plan de sauvegarde, consultez la section Affectation de ressources à un plan de sauvegarde dans le Guide du développeur. AWS Backup

[DynamoDB.5] Les tables DynamoDB doivent être balisées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::DynamoDB::Table`

AWS Configrègle : `tagged-dynamodb-table` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si une table Amazon DynamoDB possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la table ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la table n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une table DynamoDB, consultez la section Marquage des ressources dans DynamoDB dans le manuel du développeur Amazon DynamoDB.

[DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Moyenne

Type de ressource : `AWS::DynamoDB::Table`

AWS Configrègle : **`dynamodb-table-deletion-protection-enabled`**

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la protection contre la suppression est activée sur une table Amazon DynamoDB. Le contrôle échoue si la protection contre la suppression n'est pas activée sur une table DynamoDB.

Vous pouvez protéger une table DynamoDB contre toute suppression accidentelle à l'aide de la propriété de protection contre la suppression. L'activation de cette propriété pour les tables permet de garantir que les tables ne sont pas supprimées accidentellement lors des opérations de gestion des tables régulières effectuées par vos administrateurs. Cela permet d'éviter toute interruption de vos activités commerciales normales.

Correction

Pour activer la protection contre la suppression pour une table DynamoDB, consultez la section Utilisation de la protection contre la suppression dans le manuel Amazon DynamoDB Developer Guide.

[DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit

Exigences associées : NIST.800-53.r5 AC-17,, NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::DAX::Cluster`

Règle AWS Config : `dax-tls-endpoint-encryption`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon DynamoDB Accelerator (DAX) est chiffré en transit, le type de chiffrement du point de terminaison étant défini sur TLS. Le contrôle échoue si le cluster DAX n'est pas chiffré en transit.

Vous pouvez utiliser HTTPS (TLS) pour empêcher les pirates potentiels d'espionner ou de manipuler le trafic réseau à l'aide d'attaques de l'homme du milieu au d'autres attaques similaires. Vous devez uniquement autoriser les connexions chiffrées via TLS pour accéder aux clusters DAX. Toutefois, le chiffrement des données en transit peut affecter les performances. Vous devez tester votre application avec le chiffrement activé pour comprendre le profil de performance et l'impact du protocole TLS.

Correction

Vous ne pouvez pas modifier le paramètre de chiffrement TLS après avoir créé un cluster DAX. Pour chiffrer un cluster DAX existant, créez un nouveau cluster avec le chiffrement en transit activé, transférez le trafic de votre application vers celui-ci, puis supprimez l'ancien cluster. Pour plus d'informations, consultez Utilisation de la protection contre la suppression dans le Guide du développeur Amazon DynamoDB.

Contrôles Security Hub CSPM pour Amazon EC2

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Elastic Compute Cloud (Amazon EC2). Les commandes ne sont peut-être pas toutes disponibles Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement

Exigences associées : PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/72.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::::Account`

Règle AWS Config : `ebs-snapshot-public-restorable-check`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les instantanés Amazon Elastic Block Store sont configurés pour être restaurables publiquement. Le contrôle échoue si les instantanés Amazon EBS sont configurés pour être restaurables par tous.

Les instantanés EBS sont utilisés pour sauvegarder les données de vos volumes EBS sur Amazon S3 à un moment précis. Vous pouvez utiliser les instantanés pour restaurer les états précédents des volumes EBS. Il est rarement acceptable de partager un instantané avec le public. Généralement, la décision de partager un instantané publiquement a été prise par erreur ou sans une compréhension complète des implications. Cette vérification permet de s'assurer que tout ce partage a été entièrement planifié et intentionnel.

Correction

Pour rendre privé un instantané EBS public, consultez la section Partager un instantané dans le guide de l'utilisateur Amazon EC2. Pour Actions, Modifier les autorisations, choisissez Privé.

[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/55., PCI DSS version 3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/21.1, CIS AWS Foundations Benchmark v1.2. 0/4.3, CIS AWS Foundations Benchmark v1.4. 0/5.3, CIS AWS Foundations Benchmark v3.0. 0/54 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::EC2::SecurityGroup`

Règle AWS Config : `vpc-default-security-group-closed`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le groupe de sécurité par défaut d'un VPC autorise le trafic entrant ou sortant. Le contrôle échoue si le groupe de sécurité autorise le trafic entrant ou sortant.

Les règles du groupe de sécurité par défaut autorisent tout le trafic sortant et entrant à partir d'interfaces réseau (et de leurs instances associées) affectées au même groupe de sécurité. Nous vous recommandons de ne pas utiliser le groupe de sécurité par défaut. Étant donné que le groupe de sécurité par défaut ne peut pas être supprimé, vous devez modifier le paramètre des règles de groupe de sécurité par défaut pour restreindre le trafic entrant et sortant. Vous empêchez ainsi le trafic non prévu, si le groupe de sécurité par défaut est accidentellement configuré pour des ressources telles que les instances EC2.

Correction

Pour remédier à ce problème, commencez par créer de nouveaux groupes de sécurité dotés de privilèges minimaux. Pour obtenir des instructions, consultez la section Créer un groupe de sécurité dans le guide de l'utilisateur Amazon VPC. Attribuez ensuite les nouveaux groupes de sécurité à vos instances EC2. Pour obtenir des instructions, consultez Modifier le groupe de sécurité d'une instance dans le guide de l'utilisateur Amazon EC2.

Après avoir attribué les nouveaux groupes de sécurité à vos ressources, supprimez toutes les règles entrantes et sortantes des groupes de sécurité par défaut. Pour obtenir des instructions, consultez la section Configurer les règles des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

[EC2.3] Les volumes Amazon EBS joints doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EC2::Volume`

Règle AWS Config : `encrypted-volumes`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie que les volumes EBS attachés sont chiffrés. Pour réussir cette vérification, les volumes EBS doivent être en cours d'utilisation et chiffrés. Si le volume EBS n'est pas attaché, il ne fait pas partie de la portée de cette vérification.

Pour une couche supplémentaire de sécurité de vos données sensibles dans les volumes EBS, vous devez activer le chiffrement EBS au repos. Le chiffrement Amazon EBS offre une solution simple de chiffrement pour vos ressources EBS, qui n'exige pas de développer, contrôler ni sécuriser votre propre infrastructure de gestion de clés. Il utilise des clés KMS lors de la création de volumes chiffrés et de snapshots.

Pour en savoir plus sur le chiffrement Amazon EBS, consultez le manuel Amazon EC2 User Guide.

Correction

Il n'existe aucun moyen direct de chiffrer un volume ou un instantané non chiffré existant. Vous pouvez uniquement chiffrer un nouveau volume ou instantané lorsque vous le créez.

Si vous avez activé le chiffrement par défaut, Amazon EBS chiffre le nouveau volume ou instantané obtenu à l'aide de votre clé par défaut pour le chiffrement Amazon EBS. Même si vous n'avez pas

activé le chiffrement par défaut, vous pouvez activer le chiffrement lorsque vous créez un volume ou un instantané spécifique. Dans les deux cas, vous pouvez remplacer la clé par défaut pour le chiffrement Amazon EBS et choisir une clé symétrique gérée par le client.

Pour plus d'informations, consultez les sections Création d'un volume Amazon EBS et Copie d'un instantané Amazon EBS dans le guide de l'utilisateur Amazon EC2.

[EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier - Inventaire

Gravité : Moyenne

Type de ressource : `AWS::EC2::Instance`

AWS Config règle : `ec2-stopped-instance-days-check` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`AllowedDays`	Nombre de jours pendant lesquels l'instance EC2 est autorisée à être arrêtée avant de générer un échec de recherche.	Entier	`1` sur `365`	`30`

Ce contrôle vérifie si une instance Amazon EC2 a été arrêtée pendant plus de jours que le nombre de jours autorisé. Le contrôle échoue si une instance EC2 est arrêtée pendant une durée supérieure à la période maximale autorisée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période maximale autorisée, Security Hub CSPM utilise une valeur par défaut de 30 jours.

Lorsqu'une instance EC2 n'est pas exécutée pendant une longue période, cela crée un risque de sécurité car l'instance n'est pas activement maintenue (analysée, corrigée, mise à jour). S'il est lancé ultérieurement, l'absence de maintenance appropriée peut entraîner des problèmes inattendus dans votre AWS environnement. Pour maintenir en toute sécurité une instance EC2 dans un état inactif au fil du temps, démarrez-la régulièrement pour la maintenance, puis arrêtez-la après la maintenance. Idéalement, il devrait s'agir d'un processus automatisé.

> **Note**
>
> Ce contrôle évalue le nombre de jours pendant lesquels une instance EC2 a été arrêtée en utilisant l'horodatage de `StateTransitionReason` l'instance. Lorsque le `StateTransitionReason` n'inclut pas d'horodatage (par exemple lorsqu'une instance est arrêtée en raison d'une erreur interne), le contrôle utilise plutôt l'heure de lancement de l'instance. Dans ce cas, si l'heure de lancement est antérieure à la période maximale autorisée, le contrôle génère une erreur de recherche.

Correction

Pour mettre fin à une instance EC2 inactive, consultez la section Résiliation d'une instance dans le guide de l'utilisateur Amazon EC2.

[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/32.7, CIS AWS Foundations Benchmark v1.2. 0/21.9, CIS AWS Foundations Benchmark v1.4. 0/31.9, CIS AWS Foundations Benchmark v3.0. 0/3.7, NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 NIST.800-53.r5 SI-7 (8) NIST.800-53.r5 CA-7, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, PCI DSS version 3.2. 1/103.3.3, PCI DSS v3.2. 1/103.3.4, PCI DSS v3.2. 1/103.3.5, PCI DSS v3.2. 1/10.3.6

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::EC2::VPC`

Règle AWS Config : `vpc-flow-logs-enabled`

Type de calendrier : Périodique

Paramètres :

- `trafficType`: `REJECT` (non personnalisable)

Ce contrôle vérifie si les journaux de flux Amazon VPC sont trouvés et activés pour les VPC. Le type de trafic est défini sur`Reject`. Le contrôle échoue si les journaux de flux VPC ne sont pas activés pour les VPC de votre compte.

> **Note**
>
> Ce contrôle ne vérifie pas si les journaux de flux Amazon VPC sont activés via Amazon Security Lake pour le. Compte AWS

Grâce à la fonctionnalité VPC Flow Logs, vous pouvez capturer des informations sur le trafic d'adresses IP à destination et en provenance des interfaces réseau de votre VPC. Après avoir créé un journal de flux, vous pouvez consulter et récupérer ses données dans CloudWatch Logs. Pour réduire les coûts, vous pouvez également envoyer vos journaux de flux vers Amazon S3.

Security Hub CSPM vous recommande d'activer la journalisation des flux pour les rejets de paquets pour les VPC. Les journaux de flux fournissent une visibilité sur le trafic réseau qui traverse le VPC et peuvent détecter le trafic anormal ou fournir des informations lors des flux de travail de sécurité.

Par défaut, l'enregistrement inclut des valeurs pour les différents composants du flux d'adresses IP, notamment la source, la destination et le protocole. Pour plus d'informations et une description des champs de journal, consultez la section VPC Flow Logs dans le guide de l'utilisateur Amazon VPC.

Correction

Pour créer un journal de flux VPC, consultez la section Créer un journal de flux dans le guide de l'utilisateur Amazon VPC. Après avoir ouvert la console Amazon VPC, choisissez Your VPC. Pour Filtrer, choisissez Rejeter ou Tout.

[EC2.7] Le chiffrement par défaut d'EBS doit être activé

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/51.1.1, CIS AWS Foundations Benchmark v1.4. 0/22.2.1, CIS AWS Foundations Benchmark v3.0. 0/2.2.1, NIST.800-53.r5 CA-9 (1),

NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `ec2-ebs-encryption-by-default`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement au niveau du compte est activé par défaut pour les volumes Amazon Elastic Block Store (Amazon EBS). Le contrôle échoue si le chiffrement au niveau du compte n'est pas activé pour les volumes EBS.

Lorsque le chiffrement est activé pour votre compte, les volumes Amazon EBS et les copies instantanées sont chiffrés au repos. Cela ajoute un niveau de protection supplémentaire à vos données. Pour plus d'informations, consultez la section Chiffrement par défaut dans le Guide de l'utilisateur Amazon EC2.

Correction

Pour configurer le chiffrement par défaut pour les volumes Amazon EBS, consultez la section Chiffrement par défaut dans le guide de l'utilisateur Amazon EC2.

[EC2.8] Les instances EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/52.7, CIS AWS Foundations Benchmark v3.0. 0/5.6 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/2.2.6

Catégorie : Protection > Sécurité du réseau

Gravité : Élevée

Type de ressource : `AWS::EC2::Instance`

Règle AWS Config : `ec2-imdsv2-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la version des métadonnées de votre instance EC2 est configurée avec le service de métadonnées d'instance version 2 (IMDSv2). Le contrôle passe s'il `HttpTokens` est défini sur obligatoire pour IMDSv2. Le contrôle échoue s'il `HttpTokens` est défini sur`optional`.

Vous utilisez les métadonnées de l'instance pour configurer ou gérer l'instance en cours d'exécution. L'IMDS permet d'accéder à des informations d'identification temporaires fréquemment renouvelées. Ces informations d'identification éliminent le besoin de coder en dur ou de distribuer des informations d'identification sensibles aux instances manuellement ou par programmation. L'IMDS est attaché localement à chaque instance EC2. Il fonctionne sur une adresse IP spéciale « lien local » 169.254.169.254. Cette adresse IP n'est accessible que par le logiciel qui s'exécute sur l'instance.

La version 2 de l'IMDS ajoute de nouvelles protections pour les types de vulnérabilités suivants. Ces vulnérabilités pourraient être utilisées pour tenter d'accéder à l'IMDS.

- Pare-feu pour applications de sites Web ouverts
- Proxies inverses ouverts
- Server-side vulnérabilités liées à la falsification de requêtes (SSRF)
- Pare-feux de couche 3 ouverts et traduction d'adresses réseau (NAT)

Security Hub CSPM vous recommande de configurer vos instances EC2 avec IMDSv2.

Correction

Pour configurer des instances EC2 avec IMDSv2, consultez le chemin recommandé pour exiger IMDSv2 dans le guide de l'utilisateur Amazon EC2.

[EC2.9] Les instances Amazon EC2 ne doivent pas avoir d'adresse IPv4 publique

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::EC2::Instance`

Règle AWS Config : `ec2-instance-no-public-ip`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les instances EC2 possèdent une adresse IP publique. Le contrôle échoue si le `publicIp` champ est présent dans l'élément de configuration de l'instance EC2. Ce contrôle s'applique uniquement aux adresses IPv4.

Une adresse IPv4 publique est une adresse IP accessible depuis Internet. Si vous lancez votre instance avec une adresse IP publique, votre instance EC2 est accessible depuis Internet. Une adresse IPv4 privée est une adresse IP qui n'est pas accessible depuis Internet. Vous pouvez utiliser des adresses IPv4 privées pour la communication entre les instances EC2 d'un même VPC ou de votre réseau privé connecté.

Les adresses IPv6 sont uniques au monde et sont donc accessibles depuis Internet. Cependant, par défaut, tous les sous-réseaux ont l'attribut d'adressage IPv6 défini sur false. Pour plus d'informations sur IPv6, consultez la section Adressage IP dans votre VPC dans le guide de l'utilisateur Amazon VPC.

Si vous avez un cas d'utilisation légitime pour gérer des instances EC2 avec des adresses IP publiques, vous pouvez supprimer les résultats de ce contrôle. Pour plus d'informations sur les options d'architecture frontale, consultez le blog sur AWS l'architecture ou la série de AWS vidéos This Is My Architecture.

Correction

Utilisez un VPC autre que celui par défaut afin qu'aucune adresse IP publique ne soit attribuée par défaut à votre instance.

Lorsque vous lancez une instance EC2 dans un VPC par défaut, une adresse IP publique lui est attribuée. Lorsque vous lancez une instance EC2 dans un VPC autre que celui par défaut, la configuration du sous-réseau détermine si elle reçoit une adresse IP publique. Le sous-réseau possède un attribut permettant de déterminer si les nouvelles instances EC2 du sous-réseau reçoivent une adresse IP publique du pool d'adresses IPv4 public.

Vous pouvez dissocier une adresse IP publique attribuée automatiquement de votre instance EC2. Pour plus d'informations, consultez Adresses IPv4 publiques et noms d'hôte DNS externes dans le Guide l'utilisateur Amazon EC2.

[EC2.10] Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4), NIST.800-171.r2 3.1.3, 3.13.1 NIST.800-171.r2

Catégorie : Protection > Configuration réseau sécurisée > Accès privé à l'API

Gravité : Moyenne

Type de ressource : `AWS::EC2::VPC`

Règle AWS Config : vpc-endpoint-enabled

Type de calendrier : Périodique

Paramètres :

- `serviceNames`: `ec2` (non personnalisable)

Ce contrôle vérifie si un point de terminaison de service pour Amazon EC2 est créé pour chaque VPC. Le contrôle échoue si aucun point de terminaison VPC n'a été créé pour le service Amazon EC2 pour le service Amazon EC2.

Ce contrôle évalue les ressources dans un seul compte. Il ne peut pas décrire les ressources extérieures au compte. Dans la AWS Config mesure où Security Hub CSPM n'effectue pas de vérifications entre comptes, vous verrez des `FAILED` résultats concernant les VPC partagés entre comptes. Security Hub CSPM vous recommande de supprimer ces `FAILED` résultats.

Pour améliorer le niveau de sécurité de votre VPC, vous pouvez configurer Amazon EC2 pour utiliser un point de terminaison VPC d'interface. Les points de terminaison de l'interface sont AWS PrivateLink alimentés par une technologie qui vous permet d'accéder aux opérations de l'API Amazon EC2 en privé. Il limite tout le trafic réseau entre votre VPC et Amazon EC2 vers le réseau Amazon. Comme les points de terminaison ne sont pris en charge que dans la même région, vous ne pouvez pas créer de point de terminaison entre un VPC et un service d'une région différente. Cela empêche les appels d'API Amazon EC2 involontaires vers d'autres régions.

Pour en savoir plus sur la création de points de terminaison VPC pour Amazon EC2, consultez Amazon EC2 et interfacez les points de terminaison VPC dans le guide de l'utilisateur Amazon EC2.

Correction

Pour créer un point de terminaison d'interface vers Amazon EC2 à partir de la console Amazon VPC, consultez la section Créer un point de terminaison VPC dans le guide.AWS PrivateLink Pour le nom du service, choisissez com.amazonaws. ***region***.ec2.

Vous pouvez également créer et associer une politique de point de terminaison à votre point de terminaison VPC afin de contrôler l'accès à l'API Amazon EC2. Pour obtenir des instructions sur la création d'une politique de point de terminaison VPC, consultez la section Créer une politique de point de terminaison dans le guide de l'utilisateur Amazon EC2.

[EC2.12] Les EIP Amazon EC2 non utilisés doivent être supprimés

Exigences associées : PCI DSS v3.2. 1/20,4, NIST.800-53.r5 CM-8 (1)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Faible

Type de ressource : `AWS::EC2::EIP`

Règle AWS Config : `eip-attached`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les adresses IP élastiques (EIP) allouées à un VPC sont attachées à des instances EC2 ou à des interfaces réseau élastiques (ENI) en cours d'utilisation.

Un échec de recherche indique que vous avez peut-être des EIP EC2 non utilisés.

Cela vous aidera à maintenir un inventaire précis des actifs EIP dans votre environnement de données de titulaire de carte (CDE).

Correction

Pour libérer une EIP non utilisée, consultez la section Libérer une adresse IP élastique dans le guide de l'utilisateur Amazon EC2.

[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/4.1 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1, PCI DSS version 3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/22.2.2, PCI DSS v4.0. 1/1.3.1

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::EC2::SecurityGroup`

Règle AWS Config : `restricted-ssh`

Type de calendrier : changement déclenché et périodique

Paramètres : Aucun

Ce contrôle vérifie si un groupe de sécurité Amazon EC2 autorise l'entrée à partir de la version 0.0.0. 0/0 ou : :/0 vers le port 22. Le contrôle échoue si le groupe de sécurité autorise l'entrée à partir de la version 0.0.0. 0/0ou : :/0 vers le port 22.

Les groupes de sécurité autorisent le filtrage avec état du trafic réseau entrant et sortant vers des ressources AWS . Nous vous recommandons de faire en sorte qu'aucun groupe de sécurité n'autorise un accès entrant sans restriction au port 22. La suppression d'une connectivité illimitée aux services de la console à distance (SSH, par exemple) réduit le risque qu'un serveur soit compromis.

Correction

Pour interdire l'accès au port 22, supprimez la règle qui autorise un tel accès pour chaque groupe de sécurité associé à un VPC. Pour obtenir des instructions, consultez la section Mettre à jour les règles des groupes de sécurité dans le guide de l'utilisateur Amazon EC2. Après avoir sélectionné un groupe de sécurité dans la console Amazon EC2, choisissez Actions, Modifier les règles entrantes. Supprimez la règle qui autorise l'accès au port 22.

[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/42., PCI DSS version 4.0. 1/1.3.1

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::EC2::SecurityGroup`

AWS Config règle : **`restricted-common-ports`**(la règle créée est`restricted-rdp`)

Type de calendrier : changement déclenché et périodique

Paramètres : Aucun

Ce contrôle vérifie si un groupe de sécurité Amazon EC2 autorise l'entrée à partir de la version 0.0.0. 0/0 ou : :/0 sur le port 3389. Le contrôle échoue si le groupe de sécurité autorise l'entrée à partir de la version 0.0.0. 0/0ou : :/0 sur le port 3389.

Les groupes de sécurité autorisent le filtrage avec état du trafic réseau entrant et sortant vers des ressources AWS . Nous vous recommandons de faire en sorte qu'aucun groupe de sécurité n'autorise un accès entrant sans restriction au port 3389. La suppression d'une connectivité illimitée aux services de la console à distance (RDP, par exemple) réduit le risque qu'un serveur soit compromis.

Correction

Pour interdire l'accès au port 3389, supprimez la règle qui autorise un tel accès pour chaque groupe de sécurité associé à un VPC. Pour obtenir des instructions, consultez la section Mettre à jour les règles des groupes de sécurité dans le guide de l'utilisateur Amazon VPC. Après avoir sélectionné un groupe de sécurité dans la console Amazon VPC, choisissez Actions, Modifier les règles entrantes. Supprimez la règle qui autorise l'accès au port 3389.

[EC2.15] Les sous-réseaux Amazon EC2 ne doivent pas attribuer automatiquement d'adresses IP publiques

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Catégorie : Protection > Sécurité du réseau

Gravité : Moyenne

Type de ressource : `AWS::EC2::Subnet`

Règle AWS Config : `subnet-auto-assign-public-ip-disabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un sous-réseau Amazon Virtual Private Cloud (Amazon VPC) est configuré pour attribuer automatiquement des adresses IP publiques. Le contrôle échoue si le sous-réseau est configuré pour attribuer automatiquement des adresses IPv4 ou IPv6 publiques.

Les sous-réseaux possèdent des attributs qui déterminent si les interfaces réseau reçoivent automatiquement les adresses IPv4 et IPv6 publiques. Pour IPv4, cet attribut est défini sur pour les sous-réseaux par défaut et `TRUE` `FALSE` pour les sous-réseaux autres que ceux par défaut (à l'exception des sous-réseaux autres que ceux par défaut créés via l'assistant de lancement d'instance EC2, où il est défini sur). `TRUE` Pour IPv6, cet attribut est défini par défaut sur `FALSE` tous les sous-réseaux. Lorsque ces attributs sont activés, les instances lancées dans le sous-réseau reçoivent automatiquement les adresses IP correspondantes (IPv4 ou IPv6) sur leur interface réseau principale.

Correction

Pour configurer un sous-réseau afin de ne pas attribuer d'adresses IP publiques, consultez Modifier les attributs d'adressage IP de votre sous-réseau dans le guide de l'utilisateur Amazon VPC.

[EC2.16] Les listes de contrôle d'accès réseau non utilisées doivent être supprimées

Exigences associées : NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0. 1/1.2.7

Catégorie : Protection > Sécurité du réseau

Gravité : Faible

Type de ressource : `AWS::EC2::NetworkAcl`

Règle AWS Config : `vpc-network-acl-unused-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie s'il existe des listes de contrôle d'accès réseau (ACL réseau) inutilisées dans votre cloud privé virtuel (VPC). Le contrôle échoue si l'ACL réseau n'est pas associée à un sous-réseau. Le contrôle ne génère pas de résultats pour une ACL réseau par défaut non utilisée.

Le contrôle vérifie la configuration des éléments de la ressource `AWS::EC2::NetworkAcl` et détermine les relations entre les ACL du réseau.

Si la seule relation est le VPC de l'ACL réseau, le contrôle échoue.

Si d'autres relations sont répertoriées, le contrôle est transféré.

Correction

Pour obtenir des instructions sur la suppression d'un ACL réseau inutilisé, consultez Supprimer un ACL réseau dans le guide de l'utilisateur Amazon VPC. Vous ne pouvez pas supprimer l'ACL réseau par défaut ou une ACL associée à des sous-réseaux.

[EC2.17] Les instances Amazon EC2 ne doivent pas utiliser plusieurs ENI

Exigences connexes : NIST.800-53.r5 AC-4 (21)

Catégorie : Protection > Sécurité du réseau

Gravité : Faible

Type de ressource : `AWS::EC2::Instance`

Règle AWS Config : `ec2-instance-multiple-eni-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une instance EC2 utilise plusieurs interfaces réseau élastiques (ENI) ou adaptateurs Elastic Fabric (EFA). Ce contrôle passe si un seul adaptateur réseau est utilisé. Le contrôle inclut une liste de paramètres facultatifs pour identifier les ENI autorisés. Ce contrôle échoue également si une instance EC2 appartenant à un cluster Amazon EKS utilise plusieurs ENI. Si vos instances EC2 doivent disposer de plusieurs ENI dans le cadre d'un cluster Amazon EKS, vous pouvez supprimer ces résultats de contrôle.

Plusieurs ENI peuvent provoquer des instances à double hébergement, c'est-à-dire des instances dotées de plusieurs sous-réseaux. Cela peut ajouter à la complexité de la sécurité du réseau et introduire des chemins et des accès non intentionnels au réseau.

Correction

Pour détacher une interface réseau d'une instance EC2, consultez la section Détacher une interface réseau d'une instance dans le guide de l'utilisateur Amazon EC2.

[EC2.18] Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés

Exigences connexes : NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Catégorie : Protection > Configuration réseau sécurisée > Configuration du groupe de sécurité

Gravité : Élevée

Type de ressource : `AWS::EC2::SecurityGroup`

Règle AWS Config : `vpc-sg-open-only-to-authorized-ports`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`authorizedTcpPorts`	Liste des ports TCP autorisés	IntegerList (minimum de 1 article et maximum de 32 articles)	1 sur 65535	`[80,443]`
`authorizedUdpPorts`	Liste des ports UDP autorisés	IntegerList (minimum de 1 article et maximum de 32 articles)	1 sur 65535	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de sécurité Amazon EC2 autorise le trafic entrant sans restriction en provenance de ports non autorisés. L'état du contrôle est déterminé comme suit :

- Si vous utilisez la valeur par défaut pour`authorizedTcpPorts`, le contrôle échoue si le groupe de sécurité autorise le trafic entrant sans restriction depuis un port autre que les ports 80 et 443.
- Si vous fournissez des valeurs personnalisées pour `authorizedTcpPorts` ou`authorizedUdpPorts`, le contrôle échoue si le groupe de sécurité autorise un trafic entrant illimité en provenance d'un port non répertorié.

Les groupes de sécurité fournissent un filtrage dynamique du trafic réseau entrant et sortant vers. AWS Les règles des groupes de sécurité doivent respecter le principe de l'accès le moins privilégié. L'accès illimité (adresse IP avec le suffixe /0) augmente les risques d'activités malveillantes telles que le piratage, les attaques par déni de service et la perte de données. À moins qu'un port ne soit spécifiquement autorisé, le port doit refuser un accès illimité.

Correction

Pour modifier un groupe de sécurité, consultez la section Travailler avec des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

[EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé

Exigences connexes : NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Catégorie : Protection > Accès réseau restreint

Gravité : Critique

Type de ressource : `AWS::EC2::SecurityGroup`

AWS Config règle : **`restricted-common-ports`**(la règle créée est`vpc-sg-restricted-common-ports`)

Type de calendrier : changement déclenché et périodique

Paramètres : `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (non personnalisable)

Ce contrôle vérifie si le trafic entrant non restreint pour un groupe de sécurité Amazon EC2 est accessible aux ports spécifiés considérés comme présentant un risque élevé. Ce contrôle échoue si l'une des règles d'un groupe de sécurité autorise le trafic entrant depuis « 0.0.0 ». 0/0' ou ': :/0' vers ces ports.

Les groupes de sécurité autorisent le filtrage avec état du trafic réseau entrant et sortant vers des ressources AWS . Accès illimité (0.0.0. 0/0) augmente les risques d'activités malveillantes, telles que le piratage, les attaques par déni de service et la perte de données. Aucun groupe de sécurité ne doit autoriser un accès d'entrée illimité aux ports suivants :

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP 3)
- 135 (PIÈCE)
- 143 (CARTE)
- 445 (CHIFFRES)
- 1433, 1434 (MSSQL)
- 3000 (frameworks de Node.js développement Web Go et Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 433 (ahsp)
- 5000 (frameworks de développement Web en Python)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch Tableaux de bord)
- 8080 (proxy)
- 8088 (ancien port HTTP)
- 8888 (port HTTP alternatif)

- 9200 ou 9300 () OpenSearch

Correction

Pour supprimer des règles d'un groupe de sécurité, consultez la section Supprimer des règles d'un groupe de sécurité dans le guide de l'utilisateur Amazon EC2.

[EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.1.13, 3.1.20 NIST.800-171.r2

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::EC2::VPNConnection`

Règle AWS Config : `vpc-vpn-2-tunnels-up`

Type de calendrier : changement déclenché

Paramètres : Aucun

Un tunnel VPN est un lien crypté par lequel les données peuvent passer du réseau du client vers ou AWS depuis une connexion AWS Site-to-Site VPN. Chaque connexion VPN comprend deux tunnels VPN que vous pouvez utiliser simultanément pour une haute disponibilité. Il est important de s'assurer que les deux tunnels VPN sont prêts pour une connexion VPN afin de confirmer une connexion sécurisée et hautement disponible entre un AWS VPC et votre réseau distant.

Ce contrôle vérifie que les deux tunnels VPN fournis par le AWS Site-to-Site VPN sont en état UP. Le contrôle échoue si l'un ou les deux tunnels sont en panne.

Correction

Pour modifier les options du tunnel VPN, consultez la section Modification des options du tunnel Site-to-Site VPN dans le Guide de l'utilisateur du AWS Site-to-Site VPN.

[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/52.2, CIS AWS Foundations Benchmark v1.4. 0/51.1, CIS AWS Foundations Benchmark v3.0. 0/5.1, NIST.800-53.r5 AC-4 (21),

NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2,, (21) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, PCI DSS version 4.0. 1/1.3.1

Catégorie : Protection > Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::EC2::NetworkAcl`

Règle AWS Config : `nacl-no-unrestricted-ssh-rdp`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une liste de contrôle d'accès réseau (ACL réseau) autorise un accès illimité aux ports TCP par défaut pour le trafic SSH/RDP entrant. Le contrôle échoue si l'entrée entrante de l'ACL du réseau autorise un bloc CIDR source de « 0.0.0 ». 0/0' ou ': :/0' pour les ports TCP 22 ou 3389. Le contrôle ne génère pas de résultats pour une ACL réseau par défaut.

L'accès aux ports d'administration du serveur distant, tels que le port 22 (SSH) et le port 3389 (RDP), ne doit pas être accessible au public, car cela peut permettre un accès involontaire aux ressources de votre VPC.

Correction

Pour modifier les règles de trafic ACL réseau, consultez la section Utilisation des ACL réseau dans le guide de l'utilisateur Amazon VPC.

[EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés

Catégorie : Identifier - Inventaire

Gravité : Moyenne

Type de ressource :`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

Règle AWS Config : `ec2-security-group-attached-to-eni-periodic`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si des groupes de sécurité sont attachés à des instances Amazon Elastic Compute Cloud (Amazon EC2) ou à une interface réseau élastique. Le contrôle échoue si le groupe de sécurité n'est pas associé à une instance Amazon EC2 ou à une interface Elastic Network.

> **Important**
>
> Le 20 septembre 2023, Security Hub CSPM a retiré ce contrôle des normes AWS Foundational Security Best Practices et du NIST SP 800-53 Revision 5. Ce contrôle continue de faire partie de la norme de AWS Control Tower gestion des services. Ce contrôle produit un résultat positif si des groupes de sécurité sont attachés à des instances EC2 ou à une interface elastic network. Toutefois, dans certains cas d'utilisation, les groupes de sécurité indépendants ne présentent aucun risque de sécurité. Vous pouvez utiliser d'autres contrôles EC2 EC2.2, tels que,,, et EC2.13 EC2.14 EC2.18, EC2.19 pour surveiller vos groupes de sécurité.

Correction

Pour créer, attribuer et supprimer des groupes de sécurité, consultez la section Groupes de sécurité pour vos instances EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC

Exigences connexes : NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::EC2::TransitGateway`

Règle AWS Config : `ec2-transit-gateway-auto-vpc-attach-disabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les passerelles de transit EC2 acceptent automatiquement les pièces jointes VPC partagées. Ce contrôle échoue pour une passerelle de transit qui accepte automatiquement les demandes de pièces jointes VPC partagées.

L'activation permet de `AutoAcceptSharedAttachments` configurer une passerelle de transit pour qu'elle accepte automatiquement toutes les demandes de pièce jointe VPC entre comptes sans vérifier la demande ou le compte d'origine de la pièce jointe. Pour suivre les meilleures pratiques en matière d'autorisation et d'authentification, nous vous recommandons de désactiver cette fonctionnalité afin de garantir que seules les demandes de pièces jointes VPC autorisées sont acceptées.

Correction

Pour modifier une passerelle de transit, consultez la section Modifier une passerelle de transit dans le manuel Amazon VPC Developer Guide.

[EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés

Exigences connexes : NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::EC2::Instance`

Règle AWS Config : `ec2-paravirtual-instance-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le type de virtualisation d'une instance EC2 est paravirtuel. Le contrôle échoue si le `virtualizationType` de l'instance EC2 est défini sur. `paravirtual`

Linux Amazon Machine Images (AMI) utilise l'un des deux types de virtualisation suivants : machine virtuelle paravirtuelle (PV) ou machine virtuelle matérielle (HVM). Les principales différences entre les AMI de virtualisation paravirtuelle ou virtualisation HVM résident dans leur façon de démarrer et leur capacité à tirer parti des extensions matérielles spéciales (UC, réseau et stockage) pour obtenir une meilleure performance.

Traditionnellement, les invités de virtualisation paravirtuelle avaient de meilleures performances que les invités HVM. A cause des améliorations de la virtualisation HVM et de la disponibilité des pilotes de virtualisation paravirtuelle pour les AMI HVM, ce n'est plus le cas. Pour plus d'informations, consultez la section Types de virtualisation d'AMI Linux dans le guide de l'utilisateur Amazon EC2.

Correction

Pour mettre à jour une instance EC2 vers un nouveau type d'instance, consultez Modifier le type d'instance dans le guide de l'utilisateur Amazon EC2.

[EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::EC2::LaunchTemplate`

Règle AWS Config : `ec2-launch-template-public-ip-disabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les modèles de lancement Amazon EC2 sont configurés pour attribuer des adresses IP publiques aux interfaces réseau lors du lancement. Le contrôle échoue si un modèle de lancement EC2 est configuré pour attribuer une adresse IP publique aux interfaces réseau ou si au moins une interface réseau possède une adresse IP publique.

Une adresse IP publique est une adresse accessible depuis Internet. Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau peuvent être accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela peut permettre un accès involontaire à vos charges de travail.

Correction

Pour mettre à jour un modèle de lancement EC2, consultez Modifier les paramètres de l'interface réseau par défaut dans le manuel Amazon EC2 Auto Scaling User Guide.

[EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde

Catégorie : Restauration > Résilience > Sauvegardes activées

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Gravité : Faible

Type de ressource : `AWS::EC2::Volume`

AWS Config règle : **`ebs-resources-protected-by-backup-plan`**

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`backupVaultLockCheck`	Le contrôle produit un `PASSED` résultat si le paramètre est défini sur Vault Lock `true` et si la ressource utilise AWS Backup Vault Lock.	Booléen	`true` ou `false`	Aucune valeur par défaut

Ce contrôle évalue si un volume Amazon EBS en cours est `in-use` couvert par un plan de sauvegarde. Le contrôle échoue si un volume EBS n'est pas couvert par un plan de sauvegarde. Si vous définissez le `backupVaultLockCheck` paramètre égal à`true`, le contrôle est transféré uniquement si le volume EBS est sauvegardé dans un coffre-fort AWS Backup verrouillé.

Les sauvegardes vous aident à vous remettre plus rapidement en cas d'incident de sécurité. Ils renforcent également la résilience de vos systèmes. L'inclusion de volumes Amazon EBS dans un plan de sauvegarde vous permet de protéger vos données contre toute perte ou suppression involontaire.

Correction

Pour ajouter un volume Amazon EBS à un plan de AWS Backup sauvegarde, consultez la section Affectation de ressources à un plan de sauvegarde dans le manuel du AWS Backup développeur.

[EC2.33] Les pièces jointes de la passerelle de transit EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::TransitGatewayAttachment`

AWS Config règle : `tagged-ec2-transitgatewayattachment` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une pièce jointe à une passerelle de transit Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la pièce jointe à la passerelle de transit ne comporte aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la pièce jointe de la passerelle de transit n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une pièce jointe d'une passerelle de transit EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::TransitGatewayRouteTable`

AWS Config règle : `tagged-ec2-transitgatewayroutetable` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une table de routage d'une passerelle de transit Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la table de routage de la passerelle de transit ne contient aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la table de routage de la passerelle de transit n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à la table de routage d'une passerelle de transit EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.35] Les interfaces réseau EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::NetworkInterface`

AWS Config règle : `tagged-ec2-networkinterface` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une interface réseau Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si l'interface réseau ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans

le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'interface réseau n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une interface réseau EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.36] Les passerelles client EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::CustomerGateway`

AWS Config règle : `tagged-ec2-customergateway` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une passerelle client Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la passerelle client ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la passerelle client n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une passerelle client EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.37] Les adresses IP Elastic EC2 doivent être balisées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::EIP`

AWS Config règle : `tagged-ec2-eip` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une adresse IP élastique Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si l'adresse IP élastique ne possède aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'adresse IP élastique n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une adresse IP élastique EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.38] Les instances EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::Instance`

AWS Config règle : `tagged-ec2-instance` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une instance Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si l'instance ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'instance n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous

pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une instance EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.39] Les passerelles Internet EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::InternetGateway`

AWS Config règle : `tagged-ec2-internetgateway` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		aux AWS exigences.	

Ce contrôle vérifie si une passerelle Internet Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la passerelle Internet ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la passerelle Internet n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une passerelle Internet EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.40] Les passerelles NAT EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::NatGateway`

AWS Config règle : `tagged-ec2-natgateway` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une passerelle de traduction d'adresses réseau (NAT) Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la passerelle NAT ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la passerelle NAT n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif,

propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une passerelle NAT EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.41] Les ACL du réseau EC2 doivent être balisées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::NetworkAcl`

AWS Config règle : `tagged-ec2-networkacl` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une liste de contrôle d'accès réseau (ACL réseau) Amazon EC2 contient des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si l'ACL réseau ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si aucune clé n'est associée à l'ACL du réseau. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une ACL du réseau EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.42] Les tables de routage EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::RouteTable`

AWS Config règle : `tagged-ec2-routetable` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une table de routage Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la table de routage ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas

présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la table de routage n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une table de routage EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.43] Les groupes de sécurité EC2 doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::SecurityGroup`

AWS Config règle : `tagged-ec2-securitygroup` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de sécurité Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le groupe de sécurité ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de sécurité n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe de sécurité EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.44] Les sous-réseaux EC2 doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::Subnet`

AWS Config règle : `tagged-ec2-subnet` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un sous-réseau Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le sous-réseau ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le sous-réseau n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un sous-réseau EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.45] Les volumes EC2 doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::Volume`

AWS Config règle : `tagged-ec2-volume` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un volume Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le volume ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le volume n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un volume EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.46] Les Amazon VPC doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::VPC`

AWS Config règle : `tagged-ec2-vpc` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un Amazon Virtual Private Cloud (Amazon VPC) possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le VPC Amazon ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre. `requiredTagKeys` Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le VPC Amazon n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un VPC, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.47] Les services de point de terminaison Amazon VPC doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::VPCEndpointService`

AWS Config règle : `tagged-ec2-vpcendpointservice` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un service de point de terminaison Amazon VPC possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le service de point de terminaison ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le service de point de terminaison n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un service de point de terminaison Amazon VPC, consultez la section Gérer les balises dans la section Configurer un service de point de terminaison du AWS PrivateLink Guide.

[EC2.48] Les journaux de flux Amazon VPC doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::FlowLog`

AWS Config règle : `tagged-ec2-flowlog` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un journal de flux Amazon VPC contient des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le journal de flux ne contient aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le journal de flux n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un journal de flux Amazon VPC, consultez la section Marquer un journal de flux dans le guide de l'utilisateur d'Amazon VPC.

[EC2.49] Les connexions d'appairage Amazon VPC doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::VPCPeeringConnection`

AWS Config règle : `tagged-ec2-vpcpeeringconnection` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une connexion d'appairage Amazon VPC possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la connexion d'appairage ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre

`requiredTagKeys` ne sont pas présentes. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la connexion d'appairage n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une connexion d'appairage Amazon VPC, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.50] Les passerelles VPN EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::VPNGateway`

AWS Config règle : `tagged-ec2-vpngateway` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une passerelle VPN Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la passerelle VPN ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la passerelle VPN n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une passerelle VPN EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2

Exigences associées : NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 NIST.800-171.r2 3.1.12, NIST.800-171.r2 3.1.20, PCI DSS v4.0. 1/10.2.1

Catégorie : Identifier - Journalisation

Gravité : Faible

Type de ressource : `AWS::EC2::ClientVpnEndpoint`

AWS Config règle : **`ec2-client-vpn-connection-log-enabled`**

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des connexions client est activée sur un AWS Client VPN terminal. Le contrôle échoue si la journalisation des connexions client n'est pas activée sur le terminal.

Les points de terminaison VPN client permettent aux clients distants de se connecter en toute sécurité aux ressources d'un Virtual Private Cloud (VPC) dans. AWS Les journaux de connexion vous

permettent de suivre l'activité des utilisateurs sur le point de terminaison VPN et offrent une visibilité. Lorsque vous activez la journalisation des connexions, vous pouvez spécifier le nom d'un flux de journaux dans le groupe de journaux. Si vous ne spécifiez pas de flux de journal, le service Client VPN en crée un pour vous.

Correction

Pour activer la journalisation des connexions, consultez la section Activer la journalisation des connexions pour un point de terminaison Client VPN existant dans le Guide de l'AWS Client VPN administrateur.

[EC2.52] Les passerelles de transit EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::TransitGateway`

AWS Config règle : `tagged-ec2-transitgateway` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	`No default value`

Ce contrôle vérifie si une passerelle de transit Amazon EC2 possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la passerelle de transit ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans

le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la passerelle de transit n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnes Services AWS, notamment AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une passerelle de transit EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/5.3, CIS AWS Foundations Benchmark v3.0. 0/52., PCI DSS version 4.0. 1/1.3.1

Catégorie : Protection > Configuration réseau sécurisée > Configuration du groupe de sécurité

Gravité : Élevée

Type de ressource : `AWS::EC2::SecurityGroup`

Règle AWS Config : [vpc-sg-port-restriction-check]

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`ipType`	La version IP	String	Non personnalisable	`IPv4`
`restrictPorts`	Liste des ports qui doivent rejeter le trafic entrant	IntegerList	Non personnalisable	`22,3389`

Ce contrôle vérifie si un groupe de sécurité Amazon EC2 autorise l'entrée à partir de la version 0.0.0. 0/0 vers les ports d'administration du serveur distant (ports 22 et 3389). Le contrôle échoue si le groupe de sécurité autorise l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou 3389.

Les groupes de sécurité autorisent le filtrage avec état du trafic réseau entrant et sortant vers des ressources AWS . Nous recommandons qu'aucun groupe de sécurité n'autorise un accès d'entrée illimité aux ports d'administration des serveurs distants, tels que SSH vers le port 22 et RDP vers le port 3389, en utilisant les protocoles TDP (6), UDP (17) ou ALL (-1). Permettre au public d'accéder à ces ports augmente la surface d'attaque des ressources et le risque de compromission des ressources.

Correction

Pour mettre à jour une règle de groupe de sécurité EC2 afin d'interdire le trafic entrant vers les ports spécifiés, consultez la section Mettre à jour les règles du groupe de sécurité dans le guide de l'utilisateur Amazon EC2. Après avoir sélectionné un groupe de sécurité dans la console Amazon

EC2, choisissez Actions, Modifier les règles entrantes. Supprimez la règle qui autorise l'accès au port 22 ou au port 3389.

[EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/5.4, CIS AWS Foundations Benchmark v3.0. 0/53., PCI DSS version 4.0. 1/1.3.1

Catégorie : Protection > Configuration réseau sécurisée > Configuration du groupe de sécurité

Gravité : Élevée

Type de ressource : `AWS::EC2::SecurityGroup`

Règle AWS Config : `vpc-sg-port-restriction-check`

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`ipType`	La version IP	String	Non personnalisable	`IPv6`
`restrictPorts`	Liste des ports qui doivent rejeter le trafic entrant	IntegerList	Non personnalisable	`22,3389`

Ce contrôle vérifie si un groupe de sécurité Amazon EC2 autorise l'entrée depuis : :/0 vers les ports d'administration du serveur distant (ports 22 et 3389). Le contrôle échoue si le groupe de sécurité autorise l'entrée depuis : :/0 vers le port 22 ou 3389.

Les groupes de sécurité autorisent le filtrage avec état du trafic réseau entrant et sortant vers des ressources AWS . Nous recommandons qu'aucun groupe de sécurité n'autorise un accès d'entrée

illimité aux ports d'administration des serveurs distants, tels que SSH vers le port 22 et RDP vers le port 3389, en utilisant les protocoles TDP (6), UDP (17) ou ALL (-1). Permettre au public d'accéder à ces ports augmente la surface d'attaque des ressources et le risque de compromission des ressources.

Correction

Pour mettre à jour une règle de groupe de sécurité EC2 afin d'interdire le trafic entrant vers les ports spécifiés, consultez la section Mettre à jour les règles du groupe de sécurité dans le guide de l'utilisateur Amazon EC2. Après avoir sélectionné un groupe de sécurité dans la console Amazon EC2, choisissez Actions, Modifier les règles entrantes. Supprimez la règle qui autorise l'accès au port 22 ou au port 3389.

[EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Catégorie : Protéger > Gestion des accès sécurisés > Contrôle d'accès

Gravité : Moyenne

Type de ressource :`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Règle AWS Config : vpc-endpoint-enabled

Type de calendrier : Périodique

Paramètres :

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`serviceNames`	Obligatoire	Nom du service évalué par le contrôle	String	Non personnalisable	`ecr.api`

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`vpcIds`	Facultatif	Comma-separated liste des identifiants Amazon VPC pour les points de terminaison VPC. S'il est fourni, le contrôle échoue si les services spécifiés dans le `serviceName` paramètre ne possèdent pas l'un de ces points de terminaison VPC.	StringList	Personnalisez avec un ou plusieurs identifiants VPC	Aucune valeur par défaut

Ce contrôle vérifie si un cloud privé virtuel (VPC) que vous gérez possède un point de terminaison VPC d'interface pour l'API Amazon ECR. Le contrôle échoue si le VPC ne possède pas de point de terminaison VPC d'interface pour l'API ECR. Ce contrôle évalue les ressources dans un seul compte.

AWS PrivateLink permet aux clients d'accéder aux services hébergés de AWS manière hautement disponible et évolutive, tout en maintenant l'ensemble du trafic réseau au sein du AWS réseau. Les utilisateurs des services peuvent accéder PrivateLink de manière privée aux services alimentés par leur VPC ou sur site, sans utiliser d'adresses IP publiques et sans avoir à faire transiter le trafic sur Internet.

Correction

Pour configurer un point de terminaison VPC, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le Guide.AWS PrivateLink

[EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Catégorie : Protéger > Gestion des accès sécurisés > Contrôle d'accès

Gravité : Moyenne

Type de ressource :`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Règle AWS Config : vpc-endpoint-enabled

Type de calendrier : Périodique

Paramètres :

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`serviceNames`	Obligatoire	Nom du service évalué par le contrôle	String	Non personnalisable	`ecr.dkr`
`vpcIds`	Facultatif	Comma-separated liste des identifiants Amazon VPC pour les points de terminaison VPC. S'il est fourni, le contrôle échoue si les services spécifiés dans le `serviceName` paramètre ne possèdent pas l'un de ces points de	StringList	Personnalisez avec un ou plusieurs identifiants VPC	Aucune valeur par défaut

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
		terminaison VPC.			

Ce contrôle vérifie si un cloud privé virtuel (VPC) que vous gérez possède un point de terminaison VPC d'interface pour Docker Registry. Le contrôle échoue si le VPC ne possède pas de point de terminaison VPC d'interface pour Docker Registry. Ce contrôle évalue les ressources dans un seul compte.

AWS PrivateLink permet aux clients d'accéder aux services hébergés de AWS manière hautement disponible et évolutive, tout en maintenant l'ensemble du trafic réseau au sein du AWS réseau. Les utilisateurs des services peuvent accéder PrivateLink de manière privée aux services alimentés par leur VPC ou sur site, sans utiliser d'adresses IP publiques et sans avoir à faire transiter le trafic sur Internet.

Correction

Pour configurer un point de terminaison VPC, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le Guide.AWS PrivateLink

[EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Catégorie : Protéger > Gestion des accès sécurisés > Contrôle d'accès

Gravité : Moyenne

Type de ressource :`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Règle AWS Config : vpc-endpoint-enabled

Type de calendrier : Périodique

Paramètres :

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`serviceNames`	Obligatoire	Nom du service évalué par le contrôle	String	Non personnalisable	`ssm`
`vpcIds`	Facultatif	Comma-separated liste des identifiants Amazon VPC pour les points de terminaison VPC. S'il est fourni, le contrôle échoue si les services spécifiés dans le `serviceName` paramètre ne possèdent aucun de ces	StringList	Personnalisez avec un ou plusieurs identifiants VPC	Aucune valeur par défaut

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
		points de terminaison VPC.			

Ce contrôle vérifie si le cloud privé virtuel (VPC) que vous gérez possède un point de terminaison VPC d'interface pour lequel vous gérez. AWS Systems Manager Le contrôle échoue si le VPC ne possède pas de point de terminaison VPC d'interface pour Systems Manager. Ce contrôle évalue les ressources dans un seul compte.

AWS PrivateLink permet aux clients d'accéder aux services hébergés de AWS manière hautement disponible et évolutive, tout en maintenant l'ensemble du trafic réseau au sein du AWS réseau. Les utilisateurs des services peuvent accéder PrivateLink de manière privée aux services alimentés par leur VPC ou sur site, sans utiliser d'adresses IP publiques et sans avoir à faire transiter le trafic sur Internet.

Correction

Pour configurer un point de terminaison VPC, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le Guide.AWS PrivateLink

[EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Catégorie : Protéger > Gestion des accès sécurisés > Contrôle d'accès

Gravité : Moyenne

Type de ressource :`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Règle AWS Config : vpc-endpoint-enabled

Type de calendrier : Périodique

Paramètres :

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`serviceNames`	Obligatoire	Nom du service évalué par le contrôle	String	Non personnalisable	`ssm-contacts`
`vpcIds`	Facultatif	Comma-separated liste des identifiants Amazon VPC pour les points de terminaison VPC. S'il est fourni, le contrôle échoue si les services spécifiés dans le `serviceName` paramètre ne possèdent	StringList	Personnalisez avec un ou plusieurs identifiants VPC	Aucune valeur par défaut

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
		aucun de ces points de terminaison VPC.			

Ce contrôle vérifie si le cloud privé virtuel (VPC) que vous gérez possède un point de terminaison VPC d'interface pour AWS Systems Manager les contacts d'Incident Manager. Le contrôle échoue si le VPC ne possède pas de point de terminaison VPC d'interface pour les contacts de Systems Manager Incident Manager. Ce contrôle évalue les ressources dans un seul compte.

AWS PrivateLink permet aux clients d'accéder aux services hébergés de AWS manière hautement disponible et évolutive, tout en maintenant l'ensemble du trafic réseau au sein du AWS réseau. Les utilisateurs des services peuvent accéder PrivateLink de manière privée aux services alimentés par leur VPC ou sur site, sans utiliser d'adresses IP publiques et sans avoir à faire transiter le trafic sur Internet.

Correction

Pour configurer un point de terminaison VPC, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le Guide.AWS PrivateLink

[EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Catégorie : Protéger > Gestion des accès sécurisés > Contrôle d'accès

Gravité : Moyenne

Type de ressource :`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Règle AWS Config : vpc-endpoint-enabled

Type de calendrier : Périodique

Paramètres :

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`serviceNames`	Obligatoire	Nom du service évalué par le contrôle	String	Non personnalisable	`ssm-incidents`
`vpcIds`	Facultatif	Comma-separated liste des identifiants Amazon VPC pour les points de terminaison VPC. S'il est fourni, le contrôle échoue si les services spécifiés dans le `serviceName` paramètre ne	StringList	Personnalisez avec un ou plusieurs identifiants VPC	Aucune valeur par défaut

Paramètre	Obligatoire	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
		possèdent aucun de ces points de terminaison VPC.			

Ce contrôle vérifie si le cloud privé virtuel (VPC) que vous gérez possède un point de terminaison VPC d'interface pour Incident Manager. AWS Systems Manager Le contrôle échoue si le VPC ne possède pas de point de terminaison VPC d'interface pour Systems Manager Incident Manager. Ce contrôle évalue les ressources dans un seul compte.

AWS PrivateLink permet aux clients d'accéder aux services hébergés de AWS manière hautement disponible et évolutive, tout en maintenant l'ensemble du trafic réseau au sein du AWS réseau. Les utilisateurs des services peuvent accéder PrivateLink de manière privée aux services alimentés par leur VPC ou sur site, sans utiliser d'adresses IP publiques et sans avoir à faire transiter le trafic sur Internet.

Correction

Pour configurer un point de terminaison VPC, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le Guide.AWS PrivateLink

[EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

Exigences associées : PCI DSS v4.0. 1/2.2.6

Catégorie : Protection > Sécurité du réseau

Gravité : Faible

Type de ressource : `AWS::EC2::LaunchTemplate`

Règle AWS Config : ec2-launch-template-imdsv2-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un modèle de lancement Amazon EC2 est configuré avec Instance Metadata Service version 2 (IMDSv2). Le contrôle échoue s'il `HttpTokens` est défini sur`optional`.

L'exécution des ressources sur les versions logicielles prises en charge garantit des performances, une sécurité et un accès aux fonctionnalités les plus récentes. Des mises à jour régulières protègent contre les vulnérabilités, ce qui contribue à garantir une expérience utilisateur stable et efficace.

Correction

Pour exiger IMDSv2 sur un modèle de lancement EC2, consultez Configurer les options du service de métadonnées d'instance dans le guide de l'utilisateur Amazon EC2.

[EC2.171] La journalisation des connexions VPN EC2 doit être activée

Exigences associées : CIS AWS Foundations Benchmark v3.0. 0/53., PCI DSS version 4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::EC2::VPNConnection`

Règle AWS Config : ec2-vpn-connection-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si Amazon CloudWatch Logs est activé pour les deux tunnels sur une connexion AWS Site-to-Site VPN. Le contrôle échoue si les CloudWatch journaux ne sont pas activés pour une connexion Site-to-Site VPN pour les deux tunnels.

AWS Site-to-Site Les journaux VPN vous offrent une meilleure visibilité de vos déploiements Site-to-Site VPN. Grâce à cette fonctionnalité, vous avez accès aux journaux de connexion Site-to-Site VPN qui fournissent des détails sur l'établissement du tunnel de sécurité IP (IPsec), les négociations sur l'échange de clés Internet (IKE) et les messages du protocole de détection des pairs morts (DDP). Site-to-Site Les journaux VPN peuvent être publiés dans CloudWatch Logs. Cette fonctionnalité

fournit aux clients un moyen unique et cohérent d'accéder aux journaux détaillés de toutes leurs connexions Site-to-Site VPN et de les analyser.

Correction

Pour activer la journalisation par tunnel sur une connexion VPN EC2, consultez les journaux AWS Site-to-Site VPN dans le guide de l'utilisateur du AWS Site-to-Site VPN.

[EC2.172] Les paramètres d'accès public EC2 VPC Block devraient bloquer le trafic de passerelle Internet

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Moyenne

Type de ressource : `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config règle : `ec2-vpc-bpa-internet-gateway-blocked` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`vpcBpaInternetGatewayBlockMode`	Valeur de chaîne du mode d'options VPC BPA.	Enum	`block-bidirectional` , `block-ingress`	Aucune valeur par défaut

Ce contrôle vérifie si les paramètres BPA (Amazon EC2 VPC Block Public Access) sont configurés pour bloquer le trafic de passerelle Internet pour tous les Amazon VPC du. Compte AWS Le contrôle échoue si les paramètres BPA du VPC ne sont pas configurés pour bloquer le trafic de passerelle Internet. Pour que le contrôle passe, le BPA du VPC `InternetGatewayBlockMode` doit être réglé sur ou. `block-bidirectional` `block-ingress` Si le paramètre `vpcBpaInternetGatewayBlockMode` est fourni, le contrôle est transmis

uniquement si la valeur BPA du VPC pour `InternetGatewayBlockMode` correspond au paramètre.

La configuration des paramètres VPC BPA pour votre compte vous Région AWS permet d'empêcher les ressources des VPC et des sous-réseaux que vous possédez dans cette région d'atteindre ou d'être atteintes depuis Internet via des passerelles Internet et des passerelles Internet de sortie uniquement. Si vous avez besoin de VPC et de sous-réseaux spécifiques pour pouvoir accéder ou être accessibles depuis Internet, vous pouvez les exclure en configurant les exclusions BPA des VPC. Pour obtenir des instructions sur la création et la suppression d'exclusions, consultez la section Créer et supprimer des exclusions dans le guide de l'utilisateur Amazon VPC.

Correction

Pour activer le BPA bidirectionnel au niveau du compte, consultez Activer le mode bidirectionnel BPA pour votre compte dans le guide de l'utilisateur Amazon VPC. Pour activer le BPA en entrée uniquement, voir Changer le mode BPA du VPC en mode BPA en entrée uniquement. Pour activer le BPA VPC au niveau de l'organisation, voir Activer le BPA VPC au niveau de l'organisation.

[EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EC2::SpotFleet`

Règle AWS Config : ec2-spot-fleet-request-ct-encryption-at-rest

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une demande Amazon EC2 Spot Fleet spécifiant les paramètres de lancement est configurée pour activer le chiffrement de tous les volumes Amazon Elastic Block Store (Amazon EBS) attachés aux instances EC2. Le contrôle échoue si la demande Spot Fleet spécifie les paramètres de lancement et n'active pas le chiffrement pour un ou plusieurs volumes EBS spécifiés dans la demande.

Pour un niveau de sécurité supplémentaire, vous devez activer le chiffrement pour les volumes Amazon EBS. Les opérations de chiffrement ont ensuite lieu sur les serveurs qui hébergent les

instances Amazon EC2, ce qui permet de garantir la sécurité des données au repos et des données en transit entre une instance et son stockage EBS attaché. Le chiffrement Amazon EBS est une solution de chiffrement simple pour les ressources EBS associées à vos instances EC2. Avec le chiffrement EBS, vous n'êtes pas obligé de créer, de maintenir et de sécuriser votre propre infrastructure de gestion des clés. Le chiffrement EBS est utilisé AWS KMS keys lors de la création de volumes chiffrés.

> **Remarques**
>
> Ce contrôle ne génère pas de résultats pour les demandes Amazon EC2 Spot Fleet qui utilisent des modèles de lancement. Il ne génère pas non plus de résultats pour les demandes Spot Fleet qui ne spécifient pas explicitement une valeur pour le `encrypted` paramètre.

Correction

Il n'existe aucun moyen direct de chiffrer un volume Amazon EBS non chiffré existant. Vous ne pouvez chiffrer un nouveau volume que lorsque vous le créez.

Toutefois, si vous activez le chiffrement par défaut, Amazon EBS chiffre les nouveaux volumes en utilisant votre clé par défaut pour le chiffrement EBS. Si vous n'activez pas le chiffrement par défaut, vous pouvez l'activer lorsque vous créez un volume individuel. Dans les deux cas, vous pouvez remplacer la clé par défaut pour le chiffrement EBS et choisir une clé gérée par le client. AWS KMS key Pour plus d'informations sur le chiffrement EBS, consultez la section relative au chiffrement Amazon EBS dans le guide de l'utilisateur Amazon EBS.

Pour plus d'informations sur la création d'une demande Amazon EC2 Spot Fleet, consultez Create a Spot Fleet dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

[EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::DHCPOptions`

Règle AWS Config : ec2-dhcp-options-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « v4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un ensemble d'options DHCP Amazon EC2 possède les clés de balise spécifiées par le paramètre. `requiredKeyTags` Le contrôle échoue si le jeu d'options ne comporte aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le jeu d'options ne comporte aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de

nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un ensemble d'options DHCP Amazon EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.175] Les modèles de lancement EC2 doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::LaunchTemplate`

Règle AWS Config : ec2-launch-template-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « v4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un modèle de lancement Amazon EC2 possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le modèle de lancement ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags`

paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le modèle de lancement ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un modèle de lancement Amazon EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.176] Les listes de préfixes EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::PrefixList`

Règle AWS Config : ec2-prefix-list-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « v4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une liste de préfixes Amazon EC2 possède les clés de balise spécifiées par le paramètre. `requiredKeyTags` Le contrôle échoue si la liste de préfixes ne contient aucune clé de balise ou si elle ne contient pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la liste de préfixes ne contient aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de

nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à une liste de préfixes Amazon EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::TrafficMirrorSession`

Règle AWS Config : ec2-traffic-mirror-session-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « v4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une session de miroir du trafic Amazon EC2 possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si la session ne possède aucune clé de balise ou si toutes les clés spécifiées par le `requiredKeyTags` paramètre ne sont pas présentes. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle

vérifie uniquement l'existence d'une clé de balise et échoue si la session ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à une session de miroir de trafic Amazon EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::TrafficMirrorFilter`

Règle AWS Config : ec2-traffic-mirror-filter-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « v4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un filtre de miroir de trafic Amazon EC2 possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le filtre ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le filtre n'en possède aucune. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un filtre de miroir de trafic Amazon EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::EC2::TrafficMirrorTarget`

Règle AWS Config : ec2-traffic-mirror-target-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « v4 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une cible miroir de trafic Amazon EC2 possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si la cible ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la cible n'en possède aucune. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser

des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à une cible miroir de trafic Amazon EC2, consultez la section Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

[EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2

Catégorie : Protection > Sécurité du réseau

Gravité : Moyenne

Type de ressource : `AWS::EC2::NetworkInterface`

Règle AWS Config : ec2-enis-source-destination-check-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la source/destination vérification est activée pour une interface Amazon EC2 Elastic Network (ENI) gérée par les utilisateurs. Le contrôle échoue si la source/destination vérification est désactivée pour l'ENI géré par l'utilisateur. Ce contrôle vérifie uniquement les types d'ENI suivants :`aws_codestar_connections_managed`,`branch`,`efa`, `interfacelambda`, et`quicksight`.

Source/destination la vérification des instances Amazon EC2 et des ENI associées doit être activée et configurée de manière cohérente sur toutes vos instances EC2. Chaque ENI dispose de ses propres paramètres pour les source/destination contrôles. Si la source/destination vérification est activée, Amazon EC2 applique la validation des source/destination adresses, ce qui garantit qu'une instance est la source ou la destination de tout trafic qu'elle reçoit. Cela fournit une couche supplémentaire de sécurité réseau en empêchant les ressources de gérer le trafic involontaire et en empêchant l'usurpation d'adresse IP.

> **Note**
>
> Si vous utilisez une instance EC2 comme instance NAT et que vous avez désactivé la source/destination vérification de son ENI, vous pouvez utiliser une passerelle NAT à la place.

Correction

Pour plus d'informations sur l'activation source/destination des vérifications pour une ENI Amazon EC2, consultez la section Modifier les attributs de l'interface réseau dans le guide de l'utilisateur Amazon EC2.

[EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EC2::LaunchTemplate`

Règle AWS Config : ec2-launch-templates-ebs-volume-encrypted

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un modèle de lancement Amazon EC2 active le chiffrement pour tous les volumes EBS attachés. Le contrôle échoue si le paramètre de chiffrement est défini sur tous `False` les volumes EBS spécifiés par le modèle de lancement EC2.

Le chiffrement Amazon EBS est une solution de chiffrement simple pour les ressources EBS associées aux instances Amazon EC2. Avec le chiffrement EBS, vous n'êtes pas obligé de créer,

de maintenir et de sécuriser votre propre infrastructure de gestion des clés. Le chiffrement EBS est utilisé AWS KMS keys lors de la création de volumes chiffrés et de snapshots. Les opérations de chiffrement ont lieu sur les serveurs qui hébergent les instances EC2, ce qui permet de garantir la sécurité des données au repos et des données en transit entre une instance EC2 et le stockage EBS qui lui est rattaché. Pour plus d'informations, consultez la section Chiffrement Amazon EBS dans le Guide de l'utilisateur Amazon EC2.

Vous pouvez activer le chiffrement EBS lors du lancement manuel d'instances EC2 individuelles. Cependant, l'utilisation des modèles de lancement EC2 et la configuration des paramètres de chiffrement dans ces modèles présentent plusieurs avantages. Vous pouvez appliquer le chiffrement en tant que norme et garantir l'utilisation de paramètres de chiffrement cohérents. Vous pouvez également réduire le risque d'erreur et de failles de sécurité susceptibles de se produire lors du lancement manuel d'instances.

> **Note**
>
> Lorsque ce contrôle vérifie un modèle de lancement EC2, il évalue uniquement les paramètres de chiffrement EBS explicitement spécifiés par le modèle. L'évaluation n'inclut pas les paramètres de chiffrement hérités des paramètres de chiffrement EBS au niveau du compte, les mappages de périphériques par blocs AMI ou les états de chiffrement des instantanés source.

Correction

Une fois que vous avez créé un modèle de lancement Amazon EC2, vous ne pouvez pas le modifier. Vous pouvez toutefois créer une nouvelle version d'un modèle de lancement et modifier les paramètres de chiffrement dans cette nouvelle version du modèle. Vous pouvez également spécifier la nouvelle version comme version par défaut du modèle de lancement. Ensuite, si vous lancez une instance EC2 à partir d'un modèle de lancement et que vous ne spécifiez pas de version de modèle, EC2 utilise les paramètres de la version par défaut lorsqu'il lance l'instance. Pour plus d'informations, consultez Modifier un modèle de lancement dans le guide de l'utilisateur Amazon EC2.

[EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::EC2::SnapshotBlockPublicAccess`

Règle AWS Config : ebs-snapshot-block-public-access

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le blocage de l'accès public au niveau du compte est activé pour empêcher le partage des instantanés Amazon EBS avec tous. Le contrôle échoue si le blocage de l'accès public n'est pas activé pour bloquer le partage des instantanés Amazon EBS avec tous.

Pour empêcher le partage public de vos instantanés Amazon EBS, vous pouvez activer le blocage de l'accès public aux instantanés. Une fois que le blocage de l'accès public aux instantanés est activé dans une région, toute tentative de partage public d'instantanés dans cette région est automatiquement bloquée. Cela permet d'améliorer la sécurité des instantanés et de protéger les données des instantanés contre tout accès non autorisé ou involontaire.

Correction

Pour activer le blocage de l'accès public pour les instantanés, consultez la section Configurer l'accès public bloqué pour les instantanés Amazon EBS dans le guide de l'utilisateur Amazon EBS. Pour Bloquer l'accès public, choisissez Bloquer tout accès public.

[EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::EC2::VPNConnection`

Règle AWS Config : ec2-vpn-connection-ike-version-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une connexion AWS Site-to-Site VPN est configurée pour utiliser le protocole IKEv2. Le contrôle échoue si une connexion Site-to-Site VPN autorise le protocole IKEv1 ou ne se limite pas explicitement au protocole IKEv2 sur tous les tunnels VPN.

IKEv2 fournit des algorithmes cryptographiques plus puissants et des fonctionnalités de sécurité améliorées par rapport à l'ancien protocole IKEv1, notamment une protection intégrée contre les attaques par déni de service et des mécanismes d'authentification améliorés. IKEv1 présente des vulnérabilités et des faiblesses connues dans son processus d'échange de clés qui peuvent être exploitées par des attaquants pour compromettre la sécurité des tunnels VPN. En renforçant IKEv2-only les connexions, vous réduisez votre surface d'attaque et garantissez que les communications VPN utilisent des protocoles de chiffrement modernes conformes aux normes du secteur qui protègent mieux les données en transit.

Correction

Pour mettre à jour la version IKE d'un tunnel VPN sur une connexion VPN EC2, voir Modifier les options du tunnel AWS Site-to-Site VPN dans le guide de l'utilisateur du AWS Site-to-Site VPN.

Contrôles Security Hub CSPM pour Auto Scaling

Ces contrôles Security Hub CSPM évaluent le service et les ressources Amazon EC2 Auto Scaling.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB

Exigences associées : PCI DSS v3.2. 1/22, 2 NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 SI-2

Catégorie : Identifier - Inventaire

Gravité : Faible

Type de ressource : `AWS::AutoScaling::AutoScalingGroup`

Règle AWS Config : `autoscaling-group-elb-healthcheck-required`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe Amazon EC2 Auto Scaling associé à un équilibreur de charge utilise les tests de santé Elastic Load Balancing (ELB). Le contrôle échoue si le groupe Auto Scaling n'utilise pas les bilans de santé ELB.

Les bilans de santé ELB permettent de garantir qu'un groupe Auto Scaling peut déterminer l'état de santé d'une instance sur la base de tests supplémentaires fournis par l'équilibreur de charge. L'utilisation des contrôles de santé d'Elastic Load Balancing permet également de garantir la disponibilité des applications qui utilisent les groupes EC2 Auto Scaling.

Correction

Pour ajouter des tests de santé Elastic Load Balancing, consultez la section Ajouter des contrôles de santé Elastic Load Balancing dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

[AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::AutoScaling::AutoScalingGroup`

Règle AWS Config : `autoscaling-multiple-az`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM	
`minAvailabilityZones`	Nombre minimum de zones de disponibilité	Enum	`2, 3, 4, 5, 6`	`2`	

Ce contrôle vérifie si un groupe Amazon EC2 Auto Scaling couvre au moins le nombre spécifié de zones de disponibilité (AZ). Le contrôle échoue si un groupe Auto Scaling ne couvre pas au moins le nombre de AZ spécifié. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour

le nombre minimum de zones de disponibilité, Security Hub CSPM utilise une valeur par défaut de deux zones de disponibilité.

Un groupe Auto Scaling qui ne couvre pas plusieurs zones de zone ne peut pas lancer d'instances dans une autre zone de zone pour compenser l'indisponibilité de la zone de disponibilité unique configurée. Cependant, un groupe Auto Scaling avec une seule zone de disponibilité peut être préférable dans certains cas d'utilisation, tels que les tâches par lots ou lorsque les coûts de transfert inter-AZ doivent être réduits au minimum. Dans ce cas, vous pouvez désactiver ce contrôle ou supprimer ses résultats.

Correction

Pour ajouter des AZ à un groupe Auto Scaling existant, consultez la section Ajouter et supprimer des zones de disponibilité dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

[AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)

Exigences associées : NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/2.2.6

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::AutoScaling::LaunchConfiguration`

Règle AWS Config : `autoscaling-launchconfig-requires-imdsv2`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si IMDSv2 est activé sur toutes les instances lancées par les groupes Amazon EC2 Auto Scaling. Le contrôle échoue si la version du service de métadonnées d'instance (IMDS) n'est pas incluse dans la configuration de lancement ou est configurée en tant `token optional` que paramètre qui autorise IMDSv1 ou IMDSv2.

IMDS fournit des données sur votre instance que vous pouvez utiliser pour configurer ou gérer l'instance en cours d'exécution.

La version 2 de l'IMDS ajoute de nouvelles protections qui n'étaient pas disponibles dans IMDSv1 afin de mieux protéger vos instances EC2.

Correction

Un groupe Auto Scaling est associé à une configuration de lancement à la fois. Vous ne pouvez pas modifier une configuration de lancement après l'avoir créée. Pour modifier la configuration de lancement d'un groupe Auto Scaling, utilisez une configuration de lancement existante comme base pour une nouvelle configuration de lancement avec IMDSv2 activé. Pour plus d'informations, consultez Configurer les options de métadonnées d'instance pour les nouvelles instances dans le guide de l'utilisateur Amazon EC2.

[AutoScaling.4] La configuration de lancement du groupe Auto Scaling ne doit pas comporter de limite de sauts de réponse aux métadonnées supérieure à 1

> **Important**
>
> Security Hub CSPM a retiré ce contrôle en avril 2024. Pour de plus amples informations, veuillez consulter Journal des modifications pour les contrôles CSPM de Security Hub.

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::AutoScaling::LaunchConfiguration`

Règle AWS Config : `autoscaling-launch-config-hop-limit`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie le nombre de sauts réseau qu'un jeton de métadonnées peut effectuer. Le contrôle échoue si la limite de sauts de réponse des métadonnées est supérieure à1.

Le service de métadonnées d'instance (IMDS) fournit des informations de métadonnées sur une instance Amazon EC2 et est utile pour la configuration des applications. Le fait de restreindre la PUT

réponse HTTP du service de métadonnées à l'instance EC2 uniquement protège l'IMDS contre toute utilisation non autorisée.

Le champ Time To Live (TTL) du paquet IP est réduit d'une unité à chaque saut. Cette réduction peut être utilisée pour garantir que le paquet ne voyage pas en dehors d'EC2. IMDSv2 protège les instances EC2 qui peuvent avoir été mal configurées en tant que routeurs ouverts, pare-feux de couche 3, VPN, tunnels ou périphériques NAT, empêchant ainsi les utilisateurs non autorisés de récupérer des métadonnées. Avec IMDSv2, la PUT réponse contenant le jeton secret ne peut pas voyager en dehors de l'instance car la limite de sauts de réponse aux métadonnées par défaut est définie sur. 1 Toutefois, si cette valeur est supérieure à1, le jeton peut quitter l'instance EC2.

Correction

Pour modifier la limite de sauts de réponse aux métadonnées pour une configuration de lancement existante, consultez la section Modifier les options de métadonnées d'instance pour les instances existantes dans le guide de l'utilisateur Amazon EC2.

[Autoscaling.5] Les instances Amazon EC2 lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresses IP publiques

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::AutoScaling::LaunchConfiguration`

Règle AWS Config : `autoscaling-launch-config-public-ip-disabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la configuration de lancement associée à un groupe Auto Scaling attribue une adresse IP publique aux instances du groupe. Le contrôle échoue si la configuration de lancement associée attribue une adresse IP publique.

Les instances Amazon EC2 dans une configuration de lancement de groupe Auto Scaling ne doivent pas être associées à une adresse IP publique, sauf dans des cas limités. Les instances Amazon EC2 ne doivent être accessibles que derrière un équilibreur de charge au lieu d'être directement exposées à Internet.

Correction

Un groupe Auto Scaling est associé à une configuration de lancement à la fois. Vous ne pouvez pas modifier une configuration de lancement après l'avoir créée. Pour modifier la configuration du lancement d'un groupe Auto Scaling, utilisez une configuration du lancement existante comme base de la nouvelle configuration du lancement. Mettez ensuite à jour le groupe Auto Scaling de manière à utiliser la nouvelle configuration du lancement. Pour obtenir des instructions détaillées, consultez Modifier la configuration de lancement d'un groupe Auto Scaling dans le manuel Amazon EC2 Auto Scaling User Guide. Lors de la création de la nouvelle configuration de lancement, sous Configuration supplémentaire, pour Détails avancés, type d'adresse IP, choisissez Ne pas attribuer d'adresse IP publique à aucune instance.

Après avoir modifié la configuration de lancement, Auto Scaling lance de nouvelles instances avec les nouvelles options de configuration. Les instances existantes ne sont pas affectées. Pour mettre à jour une instance existante, nous vous recommandons d'actualiser votre instance ou d'autoriser le dimensionnement automatique afin de remplacer progressivement les anciennes instances par des instances plus récentes en fonction de vos politiques de résiliation. Pour plus d'informations sur la mise à jour des instances Auto Scaling, consultez Update Auto Scaling instances dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

[AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::AutoScaling::AutoScalingGroup`

Règle AWS Config : `autoscaling-multiple-instance-types`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe Amazon EC2 Auto Scaling utilise plusieurs types d'instances. Le contrôle échoue si le groupe Auto Scaling n'a qu'un seul type d'instance défini.

Vous pouvez améliorer la disponibilité en déployant votre application entre plusieurs types d'instances s'exécutant dans plusieurs zones de disponibilité. Security Hub CSPM recommande d'utiliser plusieurs types d'instances afin que le groupe Auto Scaling puisse lancer un autre type d'instance si la capacité d'instance est insuffisante dans les zones de disponibilité que vous avez choisies.

Correction

Pour créer un groupe Auto Scaling avec plusieurs types d'instances, consultez la section Groupes Auto Scaling avec plusieurs types d'instances et options d'achat dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

[AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::AutoScaling::AutoScalingGroup`

Règle AWS Config : `autoscaling-launch-template`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe Amazon EC2 Auto Scaling est créé à partir d'un modèle de lancement EC2. Ce contrôle échoue si aucun groupe Amazon EC2 Auto Scaling n'est créé avec un modèle de lancement ou si aucun modèle de lancement n'est spécifié dans une politique d'instances mixtes.

Un groupe EC2 Auto Scaling peut être créé à partir d'un modèle de lancement EC2 ou d'une configuration de lancement. Cependant, l'utilisation d'un modèle de lancement pour créer un groupe Auto Scaling garantit que vous avez accès aux dernières fonctionnalités et améliorations.

Correction

Pour créer un groupe Auto Scaling avec un modèle de lancement EC2, consultez Create an Auto Scaling group using a launch template dans le manuel Amazon EC2 Auto Scaling User Guide. Pour plus d'informations sur le remplacement d'une configuration de lancement par un modèle de lancement, consultez la section Remplacer une configuration de lancement par un modèle de lancement dans le guide de l'utilisateur Amazon EC2.

[AutoScaling.10] Les groupes EC2 Auto Scaling doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AutoScaling::AutoScalingGroup`

AWS Configrègle : `tagged-autoscaling-autoscalinggroup` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe Amazon EC2 Auto Scaling possède des balises avec les clés spécifiques définies dans le `requiredTagKeys` paramètre. Le contrôle échoue si le groupe Auto Scaling ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le

paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe Auto Scaling n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe Auto Scaling, consultez la section Groupes et instances Tag Auto Scaling dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Contrôles CSPM de Security Hub pour Amazon ECR

Ces contrôles CSPM de Security Hub évaluent le service et les ressources Amazon Elastic Container Registry (Amazon ECR).

Il se peut que ces commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée

Exigences associées : NIST.800-53.r5 RA-5 PCI DSS v4.0. 1/62.2.3, PCI DSS v4.0. 1/62.2.4

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::ECR::Repository`

Règle AWS Config : ecr-private-image-scanning-enabled

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la numérisation des images est configurée pour un référentiel Amazon ECR privé. Le contrôle échoue si le référentiel ECR privé n'est pas configuré pour le scan en mode push ou en continu.

La numérisation d'images ECR permet d'identifier les vulnérabilités logicielles dans les images de vos conteneurs. La configuration de la numérisation d'images sur les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

Correction

Pour configurer la numérisation d'images pour un référentiel ECR, consultez la section Numérisation d'images dans le guide de l'utilisateur d'Amazon Elastic Container Registry.

[ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8 (1)

Catégorie : Identifier > Inventaire > Marquage

Gravité : Moyenne

Type de ressource : `AWS::ECR::Repository`

Règle AWS Config : ecr-private-tag-immutability-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'immuabilité des balises est activée dans un référentiel ECR privé. Ce contrôle échoue si l'immuabilité des balises est désactivée dans un référentiel ECR privé. Cette règle est appliquée si l'immuabilité des balises est activée et possède la valeur `IMMUTABLE` requise.

Amazon ECR Tag Immutability permet aux clients de s'appuyer sur les balises descriptives d'une image en tant que mécanisme fiable pour suivre et identifier les images de manière unique. Une balise immuable est statique, ce qui signifie que chaque balise fait référence à une image unique. Cela améliore la fiabilité et l'évolutivité, car l'utilisation d'une balise statique entraîne toujours le déploiement de la même image. Une fois configurée, l'immuabilité des balises empêche leur remplacement, ce qui réduit la surface d'attaque.

Correction

Pour créer un référentiel avec des balises immuables configurées ou pour mettre à jour les paramètres de mutabilité des balises d'image pour un référentiel existant, consultez la section Mutabilité des balises d'image dans le guide de l'utilisateur d'Amazon Elastic Container Registry.

[ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::ECR::Repository`

Règle AWS Config : ecr-private-lifecycle-policy-configured

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si au moins une politique de cycle de vie est configurée pour un référentiel Amazon ECR. Ce contrôle échoue si aucune politique de cycle de vie n'est configurée pour un référentiel ECR.

Les politiques de cycle de vie Amazon ECR vous permettent de préciser la gestion du cycle de vie des images dans un référentiel. En configurant des politiques de cycle de vie, vous pouvez

automatiser le nettoyage des images non utilisées et l'expiration des images en fonction de leur âge ou de leur nombre. L'automatisation de ces tâches peut vous aider à éviter d'utiliser involontairement des images obsolètes dans votre référentiel.

Correction

Pour configurer une politique de cycle de vie, voir Création d'un aperçu de la politique de cycle de vie dans le guide de l'utilisateur d'Amazon Elastic Container Registry.

[ECR.4] Les référentiels publics ECR doivent être étiquetés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::ECR::PublicRepository`

AWS Config règle : `tagged-ecr-publicrepository` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un référentiel public Amazon ECR possède des balises dont les clés spécifiques sont définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le référentiel public ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le

paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le référentiel public n'est balisé avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un référentiel public ECR, consultez la section Balisage d'un référentiel public Amazon ECR dans le guide de l'utilisateur d'Amazon Elastic Container Registry.

[ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys

Exigences connexes : NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 AU-9

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::ECR::Repository`

Règle AWS Config : ecr-repository-cmk-encryption-enabled

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`kmsKeyArns`	Une liste des Amazon Resource Names (ARN) AWS KMS keys à inclure dans l'évaluation. Le contrôle génère une détection `FAILED` si un référentiel ECR n'est pas chiffré avec une clé KMS dans la liste.	StringList (maximum de 10 articles)	1 à 10 ARN de clés KMS existantes. Par exemple : `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`	Aucune valeur par défaut

Ce contrôle vérifie si un référentiel Amazon ECR est chiffré au repos et géré AWS KMS key par le client. Le contrôle échoue si le référentiel ECR n'est pas chiffré avec une clé KMS gérée par le client. Vous pouvez éventuellement spécifier une liste de clés KMS que le contrôle doit inclure dans l'évaluation.

Par défaut, Amazon ECR chiffre les données du référentiel à l'aide des clés gérées par Amazon S3 (SSE-S3), à l'aide d'un AES-256 algorithme. Pour un contrôle supplémentaire, vous pouvez configurer Amazon ECR pour crypter les données avec un AWS KMS key (SSE-KMS ou DSSE-

KMS) à la place. La clé KMS peut être : une clé Clé gérée par AWS qu'Amazon ECR crée et gère pour vous et qui possède l'alias`aws/ecr`, ou une clé gérée par le client que vous créez et gérez dans votre Compte AWS. Avec une clé KMS gérée par le client, vous avez le contrôle total de la clé. Cela inclut la définition et la mise à jour de la politique relative aux clés, la gestion des autorisations, la rotation du matériel cryptographique, l'attribution de balises, la création d'alias, ainsi que l'activation et la désactivation de la clé.

> **Note**
>
> AWS KMS prend en charge l'accès entre comptes aux clés KMS. Si un référentiel ECR est chiffré avec une clé KMS appartenant à un autre compte, ce contrôle n'effectue pas de vérifications entre comptes lorsqu'il évalue le référentiel. Le contrôle n'évalue pas si Amazon ECR peut accéder à la clé et l'utiliser lors de l'exécution d'opérations cryptographiques pour le référentiel.

Correction

Vous ne pouvez pas modifier les paramètres de chiffrement d'un référentiel ECR existant. Vous pouvez toutefois spécifier différents paramètres de chiffrement pour les référentiels ECR que vous créerez ultérieurement. Amazon ECR prend en charge l'utilisation de différents paramètres de chiffrement pour les référentiels individuels.

Pour plus d'informations sur les options de chiffrement pour les référentiels ECR, consultez la section Chiffrement au repos dans le guide de l'utilisateur Amazon ECR. Pour plus d'informations sur la gestion par le client AWS KMS keys, consultez AWS KMS keys le Guide du AWS Key Management Service développeur.

Contrôles Security Hub CSPM pour Amazon ECS

Ces contrôles Security Hub CSPM évaluent le service et les ressources Amazon Elastic Container Service (Amazon ECS). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ECS.2] Aucune adresse IP publique ne doit être attribuée automatiquement aux services ECS

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5

SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::ECS::Service`

AWS Configrègle : `ecs-service-assign-public-ip-disabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les services Amazon ECS sont configurés pour attribuer automatiquement des adresses IP publiques. Ce contrôle échoue si tel `AssignPublicIP` est le cas`ENABLED`. Ce contrôle passe si tel `AssignPublicIP` est le cas`DISABLED`.

Une adresse IP publique est une adresse IP accessible depuis Internet. Si vous lancez vos instances Amazon ECS avec une adresse IP publique, elles sont accessibles depuis Internet. Les services Amazon ECS ne doivent pas être accessibles au public, car cela peut permettre un accès involontaire à vos serveurs d'applications de conteneurs.

Correction

Vous devez d'abord créer une définition de tâche pour votre cluster qui utilise le mode `awsvpc` réseau et spécifie FARGATE pour. `requiresCompatibilities` Ensuite, pour la configuration de calcul, choisissez le type de lancement et FARGATE. Enfin, dans le champ Réseau, désactivez l'adresse IP publique pour désactiver l'attribution automatique d'adresses IP publiques à votre service.

[ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Identifier > Configuration des ressources

Gravité : Élevée

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-task-definition-pid-mode-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les définitions de tâches Amazon ECS sont configurées pour partager l'espace de noms de processus d'un hôte avec ses conteneurs. Le contrôle échoue si la définition de tâche partage l'espace de noms de processus de l'hôte avec les conteneurs qui y sont exécutés. Ce contrôle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Un espace de noms d'ID de processus (PID) permet de séparer les processus. Il empêche les processus du système d'être visibles et permet de réutiliser les PID, y compris le PID 1. Si l'espace de noms PID de l'hôte est partagé avec des conteneurs, cela permettra aux conteneurs de voir tous les processus du système hôte. Cela réduit l'avantage de l'isolation au niveau du processus entre l'hôte et les conteneurs. Ces circonstances peuvent entraîner un accès non autorisé aux processus sur l'hôte lui-même, y compris la capacité de les manipuler et d'y mettre fin. Les clients ne doivent pas partager l'espace de noms de processus de l'hôte avec les conteneurs qui s'exécutent sur celui-ci.

Correction

Pour configurer la `pidMode` définition d'une tâche, consultez la section Paramètres de définition de tâche dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés

Exigences associées : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Catégorie : Protection > Gestion des accès sécurisés > Restrictions d'accès des utilisateurs root

Gravité : Élevée

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-containers-nonprivileged

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le `privileged` paramètre de la définition du conteneur des définitions de tâches Amazon ECS est défini sur`true`. Le contrôle échoue si ce paramètre est égal à`true`. Ce contrôle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Nous vous recommandons de supprimer les privilèges élevés de vos définitions de tâches ECS. Lorsque le paramètre de privilège est défini`true`, le conteneur reçoit des privilèges élevés sur l'instance du conteneur hôte (comme l'utilisateur root).

Correction

Pour configurer le `privileged` paramètre sur une définition de tâche, consultez la section Paramètres avancés de définition de conteneur dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine

Exigences associées : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Élevée

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-containers-readonly-access

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les définitions de tâches ECS configurent les conteneurs de manière à ce qu'ils soient limités à un accès en lecture seule aux systèmes de fichiers racines montés. Le contrôle échoue si le `readonlyRootFilesystem` paramètre dans les définitions de conteneur de la définition de tâche ECS est défini sur ou si le paramètre n'existe pas dans la définition de conteneur au sein de la définition de tâche. `false` Ce contrôle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Si le `readonlyRootFilesystem` paramètre est défini sur `true` dans une définition de tâche Amazon ECS, le conteneur ECS bénéficie d'un accès en lecture seule à son système de fichiers racine. Cela réduit les vecteurs d'attaques de sécurité, car le système de fichiers racine de l'instance de conteneur ne peut pas être altéré ou écrit sans des montages de volumes explicites dotés d'autorisations de lecture-écriture pour les dossiers et répertoires du système de fichiers. L'activation de cette option est également conforme au principe du moindre privilège.

> **Note**
>
> Le `readonlyRootFilesystem` paramètre n'est pas pris en charge pour les conteneurs Windows. Les définitions de tâches `runtimePlatform` configurées pour spécifier une famille de `WINDOWS_SERVER` systèmes d'exploitation sont marquées comme `NOT_APPLICABLE` telles et ne généreront pas de résultats pour ce contrôle.

Correction

Pour accorder à un conteneur Amazon ECS un accès en lecture seule à son système de fichiers racine, ajoutez le `readonlyRootFilesystem` paramètre à la définition de tâche du conteneur et définissez la valeur du paramètre sur. `true` Pour plus d'informations sur les paramètres de définition des tâches et sur la manière de les ajouter à une définition de tâche, consultez les définitions de tâches Amazon ECS et la mise à jour d'une définition de tâche dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/8.6.2

Catégorie : Protéger > Développement sécurisé > Informations d'identification non codées en dur

Gravité : Élevée

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-no-environment-secrets

Type de calendrier : changement déclenché

Paramètres : `secretKeys` : `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, `ECS_ENGINE_AUTH_DATA` (non personnalisable)

Ce contrôle vérifie si la valeur clé de l'une des variables du `environment` paramètre des définitions de conteneur inclut `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, ou`ECS_ENGINE_AUTH_DATA`. Ce contrôle échoue si une seule variable d'environnement dans une définition de conteneur est égale à `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, ou`ECS_ENGINE_AUTH_DATA`. Ce contrôle ne couvre pas les variables environnementales transmises depuis d'autres sites tels qu'Amazon S3. Ce contrôle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

AWS Systems ManagerParameter Store peut vous aider à améliorer le niveau de sécurité de votre organisation. Nous vous recommandons d'utiliser le Parameter Store pour stocker les secrets et les informations d'identification au lieu de les transmettre directement à vos instances de conteneur ou de les coder en dur dans votre code.

Correction

Pour créer des paramètres à l'aide de SSM, consultez la section Creating Systems Manager dans le guide de l'AWS Systems Managerutilisateur. Pour plus d'informations sur la création d'une définition de tâche spécifiant un secret, consultez la section Spécification de données sensibles à l'aide de Secrets Manager dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation

Exigences connexes : NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Élevée

Type de ressource : `AWS::ECS::TaskDefinition`

AWS Configrègle : ecs-task-definition-log-configuration

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une configuration de journalisation est spécifiée pour la dernière définition de tâche Amazon ECS active. Le contrôle échoue si la `logConfiguration` propriété de la définition

de tâche n'est pas définie ou si la valeur de `logDriver` est nulle dans au moins une définition de conteneur.

La journalisation vous aide à maintenir la fiabilité, la disponibilité et les performances d'Amazon ECS. La collecte de données à partir des définitions de tâches apporte de la visibilité, ce qui peut vous aider à déboguer les processus et à identifier la cause première des erreurs. Si vous utilisez une solution de journalisation qui n'a pas besoin d'être définie dans la définition des tâches ECS (telle qu'une solution de journalisation tierce), vous pouvez désactiver ce contrôle après vous être assuré que vos journaux sont correctement capturés et transmis.

Correction

Pour définir une configuration de journal pour vos définitions de tâches Amazon ECS, consultez Spécifier une configuration de journal dans votre définition de tâche dans le guide du développeur Amazon Elastic Container Service.

[ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate

Exigences associées : NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::ECS::Service`

Règle AWS Config : ecs-fargate-latest-platform-version

Type de calendrier : changement déclenché

Paramètres :

- `latestLinuxVersion: 1.4.0`(non personnalisable)
- `latestWindowsVersion: 1.0.0`(non personnalisable)

Ce contrôle vérifie si les services Amazon ECS Fargate exécutent la dernière version de la plateforme Fargate. Ce contrôle échoue si la version de la plateforme n'est pas la plus récente.

AWS Fargateles versions de plate-forme font référence à un environnement d'exécution spécifique pour l'infrastructure de tâches Fargate, qui est une combinaison de versions d'exécution du noyau et du conteneur. De nouvelles versions de plate-forme sont publiées au fur et à mesure de l'évolution de l'environnement d'exécution. Par exemple, une nouvelle version peut être publiée pour les mises à jour du noyau ou du système d'exploitation, les nouvelles fonctionnalités, les corrections de bogues ou les mises à jour de sécurité. Des mises à jour de sécurité et des correctifs sont déployés automatiquement pour vos tâches Fargate. Si un problème de sécurité affectant une version de plate-forme est détecté, appliquez un AWS correctif à cette version.

Correction

Pour mettre à jour un service existant, y compris sa version de plateforme, consultez la section Mettre à jour un service dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.12] Les clusters ECS doivent utiliser Container Insights

Exigences connexes : NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::ECS::Cluster`

Règle AWS Config : ecs-container-insights-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les clusters ECS utilisent Container Insights. Ce contrôle échoue si Container Insights n'est pas configuré pour un cluster.

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances des clusters Amazon ECS. Utilisez CloudWatch Container Insights pour collecter, agréger et résumer les métriques et les journaux de vos applications conteneurisées et de vos microservices. CloudWatch collecte automatiquement des métriques pour de nombreuses ressources, telles que le processeur, la mémoire, le disque et le réseau. Conteneur Insights fournit également des informations de diagnostic (par exemple sur les échecs de redémarrage des

conteneurs) pour vous aider à isoler les problèmes et à les résoudre rapidement. Vous pouvez également définir des CloudWatch alarmes sur les métriques collectées par Container Insights.

Correction

Pour utiliser Container Insights, consultez la section Mettre à jour un service dans le guide de CloudWatch l'utilisateur Amazon.

[ECS.13] Les services ECS doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::ECS::Service`

AWS Configrègle : `tagged-ecs-service` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un service Amazon ECS possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le service ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le service n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un service ECS, consultez la section Marquage de vos ressources Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.14] Les clusters ECS doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::ECS::Cluster`

AWS Configrègle : `tagged-ecs-cluster` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un cluster Amazon ECS possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le cluster ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le cluster n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un cluster ECS, consultez la section Marquage de vos ressources Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.15] Les définitions de tâches ECS doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::ECS::TaskDefinition`

AWS Configrègle : `tagged-ecs-taskdefinition` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une définition de tâche Amazon ECS comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la définition de tâche ne comporte aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont

pas présentesrequiredTagKeys. Si le paramètre requiredTagKeys n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la définition de tâche n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent paraws:, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une définition de tâche ECS, consultez la section Marquage de vos ressources Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques

Exigences associées : PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::ECS::TaskSet`

AWS Configrègle : `ecs-taskset-assign-public-ip-disabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un ensemble de tâches Amazon ECS est configuré pour attribuer automatiquement des adresses IP publiques. Le contrôle échoue s'il `AssignPublicIP` est défini sur`ENABLED`.

Une adresse IP publique est accessible depuis Internet. Si vous configurez votre ensemble de tâches avec une adresse IP publique, les ressources associées à l'ensemble de tâches sont accessibles depuis Internet. Les ensembles de tâches ECS ne doivent pas être accessibles au public, car cela peut permettre un accès involontaire à vos serveurs d'applications de conteneurs.

Correction

Pour mettre à jour un ensemble de tâches ECS afin qu'il n'utilise pas d'adresse IP publique, consultez la section Mise à jour d'une définition de tâche Amazon ECS à l'aide de la console dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte

Exigences associées : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-task-definition-network-mode-not-host

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la dernière révision active d'une définition de tâche Amazon ECS utilise le mode `host` réseau. Le contrôle échoue si la dernière révision active de la définition de tâche ECS utilise le mode `host` réseau.

Lorsque vous utilisez le mode `host` réseau, la mise en réseau d'un conteneur Amazon ECS est directement liée à l'hôte sous-jacent qui exécute le conteneur. Par conséquent, ce mode permet aux conteneurs de se connecter à des services réseau privés en boucle sur l'hôte et de se faire passer pour l'hôte. D'autres inconvénients importants sont qu'il n'est pas possible de remapper un port de conteneur en mode `host` réseau et que vous ne pouvez pas exécuter plus d'une seule instanciation d'une tâche sur chaque hôte.

Correction

Pour plus d'informations sur les modes de mise en réseau et les options pour les tâches Amazon ECS hébergées sur des instances Amazon EC2, consultez les options de mise en réseau des tâches Amazon ECS pour le type de lancement EC2 dans le manuel du développeur Amazon Elastic Container Service. Pour plus d'informations sur la création d'une nouvelle révision d'une définition de tâche et la spécification d'un mode réseau différent, consultez la section Mise à jour d'une définition de tâche Amazon ECS dans ce guide.

Si la définition de tâche Amazon ECS a été créée parAWS Batch, consultez Modes de mise en réseau pour les AWS Batch tâches pour en savoir plus sur les modes de mise en réseau et l'utilisation typique des types de AWS Batch tâches et pour choisir une option sécurisée.

[ECS.18] Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS

Catégorie : Protéger > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-task-definition-efs-encryption-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la dernière révision active d'une définition de tâche Amazon ECS utilise le chiffrement en transit pour les volumes EFS. Le contrôle échoue si le chiffrement en transit est désactivé pour les volumes EFS dans la dernière révision active de la définition des tâches ECS.

Les volumes Amazon EFS fournissent un stockage de fichiers partagé simple, évolutif et persistant à utiliser avec vos tâches Amazon ECS. Amazon EFS prend en charge le chiffrement des données en transit grâce au protocole TLS (Transport Layer Security). Lorsque le chiffrement des données

en transit est déclaré comme option de montage pour votre système de fichiers EFS, Amazon EFS établit une connexion TLS sécurisée avec votre système de fichiers EFS lors du montage de votre système de fichiers.

Correction

Pour plus d'informations sur l'activation du chiffrement en transit pour la définition des tâches Amazon ECS avec les volumes EFS, consultez l'étape 5 : création d'une définition de tâche dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée

Catégorie : Protéger > Protection des données

Gravité : Moyenne

Type de ressource : `AWS::ECS::CapacityProvider`

Règle AWS Config : ecs-capacity-provider-termination-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un fournisseur de capacité Amazon ECS a activé la protection de résiliation gérée. Le contrôle échoue si la protection de terminaison gérée n'est pas activée sur un fournisseur de capacité ECS.

Les fournisseurs de capacité Amazon ECS gèrent la mise à l'échelle de l'infrastructure pour les tâches de vos clusters. Lorsque vous utilisez des instances EC2 pour votre capacité, vous utilisez le groupe Auto Scaling pour gérer les instances EC2. La protection contre la résiliation gérée permet à l'autoscaling de cluster de contrôler quelles instances sont résiliées. Lorsque vous utilisez la protection contre la résiliation gérée, Amazon ECS ne résilie que les instances EC2 qui n'ont pas de tâches Amazon ECS en cours d'exécution.

> **Note**
>
> Lors de l'utilisation de la protection contre la résiliation gérée, la mise à l'échelle gérée doit également être utilisée pour que la protection fonctionne.

Correction

Pour activer la protection de résiliation gérée pour un fournisseur de capacité Amazon ECS, consultez la section Mise à jour de la protection de résiliation gérée pour les fournisseurs de capacité Amazon ECS dans le guide du développeur Amazon Elastic Container Service.

[ECS.20] Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux

Catégorie : Protection > Gestion des accès sécurisés > Restrictions d'accès des utilisateurs root

Gravité : Moyenne

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-task-definition-linux-user-non-root

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la dernière révision active d'une définition de tâche Amazon ECS configure les conteneurs Linux pour qu'ils s'exécutent en tant qu'utilisateurs non root. Le contrôle échoue si un utilisateur root par défaut est configuré ou si la configuration utilisateur est absente pour un conteneur.

Lorsque les conteneurs Linux s'exécutent avec les privilèges root, ils présentent plusieurs risques de sécurité importants. Les utilisateurs root ont un accès illimité au conteneur. Cet accès élevé augmente le risque d'attaques visant à échapper aux conteneurs, dans le cadre desquelles un attaquant pourrait potentiellement sortir de l'isolation du conteneur et accéder au système hôte sous-jacent. Si un conteneur exécuté en tant que root est compromis, les attaquants peuvent l'exploiter pour accéder aux ressources du système hôte ou les modifier, affectant ainsi d'autres conteneurs ou l'hôte lui-même. En outre, l'accès root pourrait permettre des attaques par escalade de privilèges, permettant aux attaquants d'obtenir des autorisations supplémentaires au-delà de la portée prévue du conteneur. Le paramètre utilisateur dans les définitions de tâches ECS peut spécifier les utilisateurs dans plusieurs formats, notamment le nom d'utilisateur, l'ID utilisateur, le nom d'utilisateur avec le groupe ou l'UID avec l'ID de groupe. Il est important de tenir compte de ces différents formats lors de la configuration des définitions de tâches afin de garantir qu'aucun accès root n'est accordé par inadvertance. Conformément au principe du moindre privilège, les conteneurs doivent fonctionner avec les autorisations minimales requises en utilisant des utilisateurs non root.

Cette approche réduit considérablement la surface d'attaque potentielle et atténue l'impact des failles de sécurité potentielles.

> **Note**
>
> Ce contrôle évalue les définitions de conteneur dans une définition de tâche uniquement si elles `operatingSystemFamily` sont configurées comme `LINUX` ou `operatingSystemFamily` non dans la définition de tâche. Le contrôle génère un `FAILED` résultat pour une définition de tâche évaluée si aucune définition de conteneur dans la définition de tâche `user` n'a été configurée ou `user` configurée en tant qu'utilisateur root par défaut. Les utilisateurs root par défaut pour les `LINUX` conteneurs sont `"root"` et`"0"`.

Correction

Pour plus d'informations sur la création d'une nouvelle révision d'une définition de tâche Amazon ECS et la mise à jour du `user` paramètre dans la définition de conteneur, consultez la section Mise à jour d'une définition de tâche Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.

[ECS.21] Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows

Catégorie : Protection > Gestion des accès sécurisés > Restrictions d'accès des utilisateurs root

Gravité : Moyenne

Type de ressource : `AWS::ECS::TaskDefinition`

Règle AWS Config : ecs-task-definition-windows-user-non-admin

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la dernière révision active d'une définition de tâche Amazon ECS configure les conteneurs Windows pour qu'ils s'exécutent en tant qu'utilisateurs qui ne sont pas des administrateurs par défaut. Le contrôle échoue si un administrateur par défaut est configuré en tant qu'utilisateur ou si la configuration utilisateur est absente pour un conteneur.

Lorsque les conteneurs Windows s'exécutent avec des privilèges d'administrateur, ils présentent plusieurs risques de sécurité importants. Les administrateurs ont un accès illimité au conteneur. Cet accès élevé augmente le risque d'attaques visant à échapper aux conteneurs, dans le cadre desquelles un attaquant pourrait potentiellement sortir de l'isolation du conteneur et accéder au système hôte sous-jacent.

> **Note**
>
> Ce contrôle évalue les définitions de conteneur dans une définition de tâche uniquement si elles `operatingSystemFamily` sont configurées comme `WINDOWS_SERVER` ou `operatingSystemFamily` non dans la définition de tâche. Le contrôle générera un `FAILED` résultat pour une définition de tâche évaluée si aucune définition de conteneur dans la définition de tâche `user` n'a été configurée ou `user` configurée en tant qu'administrateur par défaut pour les `WINDOWS_SERVER` conteneurs, ce qui est le cas`"containeradministrator"`.

Correction

Pour plus d'informations sur la création d'une nouvelle révision d'une définition de tâche Amazon ECS et la mise à jour du `user` paramètre dans la définition de conteneur, consultez la section Mise à jour d'une définition de tâche Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.

Contrôles CSPM de Security Hub pour Amazon EFS

Ces contrôles CSPM Security Hub évaluent le service et les ressources Amazon Elastic File System (Amazon EFS). Il se peut que les commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.3.1, CIS AWS Foundations Benchmark v3.0. 0/24.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EFS::FileSystem`

Règle AWS Config : efs-encrypted-check

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si Amazon Elastic File System est configuré pour chiffrer les données du fichier à l'aide AWS KMS de. La vérification échoue dans les cas suivants.

- `Encrypted` est défini sur `false` dans la réponse `DescribeFileSystems`.
- La clé `KmsKeyId` de la `DescribeFileSystems` réponse ne correspond pas au paramètre `KmsKeyId` pour `efs-encrypted-check`.

Notez que ce contrôle n'utilise pas le paramètre `KmsKeyId` pour `efs-encrypted-check`. Il ne vérifie que la valeur de `Encrypted`.

Pour renforcer la sécurité de vos données sensibles dans Amazon EFS, vous devez créer des systèmes de fichiers chiffrés. Amazon EFS prend en charge le chiffrement pour les systèmes de fichiers au repos. Vous pouvez activer le chiffrement des données au repos lorsque vous créez un système de fichiers Amazon EFS. Pour en savoir plus sur le chiffrement Amazon EFS, consultez la section Chiffrement des données dans Amazon EFS dans le guide de l'utilisateur d'Amazon Elastic File System.

Correction

Pour plus d'informations sur le chiffrement d'un nouveau système de fichiers Amazon EFS, consultez la section Chiffrement des données au repos dans le Guide de l'utilisateur d'Amazon Elastic File System.

[EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegarde

Gravité : Moyenne

Type de ressource : `AWS::EFS::FileSystem`

Règle AWS Config : efs-in-backup-plan

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les systèmes de fichiers Amazon Elastic File System (Amazon EFS) sont ajoutés aux plans de sauvegarde de AWS Backup. Le contrôle échoue si les systèmes de fichiers Amazon EFS ne sont pas inclus dans les plans de sauvegarde.

L'inclusion des systèmes de fichiers EFS dans les plans de sauvegarde vous permet de protéger vos données contre la suppression et la perte de données.

Correction

Pour activer les sauvegardes automatiques pour un système de fichiers Amazon EFS existant, consultez Getting started 4 : Create Amazon EFS automatic backups dans le AWS Backup Developer Guide.

[EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine

Exigences connexes : NIST.800-53.r5 AC-6 (10)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::EFS::AccessPoint`

Règle AWS Config : efs-access-point-enforce-root-directory

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les points d'accès Amazon EFS sont configurés pour appliquer un répertoire racine. Le contrôle échoue si la valeur de `Path` est définie sur `/` (le répertoire racine par défaut du système de fichiers).

Lors de l'application forcée d'un répertoire racine, le client NFS lié au point d'accès utilise le répertoire racine configuré sur le point d'accès au lieu du répertoire racine du système de fichiers. L'application d'un répertoire racine pour un point d'accès permet de restreindre l'accès aux données

en garantissant que les utilisateurs du point d'accès ne peuvent accéder qu'aux fichiers du sous-répertoire spécifié.

Correction

Pour savoir comment appliquer un répertoire racine à un point d'accès Amazon EFS, consultez la section Appliquer un répertoire racine à un point d'accès dans le Guide de l'utilisateur d'Amazon Elastic File System.

[EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur

Exigences associées : NIST.800-53.r5 AC-6 (2), PCI DSS v4.0. 1/73.3.1

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::EFS::AccessPoint`

Règle AWS Config : efs-access-point-enforce-user-identity

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les points d'accès Amazon EFS sont configurés pour renforcer l'identité d'un utilisateur. Ce contrôle échoue si aucune identité d'utilisateur POSIX n'est définie lors de la création du point d'accès EFS.

Les points d'accès Amazon EFS sont des points d'entrée spécifiques à l'application dans un système de fichiers EFS, lesquels facilitent la gestion de l'accès des applications aux jeux de données partagés. Les points d'accès peuvent appliquer de manière forcée une identité d'utilisateur, y compris les groupes POSIX de l'utilisateur, pour toutes les demandes de système de fichiers effectuées via le point d'accès. Les points d'accès peuvent également appliquer de manière forcée un répertoire racine différent pour le système de fichiers afin que les clients puissent uniquement accéder aux données stockées dans le répertoire spécifié ou dans les sous-répertoires.

Correction

Pour appliquer l'identité d'un utilisateur à un point d'accès Amazon EFS, consultez la section Application de l'identité utilisateur à l'aide d'un point d'accès dans le Guide de l'utilisateur d'Amazon Elastic File System.

[EFS.5] Les points d'accès EFS doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::EFS::AccessPoint`

AWS Config règle : `tagged-efs-accesspoint` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un point d'accès Amazon EFS possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le point d'accès ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le point d'accès n'est balisé par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que

stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un point d'accès EFS, consultez la section Balisage des ressources Amazon EFS dans le Guide de l'utilisateur d'Amazon Elastic File System.

[EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement

Exigences associées : NIST.800-53.r5 SC-7, NIST.800-171.r2 3.1.20, PCI DSS v4.0. 1/14,44

Catégorie : Protéger > Sécurité du réseau > Ressources non accessibles au public

Gravité : Moyenne

Type de ressource : `AWS::EFS::FileSystem`

Règle AWS Config : efs-mount-target-public-accessible

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si une cible de montage Amazon EFS est associée à des sous-réseaux qui attribuent des adresses IP publiques au lancement. Le contrôle échoue si la cible de montage est associée à des sous-réseaux qui attribuent des adresses IP publiques au lancement.

Les sous-réseaux possèdent des attributs qui déterminent si les interfaces réseau créées dans le sous-réseau reçoivent automatiquement des adresses IP publiques. Pour IPv4, l'`MapPublicIpOnLaunch`attribut est défini sur pour les sous-réseaux par défaut et `TRUE` `FALSE` pour les sous-réseaux autres que ceux par défaut (à l'exception des sous-réseaux autres que ceux par défaut créés via l'assistant de lancement d'instance EC2, où il est défini sur). `TRUE` Pour IPv6, l'`AssignIpv6AddressOnCreation`attribut est défini sur `FALSE` pour tous les sous-réseaux par défaut.

Bien que les cibles de montage Amazon EFS ne puissent pas se voir attribuer d'adresses IPv4 publiques, leur placement dans des sous-réseaux configurés pour attribuer des adresses IP publiques au lancement indique que les instances colocalisées lancées dans de tels sous-réseaux susceptibles de monter le système de fichiers EFS pourraient recevoir automatiquement des adresses IP publiques, ce qui pourrait entraîner le risque que les données du système de fichiers soient accessibles depuis des hôtes adressés au public.

Les cibles de montage dans des sous-réseaux dont l'attribution automatique d'adresses IPv6 publiques est activée peuvent recevoir des adresses IPv6 routables globalement.

> **Note**
>
> Le 3 août 2026, Security Hub CSPM a supprimé ce contrôle de la norme FSBP (AWS Foundational Security Best Practices). Ce contrôle sera disponible dans la norme NIST SP 800-53 Rev. 5, la norme NIST SP 800-171 Revision 2 et la norme PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html

Correction

Pour associer une cible de montage existante à un autre sous-réseau, vous devez créer une nouvelle cible de montage dans un sous-réseau qui n'attribue pas d'adresses IP publiques au lancement, puis supprimer l'ancienne cible de montage. Pour plus d'informations sur la gestion des cibles de montage, consultez la section Création et gestion des cibles de montage et des groupes de sécurité dans le Guide de l'utilisateur d'Amazon Elastic File System.

[EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::EFS::FileSystem`

Règle AWS Config : efs-automatic-backups-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les sauvegardes automatiques sont activées sur un système de fichiers Amazon EFS. Ce contrôle échoue si les sauvegardes automatiques ne sont pas activées sur le système de fichiers EFS.

Une sauvegarde des données est une copie des données de votre système, de votre configuration ou de votre application qui est stockée séparément de l'original. L'activation de sauvegardes régulières vous permet de protéger les données importantes contre les événements imprévus tels que les pannes du système, les cyberattaques ou les suppressions accidentelles. Une stratégie de sauvegarde robuste facilite également une restauration plus rapide, la continuité des activités et la tranquillité d'esprit en cas de perte de données potentielle.

Correction

Pour plus d'informations sur l'utilisation AWS Backup des systèmes de fichiers EFS, consultez la section Sauvegarde des systèmes de fichiers EFS dans le Guide de l'utilisateur d'Amazon Elastic File System.

[EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/23.3.1

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EFS::FileSystem`

Règle AWS Config : efs-filesystem-ct-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un système de fichiers Amazon EFS chiffre les données avec AWS Key Management Service (AWS KMS). Le contrôle échoue si un système de fichiers n'est pas chiffré.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour activer le chiffrement au repos pour un nouveau système de fichiers EFS, consultez la section Chiffrement des données au repos dans le guide de l'utilisateur d'Amazon Elastic File System.

Contrôles CSPM de Security Hub pour Amazon EKS

Ces contrôles CSPM Security Hub évaluent le service et les ressources Amazon Elastic Kubernetes Service (Amazon EKS). Il se peut que les commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[EKS.1] Les points de terminaison du cluster EKS ne doivent pas être accessibles au public

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14,44

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::EKS::Cluster`

Règle AWS Config : eks-endpoint-no-public-access

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un point de terminaison de cluster Amazon EKS est accessible au public. Le contrôle échoue si un cluster EKS possède un point de terminaison accessible au public.

Lorsque vous créez un nouveau cluster, Amazon EKS crée un point de terminaison pour le serveur d'API Kubernetes géré que vous utilisez pour communiquer avec votre cluster. Par défaut, ce point de terminaison du serveur API est accessible au public sur Internet. L'accès au serveur d'API est sécurisé à l'aide d'une combinaison de fonctionnalités Gestion des identités et des accès AWS (IAM) et de contrôle d'accès basé sur les rôles (RBAC) natif de Kubernetes. En supprimant l'accès public au terminal, vous pouvez éviter toute exposition et tout accès involontaires à votre cluster.

Correction

Pour modifier l'accès aux points de terminaison d'un cluster EKS existant, consultez la section Modification de l'accès aux points de terminaison du cluster dans le guide de l'utilisateur Amazon EKS . Vous pouvez configurer l'accès aux terminaux pour un nouveau cluster EKS lors de sa création. Pour obtenir des instructions sur la création d'un nouveau cluster Amazon EKS, consultez la section Création d'un cluster Amazon EKS dans le guide de l'utilisateur Amazon EKS .

[EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/123.4

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::EKS::Cluster`

Règle AWS Config : eks-cluster-supported-version

Type de calendrier : Déclenché par un changement

Paramètres :

- `oldestVersionSupported`: `1.34` (non personnalisable)

Ce contrôle vérifie si un cluster Amazon Elastic Kubernetes Service (Amazon EKS) s'exécute sur une version de support standard de Kubernetes. Le contrôle échoue si le cluster Amazon EKS s'exécute sur une version non prise en charge ou avec support étendu.

Si votre application ne nécessite pas de version spécifique de Kubernetes, nous vous recommandons d'utiliser la dernière version disponible de Kubernetes, prise en charge par EKS pour vos clusters. Pour plus d'informations, consultez le calendrier des versions d'Amazon EKS Kubernetes et

Découvrez le cycle de vie des versions de Kubernetes sur Amazon EKS dans le guide de l'utilisateur Amazon EKS.

Correction

Pour mettre à jour un cluster EKS, voir Mettre à jour un cluster existant vers une nouvelle version de Kubernetes dans le guide de l'utilisateur Amazon EKS.

[EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés

Exigences associées : NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, PCI DSS v4.0. 1/83.2

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EKS::Cluster`

Règle AWS Config : eks-cluster-secrets-encrypted

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon EKS utilise des secrets Kubernetes chiffrés. Le contrôle échoue si les secrets Kubernetes du cluster ne sont pas chiffrés.

Lorsque vous chiffrez des secrets, vous pouvez utiliser les clés AWS Key Management Service (AWS KMS) pour chiffrer l'enveloppe des secrets Kubernetes stockés dans etcd pour votre cluster. Ce chiffrement s'ajoute au chiffrement de volume EBS qui est activé par défaut pour toutes les données (y compris les données secrètes) stockées dans etcd dans le cadre d'un cluster EKS. L'utilisation du chiffrement secret pour votre cluster EKS vous permet de déployer une stratégie de défense approfondie pour les applications Kubernetes en chiffrant les secrets Kubernetes à l'aide d'une clé KMS que vous définissez et gérez.

> **Note**
>
> Ce contrôle sera retiré après le 10 août 2026 et supprimé de toutes les normes CSPM de Security Hub applicables. À partir de la version 1.28 de Kubernetes, les clusters Amazon EKS disposent de secrets Kubernetes protégés par un cryptage d'enveloppe par défaut.

Correction

Pour activer le chiffrement secret sur un cluster EKS, consultez la section Activation du chiffrement secret sur un cluster existant dans le guide de l'utilisateur Amazon EKS .

[EKS.6] Les clusters EKS doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::EKS::Cluster`

AWS Config règle : `tagged-eks-cluster` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un cluster Amazon EKS possède des balises dont les clés spécifiques sont définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le cluster ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le cluster n'est balisé par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif,

propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un cluster EKS, consultez la section Marquage de vos ressources Amazon EKS dans le guide de l'utilisateur Amazon EKS.

[EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::EKS::IdentityProviderConfig`

AWS Config règle : `tagged-eks-identityproviderconfig` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une configuration de fournisseur d'identité Amazon EKS comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la configuration ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas disponibles`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la configuration n'est balisée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses

personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises aux configurations d'un fournisseur d'identité EKS, consultez la section Balisage de vos ressources Amazon EKS dans le guide de l'utilisateur Amazon EKS.

[EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée

Exigences associées : NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.1.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::EKS::Cluster`

Règle AWS Config : eks-cluster-log-enabled

Type de calendrier : Déclenché par un changement

Paramètres :

- `logTypes: audit`(non personnalisable)

Ce contrôle vérifie si la journalisation des audits est activée sur un cluster Amazon EKS. Le contrôle échoue si la journalisation des audits n'est pas activée pour le cluster.

> **Note**
>
> Ce contrôle ne vérifie pas si la journalisation des audits Amazon EKS est activée via Amazon Security Lake pour le Compte AWS.

La journalisation du plan de contrôle EKS fournit des journaux d'audit et de diagnostic directement depuis le plan de contrôle EKS vers Amazon CloudWatch Logs dans votre compte. Vous pouvez sélectionner les types de journaux dont vous avez besoin, et les journaux sont envoyés sous forme de flux de journaux à un groupe pour chaque cluster EKS CloudWatch. La journalisation fournit une visibilité sur l'accès et les performances des clusters EKS. En envoyant les journaux du plan de contrôle EKS pour vos clusters EKS à CloudWatch Logs, vous pouvez enregistrer les opérations à des fins d'audit et de diagnostic dans un emplacement central.

Correction

Pour activer les journaux d'audit pour votre cluster EKS, consultez la section Activation et désactivation des journaux du plan de contrôle dans le guide de l'utilisateur Amazon EKS.

[EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::EKS::Nodegroup`

Règle AWS Config : eks-nodegroup-supported-version-check

Type de calendrier : Déclenché par un changement

Paramètres :

- `oldestVersionSupported`: `1.34` (non personnalisable)

Ce contrôle vérifie si un groupe de nœuds Amazon EKS s'exécute sur une version de support standard de Kubernetes. Le contrôle échoue si le groupe de nœuds Amazon EKS s'exécute sur une version non prise en charge ou avec support étendu.

L'exécution de groupes de nœuds EKS sur des versions de Kubernetes non prises en charge signifie que ces nœuds ne reçoivent plus de correctifs de sécurité, de corrections de bogues ou de mises à jour de compatibilité de la part de. AWS Les versions non prises en charge peuvent contenir des vulnérabilités connues qui ont été corrigées dans les nouvelles versions, et elles peuvent rencontrer des problèmes de compatibilité avec les images de conteneur mises à jour Services AWS et les

outils tiers de l'écosystème Kubernetes. Si votre application ne nécessite pas de version spécifique de Kubernetes, nous vous recommandons d'utiliser la dernière version disponible de Kubernetes, prise en charge par Amazon EKS pour vos groupes de nœuds. Pour plus d'informations, consultez le calendrier des versions d'Amazon EKS Kubernetes et découvrez chaque phase des mises à jour des nœuds dans le guide de l'utilisateur Amazon EKS.

Correction

Pour mettre à jour un groupe de nœuds EKS, voir Mettre à jour un groupe de nœuds géré pour votre cluster dans le guide de l'utilisateur Amazon EKS .

Contrôles Security Hub CSPM pour ElastiCache

Ces AWS Security Hub CSPM contrôles évaluent le ElastiCache service et les ressources Amazon. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Élevée

Type de ressource :`AWS::ElastiCache::CacheCluster`, `AWS:ElastiCache:ReplicationGroup`

Règle AWS Config : elasticache-redis-cluster-automatic-backup-check

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`snapshotRetentionPeriod`	Durée minimale de conservation des instantanés en jours	Entier	1 sur 35	1

Ce contrôle évalue si les sauvegardes automatiques sont activées sur un cluster Amazon ElastiCache (Redis OSS). Le contrôle échoue si `SnapshotRetentionLimit` le cluster Redis OSS est inférieur à la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de conservation des instantanés, Security Hub CSPM utilise une valeur par défaut de 1 jour.

ElastiCache Les clusters (Redis OSS) peuvent sauvegarder leurs données. Vous pouvez utiliser la sauvegarde pour restaurer un cluster ou en créer un nouveau. La sauvegarde comprend les métadonnées du cluster, ainsi que toutes les données du cluster. Toutes les sauvegardes sont écrites sur Amazon S3, qui fournit un stockage durable. Vous pouvez restaurer vos données en créant un nouveau ElastiCache cluster et en le remplissant avec les données d'une sauvegarde. Vous pouvez gérer les sauvegardes à l'aide de l'API Console de gestion AWSAWS CLI, du et de l' ElastiCache API.

> **Note**
>
> Ce contrôle évalue également les groupes de ElastiCache réplication (Redis OSS et Valkey).

Correction

Pour plus d'informations sur la planification de sauvegardes automatiques pour un ElastiCache cluster, consultez la section Planification de sauvegardes automatiques dans le guide de ElastiCache l'utilisateur Amazon.

[ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters

Exigences associées : NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5) PCI DSS v4.0. 1/6.3.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::ElastiCache::CacheCluster`

Règle AWS Config : elasticache-auto-minor-version-upgrade-check

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle évalue si Amazon applique ElastiCache automatiquement les mises à niveau de versions mineures à un cluster de cache. Le contrôle échoue si aucune mise à niveau de version mineure n'est automatiquement appliquée au cluster de cache.

> **Note**
>
> Ce contrôle ne s'applique pas aux clusters ElastiCache Memcached.

La mise à niveau automatique des versions mineures est une fonctionnalité que vous pouvez activer sur Amazon ElastiCache pour mettre à niveau automatiquement vos clusters de cache lorsqu'une nouvelle version du moteur de cache secondaire est disponible. Ces mises à niveau peuvent inclure des correctifs de sécurité et des corrections de bogues. La mise à jour de l'installation des correctifs est une étape importante de la sécurisation des systèmes.

Correction

Pour appliquer automatiquement des mises à niveau de versions mineures à un cluster de ElastiCache cache existant, consultez la section Gestion des versions ElastiCache dans le guide de ElastiCache l'utilisateur Amazon.

[ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::ElastiCache::ReplicationGroup`

Règle AWS Config : elasticache-repl-grp-auto-failover-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le basculement automatique est activé pour un groupe de ElastiCache réplication. Le contrôle échoue si le basculement automatique n'est pas activé pour un groupe de réplication.

Lorsque le basculement automatique est activé pour un groupe de réplication, le rôle du nœud principal passe automatiquement à l'une des répliques lues. Cette promotion basée sur le basculement et les répliques vous permet de reprendre l'écriture vers le nouveau serveur principal une fois la promotion terminée, ce qui réduit le temps d'arrêt global en cas de panne.

Correction

Pour activer le basculement automatique pour un groupe de ElastiCache réplication existant, consultez la section Modification d'un ElastiCache cluster dans le guide de l' ElastiCache utilisateur Amazon. Si vous utilisez la ElastiCache console, réglez le basculement automatique sur Activé.

[ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::ElastiCache::ReplicationGroup`

Règle AWS Config : elasticache-repl-grp-encrypted-at-rest

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un groupe ElastiCache de réplication est chiffré au repos. Le contrôle échoue si le groupe de réplication n'est pas chiffré au repos.

Le chiffrement des données au repos réduit le risque qu'un utilisateur non authentifié accède aux données stockées sur disque. ElastiCache Les groupes de réplication (Redis OSS) doivent être chiffrés au repos pour renforcer la sécurité.

Correction

Pour configurer le chiffrement au repos sur un groupe de ElastiCache réplication, consultez la section Activation du chiffrement au repos dans le guide de ElastiCache l'utilisateur Amazon.

[ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElastiCache::ReplicationGroup`

Règle AWS Config : elasticache-repl-grp-encrypted-in-transit

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un groupe ElastiCache de réplication est chiffré en transit. Le contrôle échoue si le groupe de réplication n'est pas chiffré pendant le transit.

Le chiffrement des données en transit réduit le risque qu'un utilisateur non autorisé puisse espionner le trafic réseau. L'activation du chiffrement en transit sur un groupe de ElastiCache réplication chiffre

vos données chaque fois qu'elles sont déplacées d'un endroit à un autre, par exemple entre les nœuds de votre cluster ou entre votre cluster et votre application.

Correction

Pour configurer le chiffrement en transit sur un groupe de ElastiCache réplication, consultez la section Activation du chiffrement en transit dans le guide de ElastiCache l'utilisateur Amazon.

[ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé

Exigences associées : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/8.3.1

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::ElastiCache::ReplicationGroup`

Règle AWS Config : elasticache-repl-grp-redis-auth-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si Redis OSS AUTH est activé sur un groupe de réplication ElastiCache (Redis OSS). Le contrôle échoue si la version Redis OSS des nœuds du groupe de réplication est inférieure à 6.0 et `AuthToken` n'est pas utilisée.

Lorsque vous utilisez des jetons d'authentification ou des mots de passe Redis, Redis exige un mot de passe avant d'autoriser les clients à exécuter des commandes, ce qui améliore la sécurité des données. Pour Redis 6.0 et les versions ultérieures, nous recommandons d'utiliser le contrôle Role-Based d'accès (RBAC). Le RBAC n'étant pas pris en charge pour les versions de Redis antérieures à 6.0, ce contrôle évalue uniquement les versions qui ne peuvent pas utiliser la fonctionnalité RBAC.

Correction

Pour utiliser Redis AUTH sur un groupe de réplication ElastiCache (Redis OSS), consultez la section Modification du jeton AUTH sur un cluster ElastiCache (Redis OSS) existant dans le guide de l'utilisateur Amazon. ElastiCache

[ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut

Exigences connexes : NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::ElastiCache::CacheCluster`

Règle AWS Config : elasticache-subnet-group-check

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un ElastiCache cluster est configuré avec un groupe de sous-réseaux personnalisé. Le contrôle échoue si `CacheSubnetGroupName` un ElastiCache cluster possède la valeur`default`.

Lors du lancement d'un ElastiCache cluster, un groupe de sous-réseaux par défaut est créé s'il n'en existe pas déjà un. Le groupe par défaut utilise des sous-réseaux issus du Virtual Private Cloud (VPC) par défaut. Nous vous recommandons d'utiliser des groupes de sous-réseaux personnalisés qui limitent davantage les sous-réseaux dans lesquels réside le cluster et le réseau dont le cluster hérite des sous-réseaux.

Correction

Pour créer un nouveau groupe de sous-réseaux pour un ElastiCache cluster, consultez la section Création d'un groupe de sous-réseaux dans le guide de ElastiCache l'utilisateur Amazon.

Contrôles CSPM du Security Hub pour Elastic Beanstalk

Ces AWS Security Hub CSPM contrôles évaluent le AWS Elastic Beanstalk service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés

Exigences connexes : NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Catégorie : Détecter > Services de détection > Surveillance des applications

Gravité : Faible

Type de ressource : `AWS::ElasticBeanstalk::Environment`

Règle AWS Config : `beanstalk-enhanced-health-reporting-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les rapports de santé améliorés sont activés pour vos AWS Elastic Beanstalk environnements.

Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application.

Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier. L'agent de santé Elastic Beanstalk, inclus dans les Amazon Machine Images (AMI) prises en charge, évalue les journaux et les métriques des instances EC2 de l'environnement.

Pour plus d'informations, consultez la section Rapports et surveillance de l'état améliorés dans le Guide du AWS Elastic Beanstalk développeur.

Correction

Pour savoir comment activer les rapports de santé améliorés, consultez la section Activation des rapports de santé améliorés à l'aide de la console Elastic Beanstalk dans le manuel du développeur. AWS Elastic Beanstalk

[ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées

Exigences associées : NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::ElasticBeanstalk::Environment`

Règle AWS Config : `elastic-beanstalk-managed-updates-enabled`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`UpdateLevel`	Niveau de mise à jour de version	Enum	`minor`, `patch`	Aucune valeur par défaut

Ce contrôle vérifie si les mises à jour de plateforme gérées sont activées pour un environnement Elastic Beanstalk. Le contrôle échoue si aucune mise à jour de plateforme gérée n'est activée. Par défaut, le contrôle est transmis si un type de mise à jour de plateforme est activé. Vous pouvez éventuellement fournir une valeur de paramètre personnalisée pour exiger un niveau de mise à jour spécifique.

L'activation des mises à jour de plate-forme gérées garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de plate-forme disponibles pour l'environnement. La mise à jour de l'installation des correctifs est une étape importante de la sécurisation des systèmes.

Correction

Pour activer les mises à jour de plateformes gérées, voir Pour configurer les mises à jour de plateformes gérées sous Mises à jour de plateformes gérées dans le guide du AWS Elastic Beanstalk développeur.

[ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch

Exigences associées : PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Élevée

Type de ressource : `AWS::ElasticBeanstalk::Environment`

Règle AWS Config : `elastic-beanstalk-logs-to-cloudwatch`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`RetentionInDays`	Nombre de jours pendant lesquels consigner les événements avant leur expiration	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Aucune valeur par défaut

Ce contrôle vérifie si un environnement Elastic Beanstalk est configuré pour envoyer des journaux à Logs. CloudWatch Le contrôle échoue si un environnement Elastic Beanstalk n'est pas configuré pour envoyer des journaux à Logs. CloudWatch Vous pouvez éventuellement fournir une valeur personnalisée pour le `RetentionInDays` paramètre si vous souhaitez que le contrôle soit transmis uniquement si les journaux sont conservés pendant le nombre de jours spécifié avant leur expiration.

CloudWatch vous aide à collecter et à surveiller diverses mesures relatives à vos applications et à vos ressources d'infrastructure. Vous pouvez également l'utiliser CloudWatch pour configurer des actions d'alarme en fonction de métriques spécifiques. Nous vous recommandons d'intégrer Elastic CloudWatch Beanstalk pour améliorer la visibilité de votre environnement Elastic Beanstalk. Les journaux Elastic Beanstalk incluent le fichier eb-activity.log, les journaux d'accès depuis l'environnement nginx ou le serveur proxy Apache, et les journaux spécifiques à un environnement.

Correction

Pour intégrer Elastic CloudWatch Beanstalk à Logs, consultez la section Streaming des logs d'instance vers Logs dans le Guide du CloudWatch développeur. AWS Elastic Beanstalk

Contrôles CSPM de Security Hub pour Elastic Load Balancing

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Elastic Load Balancing. Il se peut que les commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ELB.1] L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS

Exigences associées : PCI DSS v3.2. 1/23.3, PCI DSS v3.2. 1/4.1, NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Catégorie : Détecter - Services de détection

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : alb-http-to-https-redirection-check

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la redirection HTTP vers HTTPS est configurée sur tous les écouteurs HTTP des équilibreurs de charge d'application. Le contrôle échoue si la redirection HTTP vers HTTPS n'est pas configurée pour l'un des écouteurs HTTP des équilibreurs de charge d'application.

Avant de commencer à utiliser votre équilibreur de charge d'application, vous devez ajouter un ou plusieurs écouteurs. Un écouteur est un processus qui utilise le protocole et le port configurés pour vérifier les demandes de connexion. Les auditeurs prennent en charge les protocoles HTTP et HTTPS. Vous pouvez utiliser un écouteur HTTPS pour transférer le travail de chiffrement et de déchiffrement à votre équilibreur de charge. Pour appliquer le chiffrement en transit, vous devez utiliser des actions de redirection avec les équilibreurs de charge d'application pour rediriger les requêtes HTTP du client vers une requête HTTPS sur le port 443.

Pour en savoir plus, consultez la section Écouteurs pour vos équilibreurs de charge d'application dans le Guide de l'utilisateur des équilibreurs de charge d'application.

Correction

Pour rediriger les requêtes HTTP vers HTTPS, vous devez ajouter une règle d'écoute Application Load Balancer ou modifier une règle existante.

Pour obtenir des instructions sur l'ajout d'une nouvelle règle, consultez la section Ajouter une règle dans le Guide de l'utilisateur des équilibreurs de charge d'application. Pour Protocole : Port, choisissez HTTP, puis entrez**80**. Pour Ajouter une action, Rediriger vers, choisissez HTTPS, puis entrez**443**.

Pour obtenir des instructions sur la modification d'une règle existante, voir Modifier une règle dans le Guide de l'utilisateur des équilibreurs de charge d'application. Pour Protocole : Port, choisissez HTTP, puis entrez**80**. Pour Ajouter une action, Rediriger vers, choisissez HTTPS, puis entrez**443**.

[ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager

Exigences connexes : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (5), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

Règle AWS Config : elb-acm-certificate-required

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le Classic Load Balancer utilise des HTTPS/SSL certificats fournis par AWS Certificate Manager (ACM). Le contrôle échoue si le Classic Load Balancer configuré avec le HTTPS/SSL récepteur n'utilise pas de certificat fourni par ACM.

Pour créer un certificat, vous pouvez utiliser ACM ou un outil prenant en charge les protocoles SSL et TLS, tel qu'OpenSSL. Security Hub CSPM vous recommande d'utiliser ACM pour créer ou importer des certificats pour votre équilibreur de charge.

ACM s'intègre aux équilibreurs de charge classiques afin que vous puissiez déployer le certificat sur votre équilibreur de charge. Vous devez également renouveler automatiquement ces certificats.

Correction

Pour plus d'informations sur l'association d'un SSL/TLS certificat ACM à un équilibreur de charge classique, consultez l'article du centre de AWS connaissances Comment associer un SSL/TLS certificat ACM à un équilibreur de charge classique, d'application ou réseau ?

[ELB.3] Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

Règle AWS Config : elb-tls-https-listeners-only

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si vos écouteurs Classic Load Balancer sont configurés avec le protocole HTTPS ou TLS pour les connexions frontales (client-équilibreur de charge). Le contrôle est applicable si un Classic Load Balancer possède des auditeurs. Si aucun écouteur n'est configuré pour votre Classic Load Balancer, le contrôle ne rapporte aucun résultat.

Le contrôle passe si les écouteurs Classic Load Balancer sont configurés avec TLS ou HTTPS pour les connexions frontales.

Le contrôle échoue si l'écouteur n'est pas configuré avec TLS ou HTTPS pour les connexions frontales.

Avant de commencer à utiliser un équilibreur de charge, vous devez ajouter un ou plusieurs écouteurs. Un écouteur est un processus qui utilise le protocole et le port configurés pour vérifier

les demandes de connexion. Les auditeurs peuvent prendre en charge à la fois le protocole HTTP et HTTPS/TLS les protocoles. Vous devez toujours utiliser un écouteur HTTPS ou TLS pour que l'équilibreur de charge effectue le travail de chiffrement et de déchiffrement en transit.

Correction

Pour remédier à ce problème, mettez à jour vos auditeurs afin qu'ils utilisent le protocole TLS ou HTTPS.

Pour remplacer tous les auditeurs non conformes par des TLS/HTTPS auditeurs

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez votre Classic Load Balancer.
4. Sous l'onglet Listeners, choisissez Edit.
5. Pour tous les auditeurs pour lesquels le protocole Load Balancer n'est pas défini sur HTTPS ou SSL, modifiez le paramètre sur HTTPS ou SSL.
6. Pour tous les auditeurs modifiés, dans l'onglet Certificats, choisissez Modifier la valeur par défaut.
7. Pour Certificats ACM et IAM, sélectionnez un certificat.
8. Choisissez Enregistrer par défaut.
9. Après avoir mis à jour tous les auditeurs, choisissez Enregistrer.

[ELB.4] L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP non valides

Exigences associées : NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/62.2.4

Catégorie : Protéger > Sécurité du réseau

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : alb-http-drop-invalid-header-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle évalue si un équilibreur de charge d'application est configuré pour supprimer les en-têtes HTTP non valides. Le contrôle échoue si la valeur de `routing.http.drop_invalid_header_fields.enabled` est définie sur`false`.

Par défaut, les équilibreurs de charge des applications ne sont pas configurés pour supprimer les valeurs d'en-tête HTTP non valides. La suppression de ces valeurs d'en-tête empêche les attaques de désynchronisation HTTP.

> **Note**
>
> Nous vous recommandons de désactiver ce contrôle s'il ELB.12 est activé dans votre compte. Pour de plus amples informations, veuillez consulter [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict.

Correction

Pour remédier à ce problème, configurez votre équilibreur de charge de manière à supprimer les champs d'en-tête non valides.

Pour configurer l'équilibreur de charge afin de supprimer les champs d'en-tête non valides

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez un équilibreur de charge d'application.
4. Dans Actions, choisissez Modifier les attributs.
5. Sous Supprimer les champs d'en-tête non valides, choisissez Activer.
6. Choisissez Enregistrer.

[ELB.5] La journalisation des applications et des équilibreurs de charge classiques doit être activée

Exigences connexes : NIST.800-53.r5 AC-4 (26) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : elb-logging-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la journalisation de l'application Load Balancer et de l'équilibreur de charge classique est activée. Le contrôle échoue si `access_logs.s3.enabled` c'est le cas`false`.

Elastic Load Balancing fournit des journaux d'accès qui capturent des informations détaillées sur les demandes envoyées à votre équilibreur de charge. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et résoudre des problèmes.

Pour en savoir plus, consultez les journaux d'accès de votre Classic Load Balancer dans le Guide de l'utilisateur des Classic Load Balancers.

Correction

Pour activer les journaux d'accès, reportez-vous à l'étape 3 : Configuration des journaux d'accès dans le Guide de l'utilisateur pour les équilibreurs de charge des applications.

[ELB.6] La protection contre la suppression doit être activée pour les équilibreurs de charge des applications, des passerelles et du réseau

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : elb-deletion-protection-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la protection contre la suppression est activée pour une application, une passerelle ou un équilibreur de charge réseau. Le contrôle échoue si la protection contre la suppression est désactivée.

Activez la protection contre la suppression pour empêcher la suppression de votre application, de votre passerelle ou de votre équilibreur de charge réseau.

Correction

Pour éviter la suppression accidentelle de votre équilibreur de charge, vous pouvez activer la protection contre la suppression. Par défaut, la protection contre la suppression est désactivée pour votre équilibreur de charge.

Si vous activez la protection contre la suppression pour votre équilibreur de charge, vous devez désactiver la protection contre la suppression avant de pouvoir supprimer l'équilibreur de charge.

Pour activer la protection contre la suppression pour un équilibreur de charge d'application, consultez la section Protection contre la suppression dans le Guide de l'utilisateur des équilibreurs de charge d'application. Pour activer la protection contre la suppression pour un équilibreur de charge de passerelle, consultez la section Protection contre la suppression dans le guide de l'utilisateur des équilibreurs de charge de passerelle. Pour activer la protection contre la suppression d'un équilibreur de charge réseau, consultez la section Protection contre la suppression dans le Guide de l'utilisateur des équilibreurs de charge réseau.

[ELB.7] Le drainage des connexions doit être activé pour les équilibreurs de charge classiques

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Restaurer > Résilience

Gravité : Faible

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config règle : `elb-connection-draining-enabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le drainage des connexions est activé pour les Classic Load Balancers.

L'activation de la vidange des connexions sur les équilibreurs de charge classiques garantit que l'équilibreur de charge arrête d'envoyer des requêtes aux instances dont l'enregistrement est annulé ou qui ne fonctionnent pas correctement. Cela permet de maintenir les connexions existantes ouvertes. Cela est particulièrement utile pour les instances des groupes Auto Scaling, afin de garantir que les connexions ne sont pas interrompues brusquement.

Correction

Pour activer le drainage des connexions sur les équilibreurs de charge classiques, voir Configurer le drainage des connexions pour votre Classic Load Balancer dans le Guide de l'utilisateur des équilibreurs de charge classiques.

[ELB.8] Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie qui est solide AWS Config durée

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

Règle AWS Config : elb-predefined-security-policy-ssl-check

Type de calendrier : Déclenché par un changement

Paramètres :

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (non personnalisable)

Ce contrôle vérifie si vos HTTPS/SSL auditeurs Classic Load Balancer utilisent la politique `ELBSecurityPolicy-TLS-1-2-2017-01` prédéfinie. Le contrôle échoue si les HTTPS/SSL écouteurs Classic Load Balancer n'utilisent `ELBSecurityPolicy-TLS-1-2-2017-01` pas.

Une politique de sécurité est une combinaison de protocoles SSL, de chiffrements et de l'option Server Order Preference. Des politiques prédéfinies contrôlent les chiffrements, les protocoles et les ordres de préférence à prendre en charge lors des négociations SSL entre un client et un équilibreur de charge.

L'utilisation `ELBSecurityPolicy-TLS-1-2-2017-01` peut vous aider à respecter les normes de conformité et de sécurité qui vous obligent à désactiver des versions spécifiques de SSL et TLS. Pour plus d'informations, consultez la section Politiques de sécurité SSL prédéfinies pour les équilibreurs de charge classiques dans le Guide de l'utilisateur des équilibreurs de charge classiques.

Correction

Pour plus d'informations sur l'utilisation de la politique de sécurité prédéfinie `ELBSecurityPolicy-TLS-1-2-2017-01` avec un équilibreur de charge classique, voir Configuration des paramètres de sécurité dans le Guide de l'utilisateur pour les équilibreurs de charge classiques.

[ELB.9] L'équilibrage de charge entre zones doit être activé pour les équilibreurs de charge classiques

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

Règle AWS Config : elb-cross-zone-load-balancing-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'équilibrage de charge entre zones est activé pour les Classic Load Balancers (CLB). Le contrôle échoue si l'équilibrage de charge entre zones n'est pas activé pour un CLB.

Un nœud d'équilibrage de charge distribue le trafic uniquement entre les cibles enregistrées dans sa zone de disponibilité. Lorsque l'équilibrage de charge entre zones est désactivé, chaque nœud d'équilibreur de charge distribue le trafic entre les cibles enregistrées dans sa zone de disponibilité uniquement. Si le nombre de cibles enregistrées n'est pas le même dans les zones de disponibilité, le trafic ne sera pas réparti de manière uniforme et les instances d'une zone risquent d'être surexploitées par rapport aux instances d'une autre zone. Lorsque l'équilibrage de charge entre zones est activé, chaque nœud d'équilibrage de charge de votre Classic Load Balancer distribue les demandes de manière uniforme entre les instances enregistrées dans toutes les zones de disponibilité activées. Pour plus de détails, consultez l'équilibrage de Cross-zone charge dans le guide de l'utilisateur d'Elastic Load Balancing.

Correction

Pour activer l'équilibrage de charge entre zones dans un équilibreur de charge classique, voir Activer l'équilibrage de charge entre zones dans le Guide de l'utilisateur des équilibreurs de charge classiques.

[ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

Règle AWS Config : clb-multiple-az

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`minAvailabilityZones`	Nombre minimum de zones de disponibilité	Enum	`2, 3, 4, 5, 6`	`2`

Ce contrôle vérifie si un équilibreur de charge classique a été configuré pour couvrir au moins le nombre spécifié de zones de disponibilité (AZ). Le contrôle échoue si le Classic Load Balancer ne couvre pas au moins le nombre spécifié d'AZ. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour le nombre minimum d'AZ, Security Hub CSPM utilise une valeur par défaut de deux AZ.

Un équilibreur de charge classique peut être configuré pour répartir les demandes entrantes entre les instances Amazon EC2 dans une ou plusieurs zones de disponibilité. Un équilibreur de charge

classique qui ne couvre pas plusieurs zones de disponibilité n'est pas en mesure de rediriger le trafic vers des cibles situées dans une autre zone de disponibilité si la seule zone de disponibilité configurée devient indisponible.

Correction

Pour ajouter des zones de disponibilité à un équilibreur de charge classique, voir Ajouter ou supprimer des sous-réseaux pour votre Classic Load Balancer dans le Guide de l'utilisateur des équilibreurs de charge classiques.

[ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict

Exigences associées : NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/62.2.4

Catégorie : Protection > Protection des données > Intégrité des données

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : alb-desync-mode-check

Type de calendrier : Déclenché par un changement

Paramètres :

- `desyncMode`: `defensive, strictest` (non personnalisable)

Ce contrôle vérifie si un équilibreur de charge d'application est configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict. Le contrôle échoue si un équilibreur de charge d'application n'est pas configuré avec le mode défensif ou le mode d'atténuation de la désynchronisation le plus strict.

Les problèmes de désynchronisation HTTP peuvent entraîner une contrebande de demandes et rendre les applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Ces vulnérabilités peuvent à leur tour entraîner le bourrage d'informations d'identification ou l'exécution de commandes non autorisées. Les équilibreurs de charge des applications configurés avec le mode défensif ou le mode d'atténuation de la désynchronisation le plus strict protègent votre application contre les problèmes de sécurité pouvant être causés par la désynchronisation HTTP.

Correction

Pour mettre à jour le mode d'atténuation de la désynchronisation d'un équilibreur de charge d'application, consultez la section Mode d'atténuation de la désynchronisation dans le Guide de l'utilisateur des équilibreurs de charge d'application.

[ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : elbv2-multiple-az

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`minAvailabilityZones`	Nombre minimum de zones de disponibilité	Enum	`2, 3, 4, 5, 6`	`2`

Ce contrôle vérifie si un Elastic Load Balancer V2 (Application, Network, or Gateway Load Balancer) a enregistré des instances provenant d'au moins le nombre spécifié de zones de disponibilité (AZ). Le contrôle échoue si un Elastic Load Balancer V2 ne possède pas d'instances enregistrées dans au moins le nombre spécifié de zones de zone de sécurité. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour le nombre minimum d'AZ, Security Hub CSPM utilise une valeur par défaut de deux AZ.

Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles (par exemple, des instances EC2, des conteneurs et des adresses IP) dans une ou plusieurs zones de disponibilité. Elastic Load Balancing met à l'échelle votre équilibreur de charge à mesure que votre trafic entrant change au fil du temps. Il est recommandé de configurer au moins deux zones de disponibilité pour garantir la disponibilité des services, car l'Elastic Load Balancer sera en mesure de diriger le trafic vers une autre zone de disponibilité si celle-ci devient indisponible. La configuration de plusieurs zones de disponibilité permettra d'éviter d'avoir un point de défaillance unique pour l'application.

Correction

Pour ajouter une zone de disponibilité à un équilibreur de charge d'application, consultez la section Zones de disponibilité de votre équilibreur de charge d'application dans le Guide de l'utilisateur des équilibreurs de charge d'application. Pour ajouter une zone de disponibilité à un équilibreur de charge réseau, consultez la section Équilibreurs de charge réseau dans le Guide de l'utilisateur des équilibreurs de charge réseau. Pour ajouter une zone de disponibilité à un équilibreur de charge de passerelle, voir Créer un équilibreur de charge de passerelle dans le Guide de l'utilisateur des équilibreurs de charge de passerelle.

[ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict

Exigences associées : NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/62.2.4

Catégorie : Protection > Protection des données > Intégrité des données

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancing::LoadBalancer`

Règle AWS Config : clb-desync-mode-check

Type de calendrier : Déclenché par un changement

Paramètres :

- `desyncMode`: `defensive, strictest` (non personnalisable)

Ce contrôle vérifie si un équilibreur de charge classique est configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict. Le contrôle échoue si le Classic Load

Balancer n'est pas configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict.

Les problèmes de désynchronisation HTTP peuvent entraîner une contrebande de demandes et rendre les applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Ces vulnérabilités peuvent à leur tour entraîner le détournement d'informations d'identification ou l'exécution de commandes non autorisées. Les équilibreurs de charge classiques configurés avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict protègent votre application contre les problèmes de sécurité pouvant être causés par la désynchronisation HTTP.

Correction

Pour mettre à jour le mode d'atténuation de la désynchronisation sur un équilibreur de charge classique, voir Modifier le mode d'atténuation de la désynchronisation dans le Guide de l'utilisateur des équilibreurs de charge classiques.

[ELB.16] Les équilibreurs de charge des applications doivent être associés à un AWS WAF ACL web

Exigences connexes : NIST.800-53.r5 AC-4 (21)

Catégorie : Protéger > Services de protection

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::LoadBalancer`

Règle AWS Config : alb-waf-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un équilibreur de charge d'application est associé à une liste de contrôle d'accès AWS WAF classique ou AWS WAF Web (ACL Web). Le contrôle échoue si le `Enabled` champ de AWS WAF configuration est défini sur`false`.

AWS WAF est un pare-feu d'applications Web qui permet de protéger les applications Web et les API contre les attaques. Avec AWS WAF, vous pouvez configurer une ACL Web, qui est un ensemble de règles qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Nous vous recommandons d'associer votre équilibreur de charge d'application à une ACL AWS WAF Web pour le protéger contre les attaques malveillantes.

Correction

Pour associer un équilibreur de charge d'application à une ACL Web, voir Associer ou dissocier une ACL Web à une AWS ressource dans le Guide du développeur. AWS WAF

[ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées

Exigences connexes : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::Listener`

Règle AWS Config : elbv2-predefined-security-policy-ssl-check

Type de calendrier : Déclenché par un changement

Paramètres `sslPolicies` : `ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-PQ-2025-09, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09` (non personnalisable)

Ce contrôle vérifie si l'écouteur HTTPS d'un équilibreur de charge d'application ou l'écouteur TLS d'un équilibreur de charge réseau est configuré pour chiffrer les données en transit à l'aide d'une politique de sécurité recommandée. Le contrôle échoue si l'écouteur HTTPS ou TLS d'un équilibreur de charge n'est pas configuré pour utiliser une politique de sécurité recommandée.

Elastic Load Balancing utilise une configuration de négociation SSL, appelée politique de sécurité, pour négocier les connexions entre un client et un équilibreur de charge. La politique de sécurité spécifie une combinaison de protocoles et de chiffrements. Le protocole établit une connexion sécurisée entre un client et un serveur. Un chiffrement est un algorithme de chiffrement qui utilise des clés de chiffrement pour créer un message codé. Pendant le processus de négociation de connexion , le client et l'équilibreur de charge présentent une liste de chiffrements et de protocoles pris en charge par chacun d'entre eux dans l'ordre de préférence. L'utilisation d'une politique de

sécurité recommandée pour un équilibreur de charge peut vous aider à respecter les normes de conformité et de sécurité.

Correction

Pour plus d'informations sur les politiques de sécurité recommandées et sur la manière de mettre à jour les écouteurs, consultez les sections suivantes des guides de l'utilisateur d'Elastic Load Balancing : politiques de sécurité pour les équilibreurs de charge d'application, politiques de sécurité pour les équilibreurs de charge réseau, mise à jour d'un écouteur HTTPS pour votre équilibreur de charge d'application et Mise à jour d'un écouteur pour votre équilibreur de charge réseau.

[ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::Listener`

Règle AWS Config : elbv2-listener-encryption-in-transit

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'écouteur d'un équilibreur de charge d'application ou d'un équilibreur de charge réseau est configuré pour utiliser un protocole sécurisé pour le chiffrement des données en transit. Le contrôle échoue si un écouteur Application Load Balancer n'est pas configuré pour utiliser le protocole HTTPS, ou si un écouteur Network Load Balancer n'est pas configuré pour utiliser le protocole TLS.

Pour chiffrer les données transmises entre un client et un équilibreur de charge, les écouteurs Elastic Load Balancer doivent être configurés pour utiliser les protocoles de sécurité standard du secteur : HTTPS pour les équilibreurs de charge d'application ou TLS pour les équilibreurs de charge réseau. Dans le cas contraire, les données transmises entre un client et un équilibreur de charge sont vulnérables à l'interception, à la falsification et à l'accès non autorisé. L'utilisation du protocole HTTPS ou TLS par un auditeur est conforme aux meilleures pratiques de sécurité et contribue à garantir la confidentialité et l'intégrité des données pendant leur transmission. Cela est particulièrement important pour les applications qui traitent des informations sensibles ou qui doivent se conformer à des normes de sécurité qui exigent le cryptage des données en transit.

Correction

Pour plus d'informations sur la configuration des protocoles de sécurité pour les auditeurs, consultez les sections suivantes des guides de l'utilisateur d'Elastic Load Balancing : Créer un écouteur HTTPS pour votre application Load Balancer et Créer un écouteur pour votre Network Load Balancer.

[ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::TargetGroup`

Règle AWS Config : elbv2-targetgroup-healthcheck-protocol-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le groupe cible pour les contrôles de santé des applications et de l'équilibreur de charge réseau utilise un protocole de transport chiffré. Le contrôle échoue si le protocole de contrôle de santé n'utilise pas le protocole HTTPS. Ce contrôle ne s'applique pas aux types de cibles Lambda.

Les équilibreurs de charge envoient des demandes de contrôle de santé aux cibles enregistrées afin de déterminer leur état et d'acheminer le trafic en conséquence. Le protocole de contrôle de santé spécifié dans la configuration du groupe cible détermine la manière dont ces contrôles sont effectués. Lorsque les protocoles de contrôle de santé utilisent des communications non cryptées telles que HTTP, les demandes et les réponses peuvent être interceptées ou manipulées pendant la transmission. Cela permet aux attaquants d'obtenir des informations sur la configuration de l'infrastructure, de modifier les résultats des bilans de santé ou de mener des attaques de type « man-in-the-middle » qui affectent les décisions de routage. L'utilisation du protocole HTTPS pour les contrôles de santé fournit une communication cryptée entre l'équilibreur de charge et ses cibles, protégeant ainsi l'intégrité et la confidentialité des informations relatives à l'état de santé.

Correction

Pour configurer des bilans de santé chiffrés pour votre groupe cible Application Load Balancer, voir Mettre à jour les paramètres de contrôle de santé d'un groupe cible Application Load Balancer dans

le Guide de l'utilisateur d'Elastic Load Balancing. Pour configurer des bilans de santé chiffrés pour votre groupe cible Network Load Balancer, voir Mettre à jour les paramètres de contrôle de santé d'un groupe cible d'un Network Load Balancer dans le Guide de l'utilisateur d'Elastic Load Balancing.

[ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::ElasticLoadBalancingV2::TargetGroup`

Règle AWS Config : elbv2-targetgroup-protocol-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un groupe cible Elastic Load Balancing utilise un protocole de transport chiffré. Ce contrôle ne s'applique pas aux groupes cibles dont le type de cible est Lambda ou ALB, ni aux groupes cibles utilisant le protocole GENEVE. Le contrôle échoue si le groupe cible n'utilise pas le protocole HTTPS, TLS ou QUIC.

Le chiffrement des données en transit les protège contre toute interception par des utilisateurs non autorisés. Les groupes cibles qui utilisent des protocoles non chiffrés (HTTP, TCP, UDP) transmettent des données sans chiffrement, ce qui les rend vulnérables aux écoutes. L'utilisation de protocoles chiffrés (HTTPS, TLS, QUIC) garantit la protection des données transmises entre les équilibreurs de charge et les cibles.

Correction

Pour utiliser un protocole chiffré, vous devez créer un nouveau groupe cible avec le protocole HTTPS, TLS ou QUIC. Le protocole du groupe cible ne peut pas être modifié après sa création. Pour créer un groupe cible pour votre Application Load Balancer, voir Créer un groupe cible pour votre Application Load Balancer dans le Guide de l'utilisateur d'Elastic Load Balancing. Pour créer un groupe cible pour votre Network Load Balancer, voir Créer un groupe cible pour votre Network Load Balancer dans le Guide de l'utilisateur d'Elastic Load Balancing.

Security Hub CSPM pour Elasticsearch

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Elasticsearch.

Il se peut que ces commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ES.1] Le chiffrement au repos doit être activé pour les domaines Elasticsearch

Exigences associées : PCI DSS v3.2. 1/34, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

Règle AWS Config : `elasticsearch-encrypted-at-rest`

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la configuration de chiffrement au repos est activée pour les domaines Elasticsearch. La vérification échoue si le chiffrement au repos n'est pas activé.

Pour renforcer la sécurité de vos données sensibles OpenSearch, vous devez les configurer pour qu'elles soient cryptées au repos. OpenSearch Les domaines Elasticsearch permettent de chiffrer les données au repos. Cette fonctionnalité permet AWS KMS de stocker et de gérer vos clés de cryptage. Pour effectuer le chiffrement, il utilise l'algorithme Advanced Encryption Standard avec des clés de 256 bits ()AES-256.

Pour en savoir plus sur le OpenSearch chiffrement au repos, consultez la section Chiffrement des données au repos pour Amazon OpenSearch Service dans le Amazon OpenSearch Service Developer Guide.

Certains types d'instances, tels que `t.small` et`t.medium`, ne prennent pas en charge le chiffrement des données au repos. Pour plus de détails, consultez la section Types d'instances pris en charge dans le Guide du développeur Amazon OpenSearch Service.

Correction

Pour activer le chiffrement au repos pour les domaines Elasticsearch nouveaux et existants, consultez la section Activation du chiffrement des données au repos dans le Amazon OpenSearch Service Developer Guide.

[ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public

Exigences associées : PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14,44

Catégorie : Protéger > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Critique

Type de ressource : `AWS::Elasticsearch::Domain`

Règle AWS Config : `elasticsearch-in-vpc-only`

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les domaines Elasticsearch se trouvent dans un VPC. Il n'évalue pas la configuration de routage du sous-réseau VPC pour déterminer l'accès public. Vous devez vous assurer que les domaines Elasticsearch ne sont pas rattachés à des sous-réseaux publics. Consultez Resource-based les politiques dans le guide du développeur Amazon OpenSearch Service. Vous devez également garantir que votre VPC est configuré conformément aux bonnes pratiques recommandées. Consultez les meilleures pratiques en matière de sécurité pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Les domaines Elasticsearch déployés au sein d'un VPC peuvent communiquer avec les ressources du VPC via le AWS réseau privé, sans avoir à passer par l'Internet public. Cette configuration renforce la sécurité en limitant l'accès aux données en transit. Les VPC fournissent un certain nombre de contrôles réseau pour sécuriser l'accès aux domaines Elasticsearch, notamment l'ACL réseau et les groupes de sécurité. Security Hub CSPM vous recommande de migrer les domaines Elasticsearch publics vers des VPC afin de tirer parti de ces contrôles.

Correction

Si vous créez un domaine avec un point de terminaison public, vous ne pouvez pas ultérieurement le placer au sein d'un VPC. Au lieu de cela, vous devez créer un nouveau domaine et migrer vos données. L'inverse est également vrai. Si vous créez un domaine dans un VPC, il ne peut pas avoir

de point de terminaison public. Au lieu de cela, vous devez créer un autre domaine ou désactiver ce contrôle.

Consultez la section Lancement de vos domaines Amazon OpenSearch Service au sein d'un VPC dans le Guide du développeur Amazon OpenSearch Service.

[ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds

Exigences associées : NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

Règle AWS Config : `elasticsearch-node-to-node-encryption-check`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement nœud à nœud est activé sur un domaine Elasticsearch. Le contrôle échoue si le chiffrement nœud à nœud n'est pas activé sur le domaine Elasticsearch. Le contrôle génère également des résultats d'échec si une version d'Elasticsearch ne prend pas en charge les contrôles de chiffrement nœud à nœud.

Le protocole HTTPS (TLS) peut être utilisé pour empêcher les attaquants potentiels d'espionner ou de manipuler le trafic réseau à l'aide d'attaques de type person-in-the-middle ou d'attaques similaires. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées. L'activation du chiffrement nœud à nœud pour les domaines Elasticsearch garantit que les communications intra-cluster sont cryptées en transit.

Cette configuration peut entraîner une baisse des performances. Vous devez connaître le compromis entre performances et le tester avant d'activer cette option.

Correction

Pour plus d'informations sur l'activation du chiffrement nœud à nœud sur les domaines nouveaux et existants, consultez la section Activation du chiffrement nœud à nœud dans le Amazon Service Developer Guide. OpenSearch

[ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée

Exigences connexes : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

Règle AWS Config : `elasticsearch-logs-to-cloudwatch`

Type de calendrier : Déclenché par un changement

Paramètres :

- `logtype = 'error'`(non personnalisable)

Ce contrôle vérifie si les domaines Elasticsearch sont configurés pour envoyer des journaux d'erreurs à Logs. CloudWatch

Vous devez activer les journaux d'erreurs pour les domaines Elasticsearch et les envoyer à CloudWatch Logs pour qu'ils soient conservés et traités. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

Correction

Pour plus d'informations sur la façon d'activer la publication de journaux, consultez la section Activation de la publication de journaux (console) dans le manuel Amazon OpenSearch Service Developer Guide.

[ES.5] La journalisation des audits doit être activée pour les domaines Elasticsearch

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104,2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

AWS Config règle : `elasticsearch-audit-logging-enabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

- `cloudWatchLogsLogGroupArnList`(non personnalisable). Security Hub CSPM ne renseigne pas ce paramètre. Comma-separated liste des groupes de CloudWatch journaux qui doivent être configurés pour les journaux d'audit.

  Cette règle s'applique `NON_COMPLIANT` si le groupe de CloudWatch journaux Logs du domaine Elasticsearch n'est pas spécifié dans cette liste de paramètres.

Ce contrôle vérifie si la journalisation des audits est activée pour les domaines Elasticsearch. Ce contrôle échoue si la journalisation des audits n'est pas activée pour un domaine Elasticsearch.

Les journaux d'audit sont hautement personnalisables. Ils vous permettent de suivre l'activité des utilisateurs sur vos clusters Elasticsearch, notamment les réussites et les échecs d'authentification, les demandes adressées OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

Correction

Pour obtenir des instructions détaillées sur l'activation des journaux d'audit, consultez la section Activation des journaux d'audit dans l'Amazon OpenSearch Service Developer Guide.

[ES.6] Les domaines Elasticsearch doivent comporter au moins trois nœuds de données

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

AWS Config règle : `elasticsearch-data-node-fault-tolerance` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les domaines Elasticsearch sont configurés avec au moins trois nœuds de données et `zoneAwarenessEnabled` si oui. `true`

Un domaine Elasticsearch nécessite au moins trois nœuds de données pour garantir une haute disponibilité et une tolérance aux pannes. Le déploiement d'un domaine Elasticsearch avec au moins trois nœuds de données garantit le fonctionnement du cluster en cas de défaillance d'un nœud.

Correction

Pour modifier le nombre de nœuds de données dans un domaine Elasticsearch

1. Ouvrez la console Amazon OpenSearch Service à l'adresse https://console.aws.amazon.com/aos/.
2. Sous Domaines, choisissez le nom du domaine que vous souhaitez modifier.
3. Choisissez Edit domain (Modifier le domaine).
4. Sous Nœuds de données, définissez Nombre de nœuds sur un nombre supérieur ou égal à`3`.

   Pour les déploiements dans trois zones de disponibilité, définissez un multiple de trois pour garantir une distribution égale entre les zones de disponibilité.
5. Sélectionnez Soumettre.

[ES.7] Les domaines Elasticsearch doivent être configurés avec au moins trois nœuds principaux dédiés

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

AWS Config règle : `elasticsearch-primary-node-fault-tolerance` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les domaines Elasticsearch sont configurés avec au moins trois nœuds principaux dédiés. Ce contrôle échoue si le domaine n'utilise pas de nœuds principaux dédiés. Ce contrôle est transféré si les domaines Elasticsearch possèdent cinq nœuds principaux dédiés. Cependant, l'utilisation de plus de trois nœuds principaux peut s'avérer inutile pour atténuer le risque de disponibilité et entraîner des coûts supplémentaires.

Un domaine Elasticsearch nécessite au moins trois nœuds principaux dédiés pour garantir une haute disponibilité et une tolérance aux pannes. Les ressources des nœuds principaux dédiés peuvent être sollicitées lors des blue/green déploiements de nœuds de données, car il existe des nœuds supplémentaires à gérer. Le déploiement d'un domaine Elasticsearch avec au moins trois nœuds principaux dédiés garantit une capacité de ressources de nœud principal suffisante et des opérations de cluster suffisantes en cas de défaillance d'un nœud.

Correction

Pour modifier le nombre de nœuds principaux dédiés dans un OpenSearch domaine

1. Ouvrez la console Amazon OpenSearch Service à l'adresse https://console.aws.amazon.com/aos/.
2. Sous Domaines, choisissez le nom du domaine que vous souhaitez modifier.
3. Choisissez Edit domain (Modifier le domaine).
4. Sous Nœuds maîtres dédiés, définissez le type d'instance sur le type d'instance souhaité.
5. Définissez un nombre de nœuds principaux égal à trois ou plus.
6. Sélectionnez Soumettre.

[ES.8] Les connexions aux domaines Elasticsearch doivent être chiffrées conformément à la dernière politique de sécurité TLS

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23,

NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::Elasticsearch::Domain`

AWS Config règle : `elasticsearch-https-required` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un point de terminaison de domaine Elasticsearch est configuré pour utiliser la dernière politique de sécurité TLS. Le contrôle échoue si le point de terminaison du domaine Elasticsearch n'est pas configuré pour utiliser la dernière politique prise en charge ou si le protocole HTTPS n'est pas activé. La dernière politique de sécurité TLS actuellement prise en charge est`Policy-Min-TLS-1-2-PFS-2023-10`.

Vous pouvez utiliser HTTPS (TLS) pour empêcher les pirates potentiels d'espionner ou de manipuler le trafic réseau à l'aide d'attaques de l'homme du milieu au d'autres attaques similaires. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées. Le chiffrement des données en transit peut affecter les performances. Vous devriez tester votre application à l'aide de cette fonctionnalité pour comprendre le profil de performances et l'impact du protocole TLS. TLS 1.2 apporte plusieurs améliorations de sécurité par rapport aux versions précédentes de TLS.

Correction

Pour activer le chiffrement TLS, utilisez l'opération UpdateDomainConfig d'API pour configurer l'DomainEndpointOptionsobjet. Cela définit le`TLSSecurityPolicy`.

[ES.9] Les domaines Elasticsearch doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::Elasticsearch::Domain`

AWS Config règle : `tagged-elasticsearch-domain` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	`No default value`

Ce contrôle vérifie si un domaine Elasticsearch possède des balises dont les clés spécifiques sont définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le domaine ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le domaine n'est balisé par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un domaine Elasticsearch, consultez la section Utilisation des balises dans le manuel Amazon OpenSearch Service Developer Guide.

Contrôles Security Hub CSPM pour Amazon EMR

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon EMR (anciennement Amazon Elastic MapReduce). Les commandes ne sont peut-être pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques

Exigences associées : PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::EMR::Cluster`

AWS Configrègle : emr-master-no-public-ip

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les nœuds maîtres des clusters Amazon EMR possèdent des adresses IP publiques. Le contrôle échoue si des adresses IP publiques sont associées à l'une des instances du nœud maître.

Les adresses IP publiques sont désignées dans le `PublicIp` champ de `NetworkInterfaces` configuration de l'instance. Ce contrôle vérifie uniquement les clusters Amazon EMR à l'état `RUNNING` or`WAITING`.

Correction

Lors du lancement, vous pouvez contrôler si une adresse IPv4 publique est attribuée à votre instance dans un sous-réseau par défaut ou non par défaut. Par défaut, cet attribut est défini sur les sous-réseaux par défaut. `true` L'attribut d'adressage public IPv4 est défini sur les sous-réseaux autres que ceux par défaut`false`, sauf s'il a été créé par l'assistant de lancement d'instance Amazon EC2. Dans ce cas, l'attribut est défini sur`true`.

Après le lancement, vous ne pouvez pas dissocier manuellement une adresse IPv4 publique de votre instance.

Pour remédier à un échec de détection, vous devez lancer un nouveau cluster dans un VPC avec un sous-réseau privé dont l'attribut d'adressage public IPv4 est défini sur. `false` Pour obtenir des instructions, consultez la section Lancer des clusters dans un VPC dans le guide de gestion Amazon EMR.

[EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé

Exigences associées : PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger > Gestion des accès sécurisés > Ressource non accessible au public

Gravité : Critique

Type de ressource : `AWS::::Account`

AWS Configrègle : emr-block-public-access

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si votre compte est configuré pour bloquer l'accès public à Amazon EMR. Le contrôle échoue si le paramètre de blocage de l'accès public n'est pas activé ou si un port autre que le port 22 est autorisé.

Le blocage de l'accès public par Amazon EMR vous empêche de lancer un cluster dans un sous-réseau public si le cluster possède une configuration de sécurité qui autorise le trafic entrant depuis des adresses IP publiques sur un port. Lorsqu'un utilisateur de votre Compte AWS lance un cluster, Amazon EMR vérifie les règles de port du groupe de sécurité du cluster et les compare à vos règles de trafic entrant. Si le groupe de sécurité dispose d'une règle entrante qui ouvre des ports aux adresses IP publiques IPv4 0.0.0. 0/0 ou IPv6 : :/0, et ces ports ne sont pas spécifiés comme des exceptions pour votre compte, Amazon EMR ne permet pas à l'utilisateur de créer le cluster.

> **Note**
>
> Le blocage de l'accès public est activé par défaut. Pour améliorer la protection du compte, nous vous recommandons de le laisser activé.

Correction

Pour configurer le blocage de l'accès public pour Amazon EMR, consultez la section Utilisation de l'accès public bloqué par Amazon EMR dans le guide de gestion Amazon EMR.

[EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::EMR::SecurityConfiguration`

Règle AWS Config : emr-security-configuration-encryption-rest

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement au repos est activé dans une configuration de sécurité Amazon EMR. Le contrôle échoue si la configuration de sécurité n'active pas le chiffrement au repos.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour activer le chiffrement au repos dans une configuration de sécurité Amazon EMR, consultez la section Configurer le chiffrement des données dans le guide de gestion Amazon EMR.

[EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport

Exigences associées : NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3)

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::EMR::SecurityConfiguration`

Règle AWS Config : emr-security-configuration-encryption-transit

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement en transit est activé dans une configuration de sécurité Amazon EMR. Le contrôle échoue si la configuration de sécurité n'active pas le chiffrement en transit.

Les données en transit font référence aux données qui se déplacent d'un emplacement à un autre, par exemple entre les nœuds de votre cluster ou entre votre cluster et votre application. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque qu'un utilisateur non autorisé puisse espionner le trafic réseau.

Correction

Pour activer le chiffrement en transit dans une configuration de sécurité Amazon EMR, consultez la section Configurer le chiffrement des données dans le guide de gestion Amazon EMR.

Security Hub CSPM contrôle pour EventBridge

Ces AWS Security Hub CSPM contrôles évaluent le EventBridge service et les ressources Amazon.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[EventBridge.2] les bus EventBridge d'événements doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Events::EventBus`

AWS Configrègle : `tagged-events-eventbus` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un bus d' EventBridge événements Amazon possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le bus d'événements ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le bus d'événements n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un bus d' EventBridge événements, consultez les EventBridge balises Amazon dans le guide de EventBridge l'utilisateur Amazon.

[EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources

Exigences associées : NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3), PCI DSS v4.0. 1/10.3.1

Catégorie : Protéger > Gestion des accès sécurisés > Ressource non accessible au public

Gravité : Faible

Type de ressource : `AWS::Events::EventBus`

Règle AWS Config : custom-eventbus-policy-attached

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un bus d'événements EventBridge personnalisé Amazon est associé à une politique basée sur les ressources. Ce contrôle échoue si le bus d'événements personnalisé n'a pas de politique basée sur les ressources.

Par défaut, aucune politique basée sur les ressources n'est attachée à un bus d'événements EventBridge personnalisé. Cela permet aux principaux associés au compte d'accéder au bus d'événements. En associant une politique basée sur les ressources au bus d'événements, vous pouvez limiter l'accès au bus d'événements à des comptes spécifiques, ainsi qu'accorder intentionnellement l'accès aux entités d'un autre compte.

Correction

Pour associer une politique basée sur les ressources à un bus d'événements EventBridge personnalisé, consultez la section Utilisation de politiques basées sur les ressources pour Amazon dans EventBridge le guide de l'utilisateur Amazon. EventBridge

[EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::Events::Endpoint`

Règle AWS Config : `global-endpoint-event-replication-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la réplication des événements est activée pour un point de terminaison EventBridge mondial Amazon. Le contrôle échoue si la réplication des événements n'est pas activée pour un point de terminaison global.

Les points de terminaison globaux contribuent à rendre votre application Regional-fault tolérante. Pour commencer, affectez une surveillance d'état Amazon Route 53 au point de terminaison. Lorsque le basculement est lancé, le bilan de santé indique un état « non fonctionnel ». Quelques minutes après le lancement du basculement, tous les événements personnalisés sont routés vers un bus d'événements dans la région secondaire et sont traités par ce bus d'événements. Lorsque vous utilisez des points de terminaison globaux, vous pouvez activer la réplication d'événements. La réplication d'événements envoie tous les événements personnalisés aux bus d'événements des régions principale et secondaire à l'aide de règles gérées. Nous recommandons d'activer la réplication des événements lors de la configuration des points de terminaison globaux. La réplication d'événements vous permet de vérifier que vos points de terminaison globaux sont correctement configurés. La réplication des événements est requise pour effectuer une récupération automatique suite à un événement de basculement. Si la réplication des événements n'est pas activée, vous devrez réinitialiser manuellement le bilan de santé de Route 53 sur « sain » avant que les événements ne soient redirigés vers la région principale.

> **Note**
>
> Si vous utilisez des bus d'événements personnalisés, vous aurez besoin d'un bus pair personnalisé dans chaque région portant le même nom et le même compte pour que le basculement fonctionne correctement. L'activation de la réplication des événements peut augmenter vos coûts mensuels. Pour plus d'informations sur les tarifs, consultez EventBridge les tarifs Amazon.

Correction

Pour activer la réplication d'événements pour les points de terminaison EventBridge globaux, consultez la section Créer un point de terminaison global dans le guide de EventBridge l'utilisateur Amazon. Pour Réplication d'événements, sélectionnez Réplication d'événements activée.

Contrôles Security Hub CSPM pour Amazon Fraud Detector

Ces contrôles CSPM du Security Hub évaluent le service et les ressources d'Amazon Fraud Detector.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::FraudDetector::EntityType`

Règle AWS Config : `frauddetector-entity-type-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un type d'entité Amazon Fraud Detector possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le type d'entité ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le type d'entité n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un type d'entité Amazon Fraud Detector (console)

1. Ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation, sélectionnez Entities.
3. Sélectionnez un type d'entité dans la liste.
4. Dans la section des balises de type d'entité, choisissez Gérer les balises.
5. Sélectionnez Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Répétez l'opération pour d'autres paires clé-valeur.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

[FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::FraudDetector::Label`

Règle AWS Config : `frauddetector-label-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une étiquette Amazon Fraud Detector comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'étiquette ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'étiquette n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des tags à une étiquette Amazon Fraud Detector (console)

1. Ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation, sélectionnez Labels.
3. Sélectionnez une étiquette dans la liste.
4. Dans la section des étiquettes, choisissez Gérer les balises.
5. Sélectionnez Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Répétez l'opération pour d'autres paires clé-valeur.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

[FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::FraudDetector::Outcome`

Règle AWS Config : `frauddetector-outcome-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un résultat d'Amazon Fraud Detector comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le résultat ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le résultat n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un résultat d'Amazon Fraud Detector (console)

1. Ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation, sélectionnez Outcomes.
3. Sélectionnez un résultat dans la liste.
4. Dans la section des balises de résultats, choisissez Gérer les balises.
5. Sélectionnez Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Répétez l'opération pour d'autres paires clé-valeur.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

[FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::FraudDetector::Variable`

Règle AWS Config : `frauddetector-variable-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une variable Amazon Fraud Detector possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la variable ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la variable n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une variable Amazon Fraud Detector (console)

1. Ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation, sélectionnez Variables.
3. Sélectionnez une variable dans la liste.
4. Dans la section des balises de variables, choisissez Gérer les balises.
5. Sélectionnez Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Répétez l'opération pour d'autres paires clé-valeur.
6. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

Contrôles Security Hub CSPM pour Amazon FSx

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon FSx. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::FSx::FileSystem`

Règle AWS Config : fsx-openzfs-copy-tags-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un système de fichiers Amazon FSx pour OpenZFS est configuré pour copier des balises vers des sauvegardes et des volumes. Le contrôle échoue si le système de fichiers OpenZFS n'est pas configuré pour copier les balises vers les sauvegardes et les volumes.

L'identification et l'inventaire de vos actifs informatiques constituent un aspect important de la gouvernance et de la sécurité. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cela est utile lorsque vous disposez de nombreuses ressources du même type, car vous pouvez identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées.

Correction

Pour plus d'informations sur la configuration d'un système de fichiers FSx pour OpenZFS afin de copier des balises vers des sauvegardes et des volumes, consultez la section Mise à jour d'un système de fichiers dans le guide de l'utilisateur Amazon FSx pour OpenZFS.

[FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes

Exigences connexes : NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::FSx::FileSystem`

Règle AWS Config : fsx-lustre-copy-tags-to-backups

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un système de fichiers Amazon FSx for Lustre est configuré pour copier des balises vers des sauvegardes et des volumes. Le contrôle échoue si le système de fichiers Lustre n'est pas configuré pour copier les balises vers les sauvegardes et les volumes.

L'identification et l'inventaire de vos actifs informatiques constituent un aspect important de la gouvernance et de la sécurité. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cela est utile lorsque vous disposez de nombreuses ressources du même type, car vous pouvez identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées.

Correction

Pour plus d'informations sur la configuration d'un système de fichiers FSx for Lustre afin de copier des balises vers des sauvegardes, consultez Copier des sauvegardes dans le Compte AWS même système dans le guide de l'utilisateur Amazon FSx for Lustre.

[FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::FSx::FileSystem`

Règle AWS Config : fsx-openzfs-deployment-type-check

Type de calendrier : Périodique

Paramètres : `deploymentTypes: MULTI_AZ_1` (non personnalisable)

Ce contrôle vérifie si un système de fichiers Amazon FSx pour OpenZFS est configuré pour utiliser le type de déploiement à zones de disponibilité multiples ()Multi-AZ. Le contrôle échoue si le système de fichiers n'est pas configuré pour utiliser le type de Multi-AZ déploiement.

Amazon FSx pour OpenZFS prend en charge plusieurs types de déploiement pour les systèmes de fichiers : Multi-AZ (HA), (HA) et Single-AZ Single-AZ (non-HA). Les types de déploiement offrent différents niveaux de disponibilité et de durabilité. Multi-AZ Les systèmes de fichiers (HA) sont composés d'une paire de serveurs de fichiers à haute disponibilité (HA) répartis sur deux zones de disponibilité (AZ). Nous recommandons d'utiliser le type de déploiement Multi-AZ (HA) pour la plupart des charges de travail de production en raison du modèle de haute disponibilité et de durabilité qu'il propose.

Correction

Vous pouvez configurer un système de fichiers Amazon FSx pour OpenZFS afin d'utiliser le type de Multi-AZ déploiement lorsque vous créez le système de fichiers. Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers FSx pour OpenZFS existant.

Pour plus d'informations sur les types et options de déploiement de FSx pour les systèmes de fichiers OpenZFS, consultez les sections Disponibilité et durabilité d'Amazon FSx pour OpenZFS et Gestion des ressources du système de fichiers dans le guide de l'utilisateur Amazon FSx pour OpenZFS.

[FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::FSx::FileSystem`

Règle AWS Config : fsx-ontap-deployment-type-check

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`deploymentTypes`	Liste des types de déploiement à inclure dans l'évaluation. Le contrôle génère une `FAILED` recherche si un système de fichiers n'est pas configuré pour utiliser un type de déploiement spécifié dans la liste.	Enum	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

Ce contrôle vérifie si un système de fichiers Amazon FSx for NetApp ONTAP est configuré pour utiliser un type de déploiement avec plusieurs zones de disponibilité (Multi-AZ). Le contrôle échoue si le système de fichiers n'est pas configuré pour utiliser un type de Multi-AZ déploiement. Vous pouvez éventuellement spécifier une liste de types de déploiement à inclure dans l'évaluation.

Amazon FSx for NetApp ONTAP prend en charge plusieurs types de déploiement pour les systèmes de fichiers : Single-AZ 1, Single-AZ 2, Multi-AZ 1 et 2. Multi-AZ Les types de déploiement offrent différents niveaux de disponibilité et de durabilité. Nous recommandons d'utiliser un type de Multi-AZ déploiement pour la plupart des charges de travail de production en raison du modèle de haute disponibilité et de durabilité proposé par les types de Multi-AZ déploiement. Multi-AZ les systèmes de fichiers prennent en charge toutes les fonctionnalités de disponibilité et de durabilité des systèmes de Single-AZ fichiers. En outre, ils sont conçus pour garantir la disponibilité continue des données même lorsqu'une zone de disponibilité (AZ) n'est pas disponible.

Correction

Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers Amazon FSx for NetApp ONTAP existant. Toutefois, vous pouvez sauvegarder les données, puis les restaurer sur un nouveau système de fichiers utilisant un type de Multi-AZ déploiement.

Pour plus d'informations sur les types et options de déploiement pour les systèmes de fichiers FSx for ONTAP, consultez les sections Disponibilité, durabilité et options de déploiement et Gestion des systèmes de fichiers dans le guide de l'utilisateur de FSx for ONTAP.

[FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::FSx::FileSystem`

Règle AWS Config : fsx-windows-deployment-type-check

Type de calendrier : Périodique

Paramètres : `deploymentTypes: MULTI_AZ_1` (non personnalisable)

Ce contrôle vérifie si un système de fichiers Amazon FSx for Windows File Server est configuré pour utiliser le type de déploiement à zones de disponibilité multiples Multi-AZ (). Le contrôle échoue si le système de fichiers n'est pas configuré pour utiliser le type de Multi-AZ déploiement.

Amazon FSx for Windows File Server prend en charge deux types de déploiement pour les systèmes de fichiers Single-AZ: Multi-AZet. Les types de déploiement offrent différents niveaux de disponibilité et de durabilité. Single-AZ les systèmes de fichiers sont composés d'une seule instance de serveur de fichiers Windows et d'un ensemble de volumes de stockage au sein d'une seule zone de disponibilité (AZ). Multi-AZ les systèmes de fichiers sont composés d'un cluster à haute disponibilité de serveurs de fichiers Windows répartis sur deux zones de disponibilité. Nous recommandons d'utiliser le type de Multi-AZ déploiement pour la plupart des charges de travail de production en raison du modèle de haute disponibilité et de durabilité qu'il fournit.

Correction

Vous pouvez configurer un système de fichiers Amazon FSx for Windows File Server afin d'utiliser Multi-AZ le type de déploiement lors de la création du système de fichiers. Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers FSx for Windows File Server existant.

Pour plus d'informations sur les types et options de déploiement des systèmes de fichiers FSx for Windows File Server, consultez les sections Disponibilité et durabilité Single-AZ : systèmes de fichiers Multi-AZ et Getting started with Amazon FSx for Windows File Server dans le guide de l'utilisateur Amazon FSx for Windows File Server.

Contrôles Security Hub CSPM pour Global Accelerator

Ces AWS Security Hub CSPM contrôles évaluent le AWS Global Accelerator service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::GlobalAccelerator::Accelerator`

AWS Configrègle : `tagged-globalaccelerator-accelerator` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS Global Accelerator accélérateur possède des balises avec les touches spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'accélérateur ne possède aucune clé de balise ou s'il ne possède pas toutes les touches spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'accélérateur n'est marqué par aucune touche. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un accélérateur global Global Accelerator, voir la section Marquage AWS Global Accelerator dans le guide du AWS Global Accelerator développeur.

Contrôles Security Hub CSPM pourAWS Glue

Ces AWS Security Hub CSPM contrôles évaluent le AWS Glue service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Glue.1]AWS Glueles emplois doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Glue::Job`

AWS Configrègle : `tagged-glue-job` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS Glue tâche possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la tâche ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la tâche n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une AWS Glue tâche, consultez les AWSbalises AWS Glue dans le guide de AWS Glue l'utilisateur.

[Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::Glue::MLTransform`

Règle AWS Config : glue-ml-transform-encrypted-at-rest

Type de calendrier : changement déclenché

Paramètres : Non

Ce contrôle vérifie si une transformation de AWS Glue machine learning est chiffrée au repos. Le contrôle échoue si la transformation de machine learning n'est pas chiffrée au repos.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour configurer le chiffrement pour les transformations de AWS Glue machine learning, consultez la section Utilisation des transformations de machine learning dans le guide de AWS Glue l'utilisateur.

[Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::Glue::Job`

Règle AWS Config : glue-spark-job-supported-version

Type de calendrier : changement déclenché

Paramètres **`minimumSupportedGlueVersion`** : `3.0` (non personnalisable)

Ce contrôle vérifie si une tâche AWS Glue for Spark est configurée pour s'exécuter sur une version prise en charge deAWS Glue. Le contrôle échoue si le job Spark est configuré pour s'exécuter sur une version antérieure à la version minimale prise en charge. AWS Glue

> **Note**
>
> Ce contrôle génère également une `FAILED` recherche pour une tâche AWS Glue for Spark si la propriété AWS Glue version (`GlueVersion`) n'existe pas ou est nulle dans l'élément de configuration (CI) de la tâche. Dans de tels cas, le résultat inclut l'annotation suivante :`GlueVersion is null or missing in glueetl job configuration`. Pour résoudre ce type de `FAILED` recherche, ajoutez la `GlueVersion` propriété à la configuration de la tâche. Pour obtenir la liste des versions et des environnements d'exécution pris en charge, consultez la section AWS GlueVersions du guide de AWS Glue l'utilisateur.

L'exécution de tâches AWS Glue Spark sur les versions actuelles de AWS Glue permet d'optimiser les performances, la sécurité et l'accès aux dernières fonctionnalités deAWS Glue. Cela peut également aider à se prémunir contre les failles de sécurité. Par exemple, une nouvelle version peut être publiée pour fournir des mises à jour de sécurité, résoudre des problèmes ou introduire de nouvelles fonctionnalités.

Correction

Pour plus d'informations sur la migration d'une tâche Spark vers une version compatible deAWS Glue, consultez la section Migration AWS Glue pour les tâches Spark dans le guide de l'AWS Glueutilisateur.

Contrôles Security Hub CSPM pour Amazon GuardDuty

Ces AWS Security Hub CSPM contrôles évaluent le GuardDuty service et les ressources Amazon. Les commandes ne sont peut-être pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[GuardDuty.1] GuardDuty doit être activé

Exigences associées : NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 RA-3 (4), NIST.800-53.r5 SA-11 (1), NIST.800-53.r5 SA-11 (6), NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SA-8 (21), NIST.800-53.r5 SA-8 (25) NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5 (1), NIST.800-53.r5 SC-5 (3) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4 (13), NIST.800-53.r5 SI-4 (2), (22), NIST.800-53.r5 SI-4 (25), NIST.800-53.r5 SI-4 (4), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.4.2, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS version 3.2. 1/114., PCI DSS version 4.0. 1/11.5.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : guardduty-enabled-centralized

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si Amazon GuardDuty est activé dans votre GuardDuty compte et dans votre région.

Il est vivement recommandé de l'activer GuardDuty dans toutes les AWS régions prises en charge. Cela permet GuardDuty de générer des informations sur des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Cela permet également GuardDuty de surveiller CloudTrail des événements globaux Services AWS tels que IAM.

Correction

Pour l'activer GuardDuty, consultez Getting Started with GuardDuty dans le guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.2] GuardDuty les filtres doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::GuardDuty::Filter`

AWS Configrègle : `tagged-guardduty-filter` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un GuardDuty filtre Amazon possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le filtre ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le filtre n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque

vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un GuardDuty filtre, consultez TagResourcele Amazon GuardDuty API Reference.

[GuardDuty.3] Les GuardDuty IPsets doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::GuardDuty::IPSet`

AWS Configrègle : `tagged-guardduty-ipset` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un Amazon GuardDuty IPSet possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'IPSet ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'IPSet n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un GuardDuty IPSet, consultez TagResourcele manuel Amazon GuardDuty API Reference.

[GuardDuty.4] les GuardDuty détecteurs doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::GuardDuty::Detector`

AWS Configrègle : `tagged-guardduty-detector` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un GuardDuty détecteur Amazon possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le détecteur ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le

paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le détecteur n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un GuardDuty détecteur, consultez TagResourcele Amazon GuardDuty API Reference.

[GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-eks-protection-audit-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la surveillance du journal d'audit GuardDuty EKS est activée. Pour un compte autonome, le contrôle échoue si la surveillance du journal d'audit GuardDuty EKS est désactivée dans le compte. Dans un environnement multi-comptes, le contrôle échoue si le compte GuardDuty administrateur délégué et tous les comptes membres n'ont pas activé la surveillance du journal d'audit EKS.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité de surveillance du journal d'audit EKS pour les comptes des membres de l'organisation. GuardDuty les comptes membres ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l' GuardDuty administrateur délégué a un compte de membre suspendu pour lequel le suivi du journal d'audit GuardDuty EKS n'est pas activé. Pour recevoir une `PASSED` constatation, l'administrateur délégué doit dissocier ces comptes suspendus. GuardDuty

GuardDuty La surveillance du journal d'audit EKS vous aide à détecter les activités potentiellement suspectes dans vos clusters Amazon Elastic Kubernetes Service (Amazon EKS). La surveillance des journaux d'audit EKS utilise les journaux d'audit Kubernetes pour capturer les activités chronologiques des utilisateurs, des applications utilisant l'API Kubernetes et du plan de contrôle.

Correction

Pour activer la surveillance du journal d'audit GuardDuty EKS, consultez la section Surveillance du journal d'audit EKS dans le guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.6] La protection GuardDuty Lambda doit être activée

Exigences associées : PCI DSS v4.0. 1/11.5.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-lambda-protection-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la protection GuardDuty Lambda est activée. Pour un compte autonome, le contrôle échoue si la protection GuardDuty Lambda est désactivée dans le compte. Dans un environnement multi-comptes, le contrôle échoue si la protection Lambda n'est pas activée sur le compte d' GuardDuty administrateur délégué et sur tous les comptes membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité de protection Lambda pour les comptes des membres de l'organisation. GuardDuty les comptes membres ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l' GuardDuty administrateur délégué a un compte de membre suspendu sur lequel la protection GuardDuty Lambda n'est pas activée. Pour recevoir une `PASSED` constatation, l'administrateur délégué doit dissocier ces comptes suspendus. GuardDuty

GuardDuty La protection Lambda vous aide à identifier les menaces de sécurité potentielles lorsqu'une AWS Lambda fonction est invoquée. Après avoir activé la protection Lambda, GuardDuty commence à surveiller les journaux d'activité du réseau Lambda associés aux fonctions Lambda de votre. Compte AWS Lorsqu'une fonction Lambda est invoquée et GuardDuty identifie un trafic réseau suspect indiquant la présence d'un code potentiellement malveillant dans votre fonction Lambda, GuardDuty elle génère un résultat.

Correction

Pour activer la protection GuardDuty Lambda, consultez la section Configuration de la protection Lambda dans le guide de l'utilisateur Amazon. GuardDuty

[GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée

Exigences associées : PCI DSS v4.0. 1/11.5.1

Catégorie : Détecter > Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-eks-protection-runtime-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la surveillance du temps d'exécution GuardDuty EKS avec gestion automatisée des agents est activée. Pour un compte autonome, le contrôle échoue si GuardDuty EKS Runtime Monitoring avec gestion automatisée des agents est désactivé dans le compte. Dans un environnement multi-comptes, le contrôle échoue si le compte GuardDuty administrateur délégué et tous les comptes membres ne disposent pas d'EKS Runtime Monitoring avec gestion automatique des agents activée.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité EKS Runtime Monitoring avec gestion automatique des agents pour les comptes des membres de l'organisation. GuardDuty les comptes membres ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l' GuardDuty administrateur délégué a un compte de membre suspendu pour lequel GuardDuty EKS Runtime Monitoring n'est pas activé. Pour recevoir une `PASSED` constatation, l'administrateur délégué doit dissocier ces comptes suspendus. GuardDuty

La protection EKS d'Amazon GuardDuty fournit une couverture de détection des menaces pour vous aider à protéger les clusters Amazon EKS au sein de votre AWS environnement. EKS Runtime Monitoring utilise des événements au niveau du système d'exploitation pour vous aider à détecter les menaces potentielles dans les nœuds et les conteneurs EKS au sein de vos clusters EKS.

Correction

Pour activer EKS Runtime Monitoring avec la gestion automatisée des agents, consultez la section Enabling GuardDuty Runtime Monitoring dans le guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-malware-protection-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la protection contre les GuardDuty programmes malveillants est activée. Pour un compte autonome, le contrôle échoue si la protection contre les GuardDuty programmes malveillants est désactivée dans le compte. Dans un environnement à comptes multiples, le contrôle échoue si la protection contre les programmes malveillants n'est pas activée sur le compte GuardDuty administrateur délégué et sur tous les comptes membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité de protection contre les programmes malveillants pour les comptes des membres de l'organisation. GuardDuty les comptes membres ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l' GuardDuty administrateur délégué possède un compte de membre suspendu pour lequel la protection contre les GuardDuty programmes malveillants n'est pas activée. Pour recevoir une `PASSED` constatation, l'administrateur délégué doit dissocier ces comptes suspendus. GuardDuty

GuardDuty Malware Protection for EC2 vous aide à détecter la présence potentielle de malwares en analysant les volumes Amazon Elastic Block Store (Amazon EBS) attachés aux instances et aux charges de travail des conteneurs Amazon Elastic Compute Cloud (Amazon EC2). Malware Protection propose des options d'analyse qui vous permettent de décider si vous souhaitez inclure ou exclure des instances EC2 et des charges de travail de conteneur spécifiques au moment de l'analyse. Il offre également la possibilité de conserver les instantanés des volumes EBS attachés aux instances EC2 ou aux charges de travail des conteneurs dans vos comptes. GuardDuty Les instantanés ne sont retenus que lorsqu'un logiciel malveillant est détecté et que des résultats de protection contre les logiciels malveillants sont générés.

Correction

Pour activer la protection contre les GuardDuty programmes malveillants pour EC2, consultez la section Configuration de l'analyse des GuardDuty-initiated programmes malveillants dans le guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.9] GuardDuty La protection RDS doit être activée

Exigences associées : PCI DSS v4.0. 1/11.5.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-rds-protection-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la protection GuardDuty RDS est activée. Pour un compte autonome, le contrôle échoue si la protection GuardDuty RDS est désactivée dans le compte. Dans un environnement multi-comptes, le contrôle échoue si la protection RDS n'est pas activée sur le compte d' GuardDuty administrateur délégué et sur tous les comptes de membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité de protection RDS pour les comptes des membres de l'organisation. GuardDuty les comptes membres ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l' GuardDuty administrateur délégué a un compte de membre suspendu pour lequel la protection GuardDuty RDS n'est pas activée. Pour recevoir une `PASSED` constatation, l'administrateur délégué doit dissocier ces comptes suspendus. GuardDuty

RDS Protection GuardDuty analyse et établit le profil de l'activité de connexion RDS pour détecter les menaces d'accès potentielles à vos bases de données Amazon Aurora (MySQL-Compatible éditions Aurora et Aurora PostgreSQL-Compatible). Cette fonctionnalité vous permet d'identifier les comportements de connexion potentiellement suspects. La protection RDS ne nécessite aucune infrastructure supplémentaire ; elle est conçue de manière à ne pas affecter les performances de vos instances de base de données. Lorsque RDS Protection détecte une tentative de connexion potentiellement suspecte ou anormale indiquant une menace pour votre base de données, elle GuardDuty génère une nouvelle découverte contenant des informations sur la base de données potentiellement compromise.

Correction

Pour activer la protection GuardDuty RDS, consultez GuardDuty la section Protection du guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.10] La protection GuardDuty S3 doit être activée

Exigences associées : PCI DSS v4.0. 1/11.5.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-s3-protection-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la protection GuardDuty S3 est activée. Pour un compte autonome, le contrôle échoue si GuardDuty S3 Protection est désactivée dans le compte. Dans un environnement multi-comptes, le contrôle échoue si S3 Protection n'est pas activé sur le compte d' GuardDuty administrateur délégué et sur tous les comptes de membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité de protection S3 pour les comptes des membres de l'organisation. GuardDuty les comptes membres ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l' GuardDuty administrateur délégué a un compte de membre suspendu pour lequel GuardDuty S3 Protection n'est pas activé. Pour recevoir une `PASSED` constatation, l'administrateur délégué doit dissocier ces comptes suspendus. GuardDuty

S3 Protection permet GuardDuty de surveiller les opérations d'API au niveau des objets afin d'identifier les risques de sécurité potentiels pour les données contenues dans vos compartiments Amazon Simple Storage Service (Amazon S3). GuardDuty surveille les menaces qui pèsent sur vos ressources S3 en analysant les événements AWS CloudTrail de gestion et les événements liés aux données CloudTrail S3.

Correction

Pour activer la protection GuardDuty S3, consultez Amazon S3 Protection dans Amazon GuardDuty dans le guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée

Catégorie : Détecter > Services de détection

Gravité : Élevée

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-runtime-monitoring-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le Runtime Monitoring est activé sur Amazon GuardDuty. Pour un compte autonome, le contrôle échoue si la surveillance du temps GuardDuty d'exécution est désactivée pour le compte. Dans un environnement multi-comptes, le contrôle échoue si la surveillance du temps GuardDuty d'exécution est désactivée pour le compte d' GuardDuty administrateur délégué et pour tous les comptes membres.

Dans un environnement multi-comptes, seul l' GuardDuty administrateur délégué peut activer ou désactiver la surveillance du temps GuardDuty d'exécution pour les comptes de son organisation. En outre, seul l' GuardDuty administrateur peut configurer et gérer les agents de sécurité GuardDuty utilisés pour la surveillance de l'exécution des AWS charges de travail et des ressources des comptes de l'organisation. GuardDuty les comptes membres ne peuvent pas activer, configurer ou désactiver la surveillance du temps d'exécution pour leurs propres comptes.

GuardDuty Runtime Monitoring observe et analyse les événements au niveau du système d'exploitation, du réseau et des fichiers pour vous aider à détecter les menaces potentielles dans des AWS charges de travail spécifiques de votre environnement. Il utilise des agents GuardDuty de sécurité qui ajoutent de la visibilité sur le comportement d'exécution, tels que l'accès aux fichiers, l'exécution des processus, les arguments de ligne de commande et les connexions réseau. Vous pouvez activer et gérer l'agent de sécurité pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces potentielles, telles que les clusters Amazon EKS et les instances Amazon EC2.

Correction

Pour plus d'informations sur la configuration et l'activation de la surveillance du temps GuardDuty d'exécution, consultez la section Surveillance du temps GuardDuty d' GuardDuty exécution et activation de la surveillance du temps d'exécution dans le guide de GuardDuty l'utilisateur Amazon.

[GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée

Catégorie : Détecter > Services de détection

Gravité : Moyenne

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-ecs-protection-runtime-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'agent de sécurité GuardDuty automatique Amazon est activé pour la surveillance de l'exécution des clusters Amazon ECS surAWS Fargate. Pour un compte autonome, le contrôle échoue si l'agent de sécurité est désactivé pour le compte. Dans un environnement multi-comptes, le contrôle échoue si l'agent de sécurité est désactivé pour le compte d' GuardDutyadministrateur délégué et pour tous les comptes de membres.

Dans un environnement multi-comptes, ce contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. Cela est dû au fait que seul l' GuardDuty administrateur délégué peut activer ou désactiver la surveillance du temps d'exécution des ECS-Fargate ressources pour les comptes de son organisation. GuardDuty les comptes membres ne peuvent pas le faire pour leurs propres comptes. En outre, ce contrôle génère des `FAILED` résultats s'il GuardDuty est suspendu pour un compte membre et si la surveillance du temps d'exécution des ECS-Fargate ressources est désactivée pour le compte membre. Pour recevoir une `PASSED` constatation, l' GuardDuty administrateur doit dissocier le compte du membre suspendu de son compte administrateur en utilisant GuardDuty.

GuardDuty Runtime Monitoring observe et analyse les événements au niveau du système d'exploitation, du réseau et des fichiers pour vous aider à détecter les menaces potentielles dans des AWS charges de travail spécifiques de votre environnement. Il utilise des agents GuardDuty de sécurité qui ajoutent de la visibilité sur le comportement d'exécution, tels que l'accès aux fichiers, l'exécution des processus, les arguments de ligne de commande et les connexions réseau. Vous pouvez activer et gérer l'agent de sécurité pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces potentielles. Cela inclut les clusters Amazon ECS surAWS Fargate.

Correction

Pour activer et gérer l'agent de sécurité pour la surveillance du temps GuardDuty d'exécution ECS-Fargate des ressources, vous devez utiliser GuardDuty directement. Vous ne pouvez pas l'activer ou le gérer manuellement pour les ECS-Fargate ressources. Pour plus d'informations sur l'activation et la gestion de l'agent de sécurité, consultez les sections Conditions requises pour le support AWS Fargate (Amazon ECS uniquement) et Gestion de l'agent de sécurité automatisé pour AWS Fargate (Amazon ECS uniquement) dans le guide de l' GuardDuty utilisateur Amazon.

[GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée

Catégorie : Détecter > Services de détection

Gravité : Moyenne

Type de ressource : `AWS::GuardDuty::Detector`

Règle AWS Config : guardduty-ec2-protection-runtime-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'agent de sécurité GuardDuty automatique Amazon est activé pour la surveillance de l'exécution des instances Amazon EC2. Pour un compte autonome, le contrôle échoue si l'agent de sécurité est désactivé pour le compte. Dans un environnement multi-comptes, le contrôle échoue si l'agent de sécurité est désactivé pour le compte d' GuardDuty administrateur délégué et pour tous les comptes de membres.

Dans un environnement multi-comptes, ce contrôle génère des résultats uniquement dans le compte d' GuardDuty administrateur délégué. En effet, seul l' GuardDuty administrateur délégué peut activer ou désactiver la surveillance du temps d'exécution des instances Amazon EC2 pour les comptes de son organisation. GuardDuty les comptes membres ne peuvent pas le faire pour leurs propres comptes. En outre, ce contrôle génère des `FAILED` résultats s'il GuardDuty est suspendu pour un compte membre et si la surveillance du temps d'exécution des instances EC2 est désactivée pour le compte membre. Pour recevoir une `PASSED` constatation, l' GuardDuty administrateur doit dissocier le compte du membre suspendu de son compte administrateur en utilisant GuardDuty.

GuardDuty Runtime Monitoring observe et analyse les événements au niveau du système d'exploitation, du réseau et des fichiers pour vous aider à détecter les menaces potentielles dans des AWS charges de travail spécifiques de votre environnement. Il utilise des agents GuardDuty de sécurité qui ajoutent de la visibilité sur le comportement d'exécution, tels que l'accès aux fichiers, l'exécution des processus, les arguments de ligne de commande et les connexions réseau. Vous pouvez activer et gérer l'agent de sécurité pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces potentielles. Cela inclut les instances Amazon EC2.

Correction

Pour plus d'informations sur la configuration et la gestion de l'agent de sécurité automatique pour la surveillance du temps GuardDuty d'exécution des instances EC2, consultez les sections Conditions

préalables à la prise en charge des instances Amazon EC2 et Activation de l'agent de sécurité automatique pour les instances Amazon EC2 dans le guide de l'utilisateur Amazon. GuardDuty

Security Hub CSPM contrôle pourGestion des identités et des accès AWS

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Gestion des identités et des accès AWS (IAM). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/12.2, CIS AWS Foundations Benchmark v1.4. 0/1.16 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, (10) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.4, PCI DSS version 3.2. 1/7.2.1

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Élevée

Type de ressource : `AWS::IAM::Policy`

Règle AWS Config : `iam-policy-no-statements-with-admin-access`

Type de calendrier : changement déclenché

Paramètres :

- `excludePermissionBoundaryPolicy: true`(non personnalisable)

Ce contrôle vérifie si la version par défaut des politiques IAM (également appelées politiques gérées par le client) dispose d'un accès administrateur en incluant une instruction `"Effect": "Allow"` avec `"Action": "*"` over`"Resource": "*"`. Le contrôle échoue si vous disposez de politiques IAM comportant une telle déclaration.

Le contrôle vérifie uniquement les stratégies gérées par le client que vous créez. Il ne vérifie pas les politiques intégrées et AWS gérées.

Les politiques IAM définissent un ensemble de privilèges accordés aux utilisateurs, aux groupes ou aux rôles. Conformément aux conseils de sécurité standard, il est AWS recommandé d'accorder le moindre privilège, c'est-à-dire de n'accorder que les autorisations nécessaires à l'exécution d'une

tâche. Si vous accordez des privilèges d'administrateur complets plutôt qu'un jeu d'autorisations minimal dont l'utilisateur a besoin, les ressources risquent d'être exposées à des actions potentiellement indésirables.

Déterminez quelles tâches doivent accomplir les utilisateurs, puis créez des stratégies pour permettre à ces derniers de réaliser uniquement ces tâches, plutôt que de leur accorder des privilèges d'administrateur complets. Il est plus sûr de commencer avec un minimum d'autorisations et d'en accordez d'autres si nécessaire. Ne commencez pas avec des autorisations trop permissives, pour essayer de les restreindre plus tard.

Vous devez supprimer les politiques IAM comportant une instruction `"Effect": "Allow"` avec `"Action": "*"` over`"Resource": "*"`.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Pour modifier vos politiques IAM afin qu'elles n'accordent pas tous les privilèges administratifs « * », consultez la section Modification des politiques IAM dans le Guide de l'utilisateur IAM.

[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.4, CIS AWS Foundations Benchmark v3.0. 0/11.5, CIS AWS Foundations Benchmark v1.2. 0/1.16 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-6, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.9, 3.13.3, PCI DSS version NIST.800-171.r2 3.2. 1/7.2.1

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Faible

Type de ressource : `AWS::IAM::User`

Règle AWS Config : `iam-user-no-policies-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si des politiques sont associées à vos utilisateurs IAM. Le contrôle échoue si des politiques sont associées à vos utilisateurs IAM. Les utilisateurs IAM doivent plutôt hériter des autorisations des groupes IAM ou assumer un rôle.

Par défaut, les utilisateurs, les groupes et les rôles IAM n'ont aucun accès aux AWS ressources. Les politiques IAM accordent des privilèges aux utilisateurs, aux groupes ou aux rôles. Nous vous recommandons d'appliquer les politiques IAM directement aux groupes et aux rôles, mais pas aux utilisateurs. L'attribution de privilèges au niveau du groupe ou du rôle réduit la complexité de la gestion des accès au fur et à mesure que le nombre d'utilisateurs augmente. La simplification de la gestion des accès peut contribuer à réduire les chances pour un mandataire de recevoir ou de conserver par inadvertance des privilèges excessifs.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous n'enregistrez que les ressources mondiales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez les ressources mondiales.

Correction

Pour résoudre ce problème, créez un groupe IAM et associez la politique au groupe. Ajoutez ensuite les utilisateurs au groupe. La stratégie est appliquée à chaque utilisateur du groupe. Pour supprimer une politique directement attachée à un utilisateur, consultez la section Ajout et suppression d'autorisations d'identité IAM dans le guide de l'utilisateur IAM.

[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.3, CIS AWS Foundations Benchmark v3.0. 0/11.4, CIS AWS Foundations Benchmark v1.4. 0/11.4, CIS AWS Foundations Benchmark v1.2. 0/14, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15), PCI DSS version 4.0. 1/83.3.9, PCI DSS v4.0. 1/8.6.3

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::IAM::User`

Règle AWS Config : `access-keys-rotated`

Type de calendrier : Périodique

Paramètres :

- `maxAccessKeyAge`: `90` (non personnalisable)

Ce contrôle vérifie si les clés d'accès actives font l'objet d'une rotation dans un délai de 90 jours.

Nous vous recommandons vivement de ne pas générer et de supprimer toutes les clés d'accès de votre compte. La meilleure pratique recommandée consiste plutôt à créer un ou plusieurs rôles IAM ou à utiliser la fédération par le biais AWS IAM Identity Center de la fédération. Vous pouvez utiliser ces méthodes pour permettre à vos utilisateurs d'accéder au Console de gestion AWS etAWS CLI.

Chaque approche a ses cas d'utilisation. La fédération est généralement préférable pour les entreprises qui disposent d'un annuaire central existant ou qui prévoient d'avoir besoin d'une quantité supérieure à la limite actuelle d'utilisateurs IAM. Les applications qui s'exécutent en dehors d'un AWS environnement ont besoin de clés d'accès pour accéder aux AWS ressources par programmation.

Toutefois, si les ressources nécessitant un accès programmatique s'exécutent à l'intérieurAWS, la meilleure pratique consiste à utiliser des rôles IAM. Les rôles vous permettent d'accorder un accès à une ressource sans coder en dur un ID de clé d'accès et une clé d'accès secrète dans la configuration.

Pour en savoir plus sur la protection de vos clés d'accès et de votre compte, consultez la section Meilleures pratiques de gestion des clés AWS d'accès dans le Références générales AWS. Consultez également le billet de blog Directives pour vous protéger Compte AWS lors de l'utilisation de l'accès programmatique.

Si vous possédez déjà une clé d'accès, Security Hub CSPM vous recommande de changer les clés d'accès tous les 90 jours. La rotation des clés d'accès permet de réduire les possibilités qu'une clé d'accès associée à un compte compromis ou résilié ne soit utilisée. Elle permet également de s'assurer qu'il n'est pas possible d'accéder aux données avec une ancienne clé qui peut avoir été

perdue, compromise ou volée. Mettez toujours à jour vos applications après avoir exécuté la rotation des clés d'accès.

Les clés d'accès sont constituées d'un ID de clé d'accès et une clé d'accès secrète. Ils sont utilisés pour signer les demandes programmatiques que vous envoyez àAWS. Les utilisateurs ont besoin de leurs propres clés d'accès pour effectuer des appels programmatiques AWS depuis les AWS CLI outils pour Windows PowerShell, les AWS SDK, ou des appels HTTP directs à l'aide des opérations d'API individuelles. Services AWS

Si votre organisation utilise AWS IAM Identity Center (IAM Identity Center), vos utilisateurs peuvent se connecter à Active Directory, à un annuaire IAM Identity Center intégré ou à un autre fournisseur d'identité (IdP) connecté à IAM Identity Center. Ils peuvent ensuite être mappés à un rôle IAM qui leur permet d'exécuter des AWS CLI commandes ou d'appeler des opérations d'AWSAPI sans avoir besoin de clés d'accès. Pour en savoir plus, consultez la section Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Pour effectuer une rotation des clés d'accès datant de plus de 90 jours, consultez la section Rotation des clés d'accès dans le guide de l'utilisateur d'IAM. Suivez les instructions pour tout utilisateur dont l'âge de la clé d'accès est supérieur à 90 jours.

[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/1.3, CIS AWS Foundations Benchmark v3.0. 0/1.4, CIS AWS Foundations Benchmark v1.4. 0/1.4, CIS AWS Foundations Benchmark v1.2. 0/11.2, PCI DSS version 3.2. 1/21.1, PCI DSS version 3.2. 1/22., PCI DSS version 3.2. 1/72.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Critique

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-root-access-key-check`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la clé d'accès de l'utilisateur root est présente.

L'utilisateur root est l'utilisateur le plus privilégié d'unCompte AWS. AWSles clés d'accès fournissent un accès programmatique à un compte donné.

Security Hub CSPM recommande de supprimer toutes les clés d'accès associées à l'utilisateur root. Cela limite les vecteurs qui peuvent être utilisés pour compromettre votre compte. Cela incite également à créer et à utiliser comptes basés sur des rôles avec moins de privilèges.

Correction

Pour supprimer la clé d'accès de l'utilisateur root, consultez la section Suppression des clés d'accès de l'utilisateur root dans le guide de l'utilisateur IAM. Pour supprimer les clés d'accès utilisateur root d'une entrée Compte AWSAWS GovCloud (US), voir Supprimer les clés d'accès utilisateur root de mon AWS GovCloud (US) compte dans le guide de AWS GovCloud (US) l'utilisateur.

[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.9, CIS AWS Foundations Benchmark v3.0. 0/1.10, CIS AWS Foundations Benchmark v1.4. 0/1.10, CIS AWS Foundations Benchmark v1.2. 0/12., NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8), PCI DSS version 4.0. 1/8.4.2

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::IAM::User`

Règle AWS Config : `mfa-enabled-for-iam-console-access`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'authentification AWS multifactorielle (MFA) est activée pour tous les utilisateurs IAM qui utilisent un mot de passe de console.

Multi-factor l'authentification (MFA) ajoute une couche de protection supplémentaire en plus du nom d'utilisateur et du mot de passe. Lorsque la MFA est activée, lorsqu'un utilisateur se connecte à un AWS site Web, il est invité à saisir son nom d'utilisateur et son mot de passe. En outre, ils sont invités à saisir un code d'authentification depuis leur dispositif AWS MFA.

Nous vous recommandons d'activer l'authentification MFA pour tous les comptes disposant d'un mot de passe de console. L'authentification MFA est conçue pour fournir une sécurité accrue pour l'accès à la console. Le mandataire d'authentification doit posséder un dispositif qui émet une clé sensible au temps et connaître des informations d'identification.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Pour ajouter une authentification MFA pour les utilisateurs IAM, consultez la section Utilisation de l'authentification multifactorielle (MFA) dans AWS le guide de l'utilisateur IAM.

[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/1.5, CIS AWS Foundations Benchmark v3.0. 0/12.6, CIS AWS Foundations Benchmark v1.4. 0/1.6, CIS AWS Foundations Benchmark v1.2. 0/11.4, PCI DSS version 3.2. 1/83.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8), PCI DSS version 4.0. 1/8.4.2

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Critique

Type de ressource : `AWS::::Account`

Règle AWS Config : `root-account-hardware-mfa-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si vous Compte AWS êtes autorisé à utiliser un dispositif d'authentification matérielle multifactorielle (MFA) pour vous connecter avec les informations d'identification de l'utilisateur root. Le contrôle échoue si le MFA matériel n'est pas activé ou si les périphériques MFA virtuels sont autorisés à se connecter avec les informations d'identification de l'utilisateur root.

Un appareil MFA virtuel peut ne pas fournir le même niveau de sécurité qu'un appareil MFA matériel. Nous vous recommandons d'utiliser un périphérique MFA virtuel uniquement pendant que vous attendez l'approbation de l'achat du matériel ou l'arrivée de votre matériel. Pour en savoir plus, consultez la section Attribuer un périphérique MFA virtuel (console) dans le guide de l'utilisateur IAM.

> **Note**
>
> Security Hub CSPM évalue ce contrôle en fonction de la présence des informations d'identification de l'utilisateur root (profil de connexion) dans un. Compte AWS Le contrôle génère `PASSED` des résultats dans les cas suivants :
>
> - Les informations d'identification de l'utilisateur root sont présentes dans le compte et le MFA matériel est activé pour l'utilisateur root.
> - Les informations d'identification de l'utilisateur root ne sont pas présentes dans le compte.
>
> Le contrôle permet de déterminer si `FAILED` les informations d'identification de l'utilisateur root sont présentes dans le compte et si le MFA matériel n'est pas activé pour l'utilisateur root.

Correction

Pour plus d'informations sur l'activation de l'authentification MFA matérielle pour l'utilisateur root, consultez la section Multi-factor Authentification for an Utilisateur racine d'un compte AWS dans le guide de l'utilisateur IAM.

[IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes

Exigences associées : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-5 (1), NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/83.3.7, PCI DSS v4.0. 1/83.3.9, PCI DSS v4.0. 1/83.10.1, PCI DSS v4.0. 1/8.6.3

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`RequireUppercaseCharacters`	Exiger au moins une majuscule dans le mot de passe	Booléen	`true` ou `false`	`true`
`RequireLowercaseCharacters`	Exiger au moins une minuscule dans le mot de passe	Booléen	`true` ou `false`	`true`
`RequireSymbols`	Exiger au moins un symbole dans le mot de passe	Booléen	`true` ou `false`	`true`
`RequireNumbers`	Exiger au moins un chiffre dans le mot de passe	Booléen	`true` ou `false`	`true`

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`MinimumPasswordLength`	Nombre minimum de caractères dans le mot de passe	Entier	8 sur 128	8
`PasswordReusePrevention`	Nombre de rotations de mots de passe avant qu'un ancien mot de passe puisse être réutilisé	Entier	12 sur 24	Aucune valeur par défaut
`MaxPasswordAge`	Nombre de jours avant l'expiration du mot de passe	Entier	1 sur 90	Aucune valeur par défaut

Ce contrôle vérifie si la politique de mot de passe du compte pour les utilisateurs IAM utilise des configurations strictes. Le contrôle échoue si la politique de mot de passe n'utilise pas de configurations fortes. À moins que vous ne fournissiez des valeurs de paramètres personnalisées, Security Hub CSPM utilise les valeurs par défaut mentionnées dans le tableau précédent. Les `MaxPasswordAge` paramètres `PasswordReusePrevention` et n'ont aucune valeur par défaut. Par conséquent, si vous excluez ces paramètres, Security Hub CSPM ignore le nombre de rotations de mots de passe et l'âge des mots de passe lors de l'évaluation de ce contrôle.

Pour y accéderConsole de gestion AWS, les utilisateurs d'IAM ont besoin de mots de passe. À titre de bonne pratique, Security Hub CSPM recommande vivement d'utiliser la fédération au lieu de créer des utilisateurs IAM. La fédération permet aux utilisateurs d'utiliser leurs informations d'identification d'entreprise existantes pour se connecter auConsole de gestion AWS. Utilisez AWS IAM Identity Center (IAM Identity Center) pour créer ou fédérer l'utilisateur, puis assumez un rôle IAM dans un compte.

Pour en savoir plus sur les fournisseurs d'identité et la fédération, consultez la section Fournisseurs d'identité et fédération dans le guide de l'utilisateur IAM. Pour en savoir plus sur IAM Identity Center, consultez le guide de l'AWS IAM Identity Centerutilisateur.

Si vous devez utiliser des utilisateurs IAM, Security Hub CSPM vous recommande d'imposer la création de mots de passe utilisateur forts. Vous pouvez définir une politique de mot de passe Compte AWS pour définir les exigences de complexité et les périodes de rotation obligatoires pour les mots de passe. Lorsque vous créez ou modifiez une politique de mot de passe, la plupart des paramètres de la politique de mot de passe sont appliqués la prochaine fois que les utilisateurs modifient leur mot de passe. Certains paramètres sont appliqués immédiatement.

Correction

Pour mettre à jour votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur d'IAM.

[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/13 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-6, PCI DSS version 3.2. 1/81.1.4, PCI DSS v4.0. 1/8.2.6

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::IAM::User`

Règle AWS Config : `iam-user-unused-credentials-check`

Type de calendrier : Périodique

Paramètres :

- `maxCredentialUsageAge`: `90` (non personnalisable)

Ce contrôle vérifie si vos utilisateurs IAM ont des mots de passe ou des clés d'accès actives qui n'ont pas été utilisés depuis 90 jours.

Les utilisateurs IAM peuvent accéder aux AWS ressources à l'aide de différents types d'informations d'identification, tels que des mots de passe ou des clés d'accès.

Security Hub CSPM vous recommande de supprimer ou de désactiver toutes les informations d'identification non utilisées pendant 90 jours ou plus. La désactivation ou la suppression des

informations d'identification inutiles permet d'éviter que des informations d'identification associées à un compte compromis ou abandonné ne soient utilisées.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Lorsque vous consultez les informations utilisateur dans la console IAM, des colonnes indiquent l'âge de la clé d'accès, l'âge du mot de passe et la dernière activité. Si la valeur dans l'une de ces colonnes est supérieure à 90 jours, rendez inactives les informations d'identification de ces utilisateurs.

Vous pouvez également utiliser les rapports d'identification pour surveiller les utilisateurs et identifier ceux qui sont restés inactifs pendant 90 jours ou plus. Vous pouvez télécharger les rapports d'identification au `.csv` format depuis la console IAM.

Après avoir identifié les comptes inactifs ou les informations d'identification non utilisées, désactivez-les. Pour obtenir des instructions, consultez la section Création, modification ou suppression d'un mot de passe utilisateur IAM (console) dans le guide de l'utilisateur IAM.

[IAM.9] La MFA doit être activée pour l'utilisateur root

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/14, PCI DSS version 3.2. 1/83.3.1, PCI DSS v4.0. 1/84.4.2, CIS AWS Foundations Benchmark v3.0. 0/1.5, CIS AWS Foundations Benchmark v1.4. 0/1.5, CIS AWS Foundations Benchmark v1.2. 0/1,13, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Critique

Type de ressource : `AWS::::Account`

Règle AWS Config : `root-account-mfa-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'authentification multifactorielle (MFA) est activée pour que l'utilisateur root IAM puisse Compte AWS se connecter à. Console de gestion AWS Le contrôle échoue si le MFA n'est pas activé pour l'utilisateur root du compte.

L'utilisateur root IAM d'un Compte AWS a un accès complet à tous les services et ressources du compte. Si le MFA est activé, l'utilisateur doit saisir un nom d'utilisateur, un mot de passe et un code d'authentification depuis son appareil AWS MFA afin de se connecter au. Console de gestion AWS La MFA ajoute une couche de protection supplémentaire en plus d'un nom d'utilisateur et d'un mot de passe.

Ce contrôle génère `PASSED` des résultats dans les cas suivants :

- Les informations d'identification de l'utilisateur root sont présentes dans le compte et le MFA est activé pour l'utilisateur root.
- Les informations d'identification de l'utilisateur root ne sont pas présentes dans le compte.

Le contrôle génère des `FAILED` résultats si les informations d'identification de l'utilisateur root sont présentes dans le compte et si le MFA n'est pas activé pour l'utilisateur root.

Correction

Pour plus d'informations sur l'activation de l'authentification MFA pour l'utilisateur root d'unCompte AWS, reportez-vous à la section Multi-factor Authentification correspondante Utilisateur racine d'un compte AWS dans le guide de l'Gestion des identités et des accès AWSutilisateur.

[IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes

Exigences associées : NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v3.2. 1/81.1.4, PCI DSS v3.2. 1/82.2.3, PCI DSS v3.2. 1/82.2.4, PCI DSS v3.2. 1/8.2.5

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS:::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la politique de mot de passe du compte pour les utilisateurs IAM utilise les configurations PCI DSS minimales suivantes.

- `RequireUppercaseCharacters`— Exige au moins une majuscule dans le mot de passe. (Valeur par défaut = `true`)
- `RequireLowercaseCharacters`— Exige au moins une minuscule dans le mot de passe. (Valeur par défaut = `true`)
- `RequireNumbers`— Exige au moins un chiffre dans le mot de passe. (Valeur par défaut = `true`)
- `MinimumPasswordLength`— Longueur minimale du mot de passe. (Par défaut = 7 ou plus)
- `PasswordReusePrevention`— Nombre de mots de passe avant d'autoriser leur réutilisation. (Par défaut = 4)
- `MaxPasswordAge`— Nombre de jours avant l'expiration du mot de passe. (Par défaut = 90)

> **Note**
>
> Le 30 mai 2025, Security Hub CSPM a supprimé ce contrôle de la norme PCI DSS v4.0.1. La norme PCI DSS v4.0.1 exige désormais que les mots de passe comportent au moins 8 caractères. Ce contrôle continue de s'appliquer à la norme PCI DSS v3.2.1, qui impose des exigences différentes en matière de mot de passe.
> Pour évaluer les politiques de mot de passe du compte par rapport aux exigences de la norme PCI DSS v4.0.1, vous pouvez utiliser le contrôle. IAM.7 Ce contrôle nécessite que les mots de passe comportent au moins 8 caractères. Il prend également en charge les valeurs personnalisées pour la longueur du mot de passe et d'autres paramètres. Le IAM.7 contrôle fait partie de la norme PCI DSS v4.0.1 du Security Hub CSPM.

Correction

Pour mettre à jour votre politique de mot de passe afin d'utiliser la configuration recommandée, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

[IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/12.5, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/8.6.3

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Les stratégies de mot de passe, en partie, font appliquer les exigences de complexité des mots de passe. Utilisez les politiques de mot de passe IAM pour vous assurer que les mots de passe utilisent des jeux de caractères différents.

Le CIS recommande que la politique de mot de passe exige au moins une lettre majuscule. La définition d'une stratégie de complexité des mots de passe accroît la résilience des comptes en cas de tentatives de connexion en force.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour la sécurité du mot de passe, sélectionnez Exiger au moins une lettre majuscule de l'alphabet latin (A—Z).

[IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/12.6, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/8.6.3

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Les stratégies de mot de passe, en partie, font appliquer les exigences de complexité des mots de passe. Utilisez les politiques de mot de passe IAM pour vous assurer que les mots de passe utilisent des jeux de caractères différents. Le CIS recommande que la politique de mot de passe exige au moins une lettre minuscule. La définition d'une stratégie de complexité des mots de passe accroît la résilience des comptes en cas de tentatives de connexion en force.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour renforcer le mot de passe, sélectionnez Exiger au moins une lettre minuscule de l'alphabet latin (A—Z).

[IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/1.7, 3.5.7 NIST.800-171.r2

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Les stratégies de mot de passe, en partie, font appliquer les exigences de complexité des mots de passe. Utilisez les politiques de mot de passe IAM pour vous assurer que les mots de passe utilisent des jeux de caractères différents.

Le CIS recommande que la politique de mot de passe exige au moins un symbole. La définition d'une stratégie de complexité des mots de passe accroît la résilience des comptes en cas de tentatives de connexion en force.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour la sécurité du mot de passe, sélectionnez Exiger au moins un caractère non alphanumérique.

[IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/1.8, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/8.6.3

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Les stratégies de mot de passe, en partie, font appliquer les exigences de complexité des mots de passe. Utilisez les politiques de mot de passe IAM pour vous assurer que les mots de passe utilisent des jeux de caractères différents.

Le CIS recommande que la politique de mot de passe exige au moins un chiffre. La définition d'une stratégie de complexité des mots de passe accroît la résilience des comptes en cas de tentatives de connexion en force.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour la sécurité du mot de passe, sélectionnez Exiger au moins un chiffre.

[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/12.7, CIS AWS Foundations Benchmark v3.0. 0/11.8, CIS AWS Foundations Benchmark v1.4. 0/1.8, CIS AWS Foundations Benchmark v1.2. 0/11.9, 3.5.7 NIST.800-171.r2

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Les stratégies de mot de passe, en partie, font appliquer les exigences de complexité des mots de passe. Utilisez les politiques de mot de passe IAM pour vous assurer que les mots de passe ont au moins une longueur donnée.

Le CIS recommande que la politique de mot de passe exige une longueur minimale de 14 caractères. La définition d'une stratégie de complexité des mots de passe accroît la résilience des comptes en cas de tentatives de connexion en force.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour la longueur minimale du mot de passe, entrez **14** ou un nombre supérieur.

[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.8, CIS AWS Foundations Benchmark v3.0. 0/11.9, CIS AWS Foundations Benchmark v1.4. 0/11.9, CIS AWS Foundations Benchmark v1.2. 0/11.0, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/8.3.7

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Faible

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le nombre de mots de passe à mémoriser est défini sur 24. Le contrôle échoue si la valeur n'est pas 24.

Les politiques de mot de passe IAM peuvent empêcher la réutilisation d'un mot de passe donné par le même utilisateur.

Le CIS recommande que la politique en matière de mots de passe empêche la réutilisation des mots de passe. Le fait d'empêcher la réutilisation des mots de passe accroît la résilience d'un compte en cas de tentatives de connexion en force.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour Empêcher la réutilisation du mot de passe, entrez**24**.

[IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/11.1, PCI DSS v4.0. 1/83.3.9, PCI DSS v4.0. 1/83.10.1

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Faible

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-password-policy`

Type de calendrier : Périodique

Paramètres : Aucun

Les politiques de mot de passe IAM peuvent exiger la rotation ou l'expiration des mots de passe après un certain nombre de jours.

Le CIS recommande que la politique en matière de mots de passe fasse expirer les mots de passe après 90 jours ou moins. Le fait de réduire la durée de vie des mots de passe accroît la résilience d'un compte en cas de tentatives de connexion en force. Il s'avère également utile d'avoir à changer régulièrement de mot de passe dans les cas suivants :

- Les mots de passe peuvent être volés ou compromis à votre insu. Cela peut se produire si un système est compromis, si un logiciel est vulnérable ou par le biais d'une menace interne.

- Certains filtres web ou serveurs proxy d'entreprise et d'administrations peuvent intercepter et enregistrer le trafic, même s'il est chiffré.
- De nombreuses personnes utilisent le même mot de passe pour plusieurs systèmes (ordinateurs au bureau et à domicile, messagerie électronique, etc.).
- Un enregistreur de frappe peut être installé sur les postes de travail des utilisateurs finaux compromis.

Correction

Pour modifier votre politique de mot de passe, consultez la section Définition d'une politique de mot de passe de compte pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Pour Activer l'expiration du mot de passe, entrez **`90`** ou un nombre inférieur.

[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.6, CIS AWS Foundations Benchmark v3.0. 0/11.7, CIS AWS Foundations Benchmark v1.4. 0/11.7, CIS AWS Foundations Benchmark v1.2. 0/12.0, NIST.800-171.r2 3.1.2, PCI DSS v4.0. 1/12.10.3

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Faible

Type de ressource : `AWS::::Account`

Règle AWS Config : `iam-policy-in-use`

Type de calendrier : Périodique

Paramètres :

- `policyARN`: `arn:`*`partition`*`:iam::aws:policy/AWSSupportAccess` (non personnalisable)
- `policyUsageType`: `ANY` (non personnalisable)

AWSfournit un centre de support qui peut être utilisé pour la notification et la réponse aux incidents, ainsi que pour le support technique et le service client.

Créez un rôle IAM pour permettre aux utilisateurs autorisés de gérer les incidents avec AWS Support. En mettant en œuvre le moindre privilège pour le contrôle d'accès, un rôle IAM nécessitera une

politique IAM appropriée pour autoriser l'accès au centre de support afin de gérer les incidents avec. Support

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Pour résoudre ce problème, créez un rôle permettant aux utilisateurs autorisés de gérer les Support incidents.

Pour créer le rôle à utiliser pourSupportaccès

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation IAM, choisissez Roles, puis Create role.
3. Pour Type de rôle, choisissez Autre Compte AWS.
4. Dans le champ Compte AWS ID de compte, entrez l'identifiant Compte AWS auquel vous souhaitez accorder l'accès à vos ressources.

   Si les utilisateurs ou les groupes qui assument ce rôle se trouvent dans le même compte, entrez le numéro de compte local.

   > **Note**
   >
   > L'administrateur du compte spécifié peut accorder l'autorisation d'assumer ce rôle à n'importe quel utilisateur de ce compte. Pour ce faire, l'administrateur attache une politique à l'utilisateur ou à un groupe qui donne l'autorisation pour l'action `sts:AssumeRole`. Dans cette stratégie, la ressource doit être l'ARN du rôle.

5. Choisissez Suivant : Autorisations.
6. Recherchez la stratégie gérée `AWSSupportAccess`.
7. Activez la case à cocher de la stratégie `AWSSupportAccess` gérée.

8. Choisissez Suivant : Balises.
9. (Facultatif) Pour ajouter des métadonnées au rôle, associez des balises sous forme de paires clé-valeur.

   Pour plus d'informations sur l'utilisation des balises dans IAM, consultez Balisage des utilisateurs et des rôles IAM dans le Guide de l'utilisateur IAM.
10. Choisissez Suivant : Vérification.
11. Dans le champ Role name (Nom de rôle), saisissez un nom pour votre rôle.

    Les noms de rôles doivent être uniques au sein de votreCompte AWS. Elles ne sont pas sensibles à la casse.
12. (Facultatif) Dans le champ Description du rôle, saisissez la description du nouveau rôle.
13. Passez en revue les informations du rôle, puis choisissez Create role (Créer un rôle).

[IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM

Exigences associées : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.5.3, NIST.800-171.r2 3.5.4, NIST.800-171.r2 3.7.5, PCI DSS v3.2. 1/83.3.1, PCI DSS v4.0. 1/8.4.2,

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::IAM::User`

Règle AWS Config : `iam-user-mfa-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'authentification multifactorielle (MFA) est activée pour les utilisateurs IAM.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région,

vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Pour ajouter l'authentification MFA pour les utilisateurs IAM, consultez la section Activation des appareils MFA pour les utilisateurs AWS dans le guide de l'utilisateur IAM.

[IAM.20] Évitez d'utiliser l'utilisateur root

Important

Security Hub CSPM a retiré ce contrôle en avril 2024. Pour de plus amples informations, veuillez consulter Journal des modifications pour les contrôles CSPM de Security Hub.

Exigences associées : CIS AWS Foundations Benchmark v1.2. 0/11.

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Faible

Type de ressource : `AWS::IAM::User`

AWS Configrègle : `use-of-root-account-test` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un utilisateur root Compte AWS est soumis à des restrictions d'utilisation. Le contrôle évalue les ressources suivantes :

- Rubriques Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrailsentiers
- Filtres métriques associés aux CloudTrail sentiers
- CloudWatch Alarmes Amazon basées sur les filtres

Cette vérification permet de `FAILED` déterminer si une ou plusieurs des affirmations suivantes sont vraies :

- Aucune CloudTrail trace n'existe dans le compte.
- Un suivi CloudTrail est activé, mais il n'est pas configuré avec au moins un suivi multirégional incluant des événements de gestion de lecture et d'écriture.
- Un suivi CloudTrail est activé, mais il n'est pas associé à un groupe de CloudWatch journaux Logs.
- Le filtre métrique exact prescrit par le Center for Internet Security (CIS) n'est pas utilisé. Le filtre métrique prescrit est `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- Aucune CloudWatch alarme basée sur le filtre métrique n'existe dans le compte.
- CloudWatch les alarmes configurées pour envoyer une notification à la rubrique SNS associée ne se déclenchent pas en fonction de la condition de l'alarme.
- La rubrique SNS n'est pas conforme aux contraintes d'envoi d'un message à une rubrique SNS.
- La rubrique SNS n'a pas au moins un abonné.

Cette vérification donne lieu à un statut de contrôle indiquant `NO_DATA` si une ou plusieurs des affirmations suivantes sont vraies :

- Un sentier multirégional est basé dans une région différente. Security Hub CSPM ne peut générer des résultats que dans la région où le trail est basé.
- Un sentier multirégional appartient à un compte différent. Security Hub CSPM peut uniquement générer des résultats pour le compte propriétaire de la piste.

Cette vérification donne lieu à un statut de contrôle indiquant `WARNING` si une ou plusieurs des affirmations suivantes sont vraies :

- Le compte courant ne possède pas la rubrique SNS référencée dans l' CloudWatch alarme.
- Le compte actuel n'a pas accès à la rubrique SNS lorsqu'il appelle l'API `ListSubscriptionsByTopic` SNS.

> **Note**
>
> Nous vous recommandons d'utiliser les traces d'organisation pour enregistrer les événements provenant de nombreux comptes d'une organisation. Les parcours d'organisation sont des sentiers multirégionaux par défaut et ne peuvent être gérés que par le compte AWS Organizations de gestion ou le compte d'administrateur CloudTrail délégué. L'utilisation

d'un suivi de l'organisation aboutit à un statut de contrôle NO_DATA pour les contrôles évalués dans les comptes des membres de l'organisation. Dans les comptes membres, Security Hub CSPM génère uniquement des résultats pour les ressources appartenant aux membres. Les résultats relatifs aux parcours de l'organisation sont générés dans le compte du propriétaire de la ressource. Vous pouvez consulter ces résultats dans votre compte d'administrateur délégué Security Hub CSPM en utilisant l'agrégation entre régions.

Il est recommandé d'utiliser les informations d'identification de votre utilisateur root uniquement lorsque cela est nécessaire pour effectuer des tâches de gestion des comptes et des services. Appliquez les politiques IAM directement aux groupes et aux rôles, mais pas aux utilisateurs. Pour obtenir des instructions sur la configuration d'un administrateur pour une utilisation quotidienne, consultez la section Création de votre premier utilisateur et de votre premier groupe d'administrateurs IAM dans le guide de l'utilisateur IAM.

Correction

Les étapes pour résoudre ce problème incluent la configuration d'une rubrique Amazon SNS, CloudTrail d'un journal, d'un filtre métrique et d'une alarme pour le filtre métrique.

Pour créer une rubrique Amazon SNS

1. Ouvrez la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Créez une rubrique Amazon SNS qui reçoit toutes les alarmes CIS.

   Créez au moins un abonné à la rubrique. Pour plus d'informations, consultez Prise en main d'Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Ensuite, configurez une option active CloudTrail qui s'applique à toutes les régions. Pour cela, suivez les étapes de correction dans the section called "[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture".

Notez le nom du groupe de CloudWatch journaux Logs que vous associez au CloudTrail parcours. Vous créez le filtre métrique pour ce groupe de journaux.

Enfin, créez le filtre métrique et l'alarme.

Pour créer un filtre de métrique et une alarme

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.

2. Dans le panneau de navigation, choisissez Groupes de journaux.
3. Cochez la case correspondant au groupe de CloudWatch journaux Logs associé au journal CloudTrail que vous avez créé.
4. Dans Actions, choisissez Create Metric Filter.
5. Sous Définir le modèle, procédez comme suit :

   a. Copiez le modèle suivant, puis collez-le dans le champ Modèle de filtre.

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. Choisissez Suivant.
6. Sous Affecter une métrique, procédez comme suit :

   a. Dans Nom du filtre, entrez le nom de votre filtre métrique.

   b. Pour Metric Namespace, entrez**`LogMetrics`**.

      Si vous utilisez le même espace de noms pour tous vos filtres de métriques log CIS, toutes les métriques CIS Benchmark sont regroupées.

   c. Dans Nom de la métrique, entrez le nom de la métrique. N'oubliez pas le nom de la métrique. Vous devrez sélectionner la métrique lorsque vous créerez l'alarme.

   d. Pour Valeur de la métrique, saisissez **1**.

   e. Choisissez Suivant.
7. Sous Vérifier et créer, vérifiez les informations que vous avez fournies pour le nouveau filtre métrique. Choisissez ensuite Créer un filtre métrique.
8. Dans le volet de navigation, choisissez Log groups, puis choisissez le filtre que vous avez créé sous Filtres métriques.
9. Cochez la case correspondant au filtre. Sélectionnez Créer une alerte.
10. Sous Spécifier la métrique et les conditions, procédez comme suit :

    a. Sous Conditions, dans le champ Seuil, sélectionnez Static.

    b. Pour Définir la condition de l'alarme, sélectionnez Greater/Equal.

    c. Pour Définir la valeur de seuil, entrez**1**.

    d. Choisissez Suivant.
11. Sous Configurer les actions, procédez comme suit :

a. Sous Déclencheur d'état d'alarme, choisissez En alarme.
b. Sous Select an SNS topic (Sélectionner une rubrique SNS), choisissez Select an existing SNS topic (Sélectionner une rubrique SNS existante).
c. Pour Envoyer une notification à, entrez le nom de la rubrique SNS que vous avez créée lors de la procédure précédente.
d. Choisissez Suivant.

12. Sous Ajouter un nom et une description, entrez un nom et une description pour l'alarme, tels que**`CIS-1.1-RootAccountUsage`**. Ensuite, sélectionnez Suivant.
13. Sous Aperçu et création, passez en revue la configuration de l'alarme. Ensuite, choisissez Créer une alarme.

[IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services

Exigences connexes : NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7),,, NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.1, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.5, NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.8, 3.3.9, 3.13.3, 3.13.4 NIST.800-171.r2 NIST.800-171.r2 NIST.800-171.r2

Catégorie : Détecter > Gestion des accès sécurisés

Gravité : Faible

Type de ressource : `AWS::IAM::Policy`

Règle AWS Config : `iam-policy-no-statements-with-full-access`

Type de calendrier : changement déclenché

Paramètres :

- `excludePermissionBoundaryPolicy`: `True` (non personnalisable)

Ce contrôle vérifie si les politiques basées sur l'identité IAM que vous créez comportent des instructions Allow qui utilisent le caractère générique* pour accorder des autorisations pour toutes les actions sur n'importe quel service. Le contrôle échoue si une déclaration de politique inclut la mention « `"Effect": "Allow"` with `"Action": "Service:*"` ».

Par exemple, l'instruction suivante dans une politique entraîne un échec de recherche.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

Le contrôle échoue également si vous utilisez `"Effect": "Allow"` avec`"NotAction": "service:*"`. Dans ce cas, l'`NotAction`élément donne accès à toutes les actions d'unService AWS, à l'exception des actions spécifiées dans`NotAction`.

Ce contrôle s'applique uniquement aux politiques IAM gérées par le client. Elle ne s'applique pas aux politiques IAM gérées parAWS.

Lorsque vous attribuez des autorisations àServices AWS, il est important de définir les actions IAM autorisées dans vos politiques IAM. Vous devez limiter les actions IAM aux seules actions nécessaires. Cela vous permet d'octroyer des autorisations de moindre privilège. Des politiques trop permissives peuvent entraîner une augmentation des privilèges si elles sont associées à un principal IAM qui n'a peut-être pas besoin d'autorisation.

Dans certains cas, vous souhaiterez peut-être autoriser les actions IAM qui ont un préfixe similaire, tel que `DescribeFlowLogs` et. `DescribeAvailabilityZones` Dans ces cas autorisés, vous pouvez ajouter un caractère générique suffixé au préfixe commun. Par exemple, `ec2:Describe*`.

Ce contrôle passe si vous utilisez une action IAM préfixée avec un caractère générique suffixé. Par exemple, l'instruction suivante figurant dans une politique aboutit à un résultat positif.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

Lorsque vous regroupez les actions IAM associées de cette manière, vous pouvez également éviter de dépasser les limites de taille de la politique IAM.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, l'enregistrement des ressources globales peut être activé dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Pour remédier à ce problème, mettez à jour vos politiques IAM afin qu'elles n'accordent pas de privilèges administratifs « * » complets. Pour plus de détails sur la modification d'une stratégie IAM, consultez la section Modification des politiques IAM dans le Guide de l'utilisateur IAM.

[IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.1, CIS AWS Foundations Benchmark v3.0. 0/1.12, CIS AWS Foundations Benchmark v1.4. 0/1.12, 3.1.2 NIST.800-171.r2

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::IAM::User`

AWS Configrègle : **`iam-user-unused-credentials-check`**

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si vos utilisateurs IAM ont des mots de passe ou des clés d'accès actives qui n'ont pas été utilisés depuis 45 jours ou plus. Pour ce faire, il vérifie si le `maxCredentialUsageAge` paramètre de la AWS Config règle est égal ou supérieur à 45.

Les utilisateurs peuvent accéder aux AWS ressources à l'aide de différents types d'informations d'identification, tels que des mots de passe ou des clés d'accès.

Le CIS vous recommande de supprimer ou de désactiver toutes les informations d'identification non utilisées depuis 45 jours ou plus. La désactivation ou la suppression des informations d'identification

inutiles permet d'éviter que des informations d'identification associées à un compte compromis ou abandonné ne soient utilisées.

La AWS Config règle de ce contrôle utilise les opérations de l'`GenerateCredentialReport`API `GetCredentialReport`et, qui ne sont mises à jour que toutes les quatre heures. Les modifications apportées aux utilisateurs IAM peuvent prendre jusqu'à quatre heures pour être visibles par ce contrôle.

> **Note**
>
> AWS Configdoit être activé dans toutes les régions dans lesquelles vous utilisez Security Hub CSPM. Cependant, vous pouvez activer l'enregistrement des ressources mondiales dans une seule région. Si vous enregistrez uniquement des ressources globales dans une seule région, vous pouvez désactiver ce contrôle dans toutes les régions, à l'exception de la région dans laquelle vous enregistrez des ressources globales.

Correction

Lorsque vous consultez les informations utilisateur dans la console IAM, des colonnes indiquent l'âge de la clé d'accès, l'âge du mot de passe et la dernière activité. Si la valeur de l'une de ces colonnes est supérieure à 45 jours, désactivez les informations d'identification de ces utilisateurs.

Vous pouvez également utiliser les rapports d'identification pour surveiller les utilisateurs et identifier ceux qui sont restés inactifs pendant 45 jours ou plus. Vous pouvez télécharger les rapports d'identification au `.csv` format depuis la console IAM.

Après avoir identifié les comptes inactifs ou les informations d'identification non utilisées, désactivez-les. Pour obtenir des instructions, consultez la section Création, modification ou suppression d'un mot de passe utilisateur IAM (console) dans le guide de l'utilisateur IAM.

[IAM.23] Les analyseurs IAM Access Analyzer doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AccessAnalyzer::Analyzer`

AWS Configrègle : `tagged-accessanalyzer-analyzer` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un analyseur géré par AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si l'analyseur ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'analyseur n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un analyseur, reportez-vous TagResourceà la référence de l'AWSAPI IAM Access Analyzer.

[IAM.24] Les rôles IAM doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IAM::Role`

AWS Configrègle : `tagged-iam-role` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un rôle Gestion des identités et des accès AWS (IAM) possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le rôle ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le rôle n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un rôle IAM, consultez la section Marquage des ressources IAM dans le guide de l'utilisateur IAM.

[IAM.25] Les utilisateurs IAM doivent être tagués

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IAM::User`

AWS Configrègle : `tagged-iam-user` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un utilisateur Gestion des identités et des accès AWS (IAM) possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'utilisateur ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'utilisateur n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un utilisateur IAM, consultez la section Marquage des ressources IAM dans le guide de l'utilisateur IAM.

[IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.8, CIS AWS Foundations Benchmark v3.0. 0/1.19

Catégorie : Identifier > Conformité

Gravité : Moyenne

Type de ressource : `AWS::IAM::ServerCertificate`

AWS Configrègle : **`iam-server-certificate-expiration-check`**

Type de calendrier : Périodique

Paramètres : Aucun

Cela permet de vérifier si un certificat de SSL/TLS serveur actif géré dans IAM a expiré. Le contrôle échoue si le certificat de SSL/TLS serveur expiré n'est pas supprimé.

Pour activer les connexions HTTPS à votre site Web ou à votre applicationAWS, vous avez besoin d'un certificat de SSL/TLS serveur. Vous pouvez utiliser IAM ou AWS Certificate Manager (ACM) pour stocker et déployer des certificats de serveur. Utilisez IAM comme gestionnaire de certificats uniquement lorsque vous devez prendre en charge les connexions HTTPS dans un environnement

Région AWS qui n'est pas pris en charge par ACM. IAM chiffre en toute sécurité vos clés privées et stocke la version chiffrée dans le magasin de certificats SSL IAM. IAM prend en charge le déploiement de certificats de serveur dans toutes les régions, mais vous devez obtenir votre certificat auprès d'un fournisseur externe pour pouvoir l'utiliser avecAWS. Vous ne pouvez pas télécharger de certificat ACM vers IAM. En outre, vous ne pouvez pas gérer vos certificats depuis la console IAM. La suppression SSL/TLS des certificats expirés élimine le risque qu'un certificat non valide soit accidentellement déployé sur une ressource, ce qui peut nuire à la crédibilité de l'application ou du site Web sous-jacent.

Correction

Pour supprimer un certificat de serveur d'IAM, consultez la section Gestion des certificats de serveur dans IAM dans le guide de l'utilisateur d'IAM.

[IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/12.1, CIS AWS Foundations Benchmark v3.0. 0/12.2

Catégorie : Protection > Gestion des accès sécurisés > Politiques IAM sécurisées

Gravité : Moyenne

Type de ressource :`AWS::IAM::Role`,`AWS::IAM::User`, `AWS::IAM::Group`

AWS Configrègle : **`iam-policy-blacklisted-check`**

Type de calendrier : changement déclenché

Paramètres :

- « PolicYarns » : « arn:aws:iam : :aws :, arn:aws-cn:iam : :aws :, arn:aws-us-gov:iam : :aws policy/ AWSCloudShellFullAccess : » policy/AWSCloudShellFullAccess policy/AWSCloudShellFullAccess

Ce contrôle vérifie si la politique AWS gérée est `AWSCloudShellFullAccess` attachée à une identité IAM (utilisateur, rôle ou groupe). Le contrôle échoue si la `AWSCloudShellFullAccess` politique est attachée à une identité IAM.

AWS CloudShellfournit un moyen pratique d'exécuter des commandes CLI surServices AWS. La politique AWS gérée `AWSCloudShellFullAccess` fournit un accès complet à CloudShell, ce qui

permet de charger et de télécharger des fichiers entre le système local de l'utilisateur et l' CloudShell environnement. Dans l' CloudShell environnement, un utilisateur dispose d'autorisations sudo et peut accéder à Internet. Par conséquent, l'association de cette politique gérée à une identité IAM leur permet d'installer un logiciel de transfert de fichiers et de transférer des données CloudShell vers des serveurs Internet externes. Nous vous recommandons de suivre le principe du moindre privilège et d'attribuer des autorisations plus restreintes à vos identités IAM.

Correction

Pour dissocier la `AWSCloudShellFullAccess` politique d'une identité IAM, consultez la section Ajouter et supprimer des autorisations d'identité IAM dans le guide de l'utilisateur IAM.

[IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/11.9, CIS AWS Foundations Benchmark v3.0. 0/1.20

Catégorie : Détecter > Services de détection > Surveillance des utilisations privilégiées

Gravité : Élevée

Type de ressource : `AWS::AccessAnalyzer::Analyzer`

AWS Configrègle : **`iam-external-access-analyzer-enabled`**

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un analyseur Compte AWS d'accès externe IAM Access Analyzer est activé. Le contrôle échoue si aucun analyseur d'accès externe n'est activé sur le compte actuellement sélectionnéRégion AWS.

Les analyseurs d'accès externes IAM Access Analyzer aident à identifier les ressources, telles que les buckets Amazon Simple Storage Service (Amazon S3) ou les rôles IAM, partagées avec une entité externe. Cela vous permet d'éviter tout accès involontaire à vos ressources et à vos données. L'analyseur d'accès IAM est régional et doit être activé dans chaque région. Pour identifier les ressources partagées avec des principaux externes, un analyseur d'accès utilise un raisonnement basé sur la logique pour analyser les politiques basées sur les ressources dans votre environnement. AWS Lorsque vous créez un analyseur d'accès externe, vous pouvez le créer et l'activer pour l'ensemble de votre organisation ou pour des comptes individuels.

> **Note**
>
> Si un compte fait partie d'une organisationAWS Organizations, ce contrôle ne prend pas en compte les analyseurs d'accès externes qui spécifient l'organisation comme zone de confiance et sont activés pour l'organisation de la région actuelle. Si votre organisation utilise ce type de configuration, envisagez de désactiver ce contrôle pour les comptes de membres individuels de votre organisation dans la région.

Correction

Pour plus d'informations sur l'activation d'un analyseur d'accès externe dans une région spécifique, voir Getting started with IAM Access Analyzer dans le guide de l'utilisateur IAM. Vous devez activer un analyseur dans chaque région dans laquelle vous souhaitez contrôler l'accès à vos ressources.

Contrôles CSPM du Security Hub pour Amazon Inspector

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Inspector.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Inspector.1] La numérisation Amazon Inspector EC2 doit être activée

Exigences associées : PCI DSS v4.0 1/11.3.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS:::Account`

Règle AWS Config : `inspector-ec2-scan-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le scan Amazon Inspector EC2 est activé. Pour un compte autonome, le contrôle échoue si le scan Amazon Inspector EC2 est désactivé dans le compte. Dans un environnement multi-comptes, le contrôle échoue si le scan EC2 n'est pas activé sur le compte administrateur délégué Amazon Inspector et sur tous les comptes membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte administrateur Amazon Inspector délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité d'analyse EC2 pour les comptes des membres de l'organisation. Les comptes membres d'Amazon Inspector ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l'administrateur délégué a un compte de membre suspendu pour lequel le scan Amazon Inspector EC2 n'est pas activé. Pour recevoir un `PASSED` résultat, l'administrateur délégué doit dissocier ces comptes suspendus dans Amazon Inspector.

L'analyse Amazon Inspector EC2 extrait les métadonnées de votre instance Amazon Elastic Compute Cloud (Amazon EC2), puis compare ces métadonnées aux règles collectées à partir des avis de sécurité pour obtenir des résultats. Amazon Inspector analyse les instances pour détecter les vulnérabilités des packages et les problèmes d'accessibilité au réseau. Pour plus d'informations sur les systèmes d'exploitation pris en charge, notamment sur les systèmes d'exploitation pouvant être analysés sans agent SSM, consultez Systèmes d'exploitation pris en charge : analyse Amazon EC2.

Correction

Pour activer le scan Amazon Inspector EC2, consultez la section Activation des scans dans le guide de l'utilisateur Amazon Inspector.

[Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée

Exigences associées : PCI DSS v4.0 1/11.3.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS:::Account`

Règle AWS Config : `inspector-ecr-scan-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le scan ECR d'Amazon Inspector est activé. Pour un compte autonome, le contrôle échoue si le scan ECR d'Amazon Inspector est désactivé dans le compte. Dans un environnement multi-comptes, le contrôle échoue si le scan ECR n'est pas activé sur le compte administrateur délégué Amazon Inspector et sur tous les comptes membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte administrateur Amazon Inspector délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité d'analyse ECR pour les comptes des membres de l'organisation. Les comptes membres d'Amazon Inspector ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l'administrateur délégué a un compte de membre suspendu pour lequel le scan ECR d'Amazon Inspector n'est pas activé. Pour recevoir un `PASSED` résultat, l'administrateur délégué doit dissocier ces comptes suspendus dans Amazon Inspector.

Amazon Inspector analyse les images des conteneurs stockées dans Amazon Elastic Container Registry (Amazon ECR) pour détecter les vulnérabilités logicielles afin de générer des informations sur les vulnérabilités des packages. Lorsque vous activez les scans Amazon Inspector pour Amazon ECR, vous définissez Amazon Inspector comme service de numérisation préféré pour votre registre privé. Cela remplace la numérisation de base, qui est fournie gratuitement par Amazon ECR, par une numérisation améliorée, qui est fournie et facturée via Amazon Inspector. L'analyse améliorée vous permet de bénéficier de l'analyse des vulnérabilités pour les packages de système d'exploitation et de langage de programmation au niveau du registre. Vous pouvez consulter les résultats découverts grâce à la numérisation améliorée au niveau de l'image, pour chaque couche de l'image, sur la console Amazon ECR. En outre, vous pouvez consulter et utiliser ces résultats dans d'autres services qui ne sont pas disponibles pour les résultats de numérisation de base, notamment AWS Security Hub CSPM Amazon EventBridge.

Correction

Pour activer le scan ECR d'Amazon Inspector, consultez la section Activation des scans dans le guide de l'utilisateur d'Amazon Inspector.

[Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée

Exigences associées : PCI DSS v4.0 1/62.2.4, PCI DSS v4.0. 1/6.3.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : `inspector-lambda-code-scan-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le scan du code Lambda d'Amazon Inspector est activé. Pour un compte autonome, le contrôle échoue si le scan du code Lambda par Amazon Inspector est désactivé dans le compte. Dans un environnement multi-comptes, le contrôle échoue si le scan du code Lambda n'est pas activé sur le compte administrateur délégué Amazon Inspector et sur tous les comptes membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte administrateur Amazon Inspector délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité de numérisation du code Lambda pour les comptes des membres de l'organisation. Les comptes membres d'Amazon Inspector ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l'administrateur délégué a un compte de membre suspendu sur lequel le scan du code Lambda d'Amazon Inspector n'est pas activé. Pour recevoir un `PASSED` résultat, l'administrateur délégué doit dissocier ces comptes suspendus dans Amazon Inspector.

Le scan du code Lambda par Amazon Inspector analyse le code d'application personnalisé au sein d'une AWS Lambda fonction pour détecter les vulnérabilités du code, sur la base des meilleures pratiques AWS de sécurité. L'analyse du code Lambda permet de détecter des défauts d'injection, des fuites de données, une cryptographie faible ou un chiffrement manquant dans votre code. Cette fonctionnalité n'est disponible Régions AWSque de manière spécifique. Vous pouvez activer le scan de code Lambda en même temps que le scan standard Lambda (voir). [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé

Correction

Pour activer la numérisation du code Lambda d'Amazon Inspector, consultez la section Activation des scans dans le guide de l'utilisateur d'Amazon Inspector.

[Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé

Exigences associées : PCI DSS v4.0 1/62.2.4, PCI DSS v4.0. 1/6.3.1

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : `inspector-lambda-standard-scan-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le scan standard Amazon Inspector Lambda est activé. Pour un compte autonome, le contrôle échoue si le scan standard Amazon Inspector Lambda est désactivé dans le compte. Dans un environnement multi-comptes, le contrôle échoue si le scan standard Lambda n'est pas activé sur le compte administrateur Amazon Inspector délégué et sur tous les comptes membres.

Dans un environnement multi-comptes, le contrôle génère des résultats uniquement dans le compte administrateur Amazon Inspector délégué. Seul l'administrateur délégué peut activer ou désactiver la fonctionnalité d'analyse standard Lambda pour les comptes des membres de l'organisation. Les comptes membres d'Amazon Inspector ne peuvent pas modifier cette configuration depuis leurs comptes. Ce contrôle génère des `FAILED` résultats si l'administrateur délégué a un compte de membre suspendu pour lequel le scan standard Amazon Inspector Lambda n'est pas activé. Pour recevoir un `PASSED` résultat, l'administrateur délégué doit dissocier ces comptes suspendus dans Amazon Inspector.

L'analyse standard Amazon Inspector Lambda identifie les vulnérabilités logicielles dans les dépendances des packages d'applications que vous ajoutez à votre code de AWS Lambda fonction et à vos couches. Si Amazon Inspector détecte une vulnérabilité dans les dépendances des packages d'applications de votre fonction Lambda, Amazon Inspector produit une recherche de `Package Vulnerability` type détaillée. Vous pouvez activer le scan de code Lambda en même temps que le scan standard Lambda (voir). [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée

Correction

Pour activer le scan standard Amazon Inspector Lambda, consultez la section Activation des scans dans le guide de l'utilisateur Amazon Inspector.

Contrôles Security Hub CSPM pourAWS IoT

Ces AWS Security Hub CSPM contrôles évaluent le AWS IoT service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoT::SecurityProfile`

AWS Configrègle : `tagged-iot-securityprofile` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un profil AWS IoT Device Defender de sécurité comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le profil de sécurité ne possède aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le profil de sécurité n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un profil AWS IoT Device Defender de sécurité, consultez la section Marquage de vos AWS IoT ressources dans le guide du AWS IoT développeur.

[IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoT::MitigationAction`

AWS Configrègle : `tagged-iot-mitigationaction` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux	`No default value`

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		AWSexigences.	

Ce contrôle vérifie si une action AWS IoT Core d'atténuation comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'action d'atténuation ne comporte aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'action d'atténuation n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une action AWS IoT Core d'atténuation, consultez la section Marquage de vos AWS IoT ressources dans le guide du AWS IoT développeur.

[IoT.3]AWS IoT Coreles dimensions doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoT::Dimension`

AWS Configrègle : `tagged-iot-dimension` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si une AWS IoT Core dimension possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la dimension ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la dimension n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une AWS IoT Core dimension, consultez la section Marquage de vos AWS IoT ressources dans le guide du AWS IoT développeur.

[IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoT::Authorizer`

AWS Configrègle : `tagged-iot-authorizer` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS IoT Core autorisateur possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'autorisateur ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'autorisateur n'est marqué par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un AWS IoT Core autorisateur, consultez la section Marquage de vos AWS IoT ressources dans le guide du AWS IoTdéveloppeur.

[IoT.5]AWS IoT Coreles alias de rôle doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoT::RoleAlias`

AWS Configrègle : `tagged-iot-rolealias` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un alias de AWS IoT Core rôle possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'alias de rôle ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'alias de rôle n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un alias de AWS IoT Core rôle, consultez la section Marquage de vos AWS IoT ressources dans le guide du AWS IoT développeur.

[IoT.6]AWS IoT Coreles politiques doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoT::Policy`

AWS Configrègle : `tagged-iot-policy` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si une AWS IoT Core politique comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la politique ne comporte aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la politique n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une AWS IoT Core politique, consultez la section Marquage de vos AWS IoT ressources dans le guide du AWS IoT développeur.

Contrôles Security Hub CSPM pourAWSIoT SiteWise

Ces AWS Security Hub CSPM contrôles évaluent le SiteWise service et les ressources de l'AWSIoT.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTSiteWise::AssetModel`

Règle AWS Config : `iotsitewise-asset-model-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un modèle SiteWise d'actif AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le modèle d'actif ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le modèle d'actif n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un modèle d' SiteWise actif AWS IoT, consultez la section Marquer vos AWS IoT SiteWise ressources dans le guide de AWS IoT SiteWise l'utilisateur.

[IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTSiteWise::Dashboard`

Règle AWS Config : `iotsitewise-dashboard-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un SiteWise tableau de bord AWS IoT comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le tableau de bord ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le tableau de bord n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un tableau de SiteWise bord AWS IoT, consultez la section Marquer vos AWS IoT SiteWise ressources dans le guide de AWS IoT SiteWise l'utilisateur.

[IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTSiteWise::Gateway`

Règle AWS Config : `iotsitewise-gateway-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une SiteWise passerelle AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la passerelle ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la passerelle n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une SiteWise passerelle AWS IoT, consultez la section Marquer vos AWS IoT SiteWise ressources dans le guide de AWS IoT SiteWise l'utilisateur.

[IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTSiteWise::Portal`

Règle AWS Config : `iotsitewise-portal-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un SiteWise portail AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le portail ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le portail n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un SiteWise portail AWS IoT, consultez la section Marquer vos AWS IoT SiteWise ressources dans le guide de AWS IoT SiteWise l'utilisateur.

[IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTSiteWise::Project`

Règle AWS Config : `iotsitewise-project-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un SiteWise projet AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le projet ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le projet n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un SiteWise projet AWS IoT, consultez la section Marquer vos AWS IoT SiteWise ressources dans le guide de AWS IoT SiteWise l'utilisateur.

Contrôles Security Hub CSPM pourAWSIoT TwinMaker

Ces AWS Security Hub CSPM contrôles évaluent le TwinMaker service et les ressources de l'AWSIoT.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTTwinMaker::SyncJob`

Règle AWS Config : `iottwinmaker-sync-job-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une tâche de TwinMaker synchronisation AWS IoT comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la tâche de synchronisation ne comporte aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la tâche de synchronisation n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif,

propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une tâche de TwinMaker synchronisation AWS IoT, consultez TagResourcele guide de AWS IoT TwinMaker l'utilisateur.

[IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTTwinMaker::Workspace`

Règle AWS Config : `iottwinmaker-workspace-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un TwinMaker espace de travail AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'espace de travail ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'espace de travail n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des tags à un TwinMaker espace de travail AWS IoT, consultez TagResourcele guide de AWS IoT TwinMaker l'utilisateur.

[IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTTwinMaker::Scene`

Règle AWS Config : `iottwinmaker-scene-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une TwinMaker scène AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la scène ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la scène n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des tags à une TwinMaker scène AWS IoT, consultez TagResourcele guide de AWS IoT TwinMaker l'utilisateur.

[IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTTwinMaker::Entity`

Règle AWS Config : `iottwinmaker-entity-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une TwinMaker entité AWS IoT possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'entité ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'entité n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une TwinMaker entité AWS IoT, consultez TagResourcele guide de AWS IoT TwinMaker l'utilisateur.

Contrôles Security Hub CSPM pourAWSIoT Wireless

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources AWS IoT Wireless.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTWireless::MulticastGroup`

Règle AWS Config : `iotwireless-multicast-group-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de multidiffusion AWS IoT Wireless possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le groupe de multidiffusion ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de multidiffusion n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un groupe de multidiffusion AWS IoT Wireless, consultez la section Marquage de vos AWS IoT Wireless ressources dans le manuel du AWS IoT Wirelessdéveloppeur.

[IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTWireless::ServiceProfile`

Règle AWS Config : `iotwireless-service-profile-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un profil de service AWS IoT Wireless comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le profil de service ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le profil de service n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à un profil de service AWS IoT Wireless, consultez la section Marquage de vos AWS IoT Wireless ressources dans le guide du AWS IoT Wireless développeur.

[IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IoTWireless::FuotaTask`

Règle AWS Config : `iotwireless-fuota-task-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une tâche de mise à jour du microprogramme AWS IoT Wireless over-the-air (FUOTA) comporte des balises avec les clés spécifiques définies dans le paramètre. `requiredKeyTags` Le contrôle échoue si la tâche FUOTA ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre `requiredKeyTags` ne sont pas toutes spécifiées. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la tâche FUOTA n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une tâche AWS IoT Wireless FUOTA, consultez la section Marquage de vos AWS IoT Wireless ressources dans le guide du AWS IoT Wirelessdéveloppeur.

Contrôles Security Hub CSPM pour Amazon IVS

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources d'Amazon Interactive Video Service (IVS).

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[IVS.1] Les paires de clés de lecture IVS doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IVS::PlaybackKeyPair`

Règle AWS Config : `ivs-playback-key-pair-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une paire de clés de lecture Amazon IVS possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la paire de clés de lecture ne possède aucune clé de balise ou si toutes les touches spécifiées dans le paramètre ne sont pas toutes spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la paire de clés de lecture n'est associée à aucune touche. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des tags à une paire de clés de lecture IVS, consultez TagResourcele manuel Amazon IVS Real-Time Streaming API Reference.

[IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IVS::RecordingConfiguration`

Règle AWS Config : `ivs-recording configuration-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une configuration d'enregistrement Amazon IVS comporte des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si la configuration d'enregistrement ne comporte aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la configuration d'enregistrement n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une configuration d'enregistrement IVS, consultez TagResourcele manuel Amazon IVS Real-Time Streaming API Reference.

[IVS.3] Les canaux IVS doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::IVS::Channel`

Règle AWS Config : `ivs-channel-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une chaîne Amazon IVS possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si le canal ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le canal n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez

créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des tags à une chaîne IVS, consultez TagResourcele manuel Amazon IVS Real-Time Streaming API Reference.

Contrôles Security Hub CSPM pour Amazon Keyspaces

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Keyspaces.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Cassandra::Keyspace`

Règle AWS Config : `cassandra-keyspace-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un espace de touches Amazon Keyspaces possède des balises avec les clés spécifiques définies dans le paramètre. `requiredKeyTags` Le contrôle échoue si le keyspace ne possède aucune clé de balise ou s'il ne contient pas toutes les touches spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le keyspace n'est marqué d'aucune touche. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des tags à un keyspace Amazon Keyspaces, consultez la section Ajouter des tags à un keyspace dans le manuel Amazon Keyspaces Developer Guide.

Contrôles CSPM du Security Hub pour Kinesis

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Kinesis.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Kinesis.1] Les flux Kinesis doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::Kinesis::Stream`

Règle AWS Config : kinesis-stream-encrypted

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les Kinesis Data Streams sont chiffrés au repos avec un chiffrement côté serveur. Ce contrôle échoue si un flux Kinesis n'est pas chiffré au repos par chiffrement côté serveur.

Server-side le chiffrement est une fonctionnalité d'Amazon Kinesis Data Streams qui chiffre automatiquement les données avant qu'elles ne soient inactives à l'aide d'un. AWS KMS key Les

données sont chiffrées avant leur écriture sur la couche de stockage du flux Kinesis et déchiffrées après leur extraction de l'espace de stockage. Par conséquent, vos données sont chiffrées au repos dans le service Amazon Kinesis Data Streams.

Correction

Pour plus d'informations sur l'activation du chiffrement côté serveur pour les flux Kinesis, voir Comment démarrer avec le chiffrement côté serveur ? dans le manuel Amazon Kinesis Developer Guide.

[Kinesis.2] Les flux Kinesis doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Kinesis::Stream`

AWS Configrègle : `tagged-kinesis-stream` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un flux de données Amazon Kinesis comporte des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le flux de données ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle

vérifie uniquement l'existence d'une clé de balise et échoue si le flux de données n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par `aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un flux de données Kinesis, consultez la section Marquage de vos flux dans Amazon Kinesis Data Streams dans le manuel Amazon Kinesis Developer Guide.

[Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate

Gravité : Moyenne

Type de ressource : `AWS::Kinesis::Stream`

Règle AWS Config : kinesis-stream-backup-retention-check

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`minimumBackupRetentionPeriod`	Nombre minimum d'heures pendant lesquelles les données doivent être conservées.	String	24 à 8760	168

Ce contrôle vérifie si la durée de conservation des données d'un flux de données Amazon Kinesis est supérieure ou égale à la période spécifiée. Le contrôle échoue si la période de conservation des données est inférieure à la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de conservation des données, Security Hub CSPM utilise une valeur par défaut de 168 heures.

Dans Kinesis Data Streams, un flux de données est une séquence ordonnée d'enregistrements de données destinés à être écrits et lus en temps réel. Les enregistrements de données sont temporairement stockés sous forme de fragments dans votre flux. La période entre le moment où un enregistrement est ajouté et celui où il n'est plus accessible est appelée la période de conservation. Kinesis Data Streams rend presque immédiatement inaccessibles les enregistrements antérieurs à la nouvelle période de conservation après la réduction de la durée de conservation. Par exemple, si la période de conservation est portée de 24 heures à 48 heures, les enregistrements ajoutés au flux 23 heures 55 minutes auparavant continuent d'être disponibles au bout de 24 heures.

Correction

Pour modifier la période de conservation des sauvegardes pour vos Kinesis Data Streams, consultez la section Modifier la période de conservation des données dans le manuel Amazon Kinesis Data Streams Developer Guide.

Contrôles Security Hub CSPM pourAWS KMS

Ces AWS Security Hub CSPM contrôles évaluent le service AWS Key Management Service (AWS KMS) et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS

Exigences associées : NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::IAM::Policy`

Règle AWS Config : iam-customer-policy-blocked-kms-actions

Type de calendrier : changement déclenché

Paramètres :

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(non personnalisable)
- `excludePermissionBoundaryPolicy`: `True` (non personnalisable)

Vérifie si la version par défaut des politiques gérées par le client IAM autorise les donneurs d'ordre à utiliser les actions de AWS KMS déchiffrement sur toutes les ressources. Le contrôle échoue si la politique est suffisamment ouverte pour autoriser `kms:Decrypt` des `kms:ReEncryptFrom` actions sur toutes les clés KMS.

Le contrôle vérifie uniquement les clés KMS dans l'élément Resource et ne prend en compte aucune condition dans l'élément Condition d'une politique. En outre, le contrôle évalue les politiques gérées par les clients attachés et non attachés. Il ne vérifie pas les politiques intégrées ni les politiques AWS gérées.

Vous pouvez ainsi contrôler qui peut utiliser vos clés KMS et accéder à vos données chiffrées. AWS KMS Les politiques IAM définissent les actions qu'une identité (utilisateur, groupe ou rôle) peut effectuer sur quelles ressources. Conformément aux meilleures pratiques de sécurité, il est AWS recommandé d'accorder le moindre privilège. En d'autres termes, vous ne devez accorder aux identités que les `kms:ReEncryptFrom` autorisations `kms:Decrypt` ou et uniquement les clés nécessaires à l'exécution d'une tâche. Dans le cas contraire, l'utilisateur pourrait utiliser des clés qui ne sont pas adaptées à vos données.

Au lieu d'accorder des autorisations pour toutes les clés, déterminez l'ensemble minimal de clés dont les utilisateurs ont besoin pour accéder aux données chiffrées. Concevez ensuite des politiques qui autorisent les utilisateurs à utiliser uniquement ces clés. Par exemple, n'`kms:Decrypt`autorisez pas l'accès à toutes les clés KMS. Au lieu de cela, autorisez `kms:Decrypt` uniquement les clés d'une région spécifique pour votre compte. En adoptant le principe du moindre privilège, vous pouvez réduire le risque de divulgation involontaire de vos données.

Correction

Pour modifier une politique gérée par le client IAM, consultez la section Modification des politiques gérées par le client dans le guide de l'utilisateur IAM. Lorsque vous modifiez votre politique, pour le `Resource` champ, indiquez le nom de ressource Amazon (ARN) de la ou des clés spécifiques sur lesquelles vous souhaitez autoriser les actions de déchiffrement.

[KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS

Exigences associées : NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource :

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Règle AWS Config : iam-inline-policy-blocked-kms-actions

Type de calendrier : changement déclenché

Paramètres :

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(non personnalisable)

Ce contrôle vérifie si les politiques intégrées à vos identités IAM (rôle, utilisateur ou groupe) autorisent les actions de AWS KMS déchiffrement et de rechiffrement sur toutes les clés KMS. Le contrôle échoue si la politique est suffisamment ouverte pour autoriser `kms:Decrypt` des `kms:ReEncryptFrom` actions sur toutes les clés KMS.

Le contrôle vérifie uniquement les clés KMS dans l'élément Resource et ne prend en compte aucune condition dans l'élément Condition d'une politique.

Vous pouvez ainsi contrôler qui peut utiliser vos clés KMS et accéder à vos données chiffrées. AWS KMS Les politiques IAM définissent les actions qu'une identité (utilisateur, groupe ou rôle) peut effectuer sur quelles ressources. Conformément aux meilleures pratiques de sécurité, il est AWS recommandé d'accorder le moindre privilège. En d'autres termes, vous ne devez accorder aux identités que les autorisations dont elles ont besoin et uniquement pour les clés nécessaires à l'exécution d'une tâche. Dans le cas contraire, l'utilisateur pourrait utiliser des clés qui ne sont pas adaptées à vos données.

Au lieu d'accorder des autorisations pour toutes les clés, déterminez l'ensemble minimal de clés dont les utilisateurs ont besoin pour accéder aux données chiffrées. Concevez ensuite des politiques qui permettent aux utilisateurs d'utiliser uniquement ces clés. Par exemple, n'`kms:Decrypt`autorisez pas l'accès à toutes les clés KMS. Accordez plutôt l'autorisation uniquement sur des clés spécifiques dans une région spécifique pour votre compte. En adoptant le principe du moindre privilège, vous pouvez réduire le risque de divulgation involontaire de vos données.

Correction

Pour modifier une politique intégrée IAM, consultez la section Modification des politiques intégrées dans le guide de l'utilisateur IAM. Lorsque vous modifiez votre politique, pour le `Resource` champ, indiquez le nom de ressource Amazon (ARN) de la ou des clés spécifiques sur lesquelles vous souhaitez autoriser les actions de déchiffrement.

[KMS.3]AWS KMS keysne doit pas être supprimé par inadvertance

Exigences connexes : NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Critique

Type de ressource : `AWS::KMS::Key`

AWS Configrègle : `kms-cmk-not-scheduled-for-deletion-2` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la suppression des clés KMS est planifiée. Le contrôle échoue si la suppression d'une clé KMS est planifiée.

Les clés KMS ne peuvent pas être récupérées une fois supprimées. Les données chiffrées sous une clé KMS sont également irrémédiablement irrécupérables si la clé KMS est supprimée. Si des données significatives ont été chiffrées sous une clé KMS dont la suppression est prévue, envisagez de les déchiffrer ou de les rechiffrer sous une nouvelle clé KMS, sauf si vous effectuez intentionnellement un effacement cryptographique.

Lorsqu'une clé KMS est programmée pour être supprimée, une période d'attente obligatoire est imposée afin de laisser le temps d'annuler la suppression, si elle a été planifiée par erreur. Le délai d'attente par défaut est de 30 jours, mais il peut être réduit à 7 jours lorsque la suppression de la clé KMS est planifiée. Pendant la période d'attente, la suppression planifiée peut être annulée et la clé KMS ne sera pas supprimée.

Pour plus d'informations sur la suppression des clés KMS, consultez la section Suppression des clés KMS dans le manuel du AWS Key Management Service développeur.

Correction

Pour annuler la suppression planifiée d'une clé KMS, voir Pour annuler la suppression de clé sous Planification et annulation de la suppression de clé (console) dans le guide du AWS Key Management Service développeur.

[KMS.4]AWS KMSla rotation des touches doit être activée

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/32.6, CIS AWS Foundations Benchmark v3.0. 0/32.6, CIS AWS Foundations Benchmark v1.4. 0/3.8, CIS AWS Foundations Benchmark v1.2. 0/2.8 NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-28 (3), PCI DSS version 3.2. 1/36.4.4, PCI DSS v4.0. 1/3.7.4

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::KMS::Key`

Règle AWS Config : cmk-backing-key-rotation-enabled

Type de calendrier : Périodique

Paramètres : Aucun

AWS KMSpermet aux clients de faire pivoter la clé de sauvegarde, qui est un élément clé stocké AWS KMS et lié à l'identifiant de clé de la clé KMS. Il s'agit de la clé de stockage utilisée pour effectuer les opérations cryptographiques telles que le chiffrement et le déchiffrement. La rotation de clé automatique conserve actuellement toutes les clés de stockage précédentes afin que le déchiffrement des données chiffrées puisse se dérouler de façon transparente.

Le CIS vous recommande d'activer la rotation des clés KMS. La rotation des clés de chiffrement contribue à réduire l'impact potentiel d'une clé compromise, puisque les données chiffrées avec une nouvelle clé ne sont pas accessibles avec une ancienne clé susceptible d'avoir été exposée.

Correction

Pour activer la rotation automatique des clés KMS, consultez la section Comment activer et désactiver la rotation automatique des clés dans le manuel du AWS Key Management Service développeur.

[KMS.5] Les clés KMS ne doivent pas être accessibles au public

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Critique

Type de ressource : `AWS::KMS::Key`

Règle AWS Config : kms-key-policy-no-public-access

Type de calendrier : changement déclenché

Paramètres : Aucun

Cela permet de vérifier si un AWS KMS key est accessible au public. Le contrôle échoue si la clé KMS est accessible au public.

La mise en œuvre de l'accès avec le moindre privilège est fondamentale pour réduire les risques de sécurité et l'impact des erreurs ou des intentions malveillantes. Si la politique clé d'un AWS KMS

key autorise l'accès à partir de comptes externes, des tiers peuvent être en mesure de chiffrer et de déchiffrer les données à l'aide de la clé. Cela pourrait entraîner une menace interne ou externe exfiltrant les données des utilisateurs de Services AWS la clé.

> **Note**
>
> Ce contrôle renvoie également un `FAILED` résultat indiquant AWS KMS key si vos configurations AWS Config empêchent d'enregistrer la politique clé dans l'élément de configuration (CI) pour la clé KMS. AWS ConfigPour renseigner la politique clé dans le CI pour la clé KMS, le AWS Configrôle doit avoir accès à la lecture de la politique clé à l'aide de l'appel d'GetKeyPolicyAPI. Pour résoudre ce type de problème`FAILED`, vérifiez les politiques qui peuvent empêcher le AWS Config rôle d'avoir un accès en lecture à la politique clé pour la clé KMS. Vérifiez par exemple les points suivants :
>
> - La politique clé pour la clé KMS.
> - Les politiques de contrôle des services (SCP) et les politiques de contrôle des ressources (RCP) AWS Organizations qui s'appliquent à votre compte.
> - Autorisations pour le AWS Config rôle, si vous n'utilisez pas le rôle AWS Configlié au service.
>
> En outre, ce contrôle n'évalue pas les conditions de politique qui utilisent des caractères génériques ou des variables. Pour produire un `PASSED` résultat, les conditions de la politique clé doivent uniquement utiliser des valeurs fixes, c'est-à-dire des valeurs qui ne contiennent pas de caractères génériques ni de variables de politique. Pour plus d'informations sur les variables de politique, reportez-vous à la section Variables et balises du Guide de Gestion des identités et des accès AWS l'utilisateur.

Correction

Pour plus d'informations sur la mise à jour de la politique clé pour unAWS KMS key, consultez la section Politiques clés du Guide du AWS Key Management Service développeur. AWS KMS

Contrôles CSPM Security Hub pour AWS Lambda

Ces AWS Security Hub CSPM contrôles évaluent le AWS Lambda service et les ressources. Les commandes ne sont peut-être pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/72.1.1, PCI DSS v4.0. 1/72.1.1

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::Lambda::Function`

Règle AWS Config : lambda-function-public-access-prohibited

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la politique basée sur les ressources de la fonction Lambda interdit l'accès public en dehors de votre compte. Le contrôle échoue si l'accès public est autorisé. Le contrôle échoue également si une fonction Lambda est invoquée depuis Amazon S3 et que la politique n'inclut aucune condition visant à limiter l'accès public, telle que`AWS:SourceAccount`. Nous vous recommandons d'utiliser d'autres conditions S3 `AWS:SourceAccount` en plus de la politique de votre bucket pour un accès plus précis.

> **Note**
>
> Ce contrôle n'évalue pas les conditions de politique qui utilisent des caractères génériques ou des variables. Pour produire un `PASSED` résultat, les conditions de la politique de la fonction Lambda ne doivent utiliser que des valeurs fixes, c'est-à-dire des valeurs qui ne contiennent pas de caractères génériques ni de variables de stratégie. Pour plus d'informations sur les variables de politique, consultez la section Variables et balises dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

La fonction Lambda ne doit pas être accessible au public, car cela peut permettre un accès involontaire au code de votre fonction.

Correction

Pour résoudre ce problème, vous devez mettre à jour la politique basée sur les ressources de votre fonction afin de supprimer des autorisations ou d'ajouter la condition. `AWS:SourceAccount` Vous pouvez uniquement mettre à jour la politique basée sur les ressources à partir de l'API Lambda ou. AWS CLI

Pour commencer, passez en revue la politique basée sur les ressources sur la console Lambda. Identifiez la déclaration de politique dont les valeurs de `Principal` champ rendent la politique publique, par exemple `"*"` ou`{ "AWS": "*" }`.

Vous ne pouvez pas modifier la politique depuis la console. Pour supprimer les autorisations de la fonction, exécutez la remove-permission commande depuis le AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

*`<function-name>`*Remplacez-la par le nom de la fonction Lambda et *`<statement-id>`* par l'ID d'instruction (`Sid`) de l'instruction que vous souhaitez supprimer.

[Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/123.4

Catégorie : Protéger - Développement sécurisé

Gravité : Moyenne

Type de ressource : `AWS::Lambda::Function`

Règle AWS Config : lambda-function-settings-check

Type de calendrier : Déclenché par un changement

Paramètres :

- `runtime`: `dotnet10, dotnet8, java25, java21, java17, java11, java8.al2, java17.al2023, java11.al2023, java8.al2023, nodejs24.x, nodejs22.x, python3.14, python3.13, python3.12, python3.11, python3.10, ruby4.0, ruby3.4, ruby3.3` (non personnalisable)

Ce contrôle vérifie si les paramètres d'exécution des AWS Lambda fonctions correspondent aux valeurs attendues définies pour les environnements d'exécution pris en charge dans chaque langue. Le contrôle échoue si la fonction Lambda n'utilise pas un environnement d'exécution pris en charge, comme indiqué dans la section Paramètres. Security Hub CSPM ignore les fonctions dont le type de package est. `Image`

Les environnements d'exécution Lambda sont conçus autour d'une combinaison de systèmes d'exploitation, de langages de programmation et de bibliothèques logicielles qui font l'objet de mises à jour de maintenance et de sécurité. Lorsqu'un composant d'exécution n'est plus pris en charge pour les mises à jour de sécurité, Lambda le rend obsolète. Même si vous ne pouvez pas créer de fonctions utilisant le runtime obsolète, la fonction est toujours disponible pour traiter les événements d'invocation. Nous vous recommandons de vous assurer que vos fonctions Lambda sont à jour et qu'elles n'utilisent pas d'environnements d'exécution obsolètes. Pour obtenir la liste des environnements d'exécution pris en charge, consultez la section Runtimes Lambda dans le Guide du AWS Lambda développeur.

Correction

Pour plus d'informations sur les environnements d'exécution et les calendriers de dépréciation pris en charge, consultez la politique de dépréciation des environnements d'exécution dans le Guide du développeur. AWS Lambda Lorsque vous migrez vos environnements d'exécution vers la dernière version, suivez la syntaxe et les conseils des éditeurs de la langue. Nous vous recommandons également d'appliquer des mises à jour d'exécution afin de réduire le risque d'impact sur vos charges de travail dans les rares cas d'incompatibilité entre les versions d'exécution.

[Lambda.3] Les fonctions Lambda doivent se trouver dans un VPC

Exigences associées : PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/1.3.4, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Faible

Type de ressource : `AWS::Lambda::Function`

AWS Config règle : lambda-inside-vpc

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une fonction Lambda est déployée dans un cloud privé virtuel (VPC). Le contrôle échoue si la fonction Lambda n'est pas déployée dans un VPC. Security Hub CSPM n'évalue pas la configuration de routage du sous-réseau VPC pour déterminer l'accessibilité publique. Les résultats des ressources Lambda @Edge peuvent échouer.

Le déploiement de ressources dans un VPC renforce la sécurité et le contrôle des configurations réseau. De tels déploiements offrent également une évolutivité et une tolérance aux pannes élevée dans plusieurs zones de disponibilité. Vous pouvez personnaliser les déploiements de VPC pour répondre aux diverses exigences des applications.

Correction

Pour configurer une fonction existante afin de se connecter à des sous-réseaux privés de votre VPC, consultez la section Configuration de l'accès au VPC dans le Guide du AWS Lambda développeur. Nous vous recommandons de choisir au moins deux sous-réseaux privés pour une haute disponibilité et au moins un groupe de sécurité répondant aux exigences de connectivité de la fonction.

[Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::Lambda::Function`

Règle AWS Config : lambda-vpc-multi-az-check

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`availabilityZones`	Nombre minimum de zones de disponibilité	Enum	`2, 3, 4, 5, 6`	2

Ce contrôle vérifie si une AWS Lambda fonction qui se connecte à un cloud privé virtuel (VPC) fonctionne dans au moins le nombre spécifié de zones de disponibilité (AZ). Le contrôle échoue si la fonction ne fonctionne pas dans au moins le nombre spécifié d'AZ. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour le nombre minimum d'AZ, Security Hub CSPM utilise une valeur par défaut de deux AZ.

Le déploiement de ressources sur plusieurs zones de disponibilité constitue une AWS bonne pratique pour garantir une haute disponibilité au sein de votre architecture. La disponibilité est un pilier essentiel du modèle de sécurité de la triade de confidentialité, d'intégrité et de disponibilité. Toutes les fonctions Lambda qui se connectent à un VPC doivent disposer d'un déploiement multi-AZ afin de garantir qu'une seule zone de défaillance n'entraîne pas une interruption totale des opérations.

Correction

Si vous configurez votre fonction pour vous connecter à un VPC de votre compte, spécifiez des sous-réseaux dans plusieurs zones de zone de disponibilité pour garantir une haute disponibilité. Pour obtenir des instructions, consultez la section Configuration de l'accès au VPC dans le Guide du AWS Lambda développeur.

Lambda exécute automatiquement d'autres fonctions dans plusieurs zones de disponibilité afin de s'assurer qu'il est disponible pour traiter les événements en cas d'interruption de service dans une seule zone.

[Lambda.6] Les fonctions Lambda doivent être balisées

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::Lambda::Function`

AWS Config règle : `tagged-lambda-function` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	`No default value`

Ce contrôle vérifie si une AWS Lambda fonction possède des balises avec les touches spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la fonction ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la fonction n'est balisée avec aucune touche. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une fonction Lambda, consultez la section Utilisation de balises sur les fonctions Lambda dans le Guide du AWS Lambda développeur.

[Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé

Exigences connexes : NIST.800-53.r5 CA-7

Catégorie : Identifier - Journalisation

Gravité : Faible

Type de ressource : `AWS::Lambda::Function`

Règle AWS Config : lambda-function-xray-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le traçage actif avec AWS X-Ray est activé pour une AWS Lambda fonction. Le contrôle échoue si le suivi actif avec X-Ray est désactivé pour la fonction Lambda.

AWS X-Ray peut fournir des fonctionnalités de suivi et de surveillance pour les AWS Lambda fonctions, ce qui permet de gagner du temps et d'économiser des efforts lors du débogage et de l'utilisation des fonctions Lambda. Il peut vous aider à diagnostiquer les erreurs et à identifier les goulots d'étranglement, les ralentissements et les délais d'attente en réduisant la latence des fonctions Lambda. Cela peut également aider à respecter les exigences de confidentialité et de conformité des données. Si vous activez le traçage actif pour une fonction Lambda, cela X-Ray fournit une vue globale du flux de données et du traitement au sein de la fonction Lambda, ce qui

peut vous aider à identifier les failles de sécurité potentielles ou les pratiques de traitement des données non conformes. Cette visibilité peut vous aider à préserver l'intégrité, la confidentialité et la conformité des données aux réglementations pertinentes.

> **Note**
>
> AWS X-Ray le traçage n'est actuellement pas pris en charge pour les fonctions Lambda avec Amazon Managed Streaming pour Apache Kafka (Amazon MSK), Apache Kafka autogéré, Amazon MQ avec ActiveMQ et RabbitMQ, ou les mappages de sources d'événements Amazon DocumentDB.

Correction

Pour plus d'informations sur l'activation du suivi actif pour une AWS Lambda fonction, voir Visualiser les appels de fonctions Lambda AWS X-Ray à l'aide du guide du AWS Lambda développeur.

Contrôles Security Hub CSPM pour Macie

Ces AWS Security Hub CSPM contrôles évaluent le service Amazon Macie.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Macie.1] Amazon Macie devrait être activé

Exigences associées : NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Catégorie : Détecter - Services de détection

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : `macie-status-check`

Type de calendrier : Périodique

Ce contrôle vérifie si Amazon Macie est activé pour un compte. Le contrôle échoue si Macie n'est pas activé pour le compte.

Amazon Macie découvre les données sensibles à l'aide de l'apprentissage automatique et de la correspondance de modèles, fournit une visibilité sur les risques liés à la sécurité des données et permet une protection automatique contre ces risques. Macie évalue automatiquement et en permanence vos compartiments Amazon Simple Storage Service (Amazon S3) en termes de sécurité et de contrôle d'accès, et génère des résultats pour vous signaler les problèmes potentiels liés à la sécurité ou à la confidentialité de vos données Amazon S3. Macie automatise également la découverte et le reporting des données sensibles, telles que les informations personnelles identifiables (PII), afin de vous permettre de mieux comprendre les données que vous stockez dans Amazon S3. Pour en savoir plus, consultez le guide de l'utilisateur d'Amazon Macie.

Correction

Pour activer Macie, consultez la section Activer Macie dans le guide de l'utilisateur Amazon Macie.

[Macie.2] La découverte automatique des données sensibles par Macie doit être activée

Exigences associées : NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::::Account`

Règle AWS Config : `macie-auto-sensitive-data-discovery-check`

Type de calendrier : Périodique

Ce contrôle vérifie si la découverte automatique des données sensibles est activée pour un compte administrateur Amazon Macie. Le contrôle échoue si la découverte automatique des données sensibles n'est pas activée pour un compte administrateur Macie. Ce contrôle s'applique uniquement aux comptes d'administrateur.

Macie automatise la découverte et le reporting des données sensibles, telles que les informations personnelles identifiables (PII), dans les compartiments Amazon Simple Storage Service (Amazon S3). Grâce à la découverte automatique des données sensibles, Macie évalue en permanence votre inventaire de compartiments et utilise des techniques d'échantillonnage pour identifier et sélectionner des objets S3 représentatifs de vos compartiments. Macie analyse ensuite les objets sélectionnés et les inspecte pour détecter la présence de données sensibles. Au fur et à mesure que les analyses progressent, Macie met à jour les statistiques, les données d'inventaire et les autres informations

qu'il fournit sur vos données S3. Macie génère également des conclusions pour signaler les données sensibles qu'elle trouve.

Correction

Pour créer et configurer des tâches de découverte automatique de données sensibles afin d'analyser des objets dans des compartiments S3, consultez la section Configuration de la découverte automatique de données sensibles pour votre compte dans le guide de l'utilisateur Amazon Macie.

Contrôles Security Hub CSPM pour Amazon MSK

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Managed Streaming for Apache Kafka (Amazon MSK). Les commandes ne sont peut-être pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier

Exigences associées : NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::MSK::Cluster`

Règle AWS Config : msk-in-cluster-node-require-tls

Type de calendrier : changement déclenché

Paramètres : Aucun

Cela permet de vérifier si un cluster Amazon MSK est chiffré en transit avec le protocole HTTPS (TLS) entre les nœuds courtiers du cluster. Le contrôle échoue si la communication en texte brut est activée pour une connexion à un nœud de cluster broker.

Le protocole HTTPS offre un niveau de sécurité supplémentaire car il utilise le protocole TLS pour déplacer les données et peut être utilisé pour empêcher les attaquants potentiels de recourir à des attaques de type « personin-the-middle » ou à des attaques similaires pour espionner ou manipuler le trafic réseau. Par défaut, Amazon MSK chiffre les données en transit avec le protocole

TLS. Toutefois, vous pouvez annuler cette valeur par défaut au moment de créer le cluster. Nous recommandons d'utiliser des connexions chiffrées via HTTPS (TLS) pour les connexions aux nœuds de courtage.

Correction

Pour plus d'informations sur la mise à jour des paramètres de chiffrement d'un cluster Amazon MSK, consultez la section Mise à jour des paramètres de sécurité d'un cluster dans le manuel Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée

Exigences connexes : NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::MSK::Cluster`

Règle AWS Config : msk-enhanced-monitoring-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon MSK dispose d'une surveillance améliorée configurée, spécifiée par un niveau de surveillance d'au moins`PER_TOPIC_PER_BROKER`. Le contrôle échoue si le niveau de surveillance du cluster est défini sur `DEFAULT` ou`PER_BROKER`.

Le niveau `PER_TOPIC_PER_BROKER` de surveillance fournit des informations plus détaillées sur les performances de votre cluster MSK et fournit également des mesures relatives à l'utilisation des ressources, telles que l'utilisation du processeur et de la mémoire. Cela vous permet d'identifier les obstacles aux performances et les modèles d'utilisation des ressources pour des sujets et des courtiers individuels. Cette visibilité peut à son tour optimiser les performances de vos courtiers Kafka.

Correction

Pour configurer la surveillance améliorée pour un cluster MSK, procédez comme suit :

1. Ouvrez la console Amazon MSK à https://console.aws.amazon.com/msk/home l'adresse ?region=us-east-1#/home/.

2. Dans le panneau de navigation, choisissez Clusters. Choisissez ensuite un cluster.
3. Pour Action, sélectionnez Modifier la surveillance.
4. Sélectionnez l'option Surveillance thématique améliorée.
5. Sélectionnez Enregistrer les modifications.

Pour plus d'informations sur les niveaux de surveillance, consultez les métriques Amazon MSK relatives à la surveillance des courtiers standard CloudWatch dans le guide du développeur Amazon Managed Streaming for Apache Kafka.

[MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport

Exigences associées : PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::KafkaConnect::Connector`

AWS Configrègle : `msk-connect-connector-encrypted` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un connecteur Amazon MSK Connect est chiffré pendant le transport. Ce contrôle échoue si le connecteur n'est pas chiffré pendant le transport.

Les données en transit font référence aux données qui se déplacent d'un emplacement à un autre, par exemple entre les nœuds de votre cluster ou entre votre cluster et votre application. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque qu'un utilisateur non autorisé puisse espionner le trafic réseau.

Correction

Vous pouvez activer le chiffrement en transit lorsque vous créez un connecteur MSK Connect. Vous ne pouvez pas modifier les paramètres de chiffrement après avoir créé un connecteur. Pour plus d'informations, consultez la section Créer un connecteur dans le guide du développeur Amazon Managed Streaming for Apache Kafka.

[MSK.4] L'accès public aux clusters MSK doit être désactivé

Catégorie : Protéger > Gestion des accès sécurisés > Ressource non accessible au public

Gravité : Critique

Type de ressource : `AWS::MSK::Cluster`

Règle AWS Config : msk-cluster-public-access-disabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si l'accès public est désactivé pour un cluster Amazon MSK. Le contrôle échoue si l'accès public est activé pour le cluster MSK.

Par défaut, les clients peuvent accéder à un cluster Amazon MSK uniquement s'ils se trouvent dans le même VPC que le cluster. Toutes les communications entre les clients Kafka et un cluster MSK sont privées par défaut et les données en streaming ne transitent pas par Internet. Toutefois, si un cluster MSK est configuré pour autoriser l'accès public, n'importe qui sur Internet peut établir une connexion avec les courtiers Apache Kafka qui s'exécutent au sein du cluster. Cela peut entraîner des problèmes tels qu'un accès non autorisé, des violations de données ou l'exploitation de vulnérabilités. Si vous limitez l'accès à un cluster en exigeant des mesures d'authentification et d'autorisation, vous pouvez contribuer à protéger les informations sensibles et à préserver l'intégrité de vos ressources.

Correction

Pour plus d'informations sur la gestion de l'accès public à un cluster Amazon MSK, consultez la section Activer l'accès public à un cluster MSK provisioned dans le guide du développeur Amazon Managed Streaming for Apache Kafka.

[MSK.5] La journalisation des connecteurs MSK doit être activée

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::KafkaConnect::Connector`

Règle AWS Config : msk-connect-connector-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée pour un connecteur Amazon MSK. Le contrôle échoue si la journalisation est désactivée pour le connecteur MSK.

Les connecteurs Amazon MSK intègrent des systèmes externes et des services Amazon à Apache Kafka en copiant en continu les données de streaming d'une source de données vers un cluster Apache Kafka, ou en copiant en continu les données d'un cluster vers un récepteur de données. MSK Connect peut écrire des événements de journal qui peuvent aider à déboguer un connecteur. Lorsque vous créez un connecteur, vous pouvez spécifier au moins zéro des destinations de journal suivantes : Amazon CloudWatch Logs, Amazon S3 et Amazon Data Firehose.

> **Note**
>
> Des valeurs de configuration sensibles peuvent apparaître dans les journaux des connecteurs si un plugin ne définit pas ces valeurs comme secrètes. Kafka Connect traite les valeurs de configuration non définies de la même manière que toute autre valeur en texte brut.

Correction

Pour activer la journalisation pour un connecteur Amazon MSK existant, vous devez recréer le connecteur avec la configuration de journalisation appropriée. Pour plus d'informations sur les options de configuration, consultez la section Logging for MSK Connect du manuel Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié

Catégorie : Protéger > Gestion des accès sécurisés > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::MSK::Cluster`

Règle AWS Config : msk-unrestricted-access-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si l'accès non authentifié est activé pour un cluster Amazon MSK. Le contrôle échoue si l'accès non authentifié est activé pour le cluster MSK.

Amazon MSK prend en charge les mécanismes d'authentification et d'autorisation des clients pour contrôler l'accès à un cluster. Ces mécanismes vérifient l'identité des clients qui se connectent au cluster et déterminent les actions que les clients peuvent effectuer. Un cluster MSK peut être configuré pour autoriser un accès non authentifié, ce qui permet à tout client connecté au réseau de publier des sujets Kafka et de s'y abonner sans fournir d'informations d'identification. L'exécution d'un cluster MSK sans authentification enfreint le principe du moindre privilège et peut exposer le cluster à un accès non autorisé. Il peut permettre à n'importe quel client d'accéder, de modifier ou de supprimer des données dans les rubriques Kafka, ce qui peut entraîner des violations de données, des modifications non autorisées des données ou des interruptions de service. Nous recommandons d'activer les mécanismes d'authentification tels que l'authentification IAM ou le protocole TLS mutuel pour garantir un contrôle d'accès approprié et garantir la conformité en matière de sécurité. SASL/SCRAM

Correction

Pour plus d'informations sur la modification des paramètres d'authentification d'un cluster Amazon MSK, consultez les sections suivantes du guide du développeur Amazon Managed Streaming for Apache Kafka : Mettre à jour les paramètres de sécurité d'un cluster Amazon MSK et Authentification et autorisation pour les API Apache Kafka.

Contrôles Security Hub CSPM pour Amazon MQ

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon MQ. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch

Exigences associées : NIST.800-53.r5 AU-2,, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-12 NIST.800-53.r5 SI-4, PCI DSS v4.0. 1/10.3.3

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::AmazonMQ::Broker`

Règle AWS Config : `mq-cloudwatch-audit-log-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un courtier Amazon MQ ActiveMQ diffuse des journaux d'audit vers Amazon Logs. CloudWatch Le contrôle échoue si le broker ne diffuse pas les journaux d'audit vers CloudWatch Logs.

En publiant les journaux des courtiers ActiveMQ dans Logs CloudWatch , vous pouvez CloudWatch créer des alarmes et des mesures qui augmentent la visibilité des informations relatives à la sécurité.

Correction

Pour diffuser les journaux du courtier ActiveMQ CloudWatch vers des journaux, consultez la section Configuration d'Amazon MQ pour les journaux ActiveMQ dans le guide du développeur Amazon MQ.

[MQ.4] Les courtiers Amazon MQ doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::AmazonMQ::Broker`

AWS Configrègle : `tagged-amazonmq-broker` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un courtier Amazon MQ possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le broker ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le broker n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un courtier Amazon MQ, consultez les ressources de balisage dans le manuel Amazon MQ Developer Guide.

[MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Faible

Type de ressource : `AWS::AmazonMQ::Broker`

Règle AWS Config : `mq-active-deployment-mode`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le mode de déploiement d'un broker Amazon MQ ActiveMQ est défini sur. active/standby Le contrôle échoue si un broker à instance unique (activé par défaut) est défini comme mode de déploiement.

Active/standby le déploiement fournit une haute disponibilité à vos courtiers Amazon MQ ActiveMQ dans un. Région AWS Le mode de active/standby déploiement inclut deux instances de courtier situées dans deux zones de disponibilité différentes, configurées dans une paire redondante. Ces courtiers communiquent de manière synchrone avec votre application, ce qui peut réduire les temps d'arrêt et les pertes de données en cas de panne.

Correction

Pour créer un nouveau courtier ActiveMQ en mode déploiement, consultez la section Création et configuration d'un courtier active/standby ActiveMQ dans le manuel Amazon MQ Developer Guide. Pour le mode de déploiement, choisissez Active/standby Broker. Vous ne pouvez pas modifier le mode de déploiement d'un broker existant. Au lieu de cela, vous devez créer un nouveau courtier et copier les paramètres de l'ancien courtier.

[MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Faible

Type de ressource : `AWS::AmazonMQ::Broker`

Règle AWS Config : `mq-rabbit-deployment-mode`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le mode de déploiement d'un courtier Amazon MQ RabbitMQ est défini sur le déploiement en cluster. Le contrôle échoue si un broker à instance unique (activé par défaut) est défini comme mode de déploiement.

Le déploiement en cluster offre une haute disponibilité à vos courtiers Amazon MQ RabbitMQ dans un. Région AWS Le déploiement du cluster est un regroupement logique de trois nœuds de courtage RabbitMQ, chacun possédant son propre volume Amazon Elastic Block Store (Amazon EBS) et un état partagé. Le déploiement du cluster garantit que les données sont répliquées sur tous les nœuds du cluster, ce qui peut réduire les temps d'arrêt et les pertes de données en cas de panne.

Correction

Pour créer un nouveau courtier RabbitMQ avec le mode de déploiement en cluster, consultez la section Création et connexion à un courtier RabbitMQ dans le guide du développeur Amazon MQ. Pour le mode de déploiement, choisissez Déploiement en cluster. Vous ne pouvez pas modifier le mode de déploiement d'un broker existant. Au lieu de cela, vous devez créer un nouveau courtier et copier les paramètres de l'ancien courtier.

Contrôles Security Hub CSPM pour Neptune

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Neptune.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-encrypted`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données Neptune est chiffré au repos. Le contrôle échoue si un cluster de base de données Neptune n'est pas chiffré au repos.

Les données au repos désignent toutes les données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement vous aide à protéger la confidentialité de ces données, réduisant ainsi le risque qu'un utilisateur non autorisé puisse y accéder. Le chiffrement de vos clusters de base de données Neptune protège vos données et métadonnées contre tout accès non autorisé. Il répond également aux exigences de conformité relatives au chiffrement des données au repos des systèmes de fichiers de production.

Correction

Vous pouvez activer le chiffrement au repos lorsque vous créez un cluster de base de données Neptune. Vous ne pouvez pas modifier les paramètres de chiffrement après avoir créé un cluster. Pour plus d'informations, consultez la section Chiffrer les ressources Neptune au repos dans le Guide de l'utilisateur de Neptune.

[Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch

Exigences connexes : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7(8), PCI DSS version 4.0. 1/10.3.3

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-cloudwatch-log-export-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données Neptune publie des journaux d'audit sur Amazon CloudWatch Logs. Le contrôle échoue si un cluster de base de données Neptune ne publie pas les journaux d'audit dans Logs. CloudWatch `EnableCloudWatchLogsExport`doit être réglé sur`Audit`.

Amazon Neptune et Amazon CloudWatch sont intégrés afin que vous puissiez recueillir et analyser les indicateurs de performance. Neptune envoie automatiquement des métriques aux alarmes CloudWatch et les prend également en charge CloudWatch . Les journaux d'audit sont hautement personnalisables. Lorsque vous auditez une base de données, chaque opération sur les données peut être surveillée et enregistrée dans une piste d'audit, y compris des informations sur le cluster de base de données auquel on accède et comment. Nous vous recommandons d'envoyer ces journaux pour vous aider CloudWatch à surveiller vos clusters de base de données Neptune.

Correction

Pour publier les journaux d'audit Neptune dans Logs, consultez la section Publication CloudWatch des journaux Neptune sur Amazon Logs CloudWatch dans le guide de l'utilisateur de Neptune. Dans la section Exportations de journaux, choisissez Audit.

[Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Critique

Type de ressource : `AWS::RDS::DBClusterSnapshot`

Règle AWS Config : `neptune-cluster-snapshot-public-prohibited`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un instantané manuel du cluster de base de données Neptune est public. Le contrôle échoue si un instantané manuel du cluster de base de données Neptune est public.

Un instantané manuel d'un cluster de base de données Neptune ne doit pas être public, sauf indication contraire. Si vous partagez un instantané manuel non chiffré en tant que public, l'instantané est accessible à tousComptes AWS. Les instantanés publics peuvent entraîner une exposition involontaire des données.

Correction

Pour supprimer l'accès public aux instantanés manuels de cluster de bases de données Neptune, consultez la section Partage d'un instantané de cluster de base de données dans le guide de l'utilisateur de Neptune.

[Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Faible

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-deletion-protection-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la protection contre les suppressions est activée sur un cluster de base de données Neptune. Le contrôle échoue si la protection contre la suppression n'est pas activée sur un cluster de base de données Neptune.

L'activation de la protection contre la suppression de clusters offre un niveau de protection supplémentaire contre la suppression accidentelle de la base de données ou la suppression par un utilisateur non autorisé. Un cluster de base de données Neptune ne peut pas être supprimé tant que la protection contre la suppression est activée. Vous devez d'abord désactiver la protection contre la suppression pour qu'une demande de suppression puisse aboutir.

Correction

Pour activer la protection contre la suppression pour un cluster de base de données Neptune existant, consultez la section Modification du cluster de base de données à l'aide de la console, de la CLI et de l'API dans le guide de l'utilisateur Amazon Aurora.

[Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées

Exigences connexes : NIST.800-53.r5 SI-12

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-backup-retention-check`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM	
`minimumBackupRetentionPeriod`	Durée minimale de conservation des sauvegardes en jours	Entier	7 sur 35	7	

Ce contrôle vérifie si les sauvegardes automatisées sont activées sur un cluster de base de données Neptune et si la période de conservation des sauvegardes est supérieure ou égale à la période spécifiée. Le contrôle échoue si les sauvegardes ne sont pas activées pour le cluster de base de données Neptune ou si la période de rétention est inférieure à la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de conservation des sauvegardes, Security Hub CSPM utilise une valeur par défaut de 7 jours.

Les sauvegardes vous aident à vous remettre plus rapidement en cas d'incident de sécurité et à renforcer la résilience de vos systèmes. En automatisant les sauvegardes de vos clusters de base de données Neptune, vous serez en mesure de restaurer vos systèmes à un moment précis et de minimiser les temps d'arrêt et les pertes de données.

Correction

Pour activer les sauvegardes automatisées et définir une période de conservation des sauvegardes pour vos clusters de base de données Neptune, consultez la section Activation des sauvegardes automatisées dans le guide de l'utilisateur Amazon RDS. Pour la période de conservation des sauvegardes, choisissez une valeur supérieure ou égale à 7.

[Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBClusterSnapshot`

Règle AWS Config : `neptune-cluster-snapshot-encrypted`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un instantané du cluster de base de données Neptune est chiffré au repos. Le contrôle échoue si un cluster de base de données Neptune n'est pas chiffré au repos.

Les données au repos désignent toutes les données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement vous aide à protéger la confidentialité de ces données, réduisant ainsi le risque qu'un utilisateur non autorisé y accède. Les données contenues dans les instantanés des clusters de base de données Neptune doivent être chiffrées au repos pour renforcer la sécurité.

Correction

Vous ne pouvez pas chiffrer un instantané de cluster de base de données Neptune existant. Au lieu de cela, vous devez restaurer le snapshot sur un nouveau cluster de base de données et activer le

chiffrement sur le cluster. Vous pouvez créer un instantané chiffré à partir du cluster chiffré. Pour obtenir des instructions, reportez-vous aux sections Restauration à partir d'un instantané de cluster de base de données et Création d'un instantané de cluster de base de données dans Neptune dans le guide de l'utilisateur de Neptune.

[Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune

Exigences connexes : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Catégorie : Protéger > Gestion des accès sécurisés > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-iam-database-authentication`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si l'authentification de base de données IAM est activée dans un cluster de base de données Neptune. Le contrôle échoue si l'authentification de base de données IAM n'est pas activée pour un cluster de base de données Neptune.

L'authentification de base de données IAM pour les clusters de bases de données Amazon Neptune élimine le besoin de stocker les informations d'identification des utilisateurs dans la configuration de la base de données, car l'authentification est gérée en externe à l'aide d'IAM. Lorsque l'authentification de base de données IAM est activée, chaque demande doit être signée à l'aide de AWS la version 4 de Signature.

Correction

Par défaut, l'authentification de base de données IAM est désactivée lorsque vous créez un cluster de base de données Neptune. Pour l'activer, consultez la section Activation de l'authentification de base de données IAM dans Neptune dans le guide de l'utilisateur de Neptune.

[Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-copy-tags-to-snapshot-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données Neptune est configuré pour copier toutes les balises dans les instantanés lors de leur création. Le contrôle échoue si un cluster de base de données Neptune n'est pas configuré pour copier des balises dans des instantanés.

L'identification et l'inventaire de vos actifs informatiques constituent un aspect crucial de la gouvernance et de la sécurité. Vous devez étiqueter les instantanés de la même manière que leurs clusters de base de données Amazon RDS parents. La copie des balises garantit que les métadonnées des instantanés de base de données correspondent à celles des clusters de base de données parents et que les politiques d'accès à l'instantané de base de données correspondent également à celles de l'instance de base de données parent.

Correction

Pour copier des balises dans des instantanés pour les clusters de base de données Neptune, consultez la section Copier des balises dans Neptune dans le guide de l'utilisateur de Neptune.

[Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `neptune-cluster-multi-az-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données Amazon Neptune possède des instances de réplication en lecture dans plusieurs zones de disponibilité (AZ). Le contrôle échoue si le cluster est déployé dans une seule zone de disponibilité.

Si une AZ n'est pas disponible et lors d'événements de maintenance réguliers, les répliques en lecture servent de cibles de basculement pour l'instance principale. En d'autres termes, si l'instance principale échoue, Neptune promeut une instance de réplica en lecture au statut d'instance principale. En revanche, si votre cluster de base de données n'inclut aucune instance de réplication en lecture, votre cluster de base de données reste indisponible en cas de défaillance de l'instance principale tant qu'elle n'a pas été recréée. Re-creating l'instance principale prend beaucoup plus de temps que la promotion d'une réplique en lecture. Pour garantir une haute disponibilité, nous vous recommandons de créer une ou plusieurs instances en lecture répliquée ayant la même classe d'instance de base de données que l'instance principale et situées dans des zones de disponibilité différentes de celles de l'instance principale.

Correction

Pour déployer un cluster de base de données Neptune dans plusieurs zones de disponibilité, consultez la section Instances de Read-replica base de données dans un cluster de base de données Neptune dans le guide de l'utilisateur de Neptune.

Contrôles Security Hub CSPM pourAWS Network Firewall

Ces AWS Security Hub CSPM contrôles évaluent le AWS Network Firewall service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::Firewall`

Règle AWS Config : netfw-multi-az-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle évalue si un pare-feu géré par le biais AWS Network Firewall est déployé dans plusieurs zones de disponibilité (AZ). Le contrôle échoue si un pare-feu est déployé dans une seule zone de disponibilité.

AWSl'infrastructure mondiale comprend plusieursRégions AWS. Les AZ sont des sites isolés physiquement séparés au sein de chaque région, connectés par un réseau à faible latence, à haut débit et hautement redondant. En déployant un pare-feu Network Firewall sur plusieurs zones de disponibilité, vous pouvez équilibrer et transférer le trafic entre les zones de disponibilité, ce qui vous permet de concevoir des solutions à haute disponibilité.

Correction

Déploiement d'un pare-feu Network Firewall sur plusieurs zones de disponibilité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Network Firewall, sélectionnez Firewalls.
3. Sur la page Pare-feu, sélectionnez le pare-feu que vous souhaitez modifier.
4. Sur la page des détails du pare-feu, choisissez l'onglet Détails du pare-feu.
5. Dans la section Politique associée et VPC, choisissez Modifier
6. Pour ajouter un nouvel AZ, choisissez Ajouter un nouveau sous-réseau. Sélectionnez l'AZ et le sous-réseau que vous souhaitez utiliser. Assurez-vous de sélectionner au moins deux AZ.
7. Choisissez Enregistrer.

[NetworkFirewall.2] La journalisation du Network Firewall doit être activée

Exigences connexes : NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, (8), NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::LoggingConfiguration`

Règle AWS Config : netfw-logging-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée pour un AWS Network Firewall pare-feu. Le contrôle échoue si la journalisation n'est pas activée pour au moins un type de journal ou si la destination de journalisation n'existe pas.

La journalisation vous aide à maintenir la fiabilité, la disponibilité et les performances de vos pare-feux. Dans Network Firewall, la journalisation fournit des informations détaillées sur le trafic réseau, notamment l'heure à laquelle le moteur dynamique a reçu un flux de paquets, des informations détaillées sur le flux de paquets et toute action de règle dynamique prise à l'encontre du flux de paquets.

Correction

Pour activer la journalisation pour un pare-feu, consultez la section Mise à jour de la configuration de journalisation d'un pare-feu dans le Guide du AWS Network Firewall développeur.

[NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, 3.13.1 NIST.800-171.r2

Catégorie : Protection > Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::FirewallPolicy`

Règle AWS Config : netfw-policy-rule-group-associated

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une politique Network Firewall est associée à des groupes de règles avec ou sans état. Le contrôle échoue si aucun groupe de règles apatride ou dynamique n'est attribué.

Une politique de pare-feu définit la manière dont votre pare-feu surveille et gère le trafic dans Amazon Virtual Private Cloud (Amazon VPC). La configuration de groupes de règles apatrides et dynamiques permet de filtrer les paquets et les flux de trafic et de définir la gestion du trafic par défaut.

Correction

Pour ajouter un groupe de règles à une politique de Network Firewall, consultez la section Mise à jour d'une politique de pare-feu dans le Guide du AWS Network Firewall développeur. Pour plus d'informations sur la création et la gestion de groupes de règles, consultez la section Groupes de règles dans AWS Network Firewall.

[NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protection > Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::FirewallPolicy`

Règle AWS Config : netfw-policy-default-action-full-packets

Type de calendrier : changement déclenché

Paramètres :

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(non personnalisable)

Ce contrôle vérifie si l'action apatride par défaut pour les paquets complets dans le cadre d'une politique Network Firewall est la suppression ou le transfert. Le contrôle passe si `Drop` ou `Forward` est sélectionné, et échoue s'il `Pass` est sélectionné.

Une politique de pare-feu définit la manière dont votre pare-feu surveille et gère le trafic dans Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic. La valeur par défaut `Pass` peut autoriser le trafic involontaire.

Correction

Pour modifier votre politique de pare-feu, consultez la section Mise à jour d'une politique de pare-feu dans le Guide du AWS Network Firewall développeur. Pour les actions par défaut sans état, choisissez Modifier. Choisissez ensuite Supprimer ou Transférer vers des groupes de règles dynamiques en tant qu'action.

[NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.14, 3.13.1, 3.13.6 NIST.800-171.r2 NIST.800-171.r2

Catégorie : Protection > Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::FirewallPolicy`

Règle AWS Config : netfw-policy-default-action-fragment-packets

Type de calendrier : changement déclenché

Paramètres :

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(non personnalisable)

Ce contrôle vérifie si l'action apatride par défaut pour les paquets fragmentés dans le cadre d'une politique Network Firewall est la suppression ou le transfert. Le contrôle passe si `Drop` ou `Forward` est sélectionné, et échoue s'il `Pass` est sélectionné.

Une politique de pare-feu définit la manière dont votre pare-feu surveille et gère le trafic dans Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic. La valeur par défaut `Pass` peut autoriser le trafic involontaire.

Correction

Pour modifier votre politique de pare-feu, consultez la section Mise à jour d'une politique de pare-feu dans le Guide du AWS Network Firewall développeur. Pour les actions par défaut sans état,

choisissez Modifier. Choisissez ensuite Supprimer ou Transférer vers des groupes de règles dynamiques en tant qu'action.

[NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide

Exigences connexes : NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, 3.13.1, 3.13.6 NIST.800-171.r2 NIST.800-171.r2

Catégorie : Protection > Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::RuleGroup`

Règle AWS Config : netfw-stateless-rule-group-not-empty

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe de règles AWS Network Firewall apatrides contient des règles. Le contrôle échoue s'il n'existe aucune règle dans le groupe de règles.

Un groupe de règles contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles apatrides vide, lorsqu'il est présent dans une politique de pare-feu, peut donner l'impression que le groupe de règles traitera le trafic. Toutefois, lorsque le groupe de règles apatrides est vide, il ne traite pas le trafic.

Correction

Pour ajouter des règles à votre groupe de règles Network Firewall, consultez la section Mise à jour d'un groupe de règles dynamique dans le Guide du AWS Network Firewall développeur. Sur la page des détails du pare-feu, pour le groupe de règles Stateless, choisissez Modifier pour ajouter des règles.

[NetworkFirewall.7] Les pare-feux Network Firewall doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::NetworkFirewall::Firewall`

AWS Configrègle : `tagged-networkfirewall-firewall` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS Network Firewall pare-feu possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le pare-feu ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le pare-feu n'est marqué d'aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un pare-feu Network Firewall, consultez les AWS Network Firewallressources relatives au balisage dans le Guide du AWS Network Firewall développeur.

[NetworkFirewall.8] Les politiques de pare-feu de Network Firewall doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::NetworkFirewall::FirewallPolicy`

AWS Configrègle : `tagged-networkfirewall-firewallpolicy` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux	`No default value`

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		AWSexigences.	

Ce contrôle vérifie si une politique de AWS Network Firewall pare-feu comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la politique de pare-feu ne comporte aucune clé de balise ou si toutes les clés ne sont pas spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la politique de pare-feu n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une politique de Network Firewall, consultez les AWS Network Firewallressources relatives au balisage dans le Guide du AWS Network Firewall développeur.

[NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protection > Sécurité du réseau

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::Firewall`

Règle AWS Config : netfw-deletion-protection-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la protection contre les suppressions est activée sur un AWS Network Firewall pare-feu. Le contrôle échoue si la protection contre la suppression n'est pas activée pour un pare-feu.

AWS Network Firewallest un pare-feu réseau géré et dynamique et un service de détection des intrusions qui vous permet d'inspecter et de filtrer le trafic à destination, en provenance ou entre vos clouds privés virtuels (VPC). Le paramètre de protection contre la suppression protège contre la suppression accidentelle du pare-feu.

Correction

Pour activer la protection contre la suppression sur un pare-feu Network Firewall existant, consultez la section Mise à jour d'un pare-feu dans le manuel du AWS Network Firewall développeur. Pour les protections contre les modifications, sélectionnez Activer. Vous pouvez également activer la protection contre la suppression en appelant l' UpdateFirewallDeleteProtectionAPI et en définissant le `DeleteProtection` champ sur. `true`

[NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protection > Sécurité du réseau

Gravité : Moyenne

Type de ressource : `AWS::NetworkFirewall::Firewall`

Règle AWS Config : netfw-subnet-change-protection-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la protection contre les modifications de sous-réseau est activée pour un AWS Network Firewall pare-feu. Le contrôle échoue si la protection contre les modifications de sous-réseau n'est pas activée pour le pare-feu.

AWS Network Firewallest un pare-feu réseau géré et dynamique et un service de détection des intrusions que vous pouvez utiliser pour inspecter et filtrer le trafic à destination, en provenance ou entre vos clouds privés virtuels (VPC). Si vous activez la protection contre les modifications de sous-réseau pour un pare-feu Network Firewall, vous pouvez protéger le pare-feu contre toute modification accidentelle des associations de sous-réseaux du pare-feu.

Correction

Pour plus d'informations sur l'activation de la protection contre les modifications de sous-réseau pour un pare-feu Network Firewall existant, consultez la section Mise à jour d'un pare-feu dans le Guide du AWS Network Firewall développeur.

Contrôles Security Hub CSPM pour Amazon Service OpenSearch

Ces AWS Security Hub CSPM contrôles évaluent le OpenSearch service et les ressources Amazon OpenSearch Service (Service). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines

Exigences associées : PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/72.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-encrypted-at-rest`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la configuration du chiffrement au repos est activée dans les OpenSearch domaines. La vérification échoue si le chiffrement au repos n'est pas activé.

Pour renforcer la sécurité des données sensibles, vous devez configurer votre domaine de OpenSearch service pour qu'il soit chiffré au repos. Lorsque vous configurez le chiffrement des données au repos, vous AWS KMS stockez et gérez vos clés de chiffrement. Pour effectuer le chiffrement, AWS KMS utilise l'algorithme Advanced Encryption Standard avec des clés de 256 bits ()AES-256.

Pour en savoir plus sur le chiffrement des OpenSearch services au repos, consultez la section Chiffrement des données au repos pour Amazon OpenSearch Service dans le manuel Amazon OpenSearch Service Developer Guide.

Correction

Pour activer le chiffrement au repos pour les OpenSearch domaines nouveaux et existants, consultez la section Activation du chiffrement des données au repos dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public

Exigences associées : PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6,

NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protection > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Critique

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-in-vpc-only`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les OpenSearch domaines se trouvent dans un VPC. Il n'évalue pas la configuration de routage du sous-réseau VPC pour déterminer l'accès public.

Vous devez vous assurer que OpenSearch les domaines ne sont pas attachés à des sous-réseaux publics. Consultez Resource-based les politiques dans le manuel Amazon OpenSearch Service Developer Guide. Vous devez également garantir que votre VPC est configuré conformément aux bonnes pratiques recommandées. Consultez les meilleures pratiques de sécurité pour votre VPC dans le guide de l'utilisateur Amazon VPC.

OpenSearch les domaines déployés au sein d'un VPC peuvent communiquer avec les ressources du VPC via le AWS réseau privé, sans qu'il soit nécessaire de passer par l'Internet public. Cette configuration augmente le niveau de sécurité en limitant l'accès aux données en transit. Les VPC fournissent un certain nombre de contrôles réseau pour sécuriser l'accès aux OpenSearch domaines, notamment les ACL réseau et les groupes de sécurité. Security Hub vous recommande de migrer OpenSearch les domaines publics vers des VPC pour tirer parti de ces contrôles.

Correction

Si vous créez un domaine avec un point de terminaison public, vous ne pouvez pas ultérieurement le placer au sein d'un VPC. Au lieu de cela, vous devez créer un nouveau domaine et migrer vos données. L'inverse est également vrai. Si vous créez un domaine dans un VPC, il ne peut pas avoir de point de terminaison public. Au lieu de cela, vous devez créer un autre domaine ou désactiver ce contrôle.

Pour obtenir des instructions, consultez la section Lancement de vos domaines Amazon OpenSearch Service au sein d'un VPC dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds

Exigences associées : NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2)

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-node-to-node-encryption-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement nœud à nœud est activé dans les OpenSearch domaines. Ce contrôle échoue si le chiffrement nœud à nœud est désactivé sur le domaine.

Le protocole HTTPS (TLS) peut être utilisé pour empêcher les attaquants potentiels d'espionner ou de manipuler le trafic réseau par le biais d'attaques de type « person-in-the-middle » ou d'attaques similaires. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées. L'activation du chiffrement nœud à nœud pour les OpenSearch domaines garantit le chiffrement des communications au sein du cluster pendant le transit.

Cette configuration peut entraîner une baisse des performances. Vous devez connaître le compromis entre les performances et le tester avant d'activer cette option.

Correction

Pour activer le chiffrement nœud à nœud sur un OpenSearch domaine, consultez la section Activation du chiffrement nœud à nœud dans le manuel Amazon Service Developer Guide. OpenSearch

[Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée

Exigences connexes : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,,

NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-logs-to-cloudwatch`

Type de calendrier : changement déclenché

Paramètres :

- `logtype = 'error'`(non personnalisable)

Ce contrôle vérifie si OpenSearch les domaines sont configurés pour envoyer des journaux d'erreurs à CloudWatch Logs. Ce contrôle échoue si la journalisation des erreurs n' CloudWatch est pas activée pour un domaine.

Vous devez activer les journaux d'erreurs pour OpenSearch les domaines et les envoyer à CloudWatch Logs pour les conserver et y répondre. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

Correction

Pour activer la publication des journaux, consultez la section Activation de la publication des journaux (console) dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-audit-logging-enabled`

Type de calendrier : changement déclenché

Paramètres :

- `cloudWatchLogsLogGroupArnList`(non personnalisable) — Security Hub CSPM ne renseigne pas ce paramètre. Comma-separated liste des groupes de CloudWatch journaux qui doivent être configurés pour les journaux d'audit.

Ce contrôle vérifie si la journalisation des audits est activée dans les OpenSearch domaines. Ce contrôle échoue si la journalisation des audits n'est pas activée pour un OpenSearch domaine.

Les journaux d'audit sont hautement personnalisables. Ils vous permettent de suivre l'activité des utilisateurs sur vos OpenSearch clusters, notamment les réussites et les échecs d'authentification, les demandesOpenSearch, les modifications d'index et les requêtes de recherche entrantes.

Correction

Pour obtenir des instructions sur l'activation des journaux d'audit, consultez la section Activation des journaux d'audit dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-data-node-fault-tolerance`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si OpenSearch les domaines sont configurés avec au moins trois nœuds de données et `zoneAwarenessEnabled` s'ils le sont`true`. Ce contrôle échoue pour un OpenSearch

domaine s'il `instanceCount` est inférieur à 3 ou s'il `zoneAwarenessEnabled` est inférieur à `3false`.

Pour atteindre une haute disponibilité et une tolérance aux pannes au niveau du cluster, un OpenSearch domaine doit comporter au moins trois nœuds de données. Le déploiement d'un OpenSearch domaine comportant au moins trois nœuds de données garantit les opérations du cluster en cas de défaillance d'un nœud.

Correction

Pour modifier le nombre de nœuds de données dans un OpenSearch domaine

1. Connectez-vous à la AWS console et ouvrez la console Amazon OpenSearch Service à l'adresse https://console.aws.amazon.com/aos/.
2. Sous Mes domaines, choisissez le nom du domaine à modifier, puis sélectionnez Modifier.
3. Sous Nœuds de données, définissez Nombre de nœuds sur un nombre supérieur à`3`. Si vous effectuez un déploiement dans trois zones de disponibilité, définissez le nombre sur un multiple de trois pour garantir une répartition égale entre les zones de disponibilité.
4. Sélectionnez Soumettre.

[Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé

Exigences connexes : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Catégorie : Protection > Gestion des accès sécurisés > Actions d'API sensibles restreintes

Gravité : Élevée

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-access-control-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le contrôle d'accès détaillé est activé dans les OpenSearch domaines. Le contrôle échoue si le contrôle d'accès détaillé n'est pas activé. Fine-grained le contrôle d'accès doit être activé `advanced-security-options` dans le OpenSearch paramètre`update-domain-config`.

Fine-grained le contrôle d'accès offre des moyens supplémentaires de contrôler l'accès à vos données sur Amazon OpenSearch Service.

Correction

Pour activer un contrôle d'accès précis, consultez le contrôle Fine-grained d'accès dans Amazon OpenSearch Service dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS

Exigences associées : NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-https-required`

Type de calendrier : changement déclenché

Paramètres :

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(non personnalisable)

Cela permet de vérifier si un point de terminaison de domaine Amazon OpenSearch Service est configuré pour utiliser la dernière politique de sécurité TLS. Le contrôle échoue si le point de terminaison du OpenSearch domaine n'est pas configuré pour utiliser la dernière politique prise en charge ou si le protocole HTTPS n'est pas activé.

Vous pouvez utiliser HTTPS (TLS) pour empêcher les pirates potentiels d'espionner ou de manipuler le trafic réseau à l'aide d'attaques de l'homme du milieu au d'autres attaques similaires. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées. Le chiffrement des données en transit peut affecter les performances. Vous devez tester votre application avec cette fonctionnalité pour comprendre le profil de performance et l'impact du protocole TLS. TLS 1.2 apporte plusieurs améliorations de sécurité par rapport aux versions précédentes de TLS.

Correction

Pour activer le chiffrement TLS, utilisez l'opération UpdateDomainConfigAPI. Configurez le DomainEndpointOptionschamp pour spécifier la valeur pour`TLSSecurityPolicy`. Pour plus d'informations, consultez la section sur le Node-to-node chiffrement dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.9] OpenSearch les domaines doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::OpenSearch::Domain`

AWS Configrègle : `tagged-opensearch-domain` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un domaine Amazon OpenSearch Service possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le domaine ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le domaine n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un domaine OpenSearch de service, consultez la section Utilisation des balises dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée

Exigences associées : NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-update-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la dernière mise à jour logicielle est installée sur un domaine Amazon OpenSearch Service. Le contrôle échoue si une mise à jour logicielle est disponible mais n'est pas installée pour le domaine.

OpenSearch Les mises à jour du logiciel de service fournissent les derniers correctifs, mises à jour et fonctionnalités de plate-forme disponibles pour l'environnement. Le fait de rester à jour grâce à l'installation des correctifs permet de garantir la sécurité et la disponibilité du domaine. Si aucune action n'est entreprise sur les mises à jour requises, le logiciel de service est mis à jour automatiquement (généralement au bout de 2 semaines). Nous recommandons de planifier les mises à jour en période de faible trafic vers le domaine afin de minimiser les interruptions de service.

Correction

Pour installer des mises à jour logicielles pour un OpenSearch domaine, consultez Démarrer une mise à jour dans le manuel Amazon OpenSearch Service Developer Guide.

[Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés

Exigences connexes : NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Faible

Type de ressource : `AWS::OpenSearch::Domain`

Règle AWS Config : `opensearch-primary-node-fault-tolerance`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un domaine Amazon OpenSearch Service est configuré avec au moins trois nœuds principaux dédiés. Le contrôle échoue si le domaine possède moins de trois nœuds principaux dédiés.

OpenSearch Le service utilise des nœuds principaux dédiés pour améliorer la stabilité du cluster. Un nœud principal dédié exécute les tâches de gestion du cluster, mais ne contient pas de données et ne répond pas aux demandes de téléchargement de données. Nous vous recommandons d'utiliser

le mode Multi-AZ en mode veille, qui ajoute trois nœuds principaux dédiés à chaque OpenSearch domaine de production.

Correction

Pour modifier le nombre de nœuds principaux d'un OpenSearch domaine, consultez la section Création et gestion de domaines Amazon OpenSearch Service dans le manuel Amazon OpenSearch Service Developer Guide.

Contrôles Security Hub CSPM pourCA privée AWS

Ces AWS Security Hub CSPM contrôles évaluent le service Autorité de certification privée AWS (CA privée AWS) et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Faible

Type de ressource : `AWS::ACMPCA::CertificateAuthority`

Règle AWS Config : `acm-pca-root-ca-disabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si CA privée AWS une autorité de certification racine (CA) est désactivée. Le contrôle échoue si l'autorité de certification racine est activée.

AvecCA privée AWS, vous pouvez créer une hiérarchie d'autorités de certification qui inclut une autorité de certification racine et des autorités de certification subordonnées. Vous devez minimiser l'utilisation de l'autorité de certification racine pour les tâches quotidiennes, en particulier dans les environnements de production. L'autorité de certification racine ne doit être utilisée que pour délivrer des certificats aux autorités de certification intermédiaires. Cela permet à l'autorité de certification racine d'être stockée hors du danger, tandis que les autorités de certification intermédiaires effectuent la tâche quotidienne d'émettre des certificats d'entité finale.

Correction

Pour désactiver l'autorité de certification racine, consultez la section Mettre à jour le statut de l'autorité de certification dans le guide de Autorité de certification privée AWS l'utilisateur.

[PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::ACMPCA::CertificateAuthority`

Règle AWS Config : `acmpca-certificate-authority-tagged`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une autorité de certification AWS privée CA possède des balises avec les clés spécifiques définies dans le paramètre`requiredKeyTags`. Le contrôle échoue si l'autorité de certification ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées dans le paramètre`requiredKeyTags`. Si le paramètre `requiredKeyTags` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'autorité de certification n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, consultez la section Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Meilleures pratiques et stratégies dans le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Correction

Pour ajouter des balises à une autorité de certification AWS privée, voir Ajouter des balises pour votre autorité de certification privée dans le guide de Autorité de certification privée AWS l'utilisateur.

Contrôles CSPM Security Hub pour Amazon RDS

Ces AWS Security Hub CSPM contrôles évaluent les ressources Amazon Relational Database Service (Amazon RDS) et Amazon RDS. Il se peut que les commandes ne soient pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[RDS.1] L'instantané RDS doit être privé

Exigences associées : PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,

NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

Règle AWS Config : `rds-snapshots-public-prohibited`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les instantanés Amazon RDS sont publics. Le contrôle échoue si les instantanés RDS sont publics. Ce contrôle évalue les instances RDS, les instances de base de données Aurora, les instances de base de données Neptune et les clusters Amazon DocumentDB.

Les instantanés RDS sont utilisés pour sauvegarder les données sur vos instances RDS à un moment donné. Ils peuvent être utilisés pour restaurer les états précédents des instances RDS.

Un instantané RDS ne doit pas être public si ce n'est pas prévu. Si vous partagez un instantané manuel non chiffré en tant que public, celui-ci est mis à la disposition de tous Comptes AWS. Cela peut entraîner une exposition involontaire des données de votre instance RDS.

Notez que si la configuration est modifiée pour autoriser l'accès public, la AWS Config règle risque de ne pas être en mesure de détecter le changement pendant 12 heures au maximum. Jusqu'à ce que la AWS Config règle détecte la modification, la vérification est réussie même si la configuration enfreint la règle.

Pour en savoir plus sur le partage d'un instantané de base de données, consultez la section Partager un instantané de base de données dans le guide de l'utilisateur Amazon RDS.

Correction

Pour supprimer l'accès public aux instantanés RDS, consultez la section Partage d'un instantané dans le guide de l'utilisateur Amazon RDS. Pour la visibilité des instantanés de base de données, nous avons choisi Privé.

[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.2.3, CIS AWS Foundations Benchmark v3.0. 0/2.3.3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/72.1.1, PCI DSS v4.0. 1/14,4

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-instance-public-access-check`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les instances Amazon RDS sont accessibles au public en évaluant le `PubliclyAccessible` champ de l'élément de configuration de l'instance.

La valeur `PubliclyAccessible` de la configuration de l'instance RDS indique si l'instance DB est publiquement accessible. Lorsque l'instance de base de données est configurée avec`PubliclyAccessible`, il s'agit d'une Internet-facing instance avec un nom DNS pouvant être résolu publiquement, qui se résout en une adresse IP publique. Lorsque l'instance de base de données n'est pas accessible publiquement, il s'agit d'une instance interne avec un nom DNS qui correspond à une adresse IP privée.

À moins que vous ne souhaitiez que votre instance RDS soit accessible au public, l'instance RDS ne doit pas être configurée avec une `PubliclyAccessible` valeur. Cela pourrait entraîner un trafic inutile vers votre instance de base de données.

Correction

Pour supprimer l'accès public aux instances de base de données RDS, consultez la section Modification d'une instance de base de données Amazon RDS dans le guide de l'utilisateur Amazon RDS. Pour Accès public, sélectionnez Non.

[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.2.1, CIS AWS Foundations Benchmark v3.0. 0/2.3.1, CIS AWS Foundations Benchmark v1.4. 0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-storage-encrypted`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement du stockage est activé pour vos instances de base de données Amazon RDS.

Ce contrôle est destiné aux instances de base de données RDS. Toutefois, il peut également générer des résultats pour les instances de base de données Aurora, les instances de base de données Neptune et les clusters Amazon DocumentDB. Si ces résultats ne sont pas utiles, vous pouvez les supprimer.

Pour une couche de sécurité supplémentaire pour vos données sensibles dans les instances DB RDS, vous devez configurer ces dernières pour qu'elles soient chiffrées au repos. Pour chiffrer vos instances et vos instantanés de base de données RDS au repos, activez l'option de chiffrement pour vos instances de base de données RDS. Les données qui sont chiffrées au repos incluent le stockage sous-jacent pour des instance DB, les sauvegardes automatisées, les réplicas en lecture et les instantanés.

Les instances de base de données chiffrées RDS utilisent l'algorithme de AES-256 chiffrement standard ouvert pour chiffrer vos données sur le serveur qui héberge vos instances de bases de données RDS. Une fois vos données chiffrées, Amazon RDS gère l'authentification de l'accès et le déchiffrement de vos données de manière transparente, avec un impact minimal sur les performances. Vous n'avez pas besoin de modifier vos applications clientes de base de données pour utiliser le chiffrement.

Le chiffrement Amazon RDS est actuellement disponible pour tous les moteurs de base de données et tous les types de stockage. Le chiffrement Amazon RDS est disponible pour la plupart des classes d'instance de base de données. Pour en savoir plus sur les classes d'instance de base de données qui ne prennent pas en charge le chiffrement Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Correction

Pour plus d'informations sur le chiffrement des instances de bases de données dans Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.4] Les instantanés du cluster RDS et les instantanés de base de données doivent être chiffrés au repos

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

Règle AWS Config : `rds-snapshot-encrypted`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un instantané de base de données RDS est chiffré. Le contrôle échoue si un instantané de base de données RDS n'est pas chiffré.

Ce contrôle est destiné aux instances de base de données RDS. Cependant, il peut également générer des résultats pour des instantanés d'instances de base de données Aurora, d'instances de base de données Neptune et de clusters Amazon DocumentDB. Si ces résultats ne sont pas utiles, vous pouvez les supprimer.

Le chiffrement des données au repos réduit le risque qu'un utilisateur non authentifié accède aux données stockées sur disque. Les données des instantanés RDS doivent être chiffrées au repos pour renforcer la sécurité.

Correction

Pour chiffrer un instantané RDS, consultez la section Chiffrement des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS. Lorsque vous chiffrez une instance de base de données RDS, les données chiffrées incluent le stockage sous-jacent de l'instance, ses sauvegardes automatisées, ses répliques de lecture et ses instantanés.

Vous ne pouvez chiffrer une instance de base de données RDS que lorsque vous la créez, et non après sa création. Cependant, parce que vous pouvez chiffrer une copie d'un instantané non chiffré, vous pouvez ajouter le chiffrement efficacement à une instance de base de données non chiffrée. Autrement dit, vous pouvez créer un instantané de votre instance de base de données et ensuite créer une copie chiffrée de l'instantané. Vous pouvez ensuite restaurer une instance de base de données à partir de l'instantané chiffré et vous aurez une copie chiffrée de votre instance de base de données d'origine.

[RDS.5] Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.2.4 NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-multi-az-support`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la haute disponibilité est activée pour vos instances de base de données RDS. Le contrôle échoue si une instance de base de données RDS n'est pas configurée avec plusieurs zones de disponibilité (AZ). Ce contrôle ne s'applique pas aux instances de base de données RDS qui font partie d'un déploiement de Multi-AZ cluster de bases de données.

La configuration des instances de base de données Amazon RDS avec AZs permet de garantir la disponibilité des données stockées. Multi-AZ les déploiements permettent un basculement

automatique en cas de problème de disponibilité des zones de disponibilité et lors de la maintenance RDS régulière.

Correction

Pour déployer vos instances de base de données dans plusieurs zones de disponibilité, consultez le guide de l'utilisateur Amazon RDS pour en faire un déploiement d' Multi-AZ instance de base de données.

[RDS.6] Une surveillance améliorée doit être configurée pour les instances de base de données RDS

Exigences connexes : NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-enhanced-monitoring-enabled`

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM	
`monitoringInterval`	Nombre de secondes entre les intervalles de collecte des métriques de surveillance	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Aucune valeur par défaut	

Ce contrôle vérifie si la surveillance améliorée est activée pour une instance de base de données Amazon Relational Database Service (Amazon RDS). Le contrôle échoue si la surveillance améliorée n'est pas activée pour l'instance. Si vous fournissez une valeur personnalisée pour le `monitoringInterval` paramètre, le contrôle ne passe que si des mesures de surveillance améliorées sont collectées pour l'instance à l'intervalle spécifié.

Dans Amazon RDS, la surveillance améliorée permet de réagir plus rapidement aux changements de performances de l'infrastructure sous-jacente. Ces changements de performances peuvent entraîner un manque de disponibilité des données. La surveillance améliorée fournit des mesures en temps réel du système d'exploitation sur lequel s'exécute votre instance de base de données RDS. Un agent est installé sur l'instance. L'agent peut obtenir des métriques de manière plus précise que ce qui est possible à partir de la couche hyperviseur.

Les métriques de la surveillance améliorée sont utiles pour évaluer l'utilisation de l'UC par différents processus ou threads sur une instance de base de données. Pour de plus amples informations sur la surveillance améliorée, veuillez consulter la rubrique Enhanced Monitoring (Surveillance améliorée) dans le Guide de l'utilisateur Amazon RDS.

Correction

Pour obtenir des instructions détaillées sur l'activation de la surveillance améliorée pour votre instance de base de données, consultez la section Configuration et activation de la surveillance améliorée dans le guide de l'utilisateur Amazon RDS.

[RDS.7] La protection contre la suppression des clusters RDS doit être activée

Exigences connexes : NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `rds-cluster-deletion-protection-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la protection contre la suppression est activée sur un cluster de bases de données RDS. Le contrôle échoue si la protection contre la suppression n'est pas activée sur un cluster de bases de données RDS.

Ce contrôle est destiné aux instances de base de données RDS. Toutefois, il peut également générer des résultats pour les instances de base de données Aurora, les instances de base de données Neptune et les clusters Amazon DocumentDB. Si ces résultats ne sont pas utiles, vous pouvez les supprimer.

L'activation de la protection contre la suppression des clusters constitue un niveau de protection supplémentaire contre la suppression accidentelle de la base de données ou la suppression par une entité non autorisée.

Lorsque la protection contre la suppression est activée, un cluster RDS ne peut pas être supprimé. Pour qu'une demande de suppression aboutisse, la protection contre la suppression doit être désactivée.

Correction

Pour activer la protection contre la suppression pour un cluster de bases de données RDS, consultez la section Modification du cluster de bases de données à l'aide de la console, de l'interface de ligne de commande et de l'API dans le guide de l'utilisateur Amazon RDS. Pour la protection contre la suppression, choisissez Activer la protection contre la suppression.

[RDS.8] La protection contre la suppression des instances de base de données RDS doit être activée

Exigences connexes : NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Faible

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-instance-deletion-protection-enabled`

Type de calendrier : Déclenché par un changement

Paramètres :

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (non personnalisable)

Ce contrôle vérifie si la protection contre la suppression est activée pour vos instances de base de données RDS qui utilisent l'un des moteurs de base de données répertoriés. Le contrôle échoue si la protection contre la suppression n'est pas activée pour une instance de base de données RDS.

L'activation de la protection contre la suppression des instances constitue un niveau de protection supplémentaire contre la suppression accidentelle de la base de données ou la suppression par une entité non autorisée.

Lorsque la protection contre la suppression est activée, une instance de base de données RDS ne peut pas être supprimée. Pour qu'une demande de suppression aboutisse, la protection contre la suppression doit être désactivée.

Correction

Pour activer la protection contre la suppression pour une instance de base de données RDS, consultez la section Modification d'une instance de base de données Amazon RDS dans le guide de l'utilisateur Amazon RDS. Pour la protection contre la suppression, choisissez Activer la protection contre la suppression.

[RDS.9] Les instances de base de données RDS doivent publier des CloudWatch journaux dans Logs

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.1.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-logging-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une instance de base de données Amazon RDS est configurée pour publier les journaux suivants sur Amazon CloudWatch Logs. Le contrôle échoue si l'instance n'est pas configurée pour publier les journaux suivants dans CloudWatch Logs :

- Oracle : alerte, audit, traçage, écouteur
- PostgreSQL : Postgresql, mise à niveau
- MySQL : audit, erreur, général, SlowQuery
- MariaDB : audit, erreur, général, SlowQuery
- SQL Server : erreur, agent

- Aurora-MySQL: Audit, Erreur, Général, SlowQuery
- Aurora-PostgreSQL: PostgreSQL

Les journaux pertinents doivent être activés dans les bases de données RDS. La journalisation de la base de données fournit des enregistrements détaillés des demandes adressées à RDS. Les journaux de base de données peuvent faciliter les audits de sécurité et d'accès et peuvent aider à diagnostiquer les problèmes de disponibilité.

Correction

Pour plus d'informations sur la publication des journaux de base de données RDS dans CloudWatch Logs, voir Spécifier les CloudWatch journaux à publier dans Logs dans le Guide de l'utilisateur Amazon RDS.

[RDS.10] L'authentification IAM doit être configurée pour les instances RDS

Exigences connexes : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Catégorie : Protéger > Gestion sécurisée des accès > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-instance-iam-authentication-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'authentification de base de données IAM est activée pour une instance de base de données RDS. Le contrôle échoue si l'authentification IAM n'est pas configurée pour les instances de base de données RDS. Ce contrôle évalue uniquement les instances RDS avec les types de moteurs suivants : `mysql`,`postgres`,`aurora`, `aurora-mysql`,`aurora-postgresql`, et`mariadb`. Une instance RDS doit également se trouver dans l'un des états suivants pour qu'une découverte soit générée : `available`,`backing-up`,`storage-optimization`, ou`storage-full`.

L'authentification de base de données IAM permet de s'authentifier auprès des instances de base de données à l'aide d'un jeton d'authentification au lieu d'un mot de passe. Le trafic réseau en provenance et à destination de la base de données est chiffré à l'aide du protocole SSL. Pour de plus

amples informations, veuillez consulter Authentification de base de données IAM dans le Guide de l'utilisateur Amazon Aurora.

Correction

Pour activer l'authentification de base de données IAM sur une instance de base de données RDS, consultez Activation et désactivation de l'authentification de base de données IAM dans le guide de l'utilisateur Amazon RDS.

[RDS.11] Les sauvegardes automatiques doivent être activées sur les instances RDS

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `db-instance-backup-enabled`

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`backupRetentionMinimum`	Durée minimale de conservation des sauvegardes en jours	Entier	`7` sur `35`	`7`
`checkReadReplicas`	Vérifie si les sauvegardes des instances de base de données RDS sont activées pour les répliques en lecture	Booléen	Non personnalisable	`false`

Ce contrôle vérifie si les sauvegardes automatiques sont activées et si une période de conservation des sauvegardes est supérieure ou égale à la période spécifiée pour une instance Amazon Relational Database Service. Les répliques lues sont exclues de l'évaluation. Le contrôle échoue si les sauvegardes ne sont pas activées pour l'instance ou si la période de rétention est inférieure à la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de conservation des sauvegardes, Security Hub CSPM utilise une valeur par défaut de 7 jours.

Les sauvegardes vous aident à vous rétablir plus rapidement après un incident de sécurité et renforcent la résilience de vos systèmes. Amazon RDS vous permet de configurer des instantanés quotidiens complets du volume d'instance. Pour plus d'informations sur les sauvegardes automatisées Amazon RDS, consultez la section Utilisation des sauvegardes dans le guide de l'utilisateur Amazon RDS.

Correction

Pour activer les sauvegardes automatisées sur une instance de base de données RDS, consultez la section Activation des sauvegardes automatisées dans le guide de l'utilisateur Amazon RDS.

[RDS.12] L'authentification IAM doit être configurée pour les clusters RDS

Exigences connexes : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Catégorie : Protéger > Gestion sécurisée des accès > Authentification sans mot de passe

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `rds-cluster-iam-authentication-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'authentification de base de données IAM est activée sur un cluster de bases de données Amazon RDS.

L'authentification de base de données IAM permet une authentification sans mot de passe pour les instances de base de données. L'authentification utilise un jeton d'authentification. Le trafic réseau en

provenance et à destination de la base de données est chiffré à l'aide du protocole SSL. Pour de plus amples informations, veuillez consulter Authentification de base de données IAM dans le Guide de l'utilisateur Amazon Aurora.

Correction

Pour activer l'authentification IAM pour un cluster de bases de données, consultez la section Activation et désactivation de l'authentification de base de données IAM dans le guide de l'utilisateur Amazon Aurora.

[RDS.13] Les mises à niveau automatiques des versions mineures de RDS doivent être activées

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.2.2, CIS AWS Foundations Benchmark v3.0. 0/2.3.2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS version 4.0. 1/63.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-automatic-minor-version-upgrade-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les mises à niveau automatiques des versions mineures sont activées sur une instance de base de données Amazon RDS. Le contrôle échoue si les mises à niveau automatiques des versions mineures ne sont pas activées pour l'instance de base de données RDS.

> **Note**
>
> Ce contrôle évalue chaque instance de base de données Amazon RDS indépendamment. Pour les clusters Amazon Aurora, les mises à niveau automatiques des versions mineures nécessitent que vous activiez ce paramètre sur le cluster. Vous devez également activer ce paramètre sur toutes les instances du cluster. La `PASSED` découverte d'une instance individuelle ne garantit pas que les mises à niveau se produiront si vous n'avez pas également activé le paramètre au niveau du cluster.

Ce contrôle ne prend pas non plus en compte les configurations qui ne prennent pas en charge les mises à niveau automatiques des versions mineures. Il s'agit notamment des clusters Aurora dans une base de données globale Aurora et des clusters Aurora MySQL avec des répliques de lecture interrégionales. Pour ces configurations, le contrôle peut produire des résultats d'évaluation qui ne reflètent pas exactement le comportement réel de mise à niveau.

Les mises à niveau automatiques des versions mineures mettent régulièrement à jour une base de données vers les versions les plus récentes du moteur de base de données. Toutefois, la mise à niveau n'inclut pas toujours la dernière version du moteur de base de données. Si vous devez conserver des versions spécifiques de vos bases de données à un moment donné, nous vous recommandons de procéder à une mise à niveau manuelle vers les versions de base de données dont vous avez besoin conformément au calendrier requis. En cas de problèmes de sécurité critiques ou lorsqu'une version atteint sa date de fin de support, Amazon RDS peut appliquer une mise à niveau mineure même si vous n'avez pas activé l'option de mise à niveau automatique des versions mineures. Pour plus d'informations, consultez la documentation de mise à niveau d'Amazon RDS pour votre moteur de base de données spécifique :

- Mises à niveau automatiques des versions mineures de RDS pour MariaDB
- Mises à niveau automatiques des versions mineures pour RDS pour MySQL
- Mises à niveau automatiques des versions mineures de RDS pour PostgreSQL
- Db2 sur les versions d'Amazon RDS
- Mises à niveau des versions mineures d'Oracle
- Mises à niveau du moteur de base de données Microsoft SQL Server

Correction

Pour activer les mises à niveau automatiques des versions mineures pour une instance de base de données existante, consultez la section Modification d'une instance de base de données Amazon RDS dans le guide de l'utilisateur Amazon RDS. Pour la mise à niveau automatique de la version mineure, sélectionnez Oui.

[RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `aurora-mysql-backtracking-enabled`

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM	
`BacktrackWindowInHours`	Nombre d'heures nécessaires pour revenir en arrière sur un cluster Aurora MySQL	Double	`0`.1 sur 72	Aucune valeur par défaut	

Ce contrôle vérifie si le retour en arrière est activé sur un cluster Amazon Aurora. Le contrôle échoue si le retour en arrière n'est pas activé sur le cluster. Si vous fournissez une valeur personnalisée pour le `BacktrackWindowInHours` paramètre, le contrôle n'est transmis que si le cluster est suivi en arrière pendant la durée spécifiée.

Les sauvegardes vous permettent de récupérer plus rapidement après un incident de sécurité. Ils renforcent également la résilience de vos systèmes. Le retour en arrière d'Aurora réduit le temps nécessaire à la restauration d'une base de données à un moment précis. Pour ce faire, il n'est pas nécessaire de restaurer la base de données.

Correction

Pour activer le retour en arrière avec Aurora, consultez la section Configuration du retour en arrière dans le guide de l'utilisateur Amazon Aurora.

Notez que vous ne pouvez pas activer le retour en arrière sur un cluster existant. Vous pouvez plutôt créer un clone sur lequel le retour en arrière est activé. Pour plus d'informations sur les limites du retour en arrière d'Aurora, consultez la liste des limitations dans Présentation du retour en arrière.

[RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.2.4 NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `rds-cluster-multi-az-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la haute disponibilité est activée pour vos clusters de bases de données RDS. Le contrôle échoue si aucun cluster de base de données RDS n'est déployé dans plusieurs zones de disponibilité (AZ).

Les clusters de bases de données RDS doivent être configurés pour plusieurs AZ afin de garantir la disponibilité des données stockées. Le déploiement sur plusieurs zones de disponibilité permet un basculement automatique en cas de problème de disponibilité d'une zone de disponibilité et lors d'événements de maintenance RDS réguliers.

Correction

Pour déployer vos clusters de bases de données dans plusieurs zones de disponibilité, consultez le guide de l'utilisateur Amazon RDS pour en faire un déploiement d' Multi-AZ instance de base de données.

Les étapes de correction diffèrent pour les bases de données globales Aurora. Pour configurer plusieurs zones de disponibilité pour une base de données globale Aurora, sélectionnez votre cluster de bases de données. Choisissez ensuite Actions et Ajouter un lecteur, puis spécifiez plusieurs AZ. Pour plus d'informations, consultez la section Ajouter des réplicas Aurora à un cluster de bases de données dans le guide de l'utilisateur Amazon Aurora.

[RDS.16] Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier - Inventaire

Gravité : Faible

Type de ressource : `AWS::RDS::DBCluster`

AWS Config règle : `rds-cluster-copy-tags-to-snapshots-enabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données Amazon Aurora est configuré pour copier automatiquement les balises dans les instantanés du cluster de bases de données lorsque les instantanés sont créés. Le contrôle échoue si le cluster de base de données Aurora n'est pas configuré pour copier automatiquement les balises dans les instantanés du cluster lors de leur création.

L'identification et l'inventaire de vos actifs informatiques constituent un aspect crucial de la gouvernance et de la sécurité. Vous devez avoir une visibilité sur tous vos clusters de base de données Amazon Aurora afin de pouvoir évaluer leur niveau de sécurité et prendre des mesures sur les points faibles potentiels. Les instantanés de base de données Aurora doivent avoir les mêmes balises que leurs clusters de bases de données parents. Dans Amazon Aurora, vous pouvez configurer un cluster de base de données pour copier automatiquement toutes les balises du cluster dans des instantanés du cluster. L'activation de ce paramètre garantit que les instantanés de base de données héritent des mêmes balises que leurs clusters de bases de données parents.

Correction

Pour plus d'informations sur la configuration d'un cluster de base de données Amazon Aurora afin de copier automatiquement les balises dans les instantanés de base de données, consultez la section Modification d'un cluster de bases de données Amazon Aurora dans le guide de l'utilisateur Amazon Aurora.

[RDS.17] Les instances de base de données RDS doivent être configurées pour copier les balises dans les instantanés

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Catégorie : Identifier - Inventaire

Gravité : Faible

Type de ressource : `AWS::RDS::DBInstance`

AWS Config règle : `rds-instance-copy-tags-to-snapshots-enabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les instances de base de données RDS sont configurées pour copier toutes les balises dans les instantanés lorsque ceux-ci sont créés.

L'identification et l'inventaire de vos actifs informatiques constituent un aspect crucial de la gouvernance et de la sécurité. Vous devez avoir une visibilité sur toutes vos instances de base de données RDS afin de pouvoir évaluer leur niveau de sécurité et prendre des mesures sur les points faibles potentiels. Les instantanés doivent être balisés de la même manière que leurs instances de base de données RDS parentes. L'activation de ce paramètre garantit que les instantanés héritent des balises de leurs instances de base de données parentes.

Correction

Pour copier automatiquement les balises dans les instantanés d'une instance de base de données RDS, consultez la section Modification d'une instance de base de données Amazon RDS dans le guide de l'utilisateur Amazon RDS. Sélectionnez Copier les balises dans les instantanés.

[RDS.19] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements de cluster critiques

Exigences connexes : NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Catégorie : Détection > Services de détection > Surveillance des applications

Gravité : Faible

Type de ressource : `AWS::RDS::EventSubscription`

AWS Config règle : `rds-cluster-event-notifications-configured` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un abonnement à un événement Amazon RDS existant pour les clusters de bases de données comporte des notifications activées pour les paires clé-valeur de type de source et de catégorie d'événement suivantes :

```
DBCluster: ["maintenance","failure"]
```

Le contrôle passe s'il n'y a aucun abonnement à un événement existant sur votre compte.

Les notifications d'événements RDS utilisent Amazon SNS pour vous informer des modifications apportées à la disponibilité ou à la configuration de vos ressources RDS. Ces notifications permettent une réponse rapide. Pour plus d'informations sur les notifications d'événements RDS, consultez la section Utilisation de la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Correction

Pour vous abonner aux notifications d'événements de cluster RDS, consultez la section S'abonner à la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS. Utilisez les valeurs suivantes :

Champ	Value
Source type (Type de source)	Clusters
Clusters à inclure	Tous les clusters
Catégories d'événements à inclure	Sélectionnez des catégories d'événements spécifiques ou Toutes les catégories d'événements

[RDS.20] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques

Exigences associées : NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115,2

Catégorie : Détection > Services de détection > Surveillance des applications

Gravité : Faible

Type de ressource : `AWS::RDS::EventSubscription`

AWS Config règle : `rds-instance-event-notifications-configured` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un abonnement à un événement Amazon RDS existant pour les instances de base de données comporte des notifications activées pour les paires clé-valeur de type de source et de catégorie d'événement suivantes :

```
DBInstance: ["maintenance","configuration change","failure"]
```

Le contrôle passe s'il n'y a aucun abonnement à un événement existant sur votre compte.

Les notifications d'événements RDS utilisent Amazon SNS pour vous informer des modifications apportées à la disponibilité ou à la configuration de vos ressources RDS. Ces notifications permettent une réponse rapide. Pour plus d'informations sur les notifications d'événements RDS, consultez la section Utilisation de la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Correction

Pour vous abonner aux notifications d'événements d'instance RDS, consultez la section S'abonner à la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS. Utilisez les valeurs suivantes :

Champ	Value
Source type (Type de source)	instances
Instances à inclure	Toutes les instances
Catégories d'événements à inclure	Sélectionnez des catégories d'événements spécifiques ou Toutes les catégories d'événements

[RDS.21] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de groupe de paramètres de base de données critiques

Exigences associées : NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115,2

Catégorie : Détection > Services de détection > Surveillance des applications

Gravité : Faible

Type de ressource : `AWS::RDS::EventSubscription`

AWS Config règle : `rds-pg-event-notifications-configured` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie s'il existe un abonnement à un événement Amazon RDS avec des notifications activées pour le type de source suivant, les paires clé-valeur de catégorie d'événement. Le contrôle passe s'il n'y a aucun abonnement à un événement existant sur votre compte.

```
DBParameterGroup: ["configuration change"]
```

Les notifications d'événements RDS utilisent Amazon SNS pour vous informer des modifications apportées à la disponibilité ou à la configuration de vos ressources RDS. Ces notifications permettent une réponse rapide. Pour plus d'informations sur les notifications d'événements RDS, consultez la section Utilisation de la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Correction

Pour vous abonner aux notifications d'événements du groupe de paramètres de base de données RDS, consultez la section S'abonner à la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS. Utilisez les valeurs suivantes :

Champ	Value
Source type (Type de source)	Groupes de paramètres
Groupes de paramètres à inclure	Tous les groupes de paramètres

Champ	Value
Catégories d'événements à inclure	Sélectionnez des catégories d'événements spécifiques ou Toutes les catégories d'événements

[RDS.22] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements critiques du groupe de sécurité des bases de données

Exigences associées : NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115,2

Catégorie : Détection > Services de détection > Surveillance des applications

Gravité : Faible

Type de ressource : `AWS::RDS::EventSubscription`

AWS Config règle : `rds-sg-event-notifications-configured` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie s'il existe un abonnement à un événement Amazon RDS avec des notifications activées pour le type de source suivant, les paires clé-valeur de catégorie d'événement. Le contrôle passe s'il n'y a aucun abonnement à un événement existant sur votre compte.

```
DBSecurityGroup: ["configuration change","failure"]
```

Les notifications d'événements RDS utilisent Amazon SNS pour vous informer des modifications apportées à la disponibilité ou à la configuration de vos ressources RDS. Ces notifications permettent une réponse rapide. Pour plus d'informations sur les notifications d'événements RDS, consultez la section Utilisation de la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Correction

Pour vous abonner aux notifications d'événements d'instance RDS, consultez la section S'abonner à la notification d'événements Amazon RDS dans le guide de l'utilisateur Amazon RDS. Utilisez les valeurs suivantes :

Champ	Value
Source type (Type de source)	Groupes de sécurité
Groupes de sécurité à inclure	Tous les groupes de sécurité
Catégories d'événements à inclure	Sélectionnez des catégories d'événements spécifiques ou Toutes les catégories d'événements

[RDS.23] Les instances RDS ne doivent pas utiliser le port par défaut d'un moteur de base de données

Exigences connexes : NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Faible

Type de ressource : `AWS::RDS::DBInstance`

AWS Config règle : `rds-no-default-ports` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster ou une instance RDS utilise un port autre que le port par défaut du moteur de base de données. Le contrôle échoue si le cluster ou l'instance RDS utilise le port par défaut. Ce contrôle ne s'applique pas aux instances RDS qui font partie d'un cluster.

Si vous utilisez un port connu pour déployer un cluster ou une instance RDS, un attaquant peut deviner des informations sur le cluster ou l'instance. L'attaquant peut utiliser ces informations conjointement avec d'autres informations pour se connecter à un cluster ou à une instance RDS ou obtenir des informations supplémentaires sur votre application.

Lorsque vous modifiez le port, vous devez également mettre à jour les chaînes de connexion existantes qui ont été utilisées pour vous connecter à l'ancien port. Vous devez également vérifier le

groupe de sécurité de l'instance de base de données pour vous assurer qu'il inclut une règle d'entrée qui autorise la connectivité sur le nouveau port.

Correction

Pour modifier le port par défaut d'une instance de base de données RDS existante, consultez la section Modification d'une instance de base de données Amazon RDS dans le guide de l'utilisateur Amazon RDS. Pour modifier le port par défaut d'un cluster de bases de données RDS existant, consultez la section Modification du cluster de bases de données à l'aide de la console, de l'interface de ligne de commande et de l'API dans le guide de l'utilisateur Amazon Aurora. Pour Port de base de données, remplacez la valeur du port par une valeur autre que celle par défaut.

[RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.2

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : `rds-cluster-default-admin-check`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de bases de données Amazon RDS a modifié le nom d'utilisateur administrateur par rapport à sa valeur par défaut. Le contrôle ne s'applique pas aux moteurs de type neptune (Neptune DB) ou docdb (DocumentDB). Cette règle échouera si le nom d'utilisateur de l'administrateur est défini sur la valeur par défaut.

Lorsque vous créez une base de données Amazon RDS, vous devez remplacer le nom d'utilisateur administrateur par défaut par une valeur unique. Les noms d'utilisateur par défaut sont connus du public et doivent être modifiés lors de la création de la base de données RDS. La modification des noms d'utilisateur par défaut réduit le risque d'accès involontaire.

Correction

Pour modifier le nom d'utilisateur administrateur associé au cluster de bases de données Amazon RDS, créez un nouveau cluster de bases de données RDS et modifiez le nom d'utilisateur administrateur par défaut lors de la création de la base de données.

[RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.2

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : `rds-instance-default-admin-check`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si vous avez modifié le nom d'utilisateur administratif pour les instances de base de données Amazon Relational Database Service (Amazon RDS) par rapport à la valeur par défaut. Le contrôle échoue si le nom d'utilisateur administratif est défini sur la valeur par défaut. Le contrôle ne s'applique pas aux moteurs de type neptune (Neptune DB) ou docdb (DocumentDB), ni aux instances RDS qui font partie d'un cluster.

Les noms d'utilisateur administratifs par défaut sur les bases de données Amazon RDS sont connus du public. Lorsque vous créez une base de données Amazon RDS, vous devez remplacer le nom d'utilisateur administratif par défaut par une valeur unique afin de réduire le risque d'accès involontaire.

Correction

Pour modifier le nom d'utilisateur administratif associé à une instance de base de données RDS, créez d'abord une nouvelle instance de base de données RDS. Modifiez le nom d'utilisateur administratif par défaut lors de la création de la base de données.

[RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde

Catégorie : Restauration > Résilience > Sauvegardes activées

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

AWS Config règle : `rds-resources-protected-by-backup-plan`

Type de programme : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`backupVaultLockCheck`	Le contrôle produit un `PASSED` résultat si le paramètre est défini sur true et que la ressource utilise AWS Backup Vault Lock.	Booléen	`true` ou `false`	Aucune valeur par défaut

Ce contrôle évalue si les instances de base de données Amazon RDS sont couvertes par un plan de sauvegarde. Ce contrôle échoue si l'instance de base de données RDS n'est pas couverte par un plan de sauvegarde. Si vous définissez le `backupVaultLockCheck` paramètre sur`true`, le contrôle n'est transmis que si l'instance est sauvegardée dans un coffre-fort AWS Backup verrouillé.

> **Note**
>
> Ce contrôle n'évalue pas les instances Neptune et DocumentDB. Il n'évalue pas non plus les instances de base de données RDS qui sont membres d'un cluster.

AWS Backup est un service de sauvegarde entièrement géré qui centralise et automatise la sauvegarde des données entre. Services AWS Avec AWS Backup, vous pouvez créer des politiques

de sauvegarde appelées plans de sauvegarde. Vous pouvez utiliser ces plans pour définir vos besoins en matière de sauvegarde, notamment la fréquence de sauvegarde de vos données et la durée de conservation de ces sauvegardes. L'inclusion d'instances de base de données RDS dans un plan de sauvegarde vous permet de protéger vos données contre toute perte ou suppression involontaire.

Correction

Pour ajouter une instance de base de données RDS à un plan de AWS Backup sauvegarde, consultez la section Affectation de ressources à un plan de sauvegarde dans le Guide du AWS Backup développeur.

[RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

AWS Config règle : `rds-cluster-encrypted-at-rest`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données RDS est chiffré au repos. Le contrôle échoue si un cluster de base de données RDS n'est pas chiffré au repos.

Les données au repos font référence à toutes les données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement vous aide à protéger la confidentialité de ces données, réduisant ainsi le risque qu'un utilisateur non autorisé puisse y accéder. Le chiffrement de vos clusters de bases de données RDS protège vos données et vos métadonnées contre tout accès non autorisé. Il répond également aux exigences de conformité pour le chiffrement des données au repos des systèmes de fichiers de production.

Correction

Vous pouvez activer le chiffrement au repos lorsque vous créez un cluster de bases de données RDS. Vous ne pouvez pas modifier les paramètres de chiffrement après avoir créé un cluster. Pour

plus d'informations, consultez la section Chiffrement d'un cluster de bases de données Amazon Aurora dans le guide de l'utilisateur Amazon Aurora.

[RDS.28] Les clusters de bases de données RDS doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBCluster`

AWS Config règle : `tagged-rds-dbcluster` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un cluster de bases de données Amazon RDS possède des balises dont les clés spécifiques sont définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le cluster de bases de données ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le cluster de bases de données n'est balisé par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif,

propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un cluster de bases de données RDS, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.29] Les instantanés du cluster de bases de données RDS doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBClusterSnapshot`

AWS Config règle : `tagged-rds-dbclustersnapshot` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un instantané de cluster de bases de données Amazon RDS possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le snapshot du cluster de bases de données ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'instantané du cluster de bases de données n'est balisé avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses

personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un instantané de cluster de bases de données RDS, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.30] Les instances de base de données RDS doivent être balisées

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBInstance`

AWS Config règle : `tagged-rds-dbinstance` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une instance de base de données Amazon RDS possède des balises dont les clés spécifiques sont définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'instance de base de données ne possède aucune clé de balise ou si elle ne possède pas toutes les clés

spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'instance de base de données n'est balisée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une instance de base de données RDS, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.31] Les groupes de sécurité RDS DB doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBSecurityGroup`

AWS Config règle : `tagged-rds-dbsecuritygroup` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de sécurité Amazon RDS DB possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le groupe de sécurité de base de données ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de sécurité de la base de données n'est balisé par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe de sécurité de base de données RDS, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.32] Les instantanés de base de données RDS doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBSnapshot`

AWS Config règle : `tagged-rds-dbsnapshot` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un instantané de base de données Amazon RDS possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le snapshot de base de données ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'instantané de base de données n'est balisé avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un instantané de base de données RDS, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.33] Les groupes de sous-réseaux de base de données RDS doivent être balisés

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBSubnetGroup`

AWS Config règle : `tagged-rds-dbsubnetgroups` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise non système que la ressource évaluée doit contenir. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de sous-réseaux de base de données Amazon RDS possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le groupe de sous-réseaux de base de données ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de sous-réseaux de base de données n'est balisé par aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les actions et les notifications des propriétaires de ressources responsables. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises à des entités IAM (utilisateurs ou rôles) et à AWS des ressources. Vous pouvez créer une politique ABAC unique ou un ensemble distinct de politiques pour vos responsables IAM. Vous

pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert l'ABAC ? AWSdans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les balises sont accessibles à de nombreuses personnes Services AWS, y compris AWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, voir Marquer vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe de sous-réseaux de base de données RDS, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.1.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

AWS Config règle : `rds-aurora-mysql-audit-logging-enabled`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de base de données Amazon Aurora MySQL est configuré pour publier des journaux d'audit sur Amazon CloudWatch Logs. Le contrôle échoue si le cluster n'est pas

configuré pour publier les journaux d'audit dans CloudWatch Logs. Le contrôle ne génère pas de résultats pour les clusters de bases de données Aurora Serverless v1.

Les journaux d'audit enregistrent l'activité de la base de données, y compris les tentatives de connexion, les modifications de données, les modifications de schéma et d'autres événements qui peuvent être audités à des fins de sécurité et de conformité. Lorsque vous configurez un cluster de bases de données Aurora MySQL pour publier des journaux d'audit dans un groupe de CloudWatch journaux dans Amazon Logs, vous pouvez effectuer une analyse en temps réel des données du journal. CloudWatch Logs conserve les bûches dans un espace de stockage très durable. Vous pouvez également créer des alarmes et afficher des mesures dans CloudWatch.

> **Note**
>
> Une autre méthode pour publier des journaux d'audit dans CloudWatch Logs consiste à activer l'audit avancé et à définir le paramètre DB au niveau du cluster sur. `server_audit_logs_upload` 1 La valeur par défaut pour le `server_audit_logs_upload parameter` est`0`. Toutefois, nous vous recommandons d'utiliser plutôt les instructions de correction suivantes pour passer ce contrôle.

Correction

Pour publier les journaux d'audit des clusters de bases de données Aurora MySQL dans CloudWatch Logs, consultez la section Publication des journaux Amazon Aurora MySQL sur Amazon CloudWatch Logs dans le guide de l'utilisateur Amazon Aurora.

[RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée

Exigences associées : NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

AWS Config règle : `rds-cluster-auto-minor-version-upgrade-enable`

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la mise à niveau automatique des versions mineures est activée pour un cluster de bases de données Amazon RDS, y compris les clusters de base de données Aurora. Le contrôle échoue si la mise à niveau automatique des versions mineures n'est pas activée pour le cluster de bases de données.

Grâce à la mise à niveau automatique des versions mineures, vous pouvez maintenir votre cluster de bases de données à jour. Les versions mineures peuvent introduire de nouvelles fonctionnalités logicielles, des corrections de bogues, des correctifs de sécurité et des améliorations de performances. En activant la mise à niveau automatique des versions mineures sur les clusters de bases de données RDS, le cluster, ainsi que les instances du cluster, recevront des mises à jour automatiques de la version mineure lorsque de nouvelles versions seront disponibles. Les mises à jour sont appliquées automatiquement pendant la fenêtre de maintenance.

Correction

Pour activer la mise à niveau automatique des versions mineures sur les clusters de Multi-AZ bases de données, consultez la section Modification d'un Multi-AZ cluster de bases de données dans le guide de l'utilisateur Amazon RDS.

Pour activer la mise à niveau automatique des versions mineures sur les clusters de bases de données Aurora, consultez la section Modification d'un cluster de bases de données Amazon Aurora dans le guide de l'utilisateur Amazon Aurora.

[RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch

Exigences associées : PCI DSS v4.0. 1/104,2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-postgresql-logs-to-cloudwatch

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`logTypes`	Comma-separated liste des types de journaux à publier dans CloudWatch Logs	StringList	Non personnalisable	`postgresql`

Ce contrôle vérifie si une instance de base de données Amazon RDS pour PostgreSQL est configurée pour publier des journaux sur Amazon CloudWatch Logs. Le contrôle échoue si l'instance de base de données PostgreSQL n'est pas configurée pour publier les types de journaux mentionnés dans le `logTypes` paramètre de CloudWatch Logs.

La journalisation de la base de données fournit des enregistrements détaillés des demandes adressées à une instance RDS. PostgreSQL génère des journaux d'événements contenant des informations utiles pour les administrateurs. La publication de ces CloudWatch journaux dans Logs centralise la gestion des journaux et vous permet d'effectuer une analyse en temps réel des données des journaux. CloudWatch Logs conserve les bûches dans un espace de stockage très durable. Vous pouvez également créer des alarmes et afficher des mesures dansCloudWatch.

Correction

Pour publier les journaux d'instance de bases de données PostgreSQL dans CloudWatch Logs, consultez la section Publication des journaux PostgreSQL dans le guide CloudWatch de l'utilisateur Amazon RDS.

[RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch

Exigences associées : PCI DSS v4.0. 1/104,2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : rds-aurora-postgresql-logs-to-cloudwatch

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de bases de données Amazon Aurora PostgreSQL est configuré pour publier des journaux sur Amazon CloudWatch Logs. Le contrôle échoue si le cluster de base de données Aurora PostgreSQL n'est pas configuré pour publier les journaux PostgreSQL dans Logs. CloudWatch

La journalisation de la base de données fournit des enregistrements détaillés des demandes adressées à un cluster RDS. Aurora PostgreSQL génère des journaux d'événements contenant des informations utiles pour les administrateurs. La publication de ces CloudWatch journaux dans Logs centralise la gestion des journaux et vous permet d'effectuer une analyse en temps réel des données des journaux. CloudWatch Logs conserve les bûches dans un espace de stockage très durable. Vous pouvez également créer des alarmes et afficher des mesures dans CloudWatch.

Correction

Pour publier les journaux du cluster de bases de données Aurora PostgreSQL dans Logs, consultez la section Publication des CloudWatch journaux Aurora PostgreSQL sur CloudWatch Amazon Logs dans le guide de l'utilisateur Amazon RDS.

[RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-postgres-instance-encrypted-in-transit

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si une connexion à une instance Amazon RDS for PostgreSQL de base de données (DB) est chiffrée en transit. Le contrôle échoue si le `rds.force_ssl` paramètre du groupe de paramètres associé à l'instance est défini sur `0` (désactivé). Ce contrôle n'évalue pas les instances de base de données RDS qui font partie d'un cluster de bases de données.

Les données en transit font référence aux données qui se déplacent d'un endroit à un autre, par exemple entre les nœuds de votre cluster ou entre votre cluster et votre application. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque qu'un utilisateur non autorisé puisse espionner le trafic réseau.

Correction

Pour exiger que toutes les connexions à votre instance de base de données RDS pour PostgreSQL utilisent le protocole SSL, consultez la section Utilisation du protocole SSL avec une instance de base de données PostgreSQL dans le guide de l'utilisateur Amazon RDS.

[RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-mysql-instance-encrypted-in-transit

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si une connexion à une instance Amazon RDS for MySQL de base de données (DB) est chiffrée en transit. Le contrôle échoue si le `rds.require_secure_transport` paramètre du groupe de paramètres associé à l'instance est défini sur `0` (désactivé). Ce contrôle n'évalue pas les instances de base de données RDS qui font partie d'un cluster de bases de données.

Les données en transit font référence aux données qui se déplacent d'un endroit à un autre, par exemple entre les nœuds de votre cluster ou entre votre cluster et votre application. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque qu'un utilisateur non autorisé puisse espionner le trafic réseau.

Correction

Pour exiger que toutes les connexions à votre instance de base de données RDS pour MySQL utilisent le protocole SSL, consultez la section relative à la prise en SSL/TLS charge des instances de bases de données MySQL sur Amazon RDS dans le guide de l'utilisateur Amazon RDS.

[RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs

Exigences connexes : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-sql-server-logs-to-cloudwatch

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`logTypes`	Liste des types de journaux qu'une instance de base de données RDS pour SQL Server doit être configurée pour publier dans CloudWatch Logs. Ce contrôle échoue si une instance de base de données n'est pas configurée pour publier un type de journal spécifié dans la liste.	EnumList (maximum de 2 articles)	`agent`, `error`	`agent`, `error`

Ce contrôle vérifie si une instance de base de données Amazon RDS pour Microsoft SQL Server est configurée pour publier des CloudWatch journaux sur Amazon Logs. Le contrôle échoue si l'instance

de base de données RDS pour SQL Server n'est pas configurée pour publier des CloudWatch journaux dans Logs. Vous pouvez éventuellement spécifier les types de journaux qu'une instance de base de données doit être configurée pour publier.

La journalisation de la base de données fournit des enregistrements détaillés des demandes adressées à une instance de base de données Amazon RDS. La publication des CloudWatch journaux dans Logs centralise la gestion des journaux et vous permet d'effectuer une analyse en temps réel des données des journaux. CloudWatch Logs conserve les bûches dans un espace de stockage très durable. En outre, vous pouvez l'utiliser pour créer des alarmes pour des erreurs spécifiques qui peuvent survenir, telles que les redémarrages fréquents enregistrés dans un journal des erreurs. De même, vous pouvez créer des alarmes pour les erreurs ou les avertissements enregistrés dans les journaux de l'agent SQL Server liés aux tâches de l'agent SQL.

Correction

Pour plus d'informations sur la publication de journaux dans les CloudWatch journaux d'une instance de base de données RDS pour SQL Server, consultez les fichiers journaux de base de données Amazon RDS pour Microsoft SQL Server dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-sqlserver-encrypted-in-transit

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si une connexion à une instance de base de données Amazon RDS pour Microsoft SQL Server est chiffrée en transit. Le contrôle échoue si le `rds.force_ssl` paramètre du groupe de paramètres associé à l'instance de base de données est défini sur`0 (off)`.

Les données en transit font référence aux données qui se déplacent d'un emplacement à un autre, par exemple entre les nœuds d'un cluster de bases de données ou entre un cluster de bases de

données et une application cliente. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque que des utilisateurs non autorisés écoutent le trafic réseau.

Correction

Pour plus d'informations sur l'activation SSL/TLS des connexions aux instances de bases de données Amazon RDS exécutant Microsoft SQL Server, consultez la section Utilisation du protocole SSL avec une instance de base de données Microsoft SQL Server dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch

Exigences connexes : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : mariadb-publish-logs-to-cloudwatch-logs

Type de programme : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`logTypes`	Liste des types de journaux qu'une instance de base de données MariaDB doit être configurée pour CloudWatch	EnumList (maximum de 4 articles)	`audit`, `error`, `general`, `slowquery`	`audit`, `error`

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
	publier dans Logs. Le contrôle génère une détection `FAILED` si une instance de base de données n'est pas configurée pour publier un type de journal spécifié dans la liste.			

Ce contrôle vérifie si une instance de base de données Amazon RDS pour MariaDB est configurée pour publier certains types de journaux sur Amazon CloudWatch Logs. Le contrôle échoue si l'instance de base de données MariaDB n'est pas configurée pour publier les journaux dans Logs. CloudWatch Vous pouvez éventuellement spécifier les types de journaux qu'une instance de base de données MariaDB doit être configurée pour publier.

La journalisation de la base de données fournit des enregistrements détaillés des demandes adressées à une instance de base de données Amazon RDS pour MariaDB. La publication de CloudWatch journaux sur Amazon Logs centralise la gestion des journaux et vous permet d'effectuer une analyse en temps réel des données des journaux. En outre, CloudWatch Logs conserve les journaux dans un espace de stockage durable, ce qui permet de prendre en charge les examens et les audits de sécurité, d'accès et de disponibilité. Avec CloudWatch Logs, vous pouvez également créer des alarmes et consulter des mesures.

Correction

Pour plus d'informations sur la configuration d'une instance de base de données Amazon RDS pour MariaDB afin de publier des journaux sur Amazon Logs, consultez la section Publication de CloudWatch journaux MariaDB sur Amazon Logs dans le guide de l' CloudWatch utilisateur d'Amazon Relational Database Service.

[RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBProxy`

Règle AWS Config : rds-proxy-tls-encryption

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un proxy de base de données Amazon RDS nécessite le protocole TLS pour toutes les connexions entre le proxy et l'instance de base de données RDS sous-jacente. Le contrôle échoue si le proxy ne nécessite pas le protocole TLS pour toutes les connexions entre le proxy et l'instance de base de données RDS.

Amazon RDS Proxy peut constituer une couche de sécurité supplémentaire entre les applications clientes et les instances de base de données RDS sous-jacentes. Par exemple, vous pouvez vous connecter à un proxy RDS à l'aide de TLS 1.3, même si l'instance de base de données sous-jacente prend en charge une ancienne version de TLS. En utilisant le proxy RDS, vous pouvez appliquer des exigences d'authentification strictes pour les applications de base de données.

Correction

Pour plus d'informations sur la modification des paramètres d'un proxy Amazon RDS afin qu'il nécessite le protocole TLS, consultez la section Modification d'un proxy RDS dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-mariadb-instance-encrypted-in-transit

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les connexions à une instance de base de données Amazon RDS pour MariaDB sont chiffrées en transit. Le contrôle échoue si le groupe de paramètres de base de données associé

à l'instance de base de données n'est pas synchronisé ou si le `require_secure_transport` paramètre du groupe de paramètres n'est pas défini sur`ON`.

> **Note**
>
> Ce contrôle n'évalue pas les instances de bases de données Amazon RDS qui utilisent des versions de MariaDB antérieures à la version 10.5. Le `require_secure_transport` paramètre n'est pris en charge que pour les versions 10.5 et ultérieures de MariaDB.

Les données en transit font référence aux données qui se déplacent d'un emplacement à un autre, par exemple entre les nœuds d'un cluster de bases de données ou entre un cluster de bases de données et une application cliente. Les données peuvent circuler sur Internet ou au sein d'un réseau privé. Le chiffrement des données en transit réduit le risque que des utilisateurs non autorisés écoutent le trafic réseau.

Correction

Pour plus d'informations sur l'activation SSL/TLS des connexions à une instance de base de données Amazon RDS pour MariaDB, consultez la section Exiger SSL/TLS toutes les connexions à une instance de base de données MariaDB dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL

Exigences connexes : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : aurora-mysql-cluster-audit-logging

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des audits est activée sur un cluster de bases de données Amazon Aurora MySQL. Le contrôle échoue si le groupe de paramètres de base de données associé au cluster de bases de données n'est pas synchronisé, si le `server_audit_logging` paramètre n'est pas défini sur ou si le `server_audit_events` paramètre est défini sur une valeur vide. `1`

Les journaux de base de données peuvent faciliter les audits de sécurité et d'accès et aider à diagnostiquer les problèmes de disponibilité. Les journaux d'audit enregistrent l'activité de la base de données, y compris les tentatives de connexion, les modifications de données, les modifications de schéma et d'autres événements qui peuvent être audités à des fins de sécurité et de conformité.

Correction

Pour plus d'informations sur l'activation de la journalisation pour un cluster de bases de données Amazon Aurora MySQL, consultez la section Publication des journaux Amazon Aurora MySQL sur Amazon CloudWatch Logs dans le guide de l'utilisateur Amazon Aurora.

[RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::RDS::DBInstance`

Règle AWS Config : rds-instance-subnet-igw-check

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si une instance de base de données Amazon RDS est déployée dans un sous-réseau public qui possède une route vers une passerelle Internet. Le contrôle échoue si l'instance de base de données RDS est déployée dans un sous-réseau qui possède une route vers une passerelle Internet et que la destination est définie sur `0.0.0.0/0` ou `::/0`.

En provisionnant vos ressources Amazon RDS dans des sous-réseaux privés, vous pouvez empêcher vos ressources RDS de recevoir du trafic entrant depuis l'Internet public, ce qui peut

empêcher tout accès involontaire à vos instances de base de données RDS. Si les ressources RDS sont provisionnées dans un sous-réseau public ouvert sur Internet, elles peuvent être vulnérables à des risques tels que l'exfiltration de données.

Correction

Pour plus d'informations sur le provisionnement d'un sous-réseau privé pour une instance de base de données Amazon RDS, consultez la section Utilisation d'une instance de base de données dans un VPC dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : rds-pgsql-cluster-copy-tags-to-snapshot-check

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de bases de données Amazon RDS pour PostgreSQL est configuré pour copier automatiquement les balises dans les instantanés du cluster de bases de données lorsque les instantanés sont créés. Le contrôle échoue si le `CopyTagsToSnapshot` paramètre est défini sur `false` pour le cluster de bases de données RDS pour PostgreSQL.

La copie de balises vers des instantanés de base de données permet de maintenir un suivi des ressources, une gouvernance et une répartition des coûts appropriés entre les ressources de sauvegarde. Cela permet une identification des ressources, un contrôle d'accès et une surveillance de la conformité cohérents à la fois pour les bases de données actives et leurs instantanés. Les snapshots correctement balisés améliorent les opérations de sécurité en garantissant que les ressources de sauvegarde héritent des mêmes métadonnées que leurs bases de données sources.

Correction

Pour plus d'informations sur la configuration d'un cluster de bases de données Amazon RDS pour PostgreSQL afin de copier automatiquement les balises dans les instantanés de base de données,

consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : rds-mysql-cluster-copy-tags-to-snapshot-check

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un cluster de bases de données Amazon RDS pour MySQL est configuré pour copier automatiquement les balises dans les instantanés du cluster de bases de données lorsque les instantanés sont créés. Le contrôle échoue si le `CopyTagsToSnapshot` paramètre est défini sur `false` pour le cluster de bases de données RDS pour MySQL.

La copie de balises vers des instantanés de base de données permet de maintenir un suivi des ressources, une gouvernance et une répartition des coûts appropriés entre les ressources de sauvegarde. Cela permet une identification des ressources, un contrôle d'accès et une surveillance de la conformité cohérents à la fois pour les bases de données actives et leurs instantanés. Les snapshots correctement balisés améliorent les opérations de sécurité en garantissant que les ressources de sauvegarde héritent des mêmes métadonnées que leurs bases de données sources.

Correction

Pour plus d'informations sur la configuration d'un cluster de bases de données Amazon RDS pour MySQL afin de copier automatiquement les balises dans les instantanés de base de données, consultez la section Balisage des ressources Amazon RDS dans le guide de l'utilisateur d'Amazon Relational Database Service.

[RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::RDS::DBCluster`

Règle AWS Config : rds-cluster-backup-retention-check

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM	
`minimumBackupRetentionPeriod`	La durée minimale de conservation des sauvegardes, en jours, pour que le contrôle puisse être vérifié	Entier	7 sur 35	7	

Ce contrôle vérifie si un cluster de bases de données RDS possède une période de rétention des sauvegardes minimale. Le contrôle échoue si la période de rétention des sauvegardes est inférieure à la valeur de paramètre spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée, Security Hub utilise une valeur par défaut de 7 jours.

Ce contrôle vérifie si un cluster de bases de données RDS possède une période de rétention des sauvegardes minimale. Le contrôle échoue si la période de rétention des sauvegardes est inférieure à la valeur de paramètre spécifiée. À moins que vous ne fournissiez une valeur de paramètre client, Security Hub utilise une valeur par défaut de 7 jours. Ce contrôle s'applique à tous les types de clusters de bases de données RDS, y compris les clusters de base de données Aurora, les clusters DocumentDB, les clusters NeptuneDB, etc.

Correction

Pour configurer la période de rétention des sauvegardes pour un cluster de bases de données RDS, modifiez les paramètres du cluster et définissez la période de rétention des sauvegardes sur au moins 7 jours (ou la valeur spécifiée dans le paramètre de contrôle). Pour obtenir des instructions

détaillées, consultez la section Période de conservation des sauvegardes dans le guide de l'utilisateur d'Amazon Relational Database Service. Pour les clusters de base de données Aurora, consultez la section Présentation de la sauvegarde et de la restauration d'un cluster de base de données Aurora dans le guide de l'utilisateur Amazon Aurora pour Aurora. Pour les autres types de clusters de bases de données (par exemple les clusters DocumentDB), consultez le guide de l'utilisateur du service correspondant pour savoir comment mettre à jour la période de rétention des sauvegardes pour le cluster.

[RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Élevée

Type de ressource : `AWS::RDS::GlobalCluster`

Règle AWS Config : rds-global-cluster-aurora-mysql-supported-version

Type de calendrier : Déclenché par un changement

Paramètres :

- `minSupportedEngineVersion`: `8.0.mysql_aurora.3.08.0` (non personnalisable)
- `longTermSupportVersion`: `8.0.mysql_aurora.3.04.0, 8.0.mysql_aurora.3.04.1, 8.0.mysql_aurora.3.04.2, 8.0.mysql_aurora.3.04.3` (non personnalisable)

Ce contrôle vérifie si un cluster global Amazon Aurora MySQL s'exécute sur une version de moteur minimale prise en charge. Le contrôle échoue si la version du moteur de cluster global Aurora MySQL est inférieure à la version minimale prise en charge spécifiée et n'est pas répertoriée dans le paramètre de version de support à long terme.

L'exécution des bases de données globales Aurora MySQL sur des versions de moteur prises en charge vous permet de vous assurer d'avoir accès aux derniers correctifs de sécurité, corrections de bogues et améliorations de performances. Les versions mineures d'Aurora MySQL ont défini des dates de fin de support standard, après lesquelles elles ne reçoivent plus de correctifs critiques. L'exécution d'une version non prise en charge peut exposer votre base de données mondiale à des failles de sécurité et entraîner des frais de support étendu Amazon RDS. Comme Aurora MySQL suit un cycle de vie de support non contigu où les versions de support à long terme (LTS) restent prises

en charge plus longtemps que les versions non LTS suivantes, ce contrôle vérifie également les versions LTS qui sont toujours sous support standard. Pour plus d'informations, consultez la section Calendriers de publication d'Amazon Aurora MySQL dans les Notes de mise à jour d'Amazon Aurora MySQL.

Correction

Pour plus d'informations sur la mise à niveau d'une base de données globale Aurora MySQL vers une version de moteur prise en charge, consultez Mise à niveau d'une base de données globale Amazon Aurora et Mise à niveau d'Aurora MySQL en modifiant la version du moteur dans le guide de l'utilisateur Amazon Aurora.

Contrôles CSPM du Security Hub pour Amazon Redshift

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Redshift. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/13.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v4.0. 1/1.4.4

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Critique

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-cluster-public-access-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les clusters Amazon Redshift sont accessibles au public. Il évalue le `PubliclyAccessible` champ dans l'élément de configuration du cluster.

L'`PubliclyAccessible`attribut de la configuration du cluster Amazon Redshift indique si le cluster est accessible au public. Lorsque le cluster est configuré avec `PubliclyAccessible` set to`true`, il s'agit d'une Internet-facing instance dont le nom DNS peut être résolu publiquement et qui est résolu en adresse IP publique.

Lorsque le cluster n'est pas accessible au public, il s'agit d'une instance interne avec un nom DNS qui se résout en une adresse IP privée. À moins que vous ne souhaitiez que votre cluster soit accessible au public, le cluster ne doit pas être configuré avec la `PubliclyAccessible` valeur définie sur`true`.

Correction

Pour mettre à jour un cluster Amazon Redshift afin de désactiver l'accès public, consultez la section Modification d'un cluster dans le guide de gestion Amazon Redshift. Réglez Accessible au public sur Non.

[Redshift.2] Les connexions aux clusters Amazon Redshift doivent être chiffrées pendant le transit

Exigences associées : NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

Règle AWS Config : redshift-require-tls-ssl

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les connexions aux clusters Amazon Redshift sont nécessaires pour utiliser le chiffrement pendant le transit. La vérification échoue si le paramètre du cluster Amazon Redshift `require_SSL` n'est pas défini sur. `True`

Le protocole TLS peut être utilisé pour empêcher les attaquants potentiels de recourir à des attaques de type « Person-in-the-middle » ou à des attaques similaires pour espionner ou manipuler le trafic réseau. Seules les connexions chiffrées via TLS devraient être autorisées. Le chiffrement des

données en transit peut affecter les performances. Vous devez tester votre application avec cette fonctionnalité pour comprendre le profil de performance et l'impact du protocole TLS.

Correction

Pour mettre à jour un groupe de paramètres Amazon Redshift afin d'exiger le chiffrement, consultez la section Modification d'un groupe de paramètres dans le guide de gestion Amazon Redshift. Réglé `require_ssl` sur True.

[Redshift.3] Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift

Exigences associées : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-13 (5)

Catégorie : Restauration > Résilience > Sauvegardes activées

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-backup-enabled

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM	
`MinRetentionPeriod`	Durée minimale de conservation des instantanés en jours	Entier	7 sur 35	7	

Ce contrôle vérifie si les instantanés automatisés sont activés dans un cluster Amazon Redshift et si la période de conservation est supérieure ou égale à la période spécifiée. Le contrôle échoue si les instantanés automatisés ne sont pas activés pour le cluster ou si la période de rétention est inférieure à la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour

la période de conservation des instantanés, Security Hub CSPM utilise une valeur par défaut de 7 jours.

Les sauvegardes vous aident à récupérer plus rapidement après un incident de sécurité. Ils renforcent la résilience de vos systèmes. Amazon Redshift prend des instantanés périodiques par défaut. Ce contrôle vérifie si les instantanés automatiques sont activés et conservés pendant au moins sept jours. Pour plus de détails sur les instantanés automatisés Amazon Redshift, consultez la section Instantanés automatisés dans le guide de gestion Amazon Redshift.

Correction

Pour mettre à jour la période de conservation des instantanés pour un cluster Amazon Redshift, consultez la section Modification d'un cluster dans le guide de gestion Amazon Redshift. Pour Backup, définissez la rétention des snapshots sur une valeur supérieure ou égale à 7.

[Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

AWS Configrègle : `redshift-cluster-audit-logging-enabled` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des audits est activée sur un cluster Amazon Redshift.

La journalisation des audits Amazon Redshift fournit des informations supplémentaires sur les connexions et les activités des utilisateurs dans votre cluster. Ces données peuvent être stockées et sécurisées dans Amazon S3 et peuvent être utiles dans le cadre d'audits et d'enquêtes de sécurité. Pour plus d'informations, consultez la section Journalisation des audits de base de données dans le guide de gestion Amazon Redshift.

Correction

Pour configurer la journalisation des audits pour un cluster Amazon Redshift, consultez la section Configuration de l'audit à l'aide de la console dans le guide de gestion Amazon Redshift.

[Redshift.6] Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), (2) NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Catégorie : Identifier > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-cluster-maintenancesettings-check

Type de calendrier : changement déclenché

Paramètres :

- `allowVersionUpgrade = true`(non personnalisable)

Ce contrôle vérifie si les mises à niveau automatiques des versions majeures sont activées pour le cluster Amazon Redshift.

L'activation des mises à niveau automatiques des versions majeures garantit que les dernières mises à jour des versions majeures des clusters Amazon Redshift sont installées pendant la période de maintenance. Ces mises à jour peuvent inclure des correctifs de sécurité et des corrections de bogues. La mise à jour de l'installation des correctifs est une étape importante de la sécurisation des systèmes.

Correction

Pour résoudre ce problème à partir deAWS CLI, utilisez la commande Amazon `modify-cluster` Redshift et définissez `--allow-version-upgrade` l'attribut. *`clustername`*est le nom de votre cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré

Exigences connexes : NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protection > Configuration réseau sécurisée > Accès privé à l'API

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-enhanced-vpc-routing-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon Redshift est `EnhancedVpcRouting` activé.

Le routage VPC amélioré force tout le `UNLOAD` trafic entre le cluster `COPY` et les référentiels de données à passer par votre VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

Correction

Pour obtenir des instructions de correction détaillées, consultez la section Activation du routage VPC amélioré dans le guide de gestion Amazon Redshift.

[Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-default-admin-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un cluster Amazon Redshift a modifié le nom d'utilisateur de l'administrateur par rapport à sa valeur par défaut. Ce contrôle échouera si le nom d'utilisateur de l'administrateur d'un cluster Redshift est défini sur. `awsuser`

Lorsque vous créez un cluster Redshift, vous devez remplacer le nom d'utilisateur administrateur par défaut par une valeur unique. Les noms d'utilisateur par défaut sont de notoriété publique et doivent être modifiés lors de la configuration. La modification des noms d'utilisateur par défaut réduit le risque d'accès involontaire.

Correction

Vous ne pouvez pas modifier le nom d'utilisateur administrateur de votre cluster Amazon Redshift après l'avoir créé. Pour créer un nouveau cluster avec un nom d'utilisateur autre que le nom d'utilisateur par défaut, consultez l'étape 1 : créer un exemple de cluster Amazon Redshift dans le guide de démarrage Amazon Redshift.

[Redshift.10] Les clusters Redshift doivent être chiffrés au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-cluster-kms-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les clusters Amazon Redshift sont chiffrés au repos. Le contrôle échoue si un cluster Redshift n'est pas chiffré au repos ou si la clé de chiffrement est différente de la clé fournie dans le paramètre de règle.

Dans Amazon Redshift, vous pouvez activer le chiffrement des bases de données pour vos clusters afin de protéger les données au repos. Lorsque vous activez le chiffrement pour un cluster, les blocs de données et les métadonnées système sont chiffrés pour le cluster et ses instantanés. Le chiffrement des données au repos est une bonne pratique recommandée car il ajoute une couche de gestion des accès à vos données. Le chiffrement des clusters Redshift au repos réduit le risque qu'un utilisateur non autorisé puisse accéder aux données stockées sur le disque.

Correction

Pour modifier un cluster Redshift afin d'utiliser le chiffrement KMS, consultez la section Modification du chiffrement du cluster dans le guide de gestion Amazon Redshift.

[Redshift.11] Les clusters Redshift doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Redshift::Cluster`

AWS Configrègle : `tagged-redshift-cluster` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un cluster Amazon Redshift possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le cluster ne possède aucune

clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le cluster n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un cluster Redshift, consultez la section Ressources de balisage dans Amazon Redshift dans le guide de gestion Amazon Redshift.

[Redshift.12] Les abonnements aux notifications d'événements Redshift doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Redshift::EventSubscription`

AWS Configrègle : `tagged-redshift-eventsubscription` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un instantané de cluster Amazon Redshift comporte des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le cliché du cluster ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le cliché du cluster n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un abonnement aux notifications d'événements Redshift, consultez les ressources de balisage dans Amazon Redshift dans le guide de gestion Amazon Redshift.

[Redshift.13] Les instantanés du cluster Redshift doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Redshift::ClusterSnapshot`

AWS Configrègle : `tagged-redshift-clustersnapshot` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux	`No default value`

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		AWSexigences.	

Ce contrôle vérifie si un instantané de cluster Amazon Redshift comporte des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le cliché du cluster ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le cliché du cluster n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un instantané de cluster Redshift, consultez la section Ressources de balisage dans Amazon Redshift dans le guide de gestion Amazon Redshift.

[Redshift.14] Les groupes de sous-réseaux du cluster Redshift doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Redshift::ClusterSubnetGroup`

AWS Configrègle : `tagged-redshift-clustersubnetgroup` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un groupe de sous-réseaux du cluster Amazon Redshift possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le groupe de sous-réseaux du cluster ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de sous-réseaux du cluster n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un groupe de sous-réseaux du cluster Redshift, consultez la section Ressources de balisage dans Amazon Redshift dans le guide de gestion Amazon Redshift.

[Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes

Exigences associées : PCI DSS v4.0 1/1.3.1

Catégorie : Protection > Configuration réseau sécurisée > Configuration du groupe de sécurité

Gravité : Élevée

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-unrestricted-port-access

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un groupe de sécurité associé à un cluster Amazon Redshift possède des règles d'entrée qui autorisent l'accès au port du cluster depuis Internet (0.0.0). 0/0 ou : :/0). Le contrôle échoue si les règles d'entrée du groupe de sécurité autorisent l'accès au port du cluster depuis Internet.

L'autorisation d'un accès entrant illimité au port du cluster Redshift (adresse IP avec un suffixe /0) peut entraîner un accès non autorisé ou des incidents de sécurité. Nous recommandons d'appliquer le principe du moindre privilège d'accès lors de la création de groupes de sécurité et de la configuration des règles de trafic entrant.

Correction

Pour limiter l'entrée sur le port du cluster Redshift à des origines restreintes, consultez la section Utiliser les règles des groupes de sécurité dans le guide de l'utilisateur Amazon VPC. Mettez à jour les règles selon lesquelles la plage de ports correspond au port du cluster Redshift et la plage de ports IP est de 0,0.0. 0/0.

[Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::Redshift::ClusterSubnetGroup`

Règle AWS Config : redshift-cluster-subnet-group-multi-az

Type de calendrier : changement déclenché

Paramètres : Aucun

Le contrôle vérifie si un groupe de sous-réseaux du cluster Amazon Redshift possède des sous-réseaux provenant de plusieurs zones de disponibilité (AZ). Le contrôle échoue si le groupe de sous-réseaux du cluster ne possède pas de sous-réseaux provenant d'au moins deux zones de disponibilité différentes.

La configuration de sous-réseaux sur plusieurs AZ permet de garantir que votre entrepôt de données Redshift peut continuer à fonctionner même en cas de panne.

Correction

Pour modifier un groupe de sous-réseaux de cluster Redshift afin qu'il couvre plusieurs zones de disponibilité, consultez la section Modification d'un groupe de sous-réseaux de cluster dans le guide de gestion Amazon Redshift.

[Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Redshift::ClusterParameterGroup`

Règle AWS Config : redshift-cluster-parameter-group-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « ▲ » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un groupe de paramètres de cluster Amazon Redshift possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le groupe de paramètres ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags`

paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le groupe de paramètres ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un groupe de paramètres de cluster Amazon Redshift, consultez la section Ressources relatives aux balises dans Amazon Redshift dans le guide de gestion Amazon Redshift.

[Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ

Catégorie : Restauration > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::Redshift::Cluster`

Règle AWS Config : redshift-cluster-multi-az-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si plusieurs déploiements de zones de disponibilité (Multi-AZ) sont activés pour un cluster Amazon Redshift. Le contrôle échoue si Multi-AZ les déploiements ne sont pas activés pour le cluster Amazon Redshift.

Amazon Redshift prend en charge les déploiements de plusieurs zones de disponibilité (Multi-AZ) pour les clusters provisionnés. Si Multi-AZ les déploiements sont activés pour un cluster, un entrepôt de données Amazon Redshift peut continuer à fonctionner en cas de panne lorsqu'un événement inattendu se produit dans une zone de disponibilité (AZ). Un Multi-AZ déploiement déploie des ressources de calcul dans plusieurs zones géographiques et ces ressources de calcul sont accessibles via un seul point de terminaison. En cas de défaillance complète d'une zone de disponibilité, les ressources de calcul restantes d'une autre zone de disponibilité sont disponibles pour poursuivre le traitement des charges de travail. Vous pouvez convertir un entrepôt de Single-AZ données existant en entrepôt Multi-AZ de données. Des ressources de calcul supplémentaires sont ensuite provisionnées dans une seconde zone de disponibilité.

Correction

Pour plus d'informations sur la configuration Multi-AZ des déploiements pour un cluster Amazon Redshift, consultez la section Conversion Single-AZ d'un entrepôt de données en entrepôt de Multi-AZ données dans le guide de gestion Amazon Redshift.

Contrôles CSPM du Security Hub pour Amazon Redshift Serverless

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Redshift Serverless. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré

Catégorie : Protection > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Élevée

Type de ressource : `AWS::RedshiftServerless::Workgroup`

Règle AWS Config : redshift-serverless-workgroup-routes-within-vpc

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le routage VPC amélioré est activé pour un groupe de travail Amazon Redshift Serverless. Le contrôle échoue si le routage VPC amélioré est désactivé pour le groupe de travail.

Si le routage VPC amélioré est désactivé pour un groupe de travail Amazon Redshift Serverless, Amazon Redshift achemine le trafic via Internet, y compris le trafic vers d'autres services du réseau. AWS Si vous activez le routage VPC amélioré pour un groupe de travail, Amazon Redshift force tout le `UNLOAD` trafic entre votre cluster `COPY` et vos référentiels de données via votre cloud privé virtuel (VPC) basé sur le service Amazon VPC. Grâce au routage VPC amélioré, vous pouvez utiliser les fonctionnalités VPC standard pour contrôler le flux de données entre votre cluster Amazon Redshift et les autres ressources. Cela inclut des fonctionnalités telles que les groupes de sécurité VPC et les politiques relatives aux terminaux, les listes de contrôle d'accès réseau (ACL) et les serveurs DNS (Domain Name System). Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic`COPY`. `UNLOAD`

Correction

Pour plus d'informations sur le routage VPC amélioré et sur la manière de l'activer pour un groupe de travail, consultez la section Contrôle du trafic réseau avec le routage VPC amélioré Redshift dans le guide de gestion Amazon Redshift.

[RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::RedshiftServerless::Workgroup`

Règle AWS Config : redshift-serverless-workgroup-encrypted-in-transit

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si des connexions à un groupe de travail Amazon Redshift Serverless sont nécessaires pour chiffrer les données en transit. Le contrôle échoue si le paramètre `require_ssl` de configuration du groupe de travail est défini sur. `false`

Un groupe de travail Amazon Redshift Serverless est un ensemble de ressources de calcul qui regroupe des ressources de calcul telles que les RPU, les groupes de sous-réseaux VPC et les groupes de sécurité. Les propriétés d'un groupe de travail incluent les paramètres réseau et de sécurité. Ces paramètres indiquent si les connexions à un groupe de travail doivent être requises pour utiliser le protocole SSL afin de chiffrer les données en transit.

Correction

Pour plus d'informations sur la mise à jour des paramètres d'un groupe de travail Amazon Redshift Serverless afin d'exiger des connexions SSL, consultez la section Connexion à Amazon Redshift Serverless dans le guide de gestion Amazon Redshift.

[RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::RedshiftServerless::Workgroup`

Règle AWS Config : redshift-serverless-workgroup-no-public-access

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'accès public est désactivé pour un groupe de travail Amazon Redshift Serverless. Il évalue les `publiclyAccessible` propriétés d'un groupe de travail Redshift Serverless. Le contrôle échoue si l'accès public est activé (`true`) pour le groupe de travail.

Le paramètre public access (`publiclyAccessible`) d'un groupe de travail Amazon Redshift Serverless indique si le groupe de travail est accessible depuis un réseau public. Si l'accès public est activé (`true`) pour un groupe de travail, Amazon Redshift crée une adresse IP élastique qui rend le groupe de travail accessible au public depuis l'extérieur du VPC. Si vous ne souhaitez pas qu'un groupe de travail soit accessible au public, désactivez-le.

Correction

Pour plus d'informations sur la modification du paramètre d'accès public pour un groupe de travail Amazon Redshift Serverless, consultez la section Affichage des propriétés d'un groupe de travail dans le guide de gestion Amazon Redshift.

[RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys

Exigences associées : NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::RedshiftServerless::Namespace`

Règle AWS Config : redshift-serverless-namespace-cmk-encryption

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`kmsKeyArns`	Une liste des Amazon Resource Names (ARN) AWS KMS keys à inclure dans l'évaluation. Le contrôle permet de déterminer si `FAILED` un espace de noms Redshift Serverless n'est pas chiffré avec une clé KMS dans la liste.	StringList (maximum de 3 articles)	1 à 3 ARN de clés KMS existantes. Par exemple : `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Aucune valeur par défaut

Ce contrôle vérifie si un espace de noms Amazon Redshift Serverless est chiffré au repos et géré par un client. AWS KMS key Le contrôle échoue si l'espace de noms Redshift Serverless n'est pas chiffré à l'aide d'une clé KMS gérée par le client. Vous pouvez éventuellement spécifier une liste de clés KMS que le contrôle doit inclure dans l'évaluation.

Dans Amazon Redshift sans serveur, un espace de noms définit un conteneur logique pour les objets de la base de données. Ce contrôle vérifie régulièrement si les paramètres de chiffrement d'un espace de noms spécifient une clé KMS gérée par le clientAWS KMS key, au lieu d'une clé KMS AWS gérée, pour le chiffrement des données dans l'espace de noms. Avec une clé KMS gérée par le client, vous avez le contrôle total de la clé. Cela inclut la définition et le maintien de la politique des clés, la gestion des subventions, la rotation du matériel cryptographique, l'attribution de balises, la création d'alias, ainsi que l'activation et la désactivation de la clé.

Correction

Pour plus d'informations sur la mise à jour des paramètres de chiffrement pour un espace de noms Amazon Redshift Serverless et sur la spécification d'un espace de noms géré par le AWS KMS key clientAWS KMS key, consultez la section Modification des paramètres d'un espace de noms dans le guide de gestion Amazon Redshift.

[RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut

Catégorie : Identifier > Configuration des ressources

Gravité : Moyenne

Type de ressource : `AWS::RedshiftServerless::Namespace`

Règle AWS Config : redshift-serverless-default-admin-check

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le nom d'utilisateur d'un espace de noms Amazon Redshift Serverless est le nom d'utilisateur d'administrateur par défaut. `admin` Le contrôle échoue si le nom d'utilisateur administrateur de l'espace de noms Redshift Serverless est. `admin`

Lorsque vous créez un espace de noms Amazon Redshift Serverless, vous devez spécifier un nom d'utilisateur administrateur personnalisé pour cet espace de noms. Le nom d'utilisateur de

l'administrateur par défaut est public knowledge. En spécifiant un nom d'utilisateur d'administrateur personnalisé, vous pouvez, par exemple, contribuer à atténuer le risque ou l'efficacité des attaques par force brute contre l'espace de noms.

Correction

Vous pouvez modifier le nom d'utilisateur administrateur d'un espace de noms Amazon Redshift Serverless à l'aide de la console ou de l'API Amazon Redshift Serverless. Pour le modifier à l'aide de la console, choisissez la configuration de l'espace de noms, puis choisissez Modifier les informations d'identification de l'administrateur dans le menu Actions. Pour le modifier par programmation, utilisez l'UpdateNamespaceopération ou, si vous utilisez laAWS CLI, exécutez la commande update-namespace. Si vous modifiez le nom d'utilisateur administrateur, vous devez également modifier le mot de passe administrateur en même temps.

[RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::RedshiftServerless::Namespace`

Règle AWS Config : redshift-serverless-publish-logs-to-cloudwatch

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un espace de noms Amazon Redshift Serverless est configuré pour exporter les connexions et les journaux des utilisateurs vers Amazon Logs. CloudWatch Le contrôle échoue si l'espace de noms Redshift Serverless n'est pas configuré pour exporter les journaux vers Logs. CloudWatch

Si vous configurez Amazon Redshift Serverless pour exporter les données du journal de connexion (`connectionlog`) et du journal utilisateur (`userlog`) vers un groupe de CloudWatch journaux dans Amazon Logs, vous pouvez collecter et stocker vos enregistrements de journal dans un stockage durable, qui peut prendre en charge les examens et audits de sécurité, d'accès et de disponibilité. Avec CloudWatch Logs, vous pouvez également effectuer une analyse en temps réel des données des journaux et les utiliser CloudWatch pour créer des alarmes et examiner les métriques.

Correction

Pour exporter les données de journal d'un espace de noms Amazon Redshift Serverless vers CloudWatch Amazon Logs, les journaux respectifs doivent être sélectionnés pour être exportés dans les paramètres de configuration de journalisation d'audit de l'espace de noms. Pour plus d'informations sur la mise à jour de ces paramètres, consultez la section Modification de la sécurité et du chiffrement dans le guide de gestion Amazon Redshift.

Contrôles Security Hub CSPM pour Route 53

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Route 53.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Route53::HealthCheck`

AWS Configrègle : `tagged-route53-healthcheck` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un bilan de santé d'Amazon Route 53 comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le bilan de santé ne comporte aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le contrôle de santé n'est associé à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un bilan de santé de Route 53, consultez la section Désignation et balisage des contrôles de santé dans le guide du développeur Amazon Route 53.

[Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,

NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Route53::HostedZone`

Règle AWS Config : `route53-query-logging-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des requêtes DNS est activée pour une zone hébergée publique Amazon Route 53. Le contrôle échoue si la journalisation des requêtes DNS n'est pas activée pour une zone hébergée publique Route 53.

L'enregistrement des requêtes DNS pour une zone hébergée Route 53 répond aux exigences de sécurité et de conformité du DNS et garantit la visibilité. Les journaux incluent des informations telles que le domaine ou le sous-domaine interrogé, la date et l'heure de la requête, le type d'enregistrement DNS (par exemple, A ou AAAA) et le code de réponse DNS (par exemple, ou). `NoError` `ServFail` Lorsque la journalisation des requêtes DNS est activée, Route 53 publie les fichiers CloudWatch journaux sur Amazon Logs.

Correction

Pour enregistrer les requêtes DNS pour les zones hébergées publiques de Route 53, consultez la section Configuration de la journalisation des requêtes DNS dans le manuel Amazon Route 53 Developer Guide.

Contrôles CSPM de Security Hub pour Amazon S3

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Simple Storage Service (Amazon S3). Les commandes ne sont peut-être pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.1.4, CIS AWS Foundations Benchmark v3.0. 0/2.1.4, CIS AWS Foundations Benchmark v1.4. 0/2.1.5, NIST.800-53.r5 AC-21

NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v4.0. 1/14,44

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : s3-account-level-public-access-blocks-periodic

Type de programme : Périodique

Paramètres :

- `ignorePublicAcls`: `true` (non personnalisable)
- `blockPublicPolicy`: `true` (non personnalisable)
- `blockPublicAcls`: `true` (non personnalisable)
- `restrictPublicBuckets`: `true` (non personnalisable)

Ce contrôle vérifie si les paramètres d'accès public du bloc Amazon S3 précédents sont configurés au niveau du compte pour un compartiment S3 à usage général. Le contrôle échoue si un ou plusieurs des paramètres de blocage de l'accès public sont définis sur`false`.

Le contrôle échoue si l'un des paramètres est défini sur ou s'il n'est pas configuré. `false`

Le bloc d'accès public Amazon S3 est conçu pour fournir des contrôles sur l'ensemble d'un compartiment S3 Compte AWS ou au niveau individuel afin de garantir que les objets ne soient jamais accessibles au public. Un accès public est accordé aux compartiments et objets via des listes de contrôle d'accès (ACL), des stratégies de compartiment, ou via les deux.

À moins que vous n'ayez l'intention de rendre vos compartiments S3 accessibles au public, vous devez configurer la fonctionnalité Amazon S3 Block Public Access au niveau du compte.

Pour en savoir plus, consultez la section Utilisation d'Amazon S3 Block Public Access dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Correction

Pour activer l'accès public bloqué à Amazon S3 pour vous Compte AWS, consultez la section Configuration des paramètres de blocage de l'accès public pour votre compte dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.2] Les compartiments S3 à usage général devraient bloquer l'accès public en lecture

Exigences associées : PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-public-read-prohibited

Type de planification : périodique et déclenchée par des changements

Paramètres : Aucun

Ce contrôle vérifie si un compartiment à usage général Amazon S3 autorise l'accès public en lecture. Il évalue les paramètres de blocage d'accès public, la stratégie de compartiment et la liste de contrôle d'accès (ACL) du compartiment. Le contrôle échoue si le bucket autorise l'accès public en lecture.

> **Note**
>
> Si un compartiment S3 possède une politique de compartiment, ce contrôle n'évalue pas les conditions de politique qui utilisent des caractères génériques ou des variables. Pour produire un `PASSED` résultat, les conditions de la politique de compartiment ne doivent utiliser que des valeurs fixes, c'est-à-dire des valeurs qui ne contiennent pas de caractères génériques ni de variables de stratégie. Pour plus d'informations sur les variables de politique, consultez la section Variables et balises dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

Certains cas d'utilisation peuvent nécessiter que tout le monde sur Internet soit capable de lire des informations depuis votre compartiment S3. Cependant, ces situations sont rares. Pour garantir l'intégrité et la sécurité de vos données, votre compartiment S3 ne doit pas être lisible publiquement.

Correction

Pour bloquer l'accès public en lecture sur vos compartiments Amazon S3, consultez Configuration des paramètres de blocage de l'accès public pour vos compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.3] Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture

Exigences associées : PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Critique

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-public-write-prohibited

Type de planification : périodique et déclenchée par des changements

Paramètres : Aucun

Ce contrôle vérifie si un compartiment à usage général Amazon S3 autorise l'accès public en écriture. Il évalue les paramètres de blocage d'accès public, la stratégie de compartiment et la liste de contrôle d'accès (ACL) du compartiment. Le contrôle échoue si le bucket autorise l'accès public en écriture.

> **Note**
>
> Si un compartiment S3 possède une politique de compartiment, ce contrôle n'évalue pas les conditions de politique qui utilisent des caractères génériques ou des variables. Pour produire un `PASSED` résultat, les conditions de la politique de compartiment ne doivent utiliser que des valeurs fixes, c'est-à-dire des valeurs qui ne contiennent pas de caractères génériques

ni de variables de stratégie. Pour plus d'informations sur les variables de politique, consultez la section Variables et balises dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

Certains cas d'utilisation nécessitent que tout le monde sur Internet puisse écrire dans votre compartiment S3. Cependant, ces situations sont rares. Pour garantir l'intégrité et la sécurité de vos données, votre compartiment S3 ne doit pas accorder l'accès public en écriture.

Correction

Pour bloquer l'accès public en écriture sur vos compartiments Amazon S3, consultez Configuration des paramètres de blocage de l'accès public pour vos compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.1.1, CIS AWS Foundations Benchmark v3.0. 0/2.1.1, CIS AWS Foundations Benchmark v1.4. 0/2.1.2, NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v3.2. 1/4.1, PCI DSS v4.0. 1/42.1.1

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-ssl-requests-only

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un compartiment à usage général Amazon S3 possède une politique qui exige que les requêtes utilisent le protocole TLS. Le contrôle échoue si la politique de bucket n'exige pas que les requêtes utilisent le protocole TLS.

Les compartiments S3 doivent avoir des politiques qui exigent que toutes les requêtes (`Action: S3:*`) n'acceptent que la transmission de données via HTTPS dans la politique de ressources S3, indiquée par la clé `aws:SecureTransport` de condition.

Correction

Pour mettre à jour une politique de compartiment Amazon S3 afin de refuser le transport non sécurisé, consultez la section Ajouter une politique de compartiment à l'aide de la console Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Ajoutez une déclaration de politique similaire à celle de la politique suivante. `amzn-s3-demo-bucket`Remplacez-le par le nom du compartiment que vous modifiez.

JSON

```
{
    "Id": "ExamplePolicy",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
}
```

Pour plus d'informations, consultez Quelle politique de compartiment S3 dois-je utiliser pour me conformer à la AWS Config règle s3-bucket-ssl-requests-only ? dans le Centre de connaissances AWS officiel.

[S3.6] Les politiques de bucket à usage général S3 devraient restreindre l'accès aux autres Comptes AWS

Exigences connexes : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.4

Catégorie : Protéger > Gestion sécurisée des accès > Actions d'opérations d'API sensibles restreintes

Gravité : Élevée

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config :s3-bucket-blacklisted-actions-prohibited

Type de calendrier : Déclenché par un changement

Paramètres :

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (non personnalisable)

Ce contrôle vérifie si une politique de compartiment à usage général d'Amazon S3 empêche les principaux d' Comptes AWS effectuer des actions refusées sur les ressources du compartiment S3. Le contrôle échoue si la politique de compartiment autorise une ou plusieurs des actions précédentes pour un principal dans un autre Compte AWS.

La mise en œuvre de l'accès au moindre privilège est fondamentale pour réduire les risques de sécurité et l'impact des erreurs ou des intentions malveillantes. Si une politique de compartiment S3 autorise l'accès à partir de comptes externes, cela peut entraîner l'exfiltration de données par une menace interne ou un attaquant.

Le `blacklistedactionpatterns` paramètre permet une évaluation réussie de la règle pour les compartiments S3. Le paramètre donne accès à des comptes externes pour les modèles d'action qui ne sont pas inclus dans la `blacklistedactionpatterns` liste.

Correction

Pour mettre à jour une politique de compartiment Amazon S3 afin de supprimer des autorisations, consultez. Ajout d'une politique de compartiment à l'aide de la console Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Sur la page Modifier la politique de compartiment, dans la zone de texte de modification de la stratégie, effectuez l'une des actions suivantes :

- Supprimez les déclarations qui accordent Comptes AWS un autre accès aux actions refusées.
- Supprimez les actions refusées autorisées des relevés.

[S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions

Exigences associées : PCI DSS v3.2. 1/2.2, NIST.800-53.r5 AU-9 (2) NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-36 (2), NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Faible

Type de ressource : `AWS::S3::Bucket`

AWS Config règle : s3-bucket-cross-region-replication-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la réplication interrégionale est activée sur un compartiment à usage général Amazon S3. Le contrôle échoue si la réplication entre régions n'est pas activée sur le bucket.

La réplication est la copie automatique et asynchrone d'objets dans des compartiments identiques ou différents. Régions AWS La réplication copie les objets nouvellement créés et les mises à jour d'objets depuis un compartiment source vers un ou plusieurs compartiments de destination. AWS les meilleures pratiques recommandent la réplication pour les compartiments source et de destination qui appartiennent au même Compte AWS groupe. En plus de la disponibilité, vous devriez envisager d'autres paramètres de sécurisation renforcée des systèmes.

Ce contrôle permet de `FAILED` trouver un compartiment de destination de réplication si la réplication entre régions n'est pas activée. S'il existe une raison légitime pour laquelle le compartiment de destination n'a pas besoin de réplication entre régions pour être activé, vous pouvez supprimer les résultats pour ce compartiment.

Correction

Pour activer Cross-Region la réplication sur un compartiment S3, consultez la section Configuration de la réplication pour les compartiments source et de destination appartenant au même compte dans le guide de l'utilisateur Amazon Simple Storage Service. Pour le compartiment source, choisissez Appliquer à tous les objets du compartiment.

[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.1.4, Indice de référence des AWS fondations de la CEI v3.0.02.1.4, Indice de référence des fondations de la CEI v1.4. AWS 0/2.1.5, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14,44

Catégorie : Protéger > Gestion sécurisée des accès > Contrôle d'accès

Gravité : Élevée

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-level-public-access-prohibited

Type de calendrier : Déclenché par un changement

Paramètres :

- `excludedPublicBuckets`(non personnalisable) — Une liste séparée par des virgules de noms de compartiments S3 publics connus et autorisés

Ce contrôle vérifie si un compartiment à usage général Amazon S3 bloque l'accès public au niveau du compartiment. Le contrôle échoue si l'un des paramètres suivants est défini sur `false` :

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Bloquer l'accès public au niveau du compartiment S3 fournit des contrôles pour garantir que les objets ne sont jamais accessibles au public. Un accès public est accordé aux compartiments et objets via des listes de contrôle d'accès (ACL), des stratégies de compartiment, ou via les deux.

À moins que vous n'ayez l'intention de rendre vos compartiments S3 accessibles au public, vous devez configurer la fonctionnalité Amazon S3 Block Public Access au niveau du compartiment.

Correction

Pour plus d'informations sur la manière de supprimer l'accès public au niveau d'un compartiment, consultez la section Bloquer l'accès public à votre stockage Amazon S3 dans le guide de l'utilisateur Amazon S3.

[S3.9] Les compartiments S3 à usage général doivent avoir la journalisation des accès au serveur activée

Exigences associées : NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.3.8, PCI DSS v4.0. 1/102.1.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-logging-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la journalisation des accès au serveur est activée pour un compartiment à usage général Amazon S3. Le contrôle échoue si la journalisation des accès au serveur n'est pas activée. Lorsque la journalisation est activée, Amazon S3 transmet les journaux d'accès d'un compartiment source à un compartiment cible choisi. Le compartiment cible doit se trouver dans le même compartiment Région AWS que le compartiment source et aucune période de rétention par défaut ne doit être configurée. La journalisation des accès au serveur n'a pas besoin d'être activée pour le compartiment de journalisation cible et vous devez supprimer les résultats pour ce compartiment.

La journalisation des accès au serveur fournit des enregistrements détaillés des demandes adressées à un bucket. Les journaux d'accès aux serveurs peuvent faciliter les audits de sécurité et d'accès. Pour plus d'informations, consultez la section Meilleures pratiques de sécurité pour Amazon S3 : Activer la journalisation des accès au serveur Amazon S3.

Correction

Pour activer la journalisation de l'accès au serveur Amazon S3, consultez la section Activation de la journalisation de l'accès au serveur Amazon S3 dans le guide de l'utilisateur Amazon S3.

[S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-version-lifecycle-policy-check

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un compartiment versionné à usage général Amazon S3 possède une configuration Lifecycle. Le contrôle échoue si le bucket n'a pas de configuration Lifecycle.

Nous vous recommandons de créer une configuration de cycle de vie pour votre compartiment S3 afin de vous aider à définir les actions que vous souhaitez qu'Amazon S3 entreprenne pendant la durée de vie d'un objet.

> **Tip**
>
> L'activation du versionnement sans gestion du cycle de vie peut entraîner une croissance illimitée du stockage et une augmentation des coûts. Chaque modification d'objet crée une nouvelle version qui est conservée indéfiniment. Configurez les règles de cycle de vie S3 pour transférer automatiquement les versions non actuelles vers des classes de stockage moins coûteuses ou les faire expirer après une période de rétention définie.

Correction

Pour plus d'informations sur la configuration du cycle de vie d'un compartiment Amazon S3, consultez les sections Utilisation de la gestion des versions S3 avec S3 Lifecycle, Définition de la configuration du cycle de vie sur un bucket et Gestion du cycle de vie des objets dans le guide de l'utilisateur Amazon S3.

[S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général

Exigences connexes : NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (4), NIST.800-171.r2 3.3.8

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-event-notifications-enabled

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`eventTypes`	Liste des types d'événements S3 préférés	EnumList (maximum de 28 articles)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`,	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
			s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:D	

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
			elete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replic	

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
			`ation:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent`	

Ce contrôle vérifie si les notifications d'événements S3 sont activées sur un compartiment à usage général Amazon S3. Le contrôle échoue si les notifications d'événements S3 ne sont pas activées sur le bucket. Si vous fournissez des valeurs personnalisées pour le `eventTypes` paramètre, le contrôle n'est transmis que si les notifications d'événements sont activées pour les types d'événements spécifiés.

Lorsque vous activez les notifications d'événements S3, vous recevez des alertes lorsque des événements spécifiques se produisent et ont un impact sur vos compartiments S3. Par exemple, vous pouvez être informé de la création, de la suppression et de la restauration d'objets. Ces notifications peuvent alerter les équipes concernées en cas de modifications accidentelles ou intentionnelles susceptibles d'entraîner un accès non autorisé aux données.

Correction

Pour plus d'informations sur la détection des modifications apportées aux compartiments et aux objets S3, consultez la section Notifications d'événements Amazon S3 dans le guide de l'utilisateur Amazon S3.

[S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3

Exigences connexes : NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Catégorie : Protéger > Gestion sécurisée des accès > Contrôle d'accès

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-acl-prohibited

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un compartiment à usage général Amazon S3 fournit des autorisations aux utilisateurs avec une liste de contrôle d'accès (ACL). Le contrôle échoue si une ACL est configurée pour gérer l'accès des utilisateurs au bucket.

Les ACL sont des mécanismes de contrôle d'accès existants antérieurs à l'IAM. Au lieu des ACL, nous vous recommandons d'utiliser des politiques de compartiment S3 ou des politiques Gestion des identités et des accès AWS (IAM) pour gérer l'accès à vos compartiments S3.

Correction

Pour passer ce contrôle, vous devez désactiver les ACL pour vos compartiments S3. Pour obtenir des instructions, consultez la section Contrôle de la propriété des objets et désactivation des listes

de contrôle d'accès pour votre compartiment dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour créer une politique de compartiment S3, consultez la section Ajouter une politique de compartiment à l'aide de la console Amazon S3. Pour créer une politique utilisateur IAM sur un compartiment S3, voir Contrôler l'accès à un compartiment à l'aide de politiques utilisateur.

[S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie

Exigences connexes : NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Catégorie : Protéger > Protection des données

Gravité : Faible

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-lifecycle-policy-check

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`targetTransitionDays`	Nombre de jours après la création de l'objet pendant lesquels les objets sont transférés vers une classe de stockage spécifiée	Entier	1 sur `36500`	Aucune valeur par défaut
`targetExpirationDays`	Nombre de jours après la création de l'objet lorsque les objets sont supprimés	Entier	1 sur `36500`	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`targetTransitionStorageClass`	Type de classe de stockage S3 de destination	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Aucune valeur par défaut

Ce contrôle vérifie si un compartiment à usage général Amazon S3 possède une configuration Lifecycle. Le contrôle échoue si le bucket n'a pas de configuration Lifecycle. Si vous fournissez des valeurs personnalisées pour un ou plusieurs des paramètres précédents, le contrôle n'est transmis que si la politique inclut la classe de stockage, l'heure de suppression ou la durée de transition spécifiées.

La création d'une configuration de cycle de vie pour votre compartiment S3 définit les actions que vous souhaitez qu'Amazon S3 entreprenne pendant la durée de vie d'un objet. Par exemple, vous pouvez transférer des objets vers une autre classe de stockage, les archiver ou les supprimer après une période spécifiée.

Correction

Pour plus d'informations sur la configuration des politiques de cycle de vie sur un compartiment Amazon S3, consultez Configuration de la configuration du cycle de vie sur un compartiment et consultez la section Gestion du cycle de vie de votre stockage dans le guide de l'utilisateur Amazon S3.

[S3.14] Les compartiments S3 à usage général doivent avoir le contrôle de version activé

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Exigences connexes : NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.3.8

Gravité : Faible

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-versioning-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le contrôle de version est activé pour un compartiment à usage général Amazon S3. Le contrôle échoue si la gestion des versions est suspendue pour le bucket.

La gestion des versions permet de conserver plusieurs variantes d'un objet dans le même compartiment S3. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer toutes les versions de tous les objets stockés dans votre compartiment S3. La gestion des versions vous permet de vous remettre à la fois en cas d'actions involontaires de l'utilisateur et de défaillances des applications.

> **Tip**
>
> L'activation du versionnement sans gestion du cycle de vie peut entraîner une croissance illimitée du stockage et une augmentation des coûts. Chaque modification d'objet crée une nouvelle version qui est conservée indéfiniment. Configurez les règles de cycle de vie S3 pour transférer automatiquement les versions non actuelles vers des classes de stockage moins coûteuses ou les faire expirer après une période de rétention définie. Pour plus d'informations, consultez les sections Utilisation de la gestion des versions S3 avec S3 Lifecycle et Gestion du cycle de vie des objets.

Correction

Pour utiliser la gestion des versions sur un compartiment S3, consultez la section Activation de la gestion des versions sur les compartiments dans le guide de l'utilisateur Amazon S3.

[S3.15] Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Exigences associées : NIST.800-53.r5 CP-6 (2), PCI DSS v4.0. 1/105,1

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-default-lock-enabled

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`mode`	Mode de rétention S3 Object Lock	Enum	`GOVERNANCE` , `COMPLIANCE`	Aucune valeur par défaut

Ce contrôle vérifie si le verrouillage des objets est activé sur un compartiment à usage général Amazon S3. Le contrôle échoue si Object Lock n'est pas activé pour le bucket. Si vous fournissez une valeur personnalisée pour le `mode` paramètre, le contrôle n'est transmis que si S3 Object Lock utilise le mode de rétention spécifié.

La fonctionnalité de verrouillage des objets S3 vous permet de stocker des objets selon un modèle WORM (write-once-read-many). Object Lock permet d'empêcher la suppression ou le remplacement des objets des compartiments S3 pendant une durée déterminée ou indéfiniment. Vous pouvez utiliser le verrouillage des objets S3 pour satisfaire aux exigences réglementaires qui nécessitent le stockage WORM, ou pour ajouter une couche supplémentaire de protection contre la suppression et les modifications d'objet.

Correction

Pour configurer Object Lock pour les compartiments S3 nouveaux et existants, consultez la section Configuration de S3 Object Lock dans le guide de l'utilisateur Amazon S3.

[S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Exigences associées : NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), (10), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 CA-9 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.8.9, NIST.800-171.r2 3.13.11 NIST.800-53.r5 AU-9, NIST.800-171.r2 3.13.16, PCI DSS v4.0. 1/35,1

Gravité : Moyenne

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-default-encryption-kms

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un compartiment à usage général Amazon S3 est chiffré avec un AWS KMS key (SSE-KMS ou DSSE-KMS). Le contrôle échoue si le compartiment est chiffré avec le chiffrement par défaut (SSE-S3).

Server-side le chiffrement (SSE) est le chiffrement des données à leur destination par l'application ou le service qui les reçoit. Sauf indication contraire de votre part, les compartiments S3 utilisent les clés gérées Amazon S3 (SSE-S3) par défaut pour le chiffrement côté serveur. Toutefois, pour plus de contrôle, vous pouvez choisir de configurer les compartiments pour utiliser le chiffrement côté serveur avec AWS KMS keys (SSE-KMS ou DSSE-KMS) à la place. Amazon S3 chiffre vos données au niveau de l'objet lorsqu'il les écrit sur les disques des centres de AWS données et les déchiffre pour vous lorsque vous y accédez.

Correction

Pour chiffrer un compartiment S3 à l'aide de SSE-KMS, consultez la section Spécifier le chiffrement côté serveur avec AWS KMS (SSE-KMS) dans le Guide de l'utilisateur Amazon S3. Pour chiffrer un compartiment S3 à l'aide de DSSE-KMS, consultez la section Spécifier le chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS) dans le guide de l'utilisateur Amazon S3.

[S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14,44

Catégorie : Protéger > Gestion sécurisée des accès > Ressource non accessible au public

Gravité : Critique

Type de ressource : `AWS::S3::AccessPoint`

Règle AWS Config : s3-access-point-public-access-blocks

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les paramètres de blocage de l'accès public d'un point d'accès Amazon S3 sont activés. Le contrôle échoue si les paramètres de blocage de l'accès public ne sont pas activés pour le point d'accès.

La fonctionnalité Amazon S3 Block Public Access vous permet de gérer l'accès à vos ressources S3 à trois niveaux : au niveau du compte, du compartiment et du point d'accès. Les paramètres de chaque niveau peuvent être configurés indépendamment, ce qui vous permet de définir différents niveaux de restrictions d'accès public à vos données. Les paramètres du point d'accès ne peuvent pas remplacer individuellement les paramètres les plus restrictifs des niveaux supérieurs (niveau du compte ou compartiment attribué au point d'accès). Au lieu de cela, les paramètres au niveau du point d'accès sont additifs, ce qui signifie qu'ils complètent et fonctionnent avec les paramètres des autres niveaux. À moins que vous ne souhaitiez qu'un point d'accès S3 soit accessible au public, vous devez activer les paramètres de blocage de l'accès public.

Correction

Actuellement, Amazon S3 ne prend pas en charge la modification des paramètres de blocage de l'accès public d'un point d'accès après que ce point d'accès a été créé. Tous les paramètres de blocage de l'accès public sont activés par défaut lorsque vous créez un nouveau point d'accès. Nous vous recommandons de garder tous les paramètres activés, sauf si vous savez que vous avez un besoin spécifique de désactiver l'un d'entre eux. Pour plus d'informations, consultez la section

Gestion de l'accès public aux points d'accès dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/2.1.2, CIS AWS Foundations Benchmark v3.0. 0/2.1.2, CIS AWS Foundations Benchmark v1.4. 0/2.1.3, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Catégorie : Protéger > Protection des données > Protection contre la suppression des données

Gravité : Faible

Type de ressource : `AWS::S3::Bucket`

Règle AWS Config : s3-bucket-mfa-delete-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si la suppression par authentification multifacteur (MFA) est activée pour un compartiment à usage général Amazon S3. Le contrôle échoue si la suppression du MFA n'est pas activée pour le bucket. Le contrôle ne produit pas de résultats pour les buckets qui ont une configuration de cycle de vie.

Si vous activez la gestion des versions pour un compartiment S3 à usage général, vous pouvez éventuellement ajouter une autre couche de sécurité en configurant la suppression MFA pour le compartiment. Dans ce cas, le propriétaire du compartiment doit inclure deux formes d'authentification dans toute demande visant à supprimer une version d'un objet du compartiment ou à modifier l'état de gestion des versions du compartiment. La suppression du MFA apporte une sécurité accrue si, par exemple, les informations d'identification de sécurité du propriétaire du bucket sont compromises. La suppression de l'authentification multifacteur peut également contribuer à prévenir les suppressions accidentelles de compartiments en demandant à l'utilisateur qui initie l'action de suppression de prouver qu'il est en possession physique d'un appareil MFA avec un code MFA, ce qui ajoute une couche supplémentaire de friction et de sécurité à l'action de suppression.

> **Note**
>
> Ce contrôle produit un `PASSED` résultat uniquement si la suppression MFA est activée pour le compartiment à usage général S3. Pour activer la suppression MFA pour un

bucket, le versionnement doit également être activé pour le bucket. Le versionnement des compartiments est une méthode qui permet de stocker plusieurs variantes d'un objet S3 dans le même compartiment. En outre, seul le propriétaire du bucket connecté en tant qu'utilisateur root peut activer la suppression MFA et effectuer des actions de suppression sur le bucket. Vous ne pouvez pas utiliser la suppression MFA avec un bucket qui possède une configuration de cycle de vie.

Correction

Pour plus d'informations sur l'activation de la gestion des versions et la configuration de la suppression des MFA pour un compartiment S3, consultez la section Configuration de la suppression des MFA dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/3.8, CIS AWS Foundations Benchmark v3.0. 0/31.8, PCI DSS v4.0. 1/102.1.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS:::Account`

Règle AWS Config : cloudtrail-all-write-s3-data-event-check

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un Compte AWS compte possède au moins un journal AWS CloudTrail multirégional qui enregistre tous les événements d'écriture de données pour les compartiments Amazon S3. Le contrôle échoue si le compte ne dispose pas d'un historique multirégional qui enregistre les événements d'écriture de données pour les compartiments S3.

Les opérations S3 au niveau de l'objet, telles que`GetObject`, et `DeleteObjectPutObject`, sont appelées événements de données. Par défaut, CloudTrail n'enregistre pas les événements de données, mais vous pouvez configurer des traces pour enregistrer les événements de données pour les compartiments S3. Lorsque vous activez la journalisation au niveau de l'objet pour les

événements d'écriture de données, vous pouvez enregistrer chaque accès individuel à un objet (fichier) dans un compartiment S3. L'activation de la journalisation au niveau de l'objet peut vous aider à répondre aux exigences de conformité des données, à effectuer une analyse de sécurité complète, à surveiller des modèles spécifiques de comportement des utilisateurs dans vos Compte AWS compartiments S3 et à prendre des mesures concernant l'activité de l'API au niveau des objets dans vos compartiments S3 à l'aide d'Amazon Events. CloudWatch Ce contrôle produit un `PASSED` résultat si vous configurez un journal multirégional qui enregistre en écriture seule ou tous les types d'événements de données pour tous les compartiments S3.

Correction

Pour activer la journalisation au niveau des objets pour les compartiments S3, consultez la section Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet

Exigences associées : CIS AWS Foundations Benchmark v5.0. 0/3.9, CIS AWS Foundations Benchmark v3.0. 0/39.9, PCI DSS v4.0. 1/102.1.1

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::::Account`

Règle AWS Config : cloudtrail-all-read-s3-data-event-check

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un Compte AWS compte possède au moins un journal AWS CloudTrail multirégional qui enregistre tous les événements de lecture de données pour les compartiments Amazon S3. Le contrôle échoue si le compte ne dispose pas d'un historique multirégional qui enregistre les événements de lecture de données pour les compartiments S3.

Les opérations S3 au niveau de l'objet, telles que`GetObject`, et `DeleteObject``PutObject`, sont appelées événements de données. Par défaut, CloudTrail n'enregistre pas les événements de données, mais vous pouvez configurer des traces pour enregistrer les événements de données

pour les compartiments S3. Lorsque vous activez la journalisation au niveau de l'objet pour les événements de lecture de données, vous pouvez enregistrer chaque accès individuel à un objet (fichier) dans un compartiment S3. L'activation de la journalisation au niveau de l'objet peut vous aider à répondre aux exigences de conformité des données, à effectuer une analyse de sécurité complète, à surveiller des modèles spécifiques de comportement des utilisateurs dans vos Compte AWS compartiments S3 et à prendre des mesures concernant l'activité de l'API au niveau des objets dans vos compartiments S3 à l'aide d'Amazon Events. CloudWatch Ce contrôle produit un `PASSED` résultat si vous configurez un journal multirégional qui enregistre en lecture seule ou tous les types d'événements de données pour tous les compartiments S3.

Correction

Pour activer la journalisation au niveau des objets pour les compartiments S3, consultez la section Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

Exigences associées : PCI DSS v4.0. 1/14,44

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::S3::MultiRegionAccessPoint`

AWS Config règle : `s3-mrap-public-access-blocked` (règle CSPM personnalisée de Security Hub)

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les paramètres de blocage de Multi-Region l'accès public d'un point d'accès Amazon S3 sont activés. Le contrôle échoue lorsque les paramètres de blocage de l' Multi-Region accès public ne sont pas activés sur le point d'accès.

Les ressources accessibles au public peuvent donner lieu à un accès non autorisé, à des violations de données ou à l'exploitation de vulnérabilités. Restreindre l'accès par le biais de mesures d'authentification et d'autorisation permet de protéger les informations sensibles et de préserver l'intégrité de vos ressources.

Correction

Par défaut, tous les paramètres de blocage de l'accès public sont activés pour un point Multi-Region d'accès S3. Pour plus d'informations, consultez la section Blocage de l'accès public à l'aide de points Multi-Region d'accès Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service. Vous ne pouvez pas modifier les paramètres de blocage de l'accès public pour un point d' Multi-Region accès une fois celui-ci créé.

[S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie

Catégorie : Protéger > Protection des données

Gravité : Faible

Type de ressource : `AWS::S3Express::DirectoryBucket`

Règle AWS Config : s3express-dir-bucket-lifecycle-rules-check

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`targetExpirationDays`	Nombre de jours, après la création de l'objet, pendant lesquels celui-ci doit expirer.	Entier	1 sur 2147483647	Aucune valeur par défaut

Ce contrôle vérifie si les règles de cycle de vie sont configurées pour un compartiment d'annuaire S3. Le contrôle échoue si les règles de cycle de vie ne sont pas configurées pour le compartiment de répertoire ou si une règle de cycle de vie pour le compartiment spécifie des paramètres d'expiration qui ne correspondent pas à la valeur de paramètre que vous spécifiez éventuellement.

Dans Amazon S3, une configuration de cycle de vie est un ensemble de règles qui définissent les actions qu'Amazon S3 doit appliquer à un groupe d'objets dans un compartiment. Pour un compartiment d'annuaire S3, vous pouvez créer une règle de cycle de vie qui spécifie la date

d'expiration des objets en fonction de leur âge (en jours). Vous pouvez également créer une règle de cycle de vie qui supprime les chargements partitionnés incomplets. Contrairement à d'autres types de compartiments S3, tels que les compartiments à usage général, les compartiments de répertoire ne prennent pas en charge d'autres types d'actions pour les règles de cycle de vie, telles que la transition d'objets entre les classes de stockage.

Correction

Pour définir une configuration de cycle de vie pour un compartiment d'annuaire S3, créez une règle de cycle de vie pour le compartiment. Pour plus d'informations, consultez la section Création et gestion d'une configuration de cycle de vie pour votre compartiment d'annuaire dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Contrôles CSPM de Security Hub pour l'IA SageMaker

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon SageMaker AI. Les commandes ne sont peut-être pas disponibles dans tous Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet

Exigences associées : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.1.1, PCI DSS v3.2. 1/13.1.1, PCI DSS v3.2. 1/13.2.2, PCI DSS v3.2. 1/13.4.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v4.0. 1/14,44

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Élevée

Type de ressource : `AWS::SageMaker::NotebookInstance`

Règle AWS Config : sagemaker-notebook-no-direct-internet-access

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si l'accès direct à Internet est désactivé pour une instance de bloc-notes SageMaker AI. Le contrôle échoue si le `DirectInternetAccess` champ est activé pour l'instance de bloc-notes.

Si vous configurez votre instance SageMaker AI sans VPC, l'accès direct à Internet est activé par défaut sur votre instance. Vous devez configurer votre instance avec un VPC et modifier le paramètre par défaut sur Désactiver—Accès à Internet via un VPC. Pour entraîner ou héberger des modèles à partir d'un ordinateur portable, vous avez besoin d'un accès Internet. Pour activer l'accès à Internet, votre VPC doit disposer d'un point de terminaison d'interface (AWS PrivateLink) ou d'une passerelle NAT et d'un groupe de sécurité qui autorise les connexions sortantes. Pour en savoir plus sur la façon de connecter une instance de bloc-notes aux ressources d'un VPC, voir Connecter une instance de bloc-notes aux ressources d'un VPC dans le guide du développeur Amazon SageMaker AI. Vous devez également vous assurer que l'accès à votre configuration d' SageMaker IA est limité aux seuls utilisateurs autorisés. Limitez les autorisations IAM qui permettent aux utilisateurs de modifier les paramètres et les ressources de l' SageMaker IA.

Correction

Vous ne pouvez pas modifier le paramètre d'accès à Internet après avoir créé une instance de bloc-notes. Au lieu de cela, vous pouvez arrêter, supprimer et recréer l'instance dont l'accès Internet est bloqué. Pour supprimer une instance de bloc-notes qui permet un accès direct à Internet, voir Utiliser des instances de bloc-notes pour créer des modèles : nettoyer dans le guide du développeur Amazon SageMaker AI. Pour recréer une instance de bloc-notes qui refuse l'accès à Internet, voir Créer une instance de bloc-notes. Pour Réseau, Accès direct à Internet, choisissez Désactiver—Accès à Internet via un VPC.

[SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Élevée

Type de ressource : `AWS::SageMaker::NotebookInstance`

Règle AWS Config : sagemaker-notebook-instance-inside-vpc

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une instance de bloc-notes Amazon SageMaker AI est lancée dans un cloud privé virtuel (VPC) personnalisé. Ce contrôle échoue si une instance de bloc-notes SageMaker AI n'est pas lancée dans un VPC personnalisé ou si elle est lancée dans le VPC du service SageMaker AI.

Les sous-réseaux sont une plage d'adresses IP au sein d'un VPC. Nous vous recommandons de conserver vos ressources dans un VPC personnalisé dans la mesure du possible afin de garantir une protection réseau sécurisée de votre infrastructure. Un Amazon VPC est un réseau virtuel qui vous Compte AWS est dédié. Avec un Amazon VPC, vous pouvez contrôler l'accès réseau et la connectivité Internet de vos instances SageMaker AI Studio et notebook.

Correction

Vous ne pouvez pas modifier le paramètre VPC après avoir créé une instance de bloc-notes. Au lieu de cela, vous pouvez arrêter, supprimer et recréer l'instance. Pour obtenir des instructions, consultez la section Utiliser des instances de bloc-notes pour créer des modèles : nettoyage dans le guide du développeur Amazon SageMaker AI.

[SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes

Exigences connexes : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Catégorie : Protéger > Gestion sécurisée des accès > Restrictions d'accès pour les utilisateurs root

Gravité : Élevée

Type de ressource : `AWS::SageMaker::NotebookInstance`

Règle AWS Config : sagemaker-notebook-instance-root-access-check

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'accès root est activé pour une instance de bloc-notes Amazon SageMaker AI. Le contrôle échoue si l'accès root est activé pour une instance SageMaker AI Notebook.

Conformément au principe du moindre privilège, il est recommandé de restreindre l'accès root aux ressources de l'instance afin d'éviter un surprovisionnement involontaire des autorisations.

Correction

Pour restreindre l'accès root aux instances de bloc-notes SageMaker AI, voir Contrôler l'accès root à une instance de bloc-notes SageMaker AI dans le guide du développeur Amazon SageMaker AI.

[SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1

Exigences connexes : NIST.800-53.r5 CP-10 NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SA-13

Catégorie : Restaurer > Résilience > Haute disponibilité

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::EndpointConfig`

Règle AWS Config : sagemaker-endpoint-config-prod-instance-count

Type de programme : Périodique

Paramètres : Aucun

Ce contrôle vérifie si les variantes de production d'un point de terminaison Amazon SageMaker AI ont un nombre initial d'instances supérieur à 1. Le contrôle échoue si les variantes de production du terminal ne possèdent qu'une seule instance initiale.

Les variantes de production exécutées avec un nombre d'instances supérieur à 1 permettent une redondance des instances multi-AZ gérée par l'IA. SageMaker Le déploiement de ressources dans plusieurs zones de disponibilité est une AWS bonne pratique pour garantir une haute disponibilité au sein de votre architecture. La haute disponibilité vous aide à vous remettre des incidents de sécurité.

> **Note**
>
> Ce contrôle s'applique uniquement à la configuration des terminaux basée sur une instance.

Correction

Pour plus d'informations sur les paramètres de configuration des terminaux, consultez la section Créer une configuration des terminaux dans le guide du développeur Amazon SageMaker AI.

[SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::Model`

Règle AWS Config : sagemaker-model-isolation-enabled

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'isolation réseau est activée sur un modèle hébergé par Amazon SageMaker AI. Le contrôle échoue si le `EnableNetworkIsolation` paramètre du modèle hébergé est défini sur`False`.

SageMaker La formation à l'IA et les conteneurs d'inférence déployés sont activés par défaut sur Internet. Si vous ne souhaitez pas que l' SageMaker IA fournisse un accès réseau externe à vos conteneurs d'entraînement ou d'inférence, vous pouvez activer l'isolation du réseau. Si vous activez l'isolation réseau, aucun appel réseau entrant ou sortant ne peut être effectué vers ou depuis le conteneur modèle, y compris les appels vers ou depuis un autre conteneur. Services AWS En outre, aucune information AWS d'identification n'est mise à la disposition de l'environnement d'exécution du conteneur. L'activation de l'isolation du réseau permet d'empêcher tout accès involontaire à vos ressources d' SageMaker IA depuis Internet.

> **Note**
>
> Le 13 août 2025, Security Hub CSPM a modifié le titre et la description de ce contrôle. Le nouveau titre et la nouvelle description reflètent plus précisément le fait que le contrôle vérifie le réglage du `EnableNetworkIsolation` paramètre des modèles hébergés par Amazon SageMaker AI. Auparavant, le titre de ce contrôle était : SageMaker models should block inbound traffic

Correction

Pour plus d'informations sur l'isolation du réseau pour les modèles d' SageMaker IA, voir Exécuter des conteneurs d'entraînement et d'inférence en mode sans Internet dans le guide du développeur Amazon SageMaker AI. Lorsque vous créez un modèle, vous pouvez activer l'isolation du réseau en définissant la valeur du `EnableNetworkIsolation` paramètre sur`True`.

[SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::SageMaker::AppImageConfig`

Règle AWS Config : sagemaker-app-image-config-tagged

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredKeyTags`	Liste de clés de balises non liées au système qui doivent être attribuées à une ressource évaluée. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si la configuration d'image d'une application Amazon SageMaker AI (`AppImageConfig`) possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si la configuration de l'image de l'application ne comporte aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la configuration de l'image de l'application ne comporte

aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et ont un `aws:` préfixe.

Une étiquette est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les actions et les notifications des propriétaires de ressources. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, consultez la section Définition des autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour ajouter des balises à la configuration d'image d'une application Amazon SageMaker AI (`AppImageConfig`), vous pouvez utiliser le AddTags fonctionnement de l'API SageMaker AI ou, si vous utilisez la AWS CLI, exécuter la commande add-tags.

[SageMaker.7] les SageMaker images doivent être étiquetées

Catégorie : Identifier > Inventaire > Marquage

Gravité : Faible

Type de ressource : `AWS::SageMaker::Image`

Règle AWS Config : sagemaker-image-tagged

Type de calendrier : Déclenché par un changement

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut de Security Hub CSPM
`requiredKeyTags`	Liste de clés de balises non liées au système qui doivent être attribuées à une ressource évaluée. Les touches des tags distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés de tag qui répondent aux AWS exigences.	Aucune valeur par défaut

Ce contrôle vérifie si une image Amazon SageMaker AI possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si l'image ne possède aucune clé de balise ou si elle ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'image ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et ont un `aws:` préfixe.

Une étiquette est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les actions et les notifications des propriétaires de ressources. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, consultez la section Définition des autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de

nombreuses personnes Services AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour ajouter des balises à une image Amazon SageMaker AI, vous pouvez utiliser le AddTags fonctionnement de l'API SageMaker AI ou, si vous utilisez le AWS CLI, exécuter la commande add-tags.

[SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge

Catégorie : Détecter > Gestion des vulnérabilités, des correctifs et des versions

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::NotebookInstance`

Règle AWS Config : sagemaker-notebook-instance-platform-version

Type de programme : Périodique

Paramètres :

- `supportedPlatformIdentifierVersions`: `notebook-al2023-v1` (non personnalisable)

Ce contrôle vérifie si une instance de bloc-notes Amazon SageMaker AI est configurée pour s'exécuter sur une plate-forme prise en charge, en fonction de l'identifiant de plate-forme spécifié pour l'instance de bloc-notes. Le contrôle échoue si l'instance de bloc-notes est configurée pour s'exécuter sur une plate-forme qui n'est plus prise en charge.

Si la plate-forme d'une instance de bloc-notes Amazon SageMaker AI n'est plus prise en charge, il est possible qu'elle ne reçoive pas de correctifs de sécurité, de corrections de bogues ou d'autres types de mises à jour. Les instances Notebook peuvent continuer à fonctionner, mais elles ne recevront pas de mises à jour de sécurité de l' SageMaker IA ni de corrections de bogues critiques. Vous assumez les risques liés à l'utilisation d'une plateforme non prise en charge. Pour plus d'informations, consultez la section JupyterLab Gestion des versions dans le guide du développeur Amazon SageMaker AI.

Correction

Pour plus d'informations sur les plateformes actuellement prises en charge par Amazon SageMaker AI et sur la manière de migrer vers celles-ci, consultez les instances de bloc-notes Amazon Linux 2 dans le guide du développeur Amazon SageMaker AI.

[SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::DataQualityJobDefinition`

Règle AWS Config : sagemaker-data-quality-job-encrypt-in-transit

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement du trafic inter-conteneurs est activé pour une définition de tâche relative à la qualité des données Amazon SageMaker AI. Le contrôle échoue si le chiffrement n'est pas activé pour le trafic inter-conteneurs dans la définition d'une tâche qui surveille la qualité et la dérive des données.

L'activation du chiffrement du trafic entre conteneurs protège les données ML sensibles lors du traitement distribué pour l'analyse de la qualité des données.

Correction

Pour plus d'informations sur le chiffrement du trafic inter-conteneurs pour Amazon SageMaker AI, consultez la section Protéger les communications entre les instances de calcul ML dans le cadre d'une formation distribuée dans le guide du développeur Amazon SageMaker AI. Lorsque vous créez une définition de tâche de qualité des données, vous pouvez activer le chiffrement du trafic inter-conteneurs en définissant la valeur du `EnableInterContainerTrafficEncryption` paramètre sur. `True`

[SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::ModelExplainabilityJobDefinition`

Règle AWS Config : sagemaker-model-explainability-job-encrypt-in-transit

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement du trafic inter-conteneurs est activé pour une définition de tâche d'explicabilité d'un SageMaker modèle Amazon. Le contrôle échoue si le chiffrement du trafic inter-conteneurs n'est pas activé dans la définition de la tâche d'explicabilité du modèle.

L'activation du chiffrement du trafic entre conteneurs protège les données ML sensibles telles que les données de modèle, les ensembles de données d'entraînement, les résultats de traitement intermédiaires, les paramètres et les pondérations des modèles lors du traitement distribué à des fins d'analyse d'explicabilité.

Correction

Pour une définition de tâche d'explicabilité d'un SageMaker modèle existante, le chiffrement du trafic inter-conteneurs ne peut pas être mis à jour sur place. Pour créer une nouvelle définition de tâche d'explicabilité du SageMaker modèle avec le chiffrement du trafic inter-conteneurs activé, utilisez l'API ou l'interface de ligne de commande ou définissez CloudFormation sur. `EnableInterContainerTrafficEncryption` `True`

[SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::DataQualityJobDefinition`

Règle AWS Config : sagemaker-data-quality-job-isolation

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'isolation réseau est activée pour une définition de tâche de surveillance de la qualité des données Amazon SageMaker AI. Le contrôle échoue si l'isolation réseau est désactivée pour la définition d'une tâche qui surveille la qualité et la dérive des données.

L'isolation du réseau réduit la surface d'attaque et empêche l'accès externe, protégeant ainsi contre les accès externes non autorisés, l'exposition accidentelle des données et l'exfiltration potentielle de données.

Correction

Pour plus d'informations sur l'isolation du réseau pour l' SageMaker IA, voir Exécuter des conteneurs de formation et d'inférence en mode sans Internet dans le guide du développeur Amazon SageMaker AI. Lorsque vous créez une définition de tâche de qualité des données, vous pouvez activer l'isolation réseau en définissant la valeur du `EnableNetworkIsolation` paramètre sur`True`.

[SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée

Catégorie : Protéger > Configuration réseau sécurisée > Configuration de la politique des ressources

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::ModelBiasJobDefinition`

Règle AWS Config : sagemaker-model-bias-job-isolation

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'isolation réseau est activée pour une définition de tâche de biais de SageMaker modèle. Le contrôle échoue si l'isolation réseau n'est pas activée pour la définition des tâches de biais du modèle.

L'isolation du réseau empêche les tâches utilisant des SageMaker modèles biaisés de communiquer avec des ressources externes via Internet. En activant l'isolation du réseau, vous vous assurez que les conteneurs de la tâche ne peuvent pas établir de connexions sortantes, ce qui réduit la surface d'attaque et protège les données sensibles contre l'exfiltration. Cela est particulièrement important pour les tâches traitant des données réglementées ou sensibles.

Correction

Pour activer l'isolation réseau, vous devez créer une nouvelle définition de tâche de biais de modèle dont le `EnableNetworkIsolation` paramètre est défini sur`True`. L'isolation du réseau ne peut pas être modifiée après la création de la définition de tâche. Pour créer une nouvelle définition des tâches liées au biais des modèles, consultez CreateModelBiasJobDefinition le guide du développeur Amazon SageMaker AI.

[SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::ModelQualityJobDefinition`

Règle AWS Config : ssagemaker-model-quality-job-encrypt-in-transit

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement en transit est activé pour le trafic inter-conteneurs dans les définitions de tâches relatives à la qualité des SageMaker modèles Amazon. Le contrôle échoue si le chiffrement du trafic inter-conteneurs n'est pas activé pour une définition de tâche de qualité de modèle.

Inter-container le chiffrement du trafic protège les données transmises entre les conteneurs lors des tâches de surveillance de la qualité des modèles distribués. Par défaut, le trafic inter-conteneurs n'est pas chiffré. L'activation du chiffrement permet de préserver la confidentialité des données pendant le traitement et favorise la conformité aux exigences réglementaires en matière de protection des données en transit.

Correction

Pour activer le chiffrement du trafic inter-conteneurs pour la définition de tâche de qualité de votre SageMaker modèle Amazon, vous devez recréer la définition de tâche avec la configuration de chiffrement en transit appropriée. Pour créer une définition de poste de qualité pour un modèle, consultez CreateModelQualityJobDefinition le guide du développeur Amazon SageMaker AI.

[SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::MonitoringSchedule`

Règle AWS Config : sagemaker-monitoring-schedule-isolation

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'isolation réseau est activée pour les planifications de SageMaker surveillance d'Amazon. Le contrôle échoue si un calendrier de surveillance est EnableNetworkIsolation défini sur faux ou n'est pas configuré

L'isolation du réseau empêche les tâches de surveillance de passer des appels réseau sortants, réduisant ainsi la surface d'attaque en éliminant l'accès à Internet depuis les conteneurs.

Correction

Pour plus d'informations sur la configuration de l'isolation réseau dans le NetworkConfig paramètre lors de la création ou de la mise à jour d'un calendrier de surveillance, consultez CreateMonitoringSchedule ou UpdateMonitoringSchedule consultez le Amazon SageMaker AI Developer Guide.

[SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::ModelBiasJobDefinition`

Règle AWS Config : sagemaker-model-bias-job-encrypt-in-transit

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement du trafic inter-conteneurs est activé pour les définitions de tâches de biais du SageMaker modèle Amazon lors de l'utilisation de plusieurs instances de calcul. Le contrôle échoue s'il `EnableInterContainerTrafficEncryption` est défini sur false ou s'il n'est pas configuré pour les définitions de tâches comportant un nombre d'instances supérieur ou égal à 2.

Inter-container le chiffrement du trafic protège les données transmises entre les instances de calcul lors des tâches de surveillance du biais du modèle distribué. Le chiffrement empêche l'accès non autorisé aux informations relatives au modèle, telles que les pondérations transmises entre les instances.

Correction

Pour activer le chiffrement du trafic inter-conteneurs pour les définitions de tâches biaisées par le SageMaker modèle, définissez le `EnableInterContainerTrafficEncryption` paramètre sur `True` lorsque la définition de tâche utilise plusieurs instances de calcul. Pour plus d'informations sur la protection des communications entre les instances de calcul ML, voir Protéger les communications entre les instances de calcul ML dans le cadre d'une formation distribuée dans le guide du développeur Amazon SageMaker AI.

[SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux

Catégorie : Protéger > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::Model`

Règle AWS Config : sagemaker-model-private-registry-required

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si un modèle Amazon SageMaker AI extrait l'image du conteneur depuis un registre privé dans un VPC pour le conteneur principal. Le contrôle échoue si l'image n'est pas configurée ou si le mode d'accès au référentiel l'est`Platform`.

L'utilisation d'un registre Docker privé dans un VPC pour les SageMaker modèles de conteneurs garantit que les images des conteneurs sont extraites de sources fiables et contrôlées au sein de votre VPC. Il garantit également l'accès aux images de conteneurs via les points de terminaison VPC, sans passer par l'Internet public.

Correction

Pour configurer des registres Docker privés pour les conteneurs d'inférence en temps réel SageMaker AI, consultez la section Utiliser un registre Docker privé pour les conteneurs d' Real-Time inférence dans le Guide du développeur Amazon SageMaker AI.

[SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::FeatureGroup`

Règle AWS Config : sagemaker-featuregroup-encryption-at-rest

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une boutique SageMaker hors ligne Amazon pour un groupe de fonctionnalités est cryptée au repos à l'aide d'une AWS KMS clé. Le contrôle échoue si le stockage S3 du magasin hors ligne d'un groupe de fonctionnalités n'est pas chiffré à l'aide d'une clé KMS.

L'utilisation de boutiques hors ligne gérées par le client AWS KMS keys pour le reste des boutiques hors ligne du groupe de SageMaker fonctionnalités offre une sécurité renforcée. Customer-managed Les clés KMS vous permettent de contrôler totalement le cycle de vie des clés de chiffrement et les politiques relatives aux clés. En outre, toutes les utilisations de clés de chiffrement peuvent être enregistrées et surveillées à des AWS CloudTrail fins d'auditabilité.

Correction

Pour plus d'informations sur l'activation du chiffrement au repos pour les boutiques hors ligne du SageMaker Feature Store à l'aide de clés AWS KMS gérées par le client, consultez la section Sécurité et contrôle d'accès dans le guide du développeur Amazon SageMaker AI.

[SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés

Exigences connexes : NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::FeatureGroup`

Règle AWS Config : sagemaker-featuregroup-online-store-encryption

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une boutique SageMaker en ligne Amazon pour un groupe de fonctionnalités avec un stockage standard est cryptée au repos à l'aide d'une AWS KMS clé. Le contrôle échoue si le chiffrement par clé KMS n'est pas configuré pour la boutique en ligne.

L'utilisation du chiffrement géré par le client AWS KMS keys dans d'autres boutiques en ligne proposant des groupes de SageMaker fonctionnalités permet de renforcer la sécurité. Customer-managed Les clés KMS vous permettent de contrôler totalement le cycle de vie des clés de chiffrement et les politiques relatives aux clés. En outre, toutes les utilisations de clés de chiffrement peuvent être enregistrées et surveillées à des AWS CloudTrail fins d'auditabilité.

Correction

Pour plus d'informations sur l'activation du chiffrement au repos pour les boutiques en ligne SageMaker Feature Store à l'aide de clés AWS KMS gérées par le client, consultez la section Sécurité et contrôle d'accès dans le guide du développeur Amazon SageMaker AI.

[SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs

Catégorie : Protéger > Configuration réseau sécurisée > Ressources au sein du VPC

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::Model`

Règle AWS Config : sagemaker-model-multicontainer-private-registry

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si les modèles Amazon SageMaker AI dotés de pipelines d'inférence multi-conteneurs extraient des images de conteneurs d'un registre Docker privé dans un VPC. Le contrôle échoue si une définition de conteneur n'a pas de configuration d'image ou si le mode d'accès au référentiel est défini sur platform.

L'utilisation d'un registre Docker privé dans un VPC pour les pipelines d'inférence multi-conteneurs SageMaker AI garantit que les images de conteneurs sont extraites de sources fiables et contrôlées au sein de votre VPC. Cela garantit que les images des conteneurs sont accessibles via les points de terminaison VPC, sans passer par l'Internet public, ce qui réduit le risque d'attaques de la chaîne d'approvisionnement ou de falsification d'images.

Correction

Pour configurer des registres Docker privés pour les conteneurs d'inférence en temps réel SageMaker AI, consultez la section Utiliser un registre Docker privé pour les conteneurs d' Real-Time inférence dans le Guide du développeur Amazon SageMaker AI.

[SageMaker.20] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir l'isolation réseau activée

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::SageMaker::ModelExplainabilityJobDefinition`

Règle AWS Config : sagemaker-model-explainability-job-network-isolation

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'isolation réseau est activée dans la définition d'une tâche d'explicabilité d'un modèle d' SageMaker IA. Le contrôle échoue si l'isolation réseau n'est pas activée dans la définition de tâche.

L'isolation du réseau empêche les conteneurs de tâches d'explicabilité des modèles d'effectuer des appels réseau sortants, ce qui réduit le risque d'exfiltration de données et fournit une défense approfondie contre les données sensibles des modèles et de formation.

Correction

Pour activer l'isolation du réseau pour la définition de tâche d'explicabilité d'un modèle d' SageMaker IA, définissez cette option sur `true` lors `NetworkConfig.EnableNetworkIsolation` de la création de la définition de tâche. Pour plus d'informations sur l'isolation du réseau pour l' SageMaker IA, voir Exécuter des conteneurs de formation et d'inférence en mode sans Internet dans le guide du développeur Amazon SageMaker AI.

[SageMaker.21] les instances de SageMaker bloc-notes doivent être chiffrées avec la gestion par le client AWS KMS clés

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::NotebookInstance`

Règle AWS Config : sagemaker-notebook-instance-storage-vol-kms-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une instance de bloc-notes SageMaker AI est configurée avec une AWS KMS clé pour le chiffrement du volume de stockage. Le contrôle échoue si aucune clé KMS n'est configurée pour l'instance du bloc-notes.

Le chiffrement des données au repos à l'aide d'une clé KMS gérée par le client fournit un contrôle d'accès supplémentaire par rapport au cryptage AWS géré par défaut. SageMaker Les instances AI Notebook stockent les blocs-notes des utilisateurs, les ensembles de données, les artefacts de modèle et les données de traitement temporaires sur des volumes de stockage ML. Une clé gérée par le client permet un contrôle précis des politiques de clés, la journalisation des CloudTrail audits de l'utilisation des clés et la conformité aux frameworks nécessitant un cryptage contrôlé par le client.

Correction

Pour configurer une clé KMS pour une instance de bloc-notes SageMaker AI, consultez la section Instances de bloc-notes, tâches SageMaker AI et points de terminaison dans le guide du développeur Amazon SageMaker AI. Notez que cela ne `KmsKeyId` peut être défini qu'au moment de la création de l'instance de bloc-notes. Pour y remédier, créez une nouvelle instance de bloc-notes avec la clé KMS spécifiée et migrez vos données depuis l'instance existante.

[SageMaker.22] les calendriers SageMaker de surveillance doivent avoir activé le cryptage du trafic inter-conteneurs

Catégorie : Protéger - Protection des données - Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::MonitoringSchedule`

Règle AWS Config : sagemaker-monitoring-schedule-traffic-encryption

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si le chiffrement est activé pour le trafic inter-conteneurs dans un calendrier de surveillance Amazon SageMaker AI. Le contrôle échoue si le chiffrement n'est pas activé pour le trafic inter-conteneurs dans la définition de la tâche de surveillance.

Inter-container le chiffrement du trafic garantit que les données transmises entre les conteneurs pendant les tâches de surveillance sont cryptées en transit. Sans ce chiffrement, les données sensibles traitées lors de la surveillance des modèles pourraient être exposées à un accès non autorisé au sein du réseau. L'activation de ce paramètre permet de répondre aux exigences de conformité en matière de protection des données en transit.

Correction

Pour un calendrier de surveillance de SageMaker l'IA existant, le chiffrement du trafic inter-conteneurs ne peut pas être mis à jour sur place. Pour créer un nouveau calendrier de surveillance de l' SageMaker IA avec le chiffrement du trafic inter-conteneurs activé, utilisez l'API ou la CLI ou CloudFormation définissez `EnableInterContainerTrafficEncryption` sur `true` `NetworkConfig` dans le`MonitoringJobDefinition`.

[SageMaker.23] les expériences SageMaker d'inférence doivent avoir un volume de stockage d'instance chiffré et géré par le client AWS KMS clés

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::InferenceExperiment`

Règle AWS Config : sagemaker-inf-experiment-instance-storage-kms-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une expérience d'inférence d' SageMaker IA est configurée avec une AWS KMS clé, par exemple le chiffrement du volume de stockage. Le contrôle échoue si aucune clé KMS n'est spécifiée pour le chiffrement du volume de stockage de l'instance.

Le chiffrement des volumes de stockage d'instance à l'aide de clés KMS gérées par le client permet de centraliser la gestion des clés, la journalisation des audits et le contrôle de la rotation des clés pour les artefacts de modèle et les données d'inférence temporaires stockées sur les instances de calcul ML lors de tests parallèles.

Correction

Pour configurer une clé KMS pour une expérience d'inférence d' SageMaker IA, spécifiez le `KmsKey` paramètre lors de l'appel`CreateInferenceExperiment`. Il `KmsKey` peut s'agir d'un ID de clé KMS, d'un ARN, d'un alias ou d'un alias ARN. Le rôle d'exécution de l' SageMaker IA doit disposer `kms:CreateGrant` d'une autorisation sur la clé. Pour plus d'informations sur la spécification d'une AWS KMS clé d' SageMaker IA gérée par le client, consultez la section Instances de bloc-notes, tâches d' SageMaker IA et points de terminaison dans le guide du développeur Amazon SageMaker AI.

[SageMaker.24] les expériences SageMaker d'inférence doivent avoir un stockage de données crypté et géré par le client AWS KMS clés

Catégorie : Protéger - Protection des données - Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SageMaker::InferenceExperiment`

Règle AWS Config : sagemaker-inf-experiment-data-storage-kms-encrypted

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si une expérience d'inférence d' SageMaker IA avec la capture de données activée possède une clé KMS configurée pour crypter les données capturées au repos. Le contrôle échoue si la configuration de stockage des données ne spécifie pas de clé KMS pour le chiffrement.

Le chiffrement des données de demande et de réponse d'inférence capturées à l'aide de clés KMS gérées par le client garantit la protection des charges utiles d'inférence sensibles stockées dans Amazon S3 grâce à des fonctionnalités centralisées de gestion des clés et d'audit.

Correction

Pour configurer une clé KMS pour le stockage de données dans le cadre d'une expérience d'inférence d' SageMaker IA, spécifiez le `KmsKey` champ à l'intérieur `DataStorageConfig` lors de l'appel`CreateInferenceExperiment`. `KmsKey`Chiffre les données de demande d'inférence et de réponse capturées au repos dans le compartiment Amazon S3 spécifié. Pour plus d'informations sur la spécification d'une AWS KMS clé d' SageMaker IA gérée par le client, consultez la section Instances de bloc-notes, tâches d' SageMaker IA et points de terminaison dans le guide du développeur Amazon SageMaker AI.

[SageMaker.25] les définitions de tâches relatives à la qualité des SageMaker modèles doivent avoir l'isolation réseau activée

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Élevée

Type de ressource : `AWS::SageMaker::ModelQualityJobDefinition`

Règle AWS Config : sagemaker-model-quality-job-definition-isolation

Type de calendrier : Déclenché par un changement

Paramètres : Aucun

Ce contrôle vérifie si l'isolation réseau est activée pour une définition de tâche de qualité d'un modèle Amazon SageMaker AI. Le contrôle échoue si l'isolation réseau n'est pas activée dans la définition de la tâche de qualité du modèle.

L'isolation du réseau réduit la surface d'attaque et empêche l'accès externe, protégeant ainsi contre les accès externes non autorisés, l'exposition accidentelle des données et l'exfiltration potentielle de données.

Correction

Lorsque vous créez une définition de tâche de qualité du modèle, vous pouvez activer l'isolation du réseau en définissant la valeur du `EnableNetworkIsolation` paramètre sur`True`. Pour plus d'informations sur l'isolation du réseau pour l' SageMaker IA, voir Exécuter des conteneurs de

formation et d'inférence en mode sans Internet dans le guide du développeur Amazon SageMaker AI.

Contrôles CSPM de Security Hub pour Secrets Manager

Ces AWS Security Hub CSPM contrôles évaluent le AWS Secrets Manager service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[SecretsManager.1] La rotation automatique des secrets des secrets de Secrets Manager doit être activée

Exigences associées : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.3.3, PCI DSS v4.0. 1/8.3.9

Catégorie : Protéger - Développement sécurisé

Gravité : Moyenne

Type de ressource : `AWS::SecretsManager::Secret`

Règle AWS Config : `secretsmanager-rotation-enabled-check`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`maximumAllowedRotationFrequency`	Nombre maximum de jours autorisés pour la fréquence de rotation secrète	Entier	1 sur 365	Aucune valeur par défaut

Ce contrôle vérifie si un secret stocké dans AWS Secrets Manager est configuré avec une rotation automatique. Le contrôle échoue si le secret n'est pas configuré avec une rotation automatique.

Si vous fournissez une valeur personnalisée pour le `maximumAllowedRotationFrequency` paramètre, le contrôle est transféré uniquement si le secret est automatiquement pivoté dans la fenêtre de temps spécifiée.

Secrets Manager vous aide à améliorer le niveau de sécurité de votre organisation. Les secrets incluent les informations d'identification de base de données, les mots de passe et les clés d'API tierces. Vous pouvez utiliser Secrets Manager pour stocker les secrets de manière centralisée, les chiffrer automatiquement, contrôler l'accès aux secrets et alterner les secrets de manière sécurisée et automatique.

Secrets Manager peut alterner les secrets. Vous pouvez utiliser la rotation pour remplacer les secrets à long terme par des secrets à court terme. La rotation de vos secrets limite la durée pendant laquelle un utilisateur non autorisé peut utiliser un secret compromis. Pour cette raison, vous devez fréquemment alterner vos secrets. Pour en savoir plus sur la rotation, voir Rotation de vos AWS Secrets Manager secrets dans le guide de AWS Secrets Manager l'utilisateur.

Correction

Pour activer la rotation automatique pour les secrets de Secrets Manager, voir Configurer la rotation automatique pour les AWS Secrets Manager secrets à l'aide de la console dans le Guide de AWS Secrets Manager l'utilisateur. Vous devez choisir et configurer une AWS Lambda fonction de rotation.

[SecretsManager.2] Les secrets de Secrets Manager configurés avec une rotation automatique devraient être correctement pivotés

Exigences associées : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.3.3, PCI DSS v4.0. 1/8.3.9

Catégorie : Protéger - Développement sécurisé

Gravité : Moyenne

Type de ressource : `AWS::SecretsManager::Secret`

Règle AWS Config : `secretsmanager-scheduled-rotation-success-check`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un AWS Secrets Manager secret a été correctement pivoté en fonction du calendrier de rotation. Le contrôle échoue si tel `RotationOccurringAsScheduled` est le cas`false`. Le contrôle évalue uniquement les secrets dont la rotation est activée.

Secrets Manager vous aide à améliorer le niveau de sécurité de votre organisation. Les secrets incluent les informations d'identification de base de données, les mots de passe et les clés d'API tierces. Vous pouvez utiliser Secrets Manager pour stocker les secrets de manière centralisée, les chiffrer automatiquement, contrôler l'accès aux secrets et alterner les secrets de manière sécurisée et automatique.

Secrets Manager peut alterner les secrets. Vous pouvez utiliser la rotation pour remplacer les secrets à long terme par des secrets à court terme. La rotation de vos secrets limite la durée pendant laquelle un utilisateur non autorisé peut utiliser un secret compromis. Pour cette raison, vous devez fréquemment alterner vos secrets.

En plus de configurer les secrets pour qu'ils pivotent automatiquement, vous devez vous assurer que ces secrets pivotent correctement en fonction du calendrier de rotation.

Pour en savoir plus sur la rotation, voir Rotation de vos AWS Secrets Manager secrets dans le guide de AWS Secrets Manager l'utilisateur.

Correction

Si la rotation automatique échoue, il est possible que Secrets Manager ait rencontré des erreurs lors de la configuration. Pour alterner les secrets dans Secrets Manager, vous utilisez une fonction Lambda qui définit la manière d'interagir avec la base de données ou le service propriétaire du secret.

Pour obtenir de l'aide pour diagnostiquer et corriger les erreurs courantes liées à la rotation des secrets, consultez la section Résolution des problèmes liés à la AWS Secrets Manager rotation des secrets dans le Guide de AWS Secrets Manager l'utilisateur.

[SecretsManager.3] Supprimer les secrets inutilisés du Gestionnaire de Secrets

Exigences connexes : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::SecretsManager::Secret`

Règle AWS Config : `secretsmanager-secret-unused`

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`unusedForDays`	Nombre maximal de jours pendant lesquels un secret peut rester inutilisé	Entier	`1` sur `365`	`90`

Ce contrôle vérifie si un AWS Secrets Manager secret a été consulté dans le délai spécifié. Le contrôle échoue si un secret n'est pas utilisé au-delà de la période spécifiée. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période d'accès, Security Hub CSPM utilise une valeur par défaut de 90 jours.

La suppression des secrets inutilisés est aussi importante que la rotation des secrets. Les secrets non utilisés peuvent être utilisés à mauvais escient par leurs anciens utilisateurs, qui n'ont plus besoin d'accéder à ces secrets. De plus, au fur et à mesure que de plus en plus d'utilisateurs accèdent à un secret, quelqu'un peut l'avoir mal géré et divulgué à une entité non autorisée, ce qui augmente le risque d'abus. La suppression des secrets non utilisés permet de révoquer l'accès secret aux utilisateurs qui n'en ont plus besoin. Cela permet également de réduire le coût d'utilisation de Secrets Manager. Il est donc essentiel de supprimer régulièrement les secrets non utilisés.

Correction

Pour supprimer les secrets inactifs de Secrets Manager, voir Supprimer un AWS Secrets Manager secret dans le Guide de AWS Secrets Manager l'utilisateur.

[SecretsManager.4] Les secrets de Secrets Manager doivent être renouvelés dans un délai spécifié

Exigences associées : NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.3.3, PCI DSS v4.0. 1/8.3.9

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::SecretsManager::Secret`

Règle AWS Config : `secretsmanager-secret-periodic-rotation`

Type de calendrier : Périodique

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`maxDaysSinceRotation`	Nombre maximum de jours pendant lesquels un secret peut rester inchangé	Entier	1 sur 180	90

Ce contrôle vérifie si un AWS Secrets Manager secret fait l'objet d'une rotation au moins une fois dans le délai spécifié. Le contrôle échoue si un secret n'est pas modifié au moins aussi fréquemment. À moins que vous ne fournissiez une valeur de paramètre personnalisée pour la période de rotation, Security Hub CSPM utilise une valeur par défaut de 90 jours.

La rotation des secrets peut vous aider à réduire le risque d'utilisation non autorisée de vos secrets dans votreCompte AWS. Les exemples incluent les informations d'identification de base de données, les mots de passe, les clés d'API tierces et même le texte arbitraire. Si vous ne modifiez pas vos secrets pendant une longue période, ils sont plus susceptibles d'être compromis.

À mesure que de plus en plus d'utilisateurs ont accès à un secret, il est plus probable que quelqu'un l'ait mal géré et l'ait divulgué à une entité non autorisée. Les secrets peuvent être divulgués à travers les journaux et les données de cache. Ils peuvent être partagés à des fins de débogage et ne pas être modifiés ou révoqués une fois le débogage terminé. Pour toutes ces raisons, les secrets doivent faire l'objet d'une rotation fréquente.

Vous pouvez configurer la rotation automatique pour les secrets dansAWS Secrets Manager. Grâce à la rotation automatique, vous pouvez remplacer les secrets à long terme par des secrets à court terme, réduisant ainsi considérablement le risque de compromission. Nous vous recommandons de configurer la rotation automatique des secrets de vos Secrets Manager. Pour plus d'informations, consultez Rotation de vos secrets AWS Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager.

Correction

Pour activer la rotation automatique pour les secrets de Secrets Manager, voir Configurer la rotation automatique pour les AWS Secrets Manager secrets à l'aide de la console dans le Guide de AWS Secrets Manager l'utilisateur. Vous devez choisir et configurer une AWS Lambda fonction de rotation.

[SecretsManager.5] Les secrets de Secrets Manager doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::SecretsManager::Secret`

AWS Configrègle : `tagged-secretsmanager-secret` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS Secrets Manager secret possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le secret ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le secret n'est marqué d'aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un secret de Secrets Manager, voir Tag AWS Secrets Manager secrets dans le Guide de AWS Secrets Manager l'utilisateur.

Contrôles Security Hub CSPM pourAWS Service Catalog

Ce AWS Security Hub CSPM contrôle évalue le AWS Service Catalog service et les ressources. Il se peut que le contrôle ne soit pas disponible du toutRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement

Exigences connexes : NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Catégorie : Protéger - Gestion de l'accès sécurisé

Gravité : Moyenne

Type de ressource : `AWS::ServiceCatalog::Portfolio`

Règle AWS Config : service-catalog-shared-within-organization

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si des AWS Service Catalog actions sont des portefeuilles au sein d'une organisation lorsque l'intégration AWS Organizations est activée. Le contrôle échoue si les portefeuilles ne sont pas partagés au sein d'une organisation.

Le partage de portfolio uniquement au sein des Organisations permet de garantir qu'un portfolio n'est pas partagé avec des personnes incorrectesComptes AWS. Pour partager un portefeuille de Service Catalog avec un compte au sein d'une organisation, Security Hub CSPM recommande d'utiliser `ORGANIZATION_MEMBER_ACCOUNT` plutôt que. `ACCOUNT` Cela simplifie l'administration en régissant l'accès accordé au compte dans l'ensemble de l'organisation. Si votre entreprise a besoin de partager des portefeuilles Service Catalog avec un compte externe, vous pouvez supprimer automatiquement les résultats de ce contrôle ou le désactiver.

Correction

Pour activer le partage de portefeuille avecAWS Organizations, consultez la section Partage avec AWS Organizations dans le guide de AWS Service Catalog l'administrateur.

Contrôles Security Hub CSPM pour Amazon SES

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Simple Email Service (Amazon SES).

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[SES.1] Les listes de contacts SES doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::SES::ContactList`

AWS Configrègle : `tagged-ses-contactlist` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une liste de contacts Amazon SES comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si la liste de contacts ne comporte aucune clé de balise ou si elle ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la liste de contacts n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal

correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une liste de contacts Amazon SES, consultez TagResourcele manuel Amazon SES API v2 Reference.

[SES.2] Les ensembles de configuration SES doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::SES::ConfigurationSet`

AWS Configrègle : `tagged-ses-configurationset` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux	Aucune valeur par défaut

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
	Les touches de tag distinguent les majuscules et minuscules.		AWSexigences.	

Ce contrôle vérifie si un ensemble de configuration Amazon SES comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le jeu de configuration ne comporte aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le jeu de configuration n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un ensemble de configuration Amazon SES, consultez TagResourcele manuel Amazon SES API v2 Reference.

[SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::SES::ConfigurationSet`

Règle AWS Config : ses-sending-tls-required

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un ensemble de configuration Amazon SES nécessite des connexions TLS. Le contrôle échoue si la politique TLS n'est pas définie sur un ensemble de configuration. `'REQUIRE'`

Par défaut, Amazon SES utilise le protocole TLS opportuniste, ce qui signifie que les e-mails peuvent être envoyés non chiffrés s'il est impossible d'établir une connexion TLS avec le serveur de messagerie destinataire. L'application du protocole TLS pour l'envoi d'e-mails garantit que les messages ne sont délivrés que lorsqu'une connexion cryptée sécurisée peut être établie. Cela permet de protéger la confidentialité et l'intégrité du contenu des e-mails lors de leur transmission entre Amazon SES et le serveur de messagerie du destinataire. S'il n'est pas possible d'établir une connexion TLS sécurisée, le message ne sera pas délivré, empêchant ainsi toute exposition potentielle d'informations sensibles.

> **Note**
>
> Bien que le protocole TLS 1.3 soit le mode de livraison par défaut pour Amazon SES, sans l'application des exigences TLS par le biais d'ensembles de configuration, les messages peuvent potentiellement être envoyés en texte brut en cas d'échec d'une connexion TLS. Pour passer ce contrôle, vous devez configurer la politique TLS `'REQUIRE'` dans les options de livraison de votre ensemble de configuration SES. Lorsque le protocole TLS est requis, les messages ne sont délivrés que s'il est possible d'établir une connexion TLS avec le serveur de courrier récepteur.

Correction

Pour configurer Amazon SES afin d'exiger des connexions TLS pour un ensemble de configuration, consultez Amazon SES et les protocoles de sécurité dans le manuel du développeur Amazon SES.

Contrôles Security Hub CSPM pour Amazon SNS

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Simple Notification Service (Amazon SNS). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[SNS.1] Les sujets SNS doivent être chiffrés au repos à l'aide deAWS KMS

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.11, 3.13.16 NIST.800-171.r2

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SNS::Topic`

Règle AWS Config : `sns-encrypted-kms`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une rubrique Amazon SNS est chiffrée au repos à l'aide de clés gérées dans AWS Key Management Service ()AWS KMS. Les contrôles échouent si la rubrique SNS n'utilise pas de clé KMS pour le chiffrement côté serveur (SSE). Par défaut, SNS stocke les messages et les fichiers à l'aide du chiffrement du disque. Pour passer ce contrôle, vous devez choisir d'utiliser plutôt une clé KMS pour le chiffrement. Cela ajoute une couche de sécurité supplémentaire et offre une plus grande flexibilité en matière de contrôle d'accès.

Le chiffrement des données au repos réduit le risque qu'un utilisateur non authentifié accède aux données stockées sur disque. AWS Les autorisations d'API sont nécessaires pour déchiffrer les données avant qu'elles puissent être lues. Nous recommandons de chiffrer les rubriques SNS à l'aide de clés KMS pour renforcer la sécurité.

Correction

Pour activer SSE pour une rubrique SNS, consultez la section Activation du chiffrement côté serveur (SSE) pour une rubrique Amazon SNS dans le manuel Amazon Simple Notification Service Developer Guide. Avant de pouvoir utiliser SSE, vous devez également configurer des AWS KMS key politiques pour autoriser le chiffrement des sujets ainsi que le chiffrement et le déchiffrement des messages. Pour plus d'informations, consultez la section Configuration AWS KMS des autorisations dans le guide du développeur Amazon Simple Notification Service.

[SNS.2] L'enregistrement de l'état de livraison doit être activé pour les messages de notification envoyés à un sujet

> **Important**
>
> Security Hub CSPM a retiré ce contrôle en avril 2024. Pour de plus amples informations, veuillez consulter Journal des modifications pour les contrôles CSPM de Security Hub.

Exigences connexes : NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::SNS::Topic`

Règle AWS Config : `sns-topic-message-delivery-notification-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée pour l'état de livraison des messages de notification envoyés à une rubrique Amazon SNS pour les points de terminaison. Ce contrôle échoue si la notification de l'état de livraison des messages n'est pas activée.

La journalisation joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances des services. L'enregistrement de l'état de livraison des messages permet de fournir des informations opérationnelles, telles que les suivantes :

- Savoir si un message a été distribué au point de terminaison Amazon SNS.

- Identifiez la réponse envoyée à Amazon SNS par le point de terminaison Amazon SNS.

- Déterminer le temps d'attente du message (le temps entre l'horodatage de publication et le transfert vers un point de terminaison Amazon SNS).

Correction

Pour configurer l'enregistrement du statut de livraison pour un sujet, consultez le statut de livraison des messages Amazon SNS dans le manuel du développeur Amazon Simple Notification Service.

[SNS.3] Les sujets SNS doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::SNS::Topic`

AWS Configrègle : `tagged-sns-topic` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si une rubrique Amazon SNS comporte des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si le sujet ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`.

Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le sujet n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une rubrique SNS, consultez la section Configuration des balises de rubrique Amazon SNS dans le manuel Amazon Simple Notification Service Developer Guide.

[SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Critique

Type de ressource : `AWS::SNS::Topic`

Règle AWS Config : sns-topic-no-public-access

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la politique d'accès aux rubriques Amazon SNS autorise l'accès public. Ce contrôle échoue si la politique d'accès aux rubriques du SNS autorise l'accès public.

Vous utilisez une politique d'accès Amazon SNS avec une rubrique particulière afin de limiter les personnes autorisées à travailler sur cette rubrique (par exemple, qui peut publier des messages ou s'y abonner). Les politiques SNS peuvent accorder l'accès à d'autres Comptes AWS utilisateurs ou à des utilisateurs appartenant aux vôtres. Compte AWS L'ajout d'un caractère générique (*) dans le `Principal` champ de la politique thématique et l'absence de conditions limitant la politique thématique peuvent entraîner une exfiltration de données, un déni de service ou une injection indésirable de messages dans votre service par un attaquant.

> **Note**
>
> Ce contrôle n'évalue pas les conditions de politique qui utilisent des caractères génériques ou des variables. Pour produire un `PASSED` résultat, les conditions de la politique d'accès Amazon SNS pour un sujet doivent uniquement utiliser des valeurs fixes, c'est-à-dire des valeurs qui ne contiennent pas de caractères génériques ni de variables de politique. Pour plus d'informations sur les variables de politique, reportez-vous à la section Variables et balises du Guide de Gestion des identités et des accès AWS l'utilisateur.

Correction

Pour mettre à jour les politiques d'accès relatives à une rubrique SNS, consultez la section Présentation de la gestion des accès dans Amazon SNS dans le manuel Amazon Simple Notification Service Developer Guide.

Contrôles Security Hub CSPM pour Amazon SQS

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources Amazon Simple Queue Service (Amazon SQS). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos

Exigences associées : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::SQS::Queue`

AWS Configrègle : `sqs-queue-encrypted` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une file d'attente Amazon SQS est chiffrée au repos. Le contrôle échoue si la file d'attente n'est pas chiffrée avec une SQS-managed clé AWS Key Management Service (SSE-SQSAWS KMS) ou une clé (SSE-KMS).

Le chiffrement des données au repos réduit le risque qu'un utilisateur non autorisé accède aux données stockées sur disque. Server-side le chiffrement (SSE) protège le contenu des messages dans les files d'attente SQS à l'aide de clés de SQS-managed chiffrement (SSE-SQS) ou de AWS KMS clés (SSE-KMS).

Correction

Pour configurer SSE pour une file d'attente SQS, consultez la section Configuration du chiffrement côté serveur (SSE) pour une file d'attente (console) dans le manuel Amazon Simple Queue Service Developer Guide.

[SQS.2] Les files d'attente SQS doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::SQS::Queue`

AWS Configrègle : `tagged-sqs-queue` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si une file d'attente Amazon SQS possède des balises avec les clés spécifiques définies dans le paramètre. `requiredTagKeys` Le contrôle échoue si la file d'attente ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si la file d'attente n'est étiquetée avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une file d'attente existante à l'aide de la console Amazon SQS, consultez la section Configuration des balises de répartition des coûts pour une file d'attente Amazon SQS (console) dans le guide du développeur Amazon Simple Queue Service.

[SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public

Catégorie : Protéger > Gestion des accès sécurisés > Ressource non accessible au public

Gravité : Critique

Type de ressource : `AWS::SQS::Queue`

Règle AWS Config : sqs-queue-no-public-access

Type de calendrier : changement déclenché

Paramètres : Aucun

Cela permet de vérifier si une politique d'accès Amazon SQS autorise l'accès public à une file d'attente SQS. Le contrôle échoue si une politique d'accès SQS autorise l'accès public à la file d'attente.

Une politique d'accès Amazon SQS peut autoriser l'accès public à une file d'attente SQS, ce qui peut permettre à un utilisateur anonyme ou à toute identité AWS IAM authentifiée d'accéder à la file d'attente. Les politiques d'accès SQS fournissent généralement cet accès en spécifiant le caractère générique (`*`) dans l'`Principal`élément de la politique, sans utiliser les conditions appropriées pour restreindre l'accès à la file d'attente, ou les deux. Si une politique d'accès SQS autorise l'accès public, des tiers peuvent être en mesure d'effectuer des tâches telles que recevoir des messages de la file d'attente, envoyer des messages à la file d'attente ou modifier la politique d'accès de la file

d'attente. Cela peut entraîner des événements tels que l'exfiltration de données, un déni de service ou l'injection de messages dans la file d'attente par un acteur malveillant.

> **Note**
>
> Ce contrôle n'évalue pas les conditions de politique qui utilisent des caractères génériques ou des variables. Pour produire un `PASSED` résultat, les conditions de la politique d'accès Amazon SQS pour une file d'attente doivent uniquement utiliser des valeurs fixes, c'est-à-dire des valeurs qui ne contiennent pas de caractères génériques ni de variables de politique. Pour plus d'informations sur les variables de politique, reportez-vous à la section Variables et balises du Guide de Gestion des identités et des accès AWS l'utilisateur.

Correction

Pour plus d'informations sur la configuration de la politique d'accès SQS pour une file d'attente SQS, consultez la section Utilisation de politiques personnalisées avec le langage de politique d'accès Amazon SQS dans le guide du développeur Amazon Simple Queue Service.

Contrôles Security Hub CSPM pour Step Functions

Ces AWS Security Hub CSPM contrôles évaluent le AWS Step Functions service et les ressources.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[StepFunctions.1] La journalisation des machines à états Step Functions doit être activée

Exigences associées : PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::StepFunctions::StateMachine`

Règle AWS Config : `step-functions-state-machine-logging-enabled`

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`logLevel`	Niveau de journalisation minimal	Enum	`ALL`, `ERROR`, `FATAL`	Aucune valeur par défaut

Cela permet de vérifier si la journalisation est activée sur une machine à AWS Step Functions états. Le contrôle échoue si la journalisation n'est pas activée sur une machine à états. Si vous fournissez une valeur personnalisée pour le `logLevel` paramètre, le contrôle est transmis uniquement si le niveau de journalisation spécifié est activé sur la machine à états.

La surveillance vous aide à maintenir la fiabilité, la disponibilité et les performances de Step Functions. Vous devez collecter autant de données de surveillance Services AWS que celles que vous utilisez afin de pouvoir corriger plus facilement les défaillances multipoints. Une configuration de journalisation définie pour vos machines d'état Step Functions vous permet de suivre l'historique d'exécution et les résultats dans Amazon CloudWatch Logs. Vous pouvez éventuellement suivre uniquement les erreurs ou les événements fatals.

Correction

Pour activer la journalisation pour une machine à états Step Functions, voir Configurer la journalisation dans le Guide du AWS Step Functions développeur.

[StepFunctions.2] Les activités de Step Functions doivent être étiquetées

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::StepFunctions::Activity`

AWS Configrègle : `tagged-stepfunctions-activity` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si une AWS Step Functions activité possède des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si l'activité ne possède aucune clé de balise ou si toutes les clés spécifiées dans le paramètre ne sont pas présentes`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'activité n'est associée à aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses

personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à une activité Step Functions, voir Tagging in Step Functions dans le manuel du AWS Step Functions développeur.

Contrôles Security Hub CSPM pour Systems Manager

Ces AWS Security Hub CSPM contrôles évaluent le service et les ressources AWS Systems Manager (SSM). Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager

Exigences associées : PCI DSS v3.2. 1/24, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), (2) NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-15 (8) NIST.800-53.r5 SA-3, NIST.800-53.r5 SI-2 (3)

Catégorie : Identifier - Inventaire

Gravité : Moyenne

Ressource évaluée : `AWS::EC2::Instance`

Ressources AWS Config d'enregistrement requises :`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

Règle AWS Config : ec2-instance-managed-by-systems-manager

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les instances EC2 arrêtées et en cours d'exécution de votre compte sont gérées parAWS Systems Manager. Systems Manager est un Service AWS outil que vous pouvez utiliser pour visualiser et contrôler votre AWS infrastructure.

Pour vous aider à maintenir la sécurité et la conformité, Systems Manager analyse vos instances gérées arrêtées ou en cours d'exécution. Une instance gérée est une machine configurée pour être utilisée avec Systems Manager. Systems Manager signale ensuite ou prend des mesures correctives en cas de violation des politiques détectées. Systems Manager vous permet également de configurer et de gérer vos instances gérées. Pour en savoir plus, consultez le AWS Systems Managerguide de l'utilisateur.

> **Note**
>
> Ce contrôle génère des `FAILED` résultats pour les instances EC2 qui sont des instances de Reprise après sinistre AWS Elastic Replication Server gérées parAWS. Une instance de serveur de réplication est une instance EC2 lancée automatiquement par Reprise après sinistre AWS Elastic pour prendre en charge la réplication continue des données à partir des serveurs sources. AWSsupprime intentionnellement l'agent Systems Manager (SSM) de ces instances afin de maintenir l'isolation et d'empêcher d'éventuels chemins d'accès involontaires.

Correction

Pour plus d'informations sur la gestion des instances EC2 avecAWS Systems Manager, consultez la section Gestion des hôtes Amazon EC2 dans AWS Systems Managerle guide de l'utilisateur. Dans la section Options de configuration de la AWS Systems Manager console, vous pouvez conserver les paramètres par défaut ou les modifier selon les besoins de votre configuration préférée.

[SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif

Exigences associées : NIST.800-53.r5 CM-8 (3) NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (3), (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), NIST.800-171.r2 3.7.1, PCI DSS v3.2. 1/62., PCI DSS version 4.0. 1/22.2.1, PCI DSS v4.0. 1/6.3.3

Catégorie : Détecter - Services de détection

Gravité : Élevée

Type de ressource : `AWS::SSM::PatchCompliance`

Règle AWS Config : ec2-managedinstance-patch-compliance-status-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si l'état de conformité du correctif de Systems Manager est `COMPLIANT` ou `NON_COMPLIANT` après l'installation du correctif sur l'instance. Le contrôle échoue si le statut de conformité est`NON_COMPLIANT`. Le contrôle vérifie uniquement les instances gérées par Systems Manager Patch Manager.

L'application de correctifs à vos instances EC2 selon les besoins de votre organisation réduit la surface d'attaque de votre Comptes AWS

Correction

Systems Manager recommande d'utiliser des politiques de correctifs pour configurer l'application de correctifs pour vos instances gérées. Vous pouvez également utiliser les documents Systems Manager, comme décrit dans la procédure suivante, pour patcher une instance.

Pour corriger les correctifs non conformes

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Pour la gestion des nœuds, choisissez Exécuter la commande, puis sélectionnez Exécuter la commande.
3. Choisissez l'option pour AWS- RunPatchBaseline.
4. Passez l'Operation (Opération) à Install (Installer).
5. Choisissez Choisir les instances manuellement, puis choisissez les instances non conformes.
6. Cliquez sur Exécuter.
7. Une fois la commande terminée, pour surveiller le nouveau statut de conformité de vos instances corrigées, choisissez Compliance dans le volet de navigation.

[SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT

Exigences associées : NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 (3), PCI DSS v3.2. 1/24., PCI DSS version 4.0. 1/22.2.1, PCI DSS v4.0. 1/6.3.3

Catégorie : Détecter - Services de détection

Gravité : Faible

Type de ressource : `AWS::SSM::AssociationCompliance`

Règle AWS Config : ec2-managedinstance-association-compliance-status-check

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si le statut de conformité de l'AWS Systems Managerassociation est `COMPLIANT` ou `NON_COMPLIANT` après l'exécution de l'association sur une instance. Le contrôle échoue si le statut de conformité de l'association est`NON_COMPLIANT`.

Une association State Manager est une configuration attribuée à vos instances gérées. La configuration définit l'état que vous souhaitez conserver sur vos instances. Par exemple, une association peut spécifier qu'un logiciel antivirus doit être installé et exécuté sur vos instances ou que certains ports doivent être fermés.

Une fois que vous avez créé une ou plusieurs associations de responsables d'État, les informations sur le statut de conformité sont immédiatement disponibles. Vous pouvez consulter l'état de conformité dans la console ou en réponse à des AWS CLI commandes ou à des actions d'API Systems Manager correspondantes. Pour les associations, Configuration Compliance indique l'état de conformité (`Compliant`ou`Non-compliant`). Il indique également le niveau de gravité attribué à l'association, tel que `Critical` ou`Medium`.

Pour en savoir plus sur la conformité des associations State Manager, voir À propos de la conformité des associations State Manager dans le Guide de AWS Systems Manager l'utilisateur.

Correction

L'échec d'une association peut être lié à différents facteurs, notamment aux cibles et aux noms de documents de Systems Manager. Pour résoudre ce problème, vous devez d'abord identifier et étudier l'association en consultant l'historique des associations. Pour obtenir des instructions sur l'affichage de l'historique des associations, reportez-vous à la section Affichage de l'historique des associations dans le Guide de AWS Systems Manager l'utilisateur.

Après avoir étudié, vous pouvez modifier l'association pour corriger le problème identifié. Vous pouvez modifier une association pour spécifier un nouveau nom, un niveau de gravité ou des cibles. Après avoir modifié une association, il AWS Systems Manager crée une nouvelle version. Pour obtenir des instructions sur la modification d'une association, voir Modification et création d'une nouvelle version d'une association dans le Guide de AWS Systems Manager l'utilisateur.

[SSM.4] Les documents SSM ne doivent pas être publics

Exigences connexes : NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Catégorie : Protéger > Configuration réseau sécurisée > Ressources non accessibles au public

Gravité : Critique

Type de ressource : `AWS::SSM::Document`

Règle AWS Config : ssm-document-not-public

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si AWS Systems Manager les documents détenus par un compte sont publics. Le contrôle échoue si les documents de Systems Manager dont `Self` le propriétaire est le propriétaire sont publics.

Les documents publics de Systems Manager peuvent autoriser un accès involontaire à vos documents. Un document public de Systems Manager peut exposer des informations précieuses sur votre compte, vos ressources et vos processus internes.

À moins que votre cas d'utilisation ne nécessite un partage public, nous vous recommandons de bloquer le partage public pour les documents Systems Manager dont `Self` le propriétaire est le propriétaire.

Correction

Pour plus d'informations sur la configuration du partage pour les documents de Systems Manager, voir Partager un document SSM dans le Guide de l'AWS Systems Managerutilisateur.

[SSM.5] Les documents SSM doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::SSM::Document`

Règle AWS Config : ssm-document-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « 2 » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS Systems Manager document possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le document ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le document ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe. Le contrôle n'évalue pas les documents Systems Manager détenus par Amazon.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources par objectif, propriétaire, environnement ou selon d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour ajouter des balises à un AWS Systems Manager document, vous pouvez utiliser le AddTagsToResourcefonctionnement de l'AWS Systems ManagerAPI ou, si vous utilisez leAWS CLI, exécuter la commande add tags-to-resource. Vous pouvez également utiliser la console AWS Systems Manager.

[SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS:::Account`

Règle AWS Config : ssm-automation-logging-enabled

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la CloudWatch journalisation Amazon est activée pour l'automatisation AWS Systems Manager (SSM). Le contrôle échoue si la CloudWatch journalisation n'est pas activée pour SSM Automation.

SSM Automation est un AWS Systems Manager outil qui vous aide à créer des solutions automatisées pour déployer, configurer et gérer les AWS ressources à grande échelle à l'aide de runbooks prédéfinis ou personnalisés. Pour répondre aux exigences opérationnelles ou de sécurité de votre organisation, vous devrez peut-être fournir un enregistrement des scripts qu'elle exécute. Vous pouvez configurer SSM Automation pour envoyer le résultat des `aws:executeScript` actions de vos runbooks vers un groupe de CloudWatch journaux Amazon Logs que vous spécifiez. Avec CloudWatch Logs, vous pouvez surveiller, stocker et accéder à des fichiers journaux provenant de différents types de fichiersServices AWS.

Correction

Pour plus d'informations sur l'activation de la CloudWatch journalisation pour SSM Automation, voir le résultat de l'action Logging Automation with CloudWatch Logs dans le guide de AWS Systems Manager l'utilisateur.

[SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM

Catégorie : Protéger > Gestion des accès sécurisés > Ressource non accessible au public

Gravité : Critique

Type de ressource : `AWS::::Account`

Règle AWS Config : ssm-automation-block-public-sharing

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si le paramètre de blocage du partage public est activé pour les AWS Systems Manager documents. Le contrôle échoue si le paramètre de partage public par blocs est désactivé pour les documents de Systems Manager.

Le paramètre de blocage du partage public pour les documents AWS Systems Manager (SSM) est un paramètre au niveau du compte. L'activation de ce paramètre peut empêcher tout accès indésirable à vos documents SSM. Si vous activez ce paramètre, votre modification n'affectera aucun document SSM que vous partagez actuellement avec le public. À moins que votre cas d'utilisation ne vous oblige à partager des documents SSM avec le public, nous vous recommandons d'activer le paramètre de blocage du partage public. Le réglage peut varier d'une personne à l'autreRégion AWS.

Correction

Pour plus d'informations sur l'activation du paramètre de blocage du partage public pour les documents AWS Systems Manager (SSM), voir Bloquer le partage public des documents SSM dans le guide de l'AWS Systems Managerutilisateur.

Contrôles Security Hub CSPM pourAWS Transfer Family

Ces AWS Security Hub CSPM contrôles évaluent le AWS Transfer Family service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[Transfer.1]AWS Transfer Familyles flux de travail doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Transfer::Workflow`

AWS Configrègle : `tagged-transfer-workflow` (règle CSPM personnalisée de Security Hub)

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredTagKeys`	Liste des clés de balise de la ressource évaluée que doit contenir la ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	`No default value`

Ce contrôle vérifie si un AWS Transfer Family flux de travail comporte des balises avec les clés spécifiques définies dans le paramètre`requiredTagKeys`. Le contrôle échoue si le flux de travail ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées dans le paramètre`requiredTagKeys`. Si le paramètre `requiredTagKeys` n'est pas fourni, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le flux de travail n'est étiqueté avec aucune clé. Les balises système, qui sont automatiquement appliquées et commencent par`aws:`, sont ignorées.

Une balise est une étiquette que vous attribuez à une AWS ressource. Elle se compose d'une clé et d'une valeur facultative. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères. Les balises peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Le balisage vous permet également de suivre les propriétaires de ressources responsables en ce qui concerne les actions et les notifications. Lorsque

vous utilisez le balisage, vous pouvez implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation, qui définit les autorisations en fonction des balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et aux AWS ressources. Vous pouvez créer une politique ABAC unique ou un ensemble de politiques distinct pour vos principaux IAM. Vous pouvez concevoir ces politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de ressource. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

> **Note**
>
> N'ajoutez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans les balises. Les tags sont accessibles à de nombreuses personnesServices AWS, notammentAWS Billing. Pour en savoir plus sur les meilleures pratiques en matière de balisage, consultez la section Marquage de vos AWS ressources dans le. Références générales AWS

Correction

Pour ajouter des balises à un flux de travail Transfer Family (console)

1. Ouvrez la AWS Transfer Family console.
2. Dans le panneau de navigation, sous ETL, sélectionnez Workflows (Flux de travail). Sélectionnez ensuite le flux de travail que vous souhaitez baliser.
3. Choisissez Gérer les balises, puis ajoutez les balises.

[Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux

Exigences associées : NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5 NIST.800-53.r5 SC-8, PCI DSS v4.0. 1/4.2.1

Catégorie : Protéger > Protection des données > Chiffrement des données en transit

Gravité : Moyenne

Type de ressource : `AWS::Transfer::Server`

Règle AWS Config : transfer-family-server-no-ftp

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si un AWS Transfer Family serveur utilise un protocole autre que le protocole FTP pour la connexion des terminaux. Le contrôle échoue si le serveur utilise le protocole FTP pour qu'un client se connecte au point de terminaison du serveur.

Le protocole FTP (File Transfer Protocol) établit la connexion du terminal via des canaux non cryptés, ce qui rend les données envoyées via ces canaux vulnérables à l'interception. L'utilisation du protocole SFTP (SSH File Transfer Protocol), du FTPS (File Transfer Protocol Secure) ou de l'AS2 (Déclaration d'applicabilité 2) offre un niveau de sécurité supplémentaire en chiffrant vos données en transit et peut être utilisée pour empêcher les attaquants potentiels de recourir à des attaques de type « personin-the-middle » ou à des attaques similaires pour espionner ou manipuler le trafic réseau.

Correction

Pour modifier le protocole d'un serveur Transfer Family, voir Modifier les protocoles de transfert de fichiers dans le guide de AWS Transfer Family l'utilisateur.

[Transfer.3] La journalisation des connecteurs Transfer Family doit être activée

Exigences connexes : NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::Transfer::Connector`

Règle AWS Config : transfer-connector-logging-enabled

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si la CloudWatch journalisation Amazon est activée pour un AWS Transfer Family connecteur. Le contrôle échoue si la CloudWatch journalisation n'est pas activée pour le connecteur.

Amazon CloudWatch est un service de surveillance et d'observabilité qui fournit une visibilité sur vos AWS ressources, y compris les AWS Transfer Family ressources. Pour Transfer Family, CloudWatch fournit un audit et une journalisation consolidés pour la progression et les résultats du flux de travail. Cela inclut plusieurs métriques définies par Transfer Family pour les flux de travail. Vous pouvez configurer Transfer Family pour qu'il enregistre automatiquement les événements du connecteur CloudWatch. Pour ce faire, vous devez spécifier un rôle de journalisation pour le connecteur. Pour le rôle de journalisation, vous créez un rôle IAM et une politique IAM basée sur les ressources qui définit les autorisations associées au rôle.

Correction

Pour plus d'informations sur l'activation de la CloudWatch journalisation pour un connecteur Transfer Family, consultez la section Amazon CloudWatch logging pour AWS Transfer Family les serveurs dans le guide de AWS Transfer Family l'utilisateur.

[Transfer.4] Les accords Transfer Family doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Transfer::Agreement`

Règle AWS Config : transfer-agreement-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « ▲ » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS Transfer Family accord possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si l'accord ne contient aucune clé de balise ou s'il ne contient pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si l'accord ne contient aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un AWS Transfer Family accord, consultez la section Méthodes de balisage des ressources dans le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

[Transfer.5] Les certificats Transfer Family doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Transfer::Certificate`

Règle AWS Config : transfer-certificate-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « ▲ » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS Transfer Family certificat possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le certificat ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le certificat ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un AWS Transfer Family certificat, consultez la section Méthodes de balisage des ressources dans le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

[Transfer.6] Les connecteurs Transfer Family doivent être étiquetés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Transfer::Connector`

Règle AWS Config : transfer-connector-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « ▲ » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS Transfer Family connecteur possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le connecteur ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le connecteur ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un AWS Transfer Family connecteur, consultez la section Méthodes de balisage des ressources dans le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

[Transfer.7] Les profils Transfer Family doivent être balisés

Catégorie : Identifier > Inventaire > Étiquetage

Gravité : Faible

Type de ressource : `AWS::Transfer::Profile`

Règle AWS Config : transfer-profile-tagged

Type de calendrier : changement déclenché

Paramètres :

Paramètre	Description	Type	Valeurs personnalisées autorisées	Valeur par défaut du Security Hub CSPM
`requiredKeyTags`	Une liste de clés de balise de type « ▲ » qui doivent être attribuées à une ressource évaluée. Les touches de tag distinguent les majuscules et minuscules.	StringList (maximum de 6 articles)	1 à 6 clés d'étiquette répondant aux AWSexigences.	Aucune valeur par défaut

Ce contrôle vérifie si un AWS Transfer Family profil possède les clés de balise spécifiées par le `requiredKeyTags` paramètre. Le contrôle échoue si le profil ne possède aucune clé de balise ou s'il ne possède pas toutes les clés spécifiées par le `requiredKeyTags` paramètre. Si vous ne spécifiez aucune valeur pour le `requiredKeyTags` paramètre, le contrôle vérifie uniquement l'existence d'une clé de balise et échoue si le profil ne possède aucune clé de balise. Le contrôle ignore les balises système, qui sont appliquées automatiquement et portent le `aws:` préfixe. Le contrôle évalue les profils locaux et les profils des partenaires.

Une balise est une étiquette que vous créez et attribuez à une AWS ressource. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Ils peuvent vous aider à identifier, organiser, rechercher et filtrer les ressources. Ils peuvent également vous aider à suivre les propriétaires des ressources pour les actions et les notifications. Vous pouvez également utiliser des balises pour implémenter le contrôle d'accès basé sur les attributs (ABAC) en tant que stratégie d'autorisation. Pour plus d'informations sur les stratégies ABAC, voir Définir les autorisations en fonction des attributs dotés d'une autorisation ABAC dans le guide de l'utilisateur IAM. Pour plus d'informations sur les balises, consultez le guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Ne stockez pas de données d'identification personnelle (PII) ni d'autres informations confidentielles ou sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS. Ils ne sont pas destinés à être utilisés pour des données privées ou sensibles.

Correction

Pour plus d'informations sur l'ajout de balises à un AWS Transfer Family profil, consultez la section Méthodes de balisage des ressources dans le Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

Contrôles Security Hub CSPM pourAWS WAF

Ces AWS Security Hub CSPM contrôles évaluent le AWS WAF service et les ressources. Il est possible que les commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée

Exigences associées : NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::WAF::WebACL`

Règle AWS Config : `waf-classic-logging-enabled`

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée pour une ACL Web AWS WAF globale. Ce contrôle échoue si la journalisation n'est pas activée pour l'ACL Web.

La journalisation joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances à l'AWS WAFéchelle mondiale. Il s'agit d'une exigence commerciale et de conformité dans de nombreuses organisations, qui vous permet de résoudre les problèmes liés au comportement des applications. Il fournit également des informations détaillées sur le trafic analysé par l'ACL Web qui y est attachéeAWS WAF.

Correction

Pour activer la journalisation pour une ACL AWS WAF Web, consultez la section Enregistrement des informations de trafic d'une ACL Web dans le Guide du AWS WAF développeur.

[WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition

Exigences connexes : NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAFRegional::Rule`

Règle AWS Config : `waf-regional-rule-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une règle AWS WAF régionale comporte au moins une condition. Le contrôle échoue si aucune condition n'est présente dans une règle.

Une règle régionale WAF peut contenir plusieurs conditions. Les conditions de la règle permettent d'inspecter le trafic et de prendre une action définie (autoriser, bloquer ou compter). Sans aucune condition, le trafic passe sans inspection. Une règle régionale WAF sans conditions, mais dont le nom ou le tag suggère d'autoriser, de bloquer ou de compter, peut laisser supposer à tort que l'une de ces actions est en cours.

Correction

Pour ajouter une condition à une règle vide, consultez la section Ajouter et supprimer des conditions dans une règle dans le Guide du AWS WAF développeur.

[WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle

Exigences connexes : NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAFRegional::RuleGroup`

Règle AWS Config : `waf-regional-rulegroup-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe de règles AWS WAF régional possède au moins une règle. Le contrôle échoue si aucune règle n'est présente au sein d'un groupe de règles.

Un groupe de règles régional WAF peut contenir plusieurs règles. Les conditions de la règle permettent d'inspecter le trafic et de prendre une action définie (autoriser, bloquer ou compter). Sans aucune règle, le trafic passe sans inspection. Un groupe de règles régional WAF sans règles, mais dont le nom ou le tag suggère d'autoriser, de bloquer ou de compter, peut laisser supposer à tort que l'une de ces actions est en cours.

Correction

Pour ajouter des règles et des conditions de règles à un groupe de règles vide, consultez les sections Ajouter et supprimer des règles dans un groupe de règles AWS WAF classique et Ajouter et supprimer des conditions dans une règle dans le Guide du AWS WAF développeur.

[WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAFRegional::WebACL`

Règle AWS Config : `waf-regional-webacl-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une ACL AWS WAF Classic Regional Web contient des règles WAF ou des groupes de règles WAF. Ce contrôle échoue si une ACL Web ne contient aucune règle WAF ou aucun groupe de règles.

Une ACL Web régionale WAF peut contenir un ensemble de règles et de groupes de règles qui inspectent et contrôlent les requêtes Web. Si une ACL Web est vide, le trafic Web peut passer sans être détecté ou traité par WAF en fonction de l'action par défaut.

Correction

Pour ajouter des règles ou des groupes de règles à une ACL Web régionale AWS WAF classique vide, consultez la section Modification d'une ACL Web dans le guide du AWS WAF développeur.

[WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAF::Rule`

Règle AWS Config : `waf-global-rule-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une règle AWS WAF globale contient des conditions. Le contrôle échoue si aucune condition n'est présente dans une règle.

Une règle globale WAF peut contenir plusieurs conditions. Les conditions d'une règle permettent d'inspecter le trafic et de prendre une action définie (autoriser, bloquer ou compter). Sans aucune condition, le trafic passe sans inspection. Une règle globale WAF sans conditions, mais dont le nom ou le tag suggère d'autoriser, de bloquer ou de compter, peut laisser supposer à tort que l'une de ces actions est en train de se produire.

Correction

Pour obtenir des instructions sur la création d'une règle et l'ajout de conditions, consultez la section Création d'une règle et ajout de conditions dans le guide du AWS WAF développeur.

[WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAF::RuleGroup`

Règle AWS Config : `waf-global-rulegroup-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un groupe de règles AWS WAF global possède au moins une règle. Le contrôle échoue si aucune règle n'est présente au sein d'un groupe de règles.

Un groupe de règles global WAF peut contenir plusieurs règles. Les conditions de la règle permettent d'inspecter le trafic et de prendre une action définie (autoriser, bloquer ou compter). Sans aucune règle, le trafic passe sans inspection. Un groupe de règles global WAF sans règles, mais dont le nom ou le tag suggère d'autoriser, de bloquer ou de compter, peut laisser supposer à tort que l'une de ces actions est en train de se produire.

Correction

Pour obtenir des instructions sur l'ajout d'une règle à un groupe de règles, consultez la section Création d'un groupe de règles AWS WAF classique dans le guide du AWS WAF développeur.

[WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Exigences connexes : NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAF::WebACL`

Règle AWS Config : `waf-global-webacl-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une ACL Web AWS WAF globale contient au moins une règle WAF ou un groupe de règles WAF. Le contrôle échoue si une ACL Web ne contient aucune règle WAF ou aucun groupe de règles.

Une ACL Web globale WAF peut contenir un ensemble de règles et de groupes de règles qui inspectent et contrôlent les requêtes Web. Si une ACL Web est vide, le trafic Web peut passer sans être détecté ou traité par WAF en fonction de l'action par défaut.

Correction

Pour ajouter des règles ou des groupes de règles à une ACL Web AWS WAF globale vide, consultez la section Modification d'une ACL Web dans le manuel du AWS WAF développeur. Pour Filtrer, choisissez Global (CloudFront).

[WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles

Exigences connexes : NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Catégorie : Protéger - Configuration réseau sécurisée

Gravité : Moyenne

Type de ressource : `AWS::WAFv2::WebACL`

Règle AWS Config : `wafv2-webacl-not-empty`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si une liste de contrôle d'accès Web (ACL Web) AWS WAF V2 contient au moins une règle ou un groupe de règles. Le contrôle échoue si une ACL Web ne contient aucune règle ou groupe de règles.

Une ACL Web vous permet de contrôler avec précision toutes les requêtes Web HTTP (S) auxquelles répond votre ressource protégée. Une ACL Web doit contenir un ensemble de règles et de groupes de règles qui inspectent et contrôlent les requêtes Web. Si une ACL Web est vide, le trafic Web peut être transmis sans être détecté ou traité AWS WAF en fonction de l'action par défaut.

Correction

Pour ajouter des règles ou des groupes de règles à une ACL Web WAFV2 vide, consultez la section Modification d'une ACL Web dans le manuel du AWS WAFdéveloppeur.

[WAF.11]AWS WAFla journalisation des ACL Web doit être activée

Exigences associées : NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Catégorie : Identifier - Journalisation

Gravité : Faible

Type de ressource : `AWS::WAFv2::WebACL`

AWS Configrègle : **`wafv2-logging-enabled`**

Type de calendrier : Périodique

Paramètres : Aucun

Ce contrôle vérifie si la journalisation est activée pour une liste de contrôle d'accès Web (ACL Web) AWS WAF V2. Ce contrôle échoue si la journalisation est désactivée pour l'ACL Web.

> **Note**
>
> Ce contrôle ne vérifie pas si la journalisation ACL AWS WAF Web est activée pour un compte via Amazon Security Lake.

La journalisation garantit la fiabilité, la disponibilité et les performances deAWS WAF. En outre, la journalisation est une exigence commerciale et de conformité dans de nombreuses organisations.

En enregistrant le trafic analysé par votre ACL Web, vous pouvez résoudre les problèmes de comportement des applications.

Correction

Pour activer la journalisation pour une ACL AWS WAF Web, consultez la section Gestion de la journalisation pour une ACL Web dans le Guide du AWS WAF développeur.

[WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles

Exigences connexes : NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Catégorie : Identifier - Journalisation

Gravité : Moyenne

Type de ressource : `AWS::WAFv2::RuleGroup`

AWS Configrègle : **`wafv2-rulegroup-logging-enabled`**

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si les CloudWatch métriques Amazon sont activées pour une AWS WAF règle ou un groupe de règles. Le contrôle échoue si les CloudWatch métriques ne sont pas activées pour la règle ou le groupe de règles.

La configuration de CloudWatch métriques sur AWS WAF les règles et les groupes de règles fournit une visibilité sur le flux de trafic. Vous pouvez voir quelles règles ACL sont déclenchées et quelles demandes sont acceptées et bloquées. Cette visibilité peut vous aider à identifier les activités malveillantes sur vos ressources associées.

Correction

Pour activer CloudWatch les métriques sur un groupe de AWS WAF règles, appelez l'UpdateRuleGroupAPI. Pour activer CloudWatch les métriques sur une AWS WAF règle, appelez l'API UpdateWebACL. Réglez le `CloudWatchMetricsEnabled` champ sur`true`. Lorsque vous utilisez la AWS WAF console pour créer des règles ou des groupes de règles, CloudWatch les métriques sont automatiquement activées.

Contrôles Security Hub CSPM pour WorkSpaces

Ces AWS Security Hub CSPM contrôles évaluent le WorkSpaces service et les ressources Amazon.

Il est possible que ces commandes ne soient pas toutes disponiblesRégions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des contrôles par région.

[WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::WorkSpaces::Workspace`

Règle AWS Config : `workspaces-user-volume-encryption-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un volume utilisateur d'un Amazon WorkSpaces WorkSpace est chiffré au repos. Le contrôle échoue si le volume WorkSpace utilisateur n'est pas chiffré au repos.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour chiffrer un volume WorkSpaces utilisateur, consultez la section Encrypt a WorkSpace dans le guide d' WorkSpaces administration Amazon.

[WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Catégorie : Protéger > Protection des données > Chiffrement des données au repos

Gravité : Moyenne

Type de ressource : `AWS::WorkSpaces::Workspace`

Règle AWS Config : `workspaces-root-volume-encryption-enabled`

Type de calendrier : changement déclenché

Paramètres : Aucun

Ce contrôle vérifie si un volume racine d'un Amazon WorkSpaces WorkSpace est chiffré au repos. Le contrôle échoue si le volume WorkSpace racine n'est pas chiffré au repos.

Les données au repos font référence aux données stockées dans un stockage persistant et non volatil pendant une durée quelconque. Le chiffrement des données au repos vous permet de protéger leur confidentialité, ce qui réduit le risque qu'un utilisateur non autorisé puisse y accéder.

Correction

Pour chiffrer un volume WorkSpaces racine, consultez la section Encrypt a WorkSpace dans le guide d' WorkSpaces administration Amazon.

Autorisations requises pour configurer les contrôles dans Security Hub CSPM

Pour afficher des informations sur les contrôles de sécurité et activer et désactiver les contrôles de sécurité dans les normes, le rôle Gestion des identités et des accès AWS (IAM) que vous utilisez pour accéder au AWS Security Hub CSPM doit être autorisé à effectuer les opérations suivantes de l'API Security Hub CSPM.

Pour obtenir les autorisations nécessaires, vous pouvez utiliser les politiques gérées par Security Hub CSPM. Vous pouvez également mettre à jour les politiques IAM personnalisées afin d'inclure des autorisations pour ces actions.

- BatchGetSecurityControls— Renvoie des informations sur un lot de contrôles de sécurité pour le compte courant etRégion AWS.
- ListSecurityControlDefinitions— Renvoie des informations sur les contrôles de sécurité qui s'appliquent à une norme spécifiée.
- ListStandardsControlAssociations— Indique si un contrôle de sécurité est actuellement activé ou désactivé dans chaque norme activée dans le compte.
- BatchGetStandardsControlAssociations— Pour un lot de contrôles de sécurité, indique si chaque contrôle est actuellement activé ou désactivé dans une norme spécifiée.
- BatchUpdateStandardsControlAssociations— Utilisé pour activer un contrôle de sécurité dans les normes qui incluent le contrôle, ou pour désactiver un contrôle dans les normes. Il s'agit d'un remplacement par lots de l'`UpdateStandardsControl`opération existante.

- BatchUpdateStandardsControlAssociations— Utilisé pour activer ou désactiver un lot de contrôles de sécurité dans les normes qui incluent ces contrôles. Il s'agit d'un remplacement par lots de l'`UpdateStandardsControl`opération existante.
- UpdateStandardsControl— Utilisé pour activer ou désactiver un seul contrôle de sécurité dans les normes qui incluent le contrôle
- DescribeStandardsControl— Renvoie des informations sur les contrôles de sécurité spécifiés.

Outre les API précédentes, vous devez ajouter l'autorisation d'appel `BatchGetControlEvaluations` à votre rôle IAM. Cette autorisation est nécessaire pour consulter l'état d'activation et de conformité d'un contrôle, les résultats pris en compte pour un contrôle et le score de sécurité global des contrôles sur la console Security Hub CSPM. Étant donné que seule la console appelle`BatchGetControlEvaluations`, cette autorisation ne correspond pas directement aux API ou AWS CLI commandes CSPM du Security Hub documentées publiquement.

Activation des contrôles dans Security Hub CSPM

Dans AWS Security Hub CSPM, un contrôle est une garantie au sein d'une norme de sécurité qui aide une organisation à protéger la confidentialité, l'intégrité et la disponibilité de ses informations. Chaque contrôle CSPM de Security Hub est lié à une ressource spécifique AWS . Lorsque vous activez un contrôle, Security Hub CSPM commence à exécuter des contrôles de sécurité pour le contrôle et génère des résultats pour celui-ci. Security Hub CSPM prend également en compte tous les contrôles activés lors du calcul des scores de sécurité.

Vous pouvez choisir d'activer un contrôle pour toutes les normes de sécurité auxquelles il s'applique. Vous pouvez également configurer l'état d'activation différemment selon les normes. Nous recommandons la première option, dans laquelle l'état d'activation d'un contrôle est aligné sur toutes les normes activées. Pour obtenir des instructions sur l'activation d'un contrôle sur toutes les normes auxquelles il est appliqué, consultezPermettre un contrôle sur l'ensemble des normes. Pour obtenir des instructions sur l'activation d'un contrôle dans des normes spécifiques, consultezActivation d'un contrôle dans une norme spécifique.

Si vous activez l'agrégation interrégionale et que vous vous connectez à une région d'agrégation, la console Security Hub CSPM affiche les contrôles disponibles dans au moins une région liée. Si un contrôle est disponible dans une région liée mais pas dans la région d'agrégation, vous ne pouvez ni activer ni désactiver ce contrôle depuis la région d'agrégation.

Vous pouvez activer et désactiver les contrôles dans chaque région à l'aide de la console Security Hub CSPM, de l'API Security Hub CSPM ou. AWS CLI

Les instructions d'activation et de désactivation des commandes varient selon que vous utilisez ou non la configuration ??? centralisée. Cette rubrique décrit les différences. La configuration centralisée est disponible pour les utilisateurs qui intègrent Security Hub CSPM et. AWS Organizations Nous vous recommandons d'utiliser une configuration centralisée pour simplifier le processus d'activation et de désactivation des contrôles dans les environnements multicomptes et multirégions. Si vous utilisez une configuration centralisée, vous pouvez activer un contrôle sur plusieurs comptes et régions à l'aide de politiques de configuration. Si vous n'utilisez pas la configuration centralisée, vous devez activer un contrôle séparément dans chaque région et chaque compte.

Permettre un contrôle sur l'ensemble des normes

Nous vous recommandons d'activer un contrôle AWS Security Hub CSPM pour toutes les normes auxquelles le contrôle s'applique. Si vous activez les résultats de contrôle consolidés, vous recevez un résultat par contrôle, même si un contrôle appartient à plusieurs normes.

Cross-standard activation dans des environnements multicomptes et multirégions

Pour activer un contrôle de sécurité sur plusieurs Comptes AWS réseaux Régions AWS, vous devez être connecté au compte administrateur CSPM délégué de Security Hub et utiliser la configuration centralisée.

Dans le cadre d'une configuration centralisée, l'administrateur délégué peut créer des politiques de configuration CSPM de Security Hub qui activent des contrôles spécifiques selon les normes activées. Vous pouvez ensuite associer la politique de configuration à des comptes et à des unités organisationnelles (UO) spécifiques ou à la racine. Une politique de configuration prend effet dans votre région d'origine (également appelée région d'agrégation) et dans toutes les régions liées.

Les politiques de configuration offrent une personnalisation. Par exemple, vous pouvez choisir d'activer tous les contrôles dans une unité d'organisation, et vous pouvez choisir d'activer uniquement les contrôles Amazon Elastic Compute Cloud (EC2) dans une autre unité d'organisation. Le niveau de granularité dépend des objectifs que vous souhaitez atteindre en matière de couverture de sécurité au sein de votre organisation. Pour obtenir des instructions sur la création d'une politique de configuration qui active des contrôles spécifiques selon les normes, consultezCréation et association de politiques de configuration.

> **Note**
>
> L'administrateur délégué peut créer des politiques de configuration pour gérer les contrôles dans toutes les normes, à l'exception de la Service-Managed norme Standard : AWS Control

Tower. Les commandes pour cette norme doivent être configurées dans le AWS Control Tower service.

Si vous souhaitez que certains comptes configurent leurs propres contrôles plutôt que l'administrateur délégué, celui-ci peut désigner ces comptes comme étant autogérés. Self-managed les comptes doivent configurer les contrôles séparément dans chaque région.

Cross-standard activation dans un compte et une région uniques

Si vous n'utilisez pas la configuration centralisée ou si vous êtes un compte autogéré, vous ne pouvez pas utiliser les politiques de configuration pour activer les contrôles de manière centralisée dans plusieurs comptes et régions. Cependant, vous pouvez suivre les étapes suivantes pour activer un contrôle dans un seul compte et une seule région.

Security Hub CSPM console

Pour permettre un contrôle des normes sur un seul compte et une seule région

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Controls dans le volet de navigation.
3. Choisissez l'onglet Désactivé.
4. Choisissez l'option à côté d'un contrôle.
5. Choisissez Activer le contrôle (cette option n'apparaît pas pour un contrôle déjà activé).
6. Répétez l'opération dans chaque région dans laquelle vous souhaitez activer le contrôle.

Security Hub CSPM API

Pour permettre un contrôle des normes sur un seul compte et une seule région

1. Invoquez l'ListStandardsControlAssociationsAPI. Fournissez un identifiant de contrôle de sécurité.

   Exemple de demande :

```
{
    "SecurityControlId": "IAM.1"
```

```
}
```

2. Invoquez l'BatchUpdateStandardsControlAssociationsAPI. Fournissez le nom de ressource Amazon (ARN) de toutes les normes dans lesquelles le contrôle n'est pas activé. Pour obtenir des ARN standard, exécutez `DescribeStandards`.
3. Définissez le `AssociationStatus` paramètre égal à`ENABLED`. Si vous suivez ces étapes pour un contrôle déjà activé, l'API renvoie une réponse au code d'état HTTP 200.

   Exemple de demande :

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Répétez l'opération dans chaque région dans laquelle vous souhaitez activer le contrôle.

AWS CLI

Pour permettre un contrôle des normes sur un seul compte et une seule région

1. Exécutez la commande list-standards-control-associations. Fournissez un identifiant de contrôle de sécurité.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Exécutez la commande batch-update-standards-control-associations. Fournissez le nom de ressource Amazon (ARN) de toutes les normes dans lesquelles le contrôle n'est pas activé. Pour obtenir des ARN standard, exécutez la `describe-standards` commande.
3. Définissez le `AssociationStatus` paramètre égal à`ENABLED`. Si vous suivez ces étapes pour un contrôle déjà activé, la commande renvoie une réponse au code d'état HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
```

```
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Répétez l'opération dans chaque région dans laquelle vous souhaitez activer le contrôle.

Activation d'un contrôle dans une norme spécifique

Lorsque vous activez une norme dans AWS Security Hub CSPM, tous les contrôles qui s'y appliquent sont automatiquement activés dans cette norme (à l'exception des normes gérées par les services). Vous pouvez ensuite désactiver et réactiver des contrôles spécifiques dans la norme. Cependant, nous vous recommandons d'aligner l'état d'activation d'un contrôle sur toutes les normes que vous avez activées. Pour obtenir des instructions sur l'activation d'un contrôle pour toutes les normes, consultezPermettre un contrôle sur l'ensemble des normes.

La page de détails d'une norme contient la liste des contrôles applicables à la norme, ainsi que des informations sur les contrôles actuellement activés et désactivés dans cette norme.

Sur la page des détails des normes, vous pouvez également activer les contrôles dans des normes spécifiques. Vous devez activer les contrôles dans des normes spécifiques séparément dans chaque Compte AWS et Région AWS. Lorsque vous activez un contrôle dans des normes spécifiques, cela n'affecte que le compte courant et la région.

Pour activer un contrôle dans une norme, vous devez d'abord activer au moins une norme à laquelle le contrôle s'applique. Pour obtenir des instructions sur l'activation d'une norme, consultezMise en place d'une norme de sécurité. Lorsque vous activez un contrôle dans une ou plusieurs normes, Security Hub CSPM commence à générer des résultats pour ce contrôle. Security Hub CSPM inclut l'état du contrôle dans le calcul du score de sécurité global et des scores de sécurité standard. Même si vous activez un contrôle dans plusieurs normes, vous ne recevrez qu'un seul résultat par contrôle de sécurité pour toutes les normes si vous activez les résultats des contrôles consolidés. Pour plus d'informations, consultez la section Résultats de contrôle consolidés (français non garanti).

Pour activer un contrôle dans une norme, le contrôle doit être disponible dans votre région actuelle. Pour plus d'informations, consultez la section Disponibilité des contrôles par région.

Suivez ces étapes pour activer un contrôle CSPM Security Hub dans une norme spécifique. Au lieu des étapes suivantes, vous pouvez également utiliser l'action d'`UpdateStandardsControl`API pour activer les contrôles dans une norme spécifique. Pour obtenir des instructions sur l'activation d'un contrôle dans toutes les normes, consultezCross-standard activation dans un compte et une région uniques.

Security Hub CSPM console

Pour activer un contrôle dans une norme spécifique

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Normes de sécurité dans le volet de navigation.
3. Choisissez Afficher les résultats pour la norme appropriée.
4. Sélectionnez un contrôle.
5. Choisissez Activer le contrôle (cette option n'apparaît pas pour un contrôle déjà activé). Confirmez en choisissant Activer.

Security Hub CSPM API

Pour activer un contrôle dans une norme spécifique

1. `ListSecurityControlDefinitions`Exécutez et fournissez un ARN standard pour obtenir une liste des contrôles disponibles pour une norme spécifique. Pour obtenir un ARN standard, exécutez `DescribeStandards`. Cette API renvoie des identifiants de contrôle de sécurité indépendants des normes, et non des identifiants de contrôle spécifiques aux normes.

   Exemple de demande :

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Exécutez `ListStandardsControlAssociations` et fournissez un ID de contrôle spécifique pour renvoyer l'état d'activation actuel d'un contrôle dans chaque norme.

   Exemple de demande :

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Exécutez BatchUpdateStandardsControlAssociations. Indiquez l'ARN de la norme dans laquelle vous souhaitez activer le contrôle.
4. Définissez le `AssociationStatus` paramètre égal à`ENABLED`.

   Exemple de demande :

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Pour activer un contrôle dans une norme spécifique

1. Exécutez la `list-security-control-definitions` commande et fournissez un ARN standard pour obtenir la liste des contrôles disponibles pour une norme spécifique. Pour obtenir un ARN standard, exécutez`describe-standards`. Cette commande renvoie des identifiants de contrôle de sécurité indépendants des normes, et non des identifiants de contrôle spécifiques aux normes.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Exécutez la `list-standards-control-associations` commande et fournissez un ID de contrôle spécifique pour renvoyer l'état d'activation actuel d'un contrôle dans chaque norme.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Exécutez la commande `batch-update-standards-control-associations`. Indiquez l'ARN de la norme dans laquelle vous souhaitez activer le contrôle.
4. Définissez le `AssociationStatus` paramètre égal à`ENABLED`.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
```

```
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Activation automatique de nouveaux contrôles dans les normes activées

AWSSecurity Hub CSPM publie régulièrement de nouveaux contrôles et les ajoute à une ou plusieurs normes. Vous pouvez choisir d'activer automatiquement les nouveaux contrôles dans vos normes activées.

Nous vous recommandons d'utiliser la configuration centrale du Security Hub CSPM pour activer automatiquement les nouveaux contrôles de sécurité. Vous pouvez créer des politiques de configuration qui incluent une liste de contrôles à désactiver selon les normes. Toutes les autres commandes, y compris celles récemment publiées, sont activées par défaut. Vous pouvez également créer des politiques qui incluent une liste de contrôles à activer selon les normes. Toutes les autres commandes, y compris celles récemment publiées, sont désactivées par défaut. Pour de plus amples informations, veuillez consulter Comprendre la configuration centrale dans Security Hub CSPM.

Security Hub CSPM n'active pas de nouveaux contrôles lorsqu'ils sont ajoutés à une norme que vous n'avez pas activée.

Les instructions suivantes s'appliquent uniquement si vous n'utilisez pas la configuration centralisée.

Choisissez votre méthode d'accès préférée et suivez les étapes pour activer automatiquement les nouveaux contrôles dans les normes activées.

> **Note**
>
> Lorsque vous activez automatiquement de nouvelles commandes à l'aide des instructions suivantes, vous pouvez interagir avec les commandes dans la console et par programmation immédiatement après leur publication. Toutefois, le statut par défaut temporaire des contrôles activés automatiquement est Désactivé. Plusieurs jours peuvent être nécessaires pour que Security Hub CSPM traite la version de contrôle et désigne le contrôle comme étant activé dans votre compte. Pendant la période de traitement, vous pouvez activer ou désactiver manuellement un contrôle, et Security Hub CSPM conservera cette désignation, que l'activation automatique du contrôle soit activée ou non.

Security Hub CSPM console

Pour activer automatiquement les nouvelles commandes

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Paramètres, puis cliquez sur l'onglet Général.
3. Sous Contrôles, choisissez Modifier.
4. Activez les Auto-enable nouvelles commandes dans les normes activées.
5. Choisissez Enregistrer.

Security Hub CSPM API

Pour activer automatiquement les nouvelles commandes

1. Exécutez `UpdateSecurityHubConfiguration`.
2. Pour activer automatiquement de nouvelles commandes pour les normes activées, définissez `AutoEnableControls` sur`true`. Si vous ne souhaitez pas activer automatiquement les nouvelles commandes, définissez le paramètre `AutoEnableControls` sur false.

AWS CLI

Pour activer automatiquement les nouvelles commandes

1. Exécutez la commande `update-security-hub-configuration`.
2. Pour activer automatiquement de nouvelles commandes pour les normes activées, spécifiez`--auto-enable-controls`. Si vous ne souhaitez pas activer automatiquement les nouvelles commandes, spécifiez`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Exemple de commande

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Si vous n'activez pas automatiquement les nouvelles commandes, vous devez les activer manuellement. Pour obtenir des instructions, veuillez consulter Activation des contrôles dans Security Hub CSPM.

Désactivation des contrôles dans Security Hub CSPM

Pour réduire le bruit de détection, il peut être utile de désactiver les commandes qui ne sont pas adaptées à votre environnement. Dans AWS Security Hub CSPM, vous pouvez désactiver un contrôle pour toutes les normes de sécurité ou uniquement pour des normes spécifiques.

Si vous désactivez un contrôle pour toutes les normes, voici ce qui se produit :

- Les contrôles de sécurité pour le contrôle ne sont plus effectués.
- Aucun résultat supplémentaire n'est généré pour le contrôle.
- Les résultats existants ne sont plus mis à jour pour le contrôle.
- Les résultats existants pour le contrôle sont archivés automatiquement, généralement dans un délai de 3 à 5 jours, dans la mesure du possible.
- Security Hub CSPM supprime toutes les AWS Config règles associées qu'il a créées pour le contrôle.

Si vous désactivez un contrôle pour des normes spécifiques uniquement, Security Hub CSPM arrête d'exécuter des contrôles de sécurité pour le contrôle uniquement pour ces normes. Cela supprime également le contrôle des calculs du score de sécurité pour chacune de ces normes. Si le contrôle est activé dans d'autres normes, Security Hub CSPM conserve la AWS Config règle associée, le cas échéant, et continue à effectuer des contrôles de sécurité pour le contrôle pour les autres normes. Security Hub CSPM inclut également le contrôle lorsqu'il calcule le score de sécurité pour chacune des autres normes, ce qui affecte votre score de sécurité récapitulatif.

Si vous désactivez une norme, toutes les commandes qui s'appliquent à la norme sont automatiquement désactivées pour cette norme. Cependant, les contrôles pourraient continuer à être activés dans d'autres normes. Lorsque vous désactivez une norme, Security Hub CSPM n'enregistre pas les commandes qui ont été désactivées pour la norme. Par conséquent, si vous réactivez ultérieurement la même norme, toutes les commandes qui s'y appliquent sont automatiquement activées. Pour plus d'informations sur la désactivation d'une norme, consultezDésactivation d'une norme.

La désactivation d'un contrôle n'est pas une action permanente. Supposons que vous désactiviez un contrôle, puis que vous activiez une norme qui inclut ce contrôle. Le contrôle est ensuite activé pour

cette norme. Lorsque vous activez une norme dans Security Hub CSPM, toutes les commandes qui s'appliquent à la norme sont automatiquement activées. Pour plus d'informations sur l'activation d'une norme, consultezActivation d'une norme.

Rubriques

- Désactivation d'un contrôle entre les normes
- Désactivation d'un contrôle dans une norme spécifique
- Contrôles suggérés à désactiver dans Security Hub CSPM

Désactivation d'un contrôle entre les normes

Nous vous recommandons de désactiver un contrôle CSPM AWS Security Hub pour toutes les normes afin de maintenir l'alignement dans l'ensemble de votre organisation. Si vous désactivez un contrôle uniquement dans des normes spécifiques, vous continuez à recevoir des résultats pour le contrôle s'il est activé dans d'autres normes.

Cross-standard désactivation dans plusieurs comptes et régions

Pour désactiver un contrôle de sécurité sur plusieurs réseaux Comptes AWS et Régions AWS, vous devez utiliser une configuration centralisée.

Lorsque vous utilisez la configuration centralisée, l'administrateur délégué peut créer des politiques de configuration CSPM de Security Hub qui désactivent des contrôles spécifiques selon les normes activées. Vous pouvez ensuite associer la politique de configuration à des comptes spécifiques, à des unités d'organisation ou à la racine. Une politique de configuration prend effet dans votre région d'origine (également appelée région d'agrégation) et dans toutes les régions liées.

Les politiques de configuration offrent une personnalisation. Par exemple, vous pouvez choisir de désactiver tous les AWS CloudTrail contrôles d'une unité d'organisation, et vous pouvez choisir de désactiver tous les contrôles IAM d'une autre unité d'organisation. Le niveau de granularité dépend des objectifs que vous souhaitez atteindre en matière de couverture de sécurité au sein de votre organisation. Pour obtenir des instructions sur la création d'une politique de configuration qui désactive les contrôles spécifiés dans toutes les normes, consultezCréation et association de politiques de configuration.

> **Note**
>
> L'administrateur délégué peut créer des politiques de configuration pour gérer les contrôles dans toutes les normes, à l'exception de la Service-Managed norme Standard : AWS Control

Tower. Les commandes pour cette norme doivent être configurées dans le AWS Control Tower service.

Si vous souhaitez que certains comptes configurent leurs propres contrôles plutôt que l'administrateur délégué, celui-ci peut désigner ces comptes comme étant autogérés. Self-managed les comptes doivent configurer les contrôles séparément dans chaque région.

Cross-standard invalidité dans un seul compte et une seule région

Si vous n'utilisez pas la configuration centralisée ou si vous êtes un compte autogéré, vous ne pouvez pas utiliser les politiques de configuration pour désactiver les contrôles de manière centralisée dans plusieurs comptes et régions. Cependant, vous pouvez désactiver un contrôle dans un seul compte et une seule région.

Security Hub CSPM console

Pour désactiver un contrôle entre les normes dans un compte et une région

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Controls dans le volet de navigation.
3. Choisissez l'option à côté d'un contrôle.
4. Choisissez Désactiver le contrôle. Cette option n'apparaît pas pour un contrôle déjà désactivé.
5. Sélectionnez la raison de la désactivation du contrôle, puis confirmez en choisissant Désactiver.
6. Répétez l'opération dans chaque région dans laquelle vous souhaitez désactiver le contrôle.

Security Hub CSPM API

Pour désactiver un contrôle entre les normes dans un compte et une région

1. Invoquez l'ListStandardsControlAssociationsAPI. Fournissez un identifiant de contrôle de sécurité.

   Exemple de demande :

```
{
    "SecurityControlId": "IAM.1"
}
```

2. Invoquez l'BatchUpdateStandardsControlAssociationsAPI. Fournissez l'ARN de toutes les normes dans lesquelles le contrôle est activé. Pour obtenir des ARN standard, exécutez `DescribeStandards`.
3. Définissez le `AssociationStatus` paramètre égal à`DISABLED`. Si vous suivez ces étapes pour un contrôle déjà désactivé, l'API renvoie une réponse au code d'état HTTP 200.

   Exemple de demande :

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
 applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. Répétez l'opération dans chaque région dans laquelle vous souhaitez désactiver le contrôle.

AWS CLI

Pour désactiver un contrôle entre les normes dans un compte et une région

1. Exécutez la commande list-standards-control-associations. Fournissez un identifiant de contrôle de sécurité.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Exécutez la commande batch-update-standards-control-associations. Fournissez l'ARN de toutes les normes dans lesquelles le contrôle est activé. Pour obtenir des ARN standard, exécutez la `describe-standards` commande.
3. Définissez le `AssociationStatus` paramètre égal à`DISABLED`. Si vous suivez ces étapes pour un contrôle déjà désactivé, la commande renvoie une réponse au code d'état HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. Répétez l'opération dans chaque région dans laquelle vous souhaitez désactiver le contrôle.

Désactivation d'un contrôle dans une norme spécifique

Vous pouvez désactiver un contrôle uniquement dans des normes de sécurité spécifiques, au lieu de désactiver un contrôle dans toutes les normes. Si le contrôle s'applique à d'autres normes activées, AWS Security Hub CSPM continue d'exécuter des contrôles de sécurité pour le contrôle et vous continuez à recevoir les résultats du contrôle.

Nous vous recommandons d'aligner l'état d'activation d'un contrôle sur toutes les normes activées auxquelles le contrôle s'applique. Pour plus d'informations sur la désactivation d'un contrôle pour toutes les normes auxquelles il s'applique, consultezDésactivation d'un contrôle entre les normes.

Sur la page détaillée des normes, vous pouvez également désactiver les contrôles dans des normes spécifiques. Vous devez désactiver les contrôles dans des normes spécifiques séparément dans chaque Compte AWS et Région AWS. Lorsque vous désactivez un contrôle dans des normes spécifiques, cela n'affecte que le compte courant et la région.

Choisissez votre méthode préférée et suivez ces étapes pour désactiver un contrôle dans une ou plusieurs normes spécifiques.

Security Hub CSPM console

Pour désactiver un contrôle dans une norme spécifique

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Choisissez Normes de sécurité dans le volet de navigation. Choisissez Afficher les résultats pour la norme appropriée.

3. Sélectionnez un contrôle.
4. Choisissez Désactiver le contrôle. Cette option n'apparaît pas pour un contrôle déjà désactivé.
5. Indiquez la raison de la désactivation du contrôle et confirmez en choisissant Désactiver.

Security Hub CSPM API

Pour désactiver un contrôle dans une norme spécifique

1. ListSecurityControlDefinitionsExécutez et fournissez un ARN standard pour obtenir une liste des contrôles disponibles pour une norme spécifique. Pour obtenir un ARN standard, exécutez DescribeStandards. Cette API renvoie des identifiants de contrôle de sécurité indépendants des normes, et non des identifiants de contrôle spécifiques aux normes.

   Exemple de demande :

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Exécutez ListStandardsControlAssociations et fournissez un ID de contrôle spécifique pour renvoyer l'état d'activation actuel d'un contrôle dans chaque norme.

   Exemple de demande :

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Exécutez BatchUpdateStandardsControlAssociations. Indiquez l'ARN de la norme dans laquelle vous souhaitez désactiver le contrôle.
4. Définissez le `AssociationStatus` paramètre égal à`DISABLED`. Si vous suivez ces étapes pour un contrôle déjà désactivé, l'API renvoie une réponse au code d'état HTTP 200.

   Exemple de demande :

   ```
   {
   ```

```
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

Pour désactiver un contrôle dans une norme spécifique

1. Exécutez la `list-security-control-definitions` commande et fournissez un ARN standard pour obtenir la liste des contrôles disponibles pour une norme spécifique. Pour obtenir un ARN standard, exécutez`describe-standards`. Cette commande renvoie des identifiants de contrôle de sécurité indépendants des normes, et non des identifiants de contrôle spécifiques aux normes.

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --
   standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0"
   ```

2. Exécutez la `list-standards-control-associations` commande et fournissez un ID de contrôle spécifique pour renvoyer l'état d'activation actuel d'un contrôle dans chaque norme.

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

3. Exécutez la commande `batch-update-standards-control-associations`. Indiquez l'ARN de la norme dans laquelle vous souhaitez désactiver le contrôle.
4. Définissez le `AssociationStatus` paramètre égal à`DISABLED`. Si vous suivez ces étapes pour un contrôle déjà activé, la commande renvoie une réponse au code d'état HTTP 200.

   ```
   aws securityhub  --region us-east-1 batch-update-standards-control-
   associations --standards-control-association-updates '[{"SecurityControlId":
    "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
   foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
    "UpdatedReason": "Not applicable to environment"}]'
   ```

Contrôles suggérés à désactiver dans Security Hub CSPM

Nous vous recommandons de désactiver certains contrôles CSPM du AWS Security Hub afin de réduire le bruit lié à la recherche et les coûts d'utilisation.

Contrôles utilisant des ressources globales

Certains Services AWS prennent en charge les ressources globales, ce qui signifie que vous pouvez accéder à la ressource depuis n'importe quel endroitRégion AWS. Pour économiser sur le coûtAWS Config, vous pouvez désactiver l'enregistrement des ressources mondiales dans toutes les régions sauf une. Une fois cette opération effectuée, Security Hub CSPM continue d'effectuer des contrôles de sécurité dans toutes les régions où un contrôle est activé et vous facture en fonction du nombre de contrôles par compte et par région. Par conséquent, pour réduire le bruit lié à la recherche et économiser sur le coût du Security Hub CSPM, vous devez également désactiver les contrôles impliquant des ressources mondiales dans toutes les régions, à l'exception de la région qui enregistre les ressources mondiales.

Si un contrôle implique des ressources globales mais n'est disponible que dans une seule région, sa désactivation dans cette région vous empêche d'obtenir des résultats pour la ressource sous-jacente. Dans ce cas, nous vous recommandons de garder le contrôle activé. Lorsque vous utilisez l'agrégation entre régions, la région dans laquelle le contrôle est disponible doit être la région d'agrégation ou l'une des régions liées. Les contrôles suivants concernent des ressources mondiales mais ne sont disponibles que dans une seule région :

- Toutes les CloudFront commandes — Disponible uniquement dans la région de l'est des États-Unis (Virginie du Nord)
- GlobalAccelerator.1— Disponible uniquement dans la région ouest des États-Unis (Oregon)
- Route53.2— Disponible uniquement dans la région de l'est des États-Unis (Virginie du Nord)
- WAF.1, WAF.6, WAF.7, WAF.8 — Disponible uniquement dans la région USA Est (Virginie du Nord)

> **Note**
>
> Si vous utilisez une configuration centralisée, Security Hub CSPM désactive automatiquement les contrôles impliquant des ressources globales dans toutes les régions, à l'exception de la région d'origine. Les autres contrôles que vous choisissez d'activer par le biais d'une politique de configuration sont activés dans toutes les régions où ils sont

disponibles. Pour limiter les résultats de ces contrôles à une seule région, vous pouvez mettre à jour les paramètres de votre AWS Config enregistreur et désactiver l'enregistrement des ressources globales dans toutes les régions, à l'exception de la région d'origine.
Si un contrôle activé impliquant des ressources globales n'est pas pris en charge dans la région d'origine, Security Hub CSPM essaie d'activer le contrôle dans une région liée où le contrôle est pris en charge. Avec la configuration centralisée, vous ne pouvez pas couvrir un contrôle qui n'est pas disponible dans la région d'origine ou dans l'une des régions associées. Pour plus d'informations sur la configuration centrale, consultezComprendre la configuration centrale dans Security Hub CSPM.

Pour les contrôles dotés d'un type de calendrier périodique, il est nécessaire de les désactiver dans Security Hub CSPM pour empêcher la facturation. La définition du AWS Config paramètre `includeGlobalResourceTypes` sur `false` n'affecte pas les contrôles périodiques du Security Hub CSPM.

Les contrôles CSPM du Security Hub suivants utilisent des ressources globales :

- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée

- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services

- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

CloudTrail contrôles de journalisation

Le CloudTrail.2contrôle évalue l'utilisation de AWS Key Management Service (AWS KMS) pour chiffrer les journaux de suiviAWS CloudTrail. Si vous enregistrez ces traces dans un compte de journalisation centralisé, vous devez activer ce contrôle uniquement dans le compte et dans l'endroit Région AWS où la journalisation centralisée a lieu.

Si vous utilisez la configuration centralisée, le statut d'activation d'un contrôle est aligné sur la région d'origine et sur les régions associées. Vous ne pouvez pas désactiver un contrôle dans certaines régions et l'activer dans d'autres. Dans ce cas, vous pouvez supprimer les résultats du CloudTrail.2 contrôle afin de réduire le bruit de recherche.

CloudWatch commandes d'alarme

Si vous préférez utiliser Amazon GuardDuty pour la détection des anomalies plutôt que les CloudWatch alarmes Amazon, vous pouvez désactiver les commandes suivantes, qui se concentrent sur les CloudWatch alarmes :

- [CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »
- [CloudWatch.2] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les appels d'API non autorisés
- [CloudWatch.3] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la connexion à la console de gestion sans MFA
- [CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM
- [CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration
- [CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification
- [CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client
- [CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3
- [CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration
- [CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité
- [CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)
- [CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau
- [CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage
- [CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC

Comprendre les contrôles de sécurité et les scores dans Security Hub CSPM

Pour chaque contrôle que vous activez, AWS Security Hub CSPM exécute des contrôles de sécurité. Un contrôle de sécurité produit un résultat qui vous indique si une AWS ressource spécifique est conforme aux règles incluses dans le contrôle.

Certains contrôles sont effectués selon un calendrier périodique. Les autres contrôles ne sont exécutés qu'en cas de modification de l'état de la ressource. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

De nombreux contrôles de sécurité utilisent des règles AWS Config gérées ou personnalisées pour établir les exigences de conformité. Pour exécuter ces vérifications, vous devez configurer AWS Config et activer l'enregistrement des ressources pour les ressources requises. Pour plus d'informations sur la configurationAWS Config, consultezActivation et configuration AWS Config pour Security Hub CSPM. Pour obtenir la liste des AWS Config ressources que vous devez enregistrer pour chaque norme, consultezObligatoireAWS Configressources pour les résultats des contrôles. Les autres contrôles utilisent des fonctions Lambda personnalisées, qui sont gérées par Security Hub CSPM et ne nécessitent aucun prérequis.

Lorsque Security Hub CSPM exécute des contrôles de sécurité, il génère des résultats et leur attribue un statut de conformité. Pour plus d'informations sur le statut de conformité, consultezÉvaluation de l'état de conformité des résultats du Security Hub CSPM.

Security Hub CSPM utilise l'état de conformité des résultats des contrôles pour déterminer un état de contrôle global. Sur la base de l'état du contrôle, Security Hub CSPM calcule également un score de sécurité pour tous les contrôles activés et pour des normes spécifiques. Pour plus d'informations, consultez the section called "État de conformité et statut de contrôle" et the section called "Calcul des scores de sécurité".

Si vous avez activé les résultats de contrôle consolidés, Security Hub CSPM génère un résultat unique même lorsqu'un contrôle est associé à plusieurs normes. Pour de plus amples informations, veuillez consulter Conclusions de contrôle consolidées.

Rubriques

- ObligatoireAWS Configressources pour les résultats des contrôles
- Planification de l'exécution des vérifications de sécurité
- Génération et mise à jour des résultats de contrôle

- Évaluation de l'état de conformité et de l'état du contrôle
- Calcul des scores de sécurité

ObligatoireAWS Configressources pour les résultats des contrôles

> **Note**
>
> Si vous utilisez Security Hub (CSPM) et Security Hub, la configuration de l'enregistrement des ressources est gérée pour vous. Security Hub crée un enregistreur de configuration lié à un service AWS Config et obtient des informations directes sur toutes les ressources liées aux contrôles pris en charge dans Security Hub CSPM. Pour de plus amples informations, veuillez consulter Utilisation de l'enregistreur de configuration lié au service.

Dans AWS Security Hub CSPM, certains contrôles utilisent des AWS Config règles liées aux services qui détectent les modifications de configuration de vos ressources. AWS Pour que Security Hub CSPM puisse générer des résultats précis pour ces contrôles, vous devez activer AWS Config et activer l'enregistrement des ressources dans. AWS Config Pour plus d'informations sur la manière dont Security Hub CSPM utilise AWS Config les règles et sur la manière de les activer et de les configurerAWS Config, consultez. Activation et configuration AWS Config pour Security Hub CSPM Pour obtenir des informations détaillées sur l'enregistrement des ressources, consultez la section Utilisation de l'enregistreur de configuration dans le manuel du AWS Config développeur.

Pour recevoir des résultats de contrôle précis, vous devez activer l'enregistrement des AWS Config ressources pour les contrôles activés avec un type de planification déclenché par des modifications. Certains contrôles dotés d'un type de calendrier périodique nécessitent également un enregistrement des ressources. Cette page répertorie les ressources requises pour ces contrôles Security Hub CSPM.

Les contrôles CSPM du Security Hub peuvent s'appuyer sur des AWS Config règles gérées ou sur des règles CSPM personnalisées du Security Hub. Assurez-vous qu'aucune politique Gestion des identités et des accès AWS (IAM) ou politique AWS Organizations gérée n'AWS Configempêche d'avoir l'autorisation d'enregistrer vos ressources. Les contrôles CSPM du Security Hub évaluent directement les configurations des ressources et ne tiennent pas compte AWS Organizations des politiques.

> **Note**
>
> Régions AWSLorsqu'un contrôle n'est pas disponible, la ressource correspondante n'est pas disponible dansAWS Config. Pour obtenir la liste de ces limites, voirLimites régionales des contrôles CSPM du Security Hub.

Rubriques

- Ressources requises pour tous les contrôles Security Hub CSPM
- Ressources nécessaires pourAWSNorme sur les meilleures pratiques de sécurité fondamentales
- Ressources nécessaires pour le CISAWSBenchmark des fondations
- Ressources requises pour la norme NIST SP 800-53 Revision 5
- Ressources requises pour la norme NIST SP 800-171 Revision 2
- Ressources requises pour la norme PCI DSS v3.2.1
- Ressources nécessaires pourAWSNorme de balisage des ressources

Ressources requises pour tous les contrôles Security Hub CSPM

Pour que Security Hub CSPM puisse générer des résultats pour les contrôles déclenchés par des modifications qui sont activés et utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config Ce tableau indique également quels contrôles évaluent un type de ressource particulier. Un seul contrôle peut évaluer plusieurs types de ressources.

Service AWS	Types de ressources	Contrôles associés
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3

Service AWS	Types de ressources	Contrôles associés
		APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
	`AWS::ApiGateway::DomainName`	APIGateway.11
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig.1
	`AWS::AppConfig::ConfigurationProfile`	AppConfig.2
	`AWS::AppConfig::Environment`	AppConfig.3
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1

Service AWS	Types de ressources	Contrôles associés
	`AWS::AppRunner::VpcConnector`	AppRunner.2
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5
	`AWS::AppSync::ApiCache`	AppSync.1 AppSync.6
AWS Backup	`AWS::Backup::BackupPlan`	Backup.5
	`AWS::Backup::BackupVault`	Backup.3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	Backup.4
AWS Batch	`AWS::Batch::ComputeEnvironment`	Batch.3 Batch.4
	`AWS::Batch::JobQueue`	Batch.1
	`AWS::Batch::SchedulingPolicy`	Batch.2

Service AWS	Types de ressources	Contrôles associés
Amazon Bedrock	`AWS::Bedrock::DataSource`	Bedrock.1
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::BrowserCustom`	BedrockAgentCore.5 BedrockAgentCore.6
	`AWS::BedrockAgentCore::CodeInterpreterCustom`	BedrockAgentCore.7
	`AWS::BedrockAgentCore::Gateway`	BedrockAgentCore.2 BedrockAgentCore.4
	`AWS::BedrockAgentCore::Memory`	BedrockAgentCore.3
	`AWS::BedrockAgentCore::Runtime`	BedrockAgentCore.1
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2

Service AWS	Types de ressources	Contrôles associés
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2 CloudFormation.3 CloudFormation.4
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14 CloudFront.15 CloudFront.16 CloudFront.17
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9

Service AWS	Types de ressources	Contrôles associés
	`AWS::CloudTrail::EventDataStore`	CloudTrail.11
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	`AWS::CodeBuild::ReportGroup`	CodeBuild.7
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
CodeGuru Réviseur Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1

Service AWS	Types de ressources	Contrôles associés
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2
	`AWS::Cognito::UserPool`	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
Client Amazon Connect	`AWS::CustomerProfiles::ObjectType`	Connect.1
	`AWS::Connect::Instance`	Connect.2
AWS DataSync	`AWS::DataSync::Task`	DataSync.1 DataSync.2
Amazon Detective	`AWS::Detective::Graph`	Detective.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2
	`AWS::DMS::Endpoint`	DMS.9 DMS.10 DMS.11 DMS.12

Service AWS	Types de ressources	Contrôles associés
	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6 DMS.13
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::DHCPOptions`	EC2.174

Service AWS	Types de ressources	Contrôles associés
	AWS::EC2::EIP	EC2.12 EC2.37
	AWS::EC2::FlowLog	EC2.48
	AWS::EC2::Instance	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	AWS::EC2::InternetGateway	EC2.39
	AWS::EC2::LaunchTemplate	EC2.25 EC2.170 EC2.175 EC2.181
	AWS::EC2::NatGateway	EC2.40

Service AWS	Types de ressources	Contrôles associés
	AWS::EC2::NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2::NetworkInterface	EC2.22 EC2.35 EC2.180
	AWS::EC2::PrefixList	EC2.176
	AWS::EC2::RouteTable	EC2.42
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2::SnapshotBlockPublicAccess	EC2.182
	AWS::EC2::SpotFleet	EC2.173

Service AWS	Types de ressources	Contrôles associés
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache.7
	AWS::EC2::TrafficMirrorFilter	EC2.178
	AWS::EC2::TrafficMirrorSession	EC2.177
	AWS::EC2::TrafficMirrorTarget	EC2.179
	AWS::EC2::TransitGateway	EC2.23 EC2.52
	AWS::EC2::TransitGatewayAttachment	EC2.33
	AWS::EC2::TransitGatewayRouteTable	EC2.34
	AWS::EC2::Volume	EC2.3 EC2.45

Service AWS	Types de ressources	Contrôles associés
	`AWS::EC2::VPC`	EC2.6 EC2.46
	`AWS::EC2::VPCBlockPublicAccessOptions`	EC2.172
	`AWS::EC2::VPCEndpointService`	EC2.47
	`AWS::EC2::VPCPeeringConnection`	EC2.49
	`AWS::EC2::VPNConnection`	EC2.20 EC2.171 EC2.183
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10

Service AWS	Types de ressources	Contrôles associés
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::CapacityProvider`	ECS.19

Service AWS	Types de ressources	Contrôles associés
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13
	`AWS::ECS::TaskDefinition`	ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17 ECS.18 ECS.20 ECS.21
	`AWS::ECS::TaskSet`	ECS.16
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
	`AWS::EFS::FileSystem`	EFS.7 EFS.8

Service AWS	Types de ressources	Contrôles associés
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7
	`AWS::EKS::Nodegroup`	EKS.9
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::Listener`	ELB.17 ELB.18

Service AWS	Types de ressources	Contrôles associés
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	`AWS::EMR::SecurityConfiguration`	EMR.3 EMR.4
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4

Service AWS	Types de ressources	Contrôles associés
Amazon Fraud Detector	`AWS::FraudDetector::EntityType`	FraudDetector.1
	`AWS::FraudDetector::Label`	FraudDetector.2
	`AWS::FraudDetector::Outcome`	FraudDetector.3
	`AWS::FraudDetector::Variable`	FraudDetector.4
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1
AWS Glue	`AWS::Glue::Job`	Glue.1 Glue.4
	`AWS::Glue::MLTransform`	Glue.3
Amazon GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2
	`AWS::GuardDuty::IPSet`	GuardDuty.3

Service AWS	Types de ressources	Contrôles associés
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23

Service AWS	Types de ressources	Contrôles associés
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::PlaybackKeyPair`	IVS.1
	`AWS::IVS::RecordingConfiguration`	IVS.2
	`AWS::IVS::Channel`	IVS.3
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWSÉvénements IoT	`AWS::IoTEvents::AlarmModel`	IoTEvents.3

Service AWS	Types de ressources	Contrôles associés
	`AWS::IoTEvents::DetectorModel`	IoTEvents.2
	`AWS::IoTEvents::Input`	IoTEvents.1
AWSIoT SiteWise	`AWS::IoTSiteWise::AssetModel`	IoTSiteWise.1
	`AWS::IoTSiteWise::Dashboard`	IoTSiteWise.2
	`AWS::IoTSiteWise::Gateway`	IoTSiteWise.3
	`AWS::IoTSiteWise::Portal`	IoTSiteWise.4
	`AWS::IoTSiteWise::Project`	IoTSiteWise.5
AWSIoT TwinMaker	`AWS::IoTTwinMaker::Entity`	IoTTwinMaker.4
	`AWS::IoTTwinMaker::Scene`	IoTTwinMaker.3

Service AWS	Types de ressources	Contrôles associés
	`AWS::IoTTwinMaker::SyncJob`	IoTTwinMaker.1
	`AWS::IoTTwinMaker::Workspace`	IoTTwinMaker.2
AWSIoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoTWireless.1
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces (pour Apache Cassandra)	`AWS::Cassandra::Keyspace`	Keyspaces.1
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2 Kinesis.3
AWS Key Management Service(AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 KMS.5 S3.17

Service AWS	Types de ressources	Contrôles associés
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6 Lambda.7
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2 MSK.4 MSK.6
	`AWS::KafkaConnect::Connector`	MSK.3 MSK.5
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9 NetworkFirewall.10

Service AWS	Types de ressources	Contrôles associés
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
CA privée AWS	`AWS::ACMPCA::CertificateAuthority`	PCA.2

Service AWS	Types de ressources	Contrôles associés
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

Service AWS	Types de ressources	Contrôles associés
		RDS.37 RDS.47 RDS.48
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

Service AWS	Types de ressources	Contrôles associés
	AWS::RDS::DBInstance	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.23 RDS.25 RDS.30 RDS.36 RDS.40
	AWS::RDS::DBSecurityGroup	RDS.31
	AWS::RDS::DBSnapshot	RDS.1 RDS.4 RDS.32

Service AWS	Types de ressources	Contrôles associés
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
	`AWS::RDS::GlobalCluster`	RDS.51
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.10 Redshift.11 Redshift.18
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2 Redshift.17

Service AWS	Types de ressources	Contrôles associés
	`AWS::Redshift::ClusterSnapshot`	Redshift.13
	`AWS::Redshift::ClusterSubnetGroup`	Redshift.14 Redshift.16
	`AWS::Redshift::EventSubscription`	Redshift.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

Service AWS	Types de ressources	Contrôles associés
	`AWS::S3::Bucket`	CloudTrail.6 CloudTrail.7 S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
	`AWS::S3::MultiRegionAccessPoint`	S3.24

Service AWS	Types de ressources	Contrôles associés
	`AWS::S3Express::DirectoryBucket`	S3.25
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker.7
	`AWS::SageMaker::InferenceExperiment`	SageMaker.23 SageMaker.24
	`AWS::SageMaker::Model`	SageMaker.5 SageMaker.16 SageMaker.19
	`AWS::SageMaker::ModelExplainabilityJobDefinition`	SageMaker.20
	`AWS::SageMaker::ModelQualityJobDefinition`	SageMaker.25
	`AWS::SageMaker::MonitoringSchedule`	SageMaker.22

Service AWS	Types de ressources	Contrôles associés
	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3 SageMaker.21
	`AWS::SageMaker::FeatureGroup`	SageMaker.17 SageMaker.18
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2 SES.3
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3 SNS.4
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2 SQS.3

Service AWS	Types de ressources	Contrôles associés
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Systems Manager SM)	`AWS::SSM::Document`	SSM.5
AWS Transfer Family	`AWS::Transfer::Agreement`	Transfer.4
	`AWS::Transfer::Certificate`	Transfer.5
	`AWS::Transfer::Connector`	Transfer.3 Transfer.6
	`AWS::Transfer::Profile`	Transfer.7
	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.1 WAF.8

Service AWS	Types de ressources	Contrôles associés
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`	WorkSpaces.1 WorkSpaces.2

Ressources nécessaires pourAWSNorme sur les meilleures pratiques de sécurité fondamentales

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications qui s'appliquent à la norme AWS Foundational Security Best Practices (v.1.0.0), sont activés et utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config Pour plus d'informations sur cette norme, consultezAWS Norme fondamentale des meilleures pratiques de sécurité dans Security Hub CSPM.

Service AWS	Types de ressources
Amazon API Gateway	`AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

Service AWS	Types de ressources
AWS AppSync	`AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock	`AWS::Bedrock::DataSource`
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::BrowserCustom` , `AWS::BedrockAgentCore::CodeInterpreterCustom` , `AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Runtime`
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project` , `AWS::CodeBuild::ReportGroup`
Amazon Cognito	`AWS::Cognito::IdentityPool` , `AWS::Cognito::UserPool`
AWS CloudTrail	`AWS::CloudTrail::EventDataStore`
Client Amazon Connect	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Service AWS	Types de ressources
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::SnapshotBlockPublicAccess` , `AWS::EC2::SpotFleet` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPCBlockPublicAccessOptions` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::CapacityProvider` , `AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition` , `AWS::ECS::TaskSet`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint` , `AWS::EFS::FileSystem`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::Nodegroup`

Service AWS	Types de ressources
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
AWS Glue	`AWS::Glue::Job` , `AWS::Glue::MLTransform`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Key Management Service(AWS KMS)	`AWS::KMS::Key`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster` , `AWS::KafkaConnect::Connector`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`

Service AWS	Types de ressources
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBProxy` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription` , `AWS::RDS::GlobalCluster`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Redshift sans serveur	`AWS::RedshiftServerless::Workgroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket` , `AWS::S3::MultiRegionAccessPoint` , `AWS::S3Express::DirectoryBucket`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::InferenceExperiment` , `AWS::SageMaker::Model` , `AWS::SageMaker::ModelExplainabilityJobDefinition` , `AWS::SageMaker::ModelQualityJobDefinition` , `AWS::SageMaker::MonitoringSchedule` , `AWS::SageMaker::NotebookInstance`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Service AWS	Types de ressources
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`

Ressources nécessaires pour le CISAWSBenchmark des fondations

Pour effectuer des contrôles de sécurité pour les contrôles activés qui s'appliquent au Center for Internet Security (CIS) AWS Foundations Benchmark, Security Hub CSPM exécute les étapes d'audit exactes prescrites pour les contrôles ou utilise des règles AWS Config gérées spécifiques. Pour plus d'informations sur cette norme dans Security Hub CSPM, consultez. CIS AWS Point de référence des fondations en matière de sécurité CSPM

Ressources requises pour CIS v5.0.0

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications de CIS v5.0.0 activés qui utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config

Service AWS	Types de ressources
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::FileSystem`

Service AWS	Types de ressources
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance` , `AWS::RDS::DBCluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Ressources requises pour CIS v3.0.0

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications de CIS v3.0.0 activés qui utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config

Service AWS	Types de ressources
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Ressources requises pour CIS v1.4.0

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications de CIS v1.4.0 activés qui utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config

Service AWS	Types de ressources
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Policy` , `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Ressources requises pour CIS v1.2.0

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications de CIS v1.2.0 activés qui utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config

Service AWS	Types de ressources
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::SecurityGroup`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Policy` , `AWS::IAM::User`

Ressources requises pour la norme NIST SP 800-53 Revision 5

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications qui s'appliquent à la norme NIST SP 800-53 Revision 5, sont activés et utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config Pour plus d'informations sur cette norme, consultezNIST SP 800-53 Révision 5 dans Security Hub CSPM.

Service AWS	Types de ressources
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory`
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`

Service AWS	Types de ressources
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service(AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`

Service AWS	Types de ressources
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Service AWS	Types de ressources
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Ressources requises pour la norme NIST SP 800-171 Revision 2

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles déclenchés par des modifications qui s'appliquent à la norme NIST SP 800-171 Revision 2, sont activés et utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config Pour plus d'informations sur cette norme, consultezNIST SP 800-171 Revision 2 dans Security Hub CSPM.

Service AWS	Types de ressources
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`

Service AWS	Types de ressources
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Ressources requises pour la norme PCI DSS v3.2.1

Pour que Security Hub CSPM puisse rapporter avec précision les résultats des contrôles qui s'appliquent à la version 3.2.1 de la norme de sécurité des données du secteur des cartes de paiement (PCI DSS), sont activés et utilisent une AWS Config règle, vous devez enregistrer les types de ressources suivants dans. AWS Config Pour plus d'informations sur cette norme, consultezPCI DSS dans Security Hub CSPM.

Service AWS	Types de ressources
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::SecurityGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot`
Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

Ressources nécessaires pourAWSNorme de balisage des ressources

Tous les contrôles qui s'appliquent à la norme de balisage AWS des ressources sont déclenchés par des modifications et utilisent une AWS Config règle. Pour que Security Hub CSPM puisse rapporter avec précision les résultats de ces contrôles, vous devez enregistrer les types de ressources suivants dans. AWS Config Pour plus d'informations sur cette norme, consultezAWS Norme de balisage des ressources dans Security Hub CSPM.

Service AWS	Types de ressources
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`
AWS AppConfig	`AWS::AppConfig::Application` , `AWS::AppConfig::ConfigurationProfile` , `AWS::AppConfig::Environment` , `AWS::AppConfig::ExtensionAssociation`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` , `AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::BackupPlan` , `AWS::Backup::BackupVault` , `AWS::Backup::RecoveryPlan` , `AWS::Backup::ReportPlan`
AWS Batch	`AWS::Batch::ComputeEnvironment` , `AWS::Batch::JobQueue` , `AWS::Batch::SchedulingPolicy`
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`

Service AWS	Types de ressources
Amazon CodeGuru	`AWS::CodeGuruProfiler::ProfilingGroup` , `AWS::CodeGuruReviewer::RepositoryAssociation`
Client Amazon Connect	`AWS::CustomerProfiles::ObjectType`

AWS Database Migration Service(AWS DMS)	`AWS::DMS::Certificate` , `AWS::DMS::EventSubscription`
	
	`AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationSubnetGroup`

AWS DataSync	`AWS::DataSync::Task`
Amazon Detective	`AWS::Detective::Graph`
Amazon DynamoDB	`AWS::DynamoDB::Trail`

Service AWS	Types de ressources
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway` , `AWS::EC2::DHCPOptions` , `AWS::EC2::EIP` , `AWS::EC2::FlowLog` , `AWS::EC2::Instance` , `AWS::EC2::InternetGateway` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NatGateway` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::PrefixList` , `AWS::EC2::RouteTable` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TrafficMirrorFilter` , `AWS::EC2::TrafficMirrorSession` , `AWS::EC2::TrafficMirrorTarget` , `AWS::EC2::TransitGateway` , `AWS::EC2::TransitGatewayAttachment` , `AWS::EC2::TransitGatewayRouteTable` , `AWS::EC2::Volume` , `AWS::EC2::VPC` , `AWS::EC2::VPCEndpointService` , `AWS::EC2::VPCPeeringConnection` , `AWS::EC2::VPNGateway`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`

Service AWS	Types de ressources
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`

Amazon Fraud Detector	`AWS::FraudDetector::EntityType` , `AWS::FraudDetector::Label`
	
	`AWS::FraudDetector::Outcome` , `AWS::FraudDetector::Variable`

AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`
Amazon GuardDuty	`AWS::GuardDuty::Detector` , `AWS::GuardDuty::Filter` , `AWS::GuardDuty::IPSet`
Gestion des identités et des accès AWS(JE SUIS)	`AWS::IAM::Role` , `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer(Analyseur d'accès IAM)	`AWS::AccessAnalyzer::Analyzer`
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`

Service AWS	Types de ressources
AWS IoTÉvénements	`AWS::IoTEvents::AlarmModel` , `AWS::IoTEvents::DetectorModel` , `AWS::IoTEvents::Input`
AWS IoTSiteWise	`AWS::IoTSiteWise::Dashboard` , `AWS::IoTSiteWise::Gateway` , `AWS::IoTSiteWise::Portal` , `AWS::IoTSiteWise::Project`
AWS IoTTwinMaker	`AWS::IoTTwinMaker::Entity` , `AWS::IoTTwinMaker::Scene` , `AWS::IoTTwinMaker::SyncJob` , `AWS::IoTTwinMaker::Workspace`
AWS IoTSans fil	`AWS::IoTWireless::FuotaTask` , `AWS::IoTWireless::MulticastGroup` , `AWS::IoTWireless::ServiceProfile`
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::Channel` , `AWS::IVS::PlaybackKeyPair` , `AWS::IVS::RecordingConfiguration`
Amazon Keyspaces (pour Apache Cassandra)	`AWS::Cassandra::Keyspace`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`

Service AWS	Types de ressources
Autorité de certification privée AWS	`AWS::ACMPCA::CertificateAuthority`
Amazon Relational Database Service	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSecurityGroup` , `AWS::RDS::DBSnapshot` , `AWS::RDS::DBSubnetGroup`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterParameterGroup` , `AWS::Redshift::ClusterSnapshot` , `AWS::Redshift::ClusterSubnetGroup` , `AWS::Redshift::EventSubscription`
Amazon Route 53	`AWS::Route53::HealthCheck`
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig` , `AWS::SageMaker::Image`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` , `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager(SSM)	`AWS::SSM::Document`

Service AWS	Types de ressources
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

Planification de l'exécution des vérifications de sécurité

Une fois que vous avez activé une norme de sécurité, AWS Security Hub CSPM commence à exécuter toutes les vérifications dans les deux heures. La plupart des contrôles commencent à être exécutés dans les 25 minutes. Security Hub CSPM exécute des vérifications en évaluant la règle sous-jacente à un contrôle. Jusqu'à ce qu'un contrôle termine sa première série de vérifications, son statut est Aucune donnée.

Lorsque vous activez une nouvelle norme, Security Hub CSPM peut mettre jusqu'à 24 heures à générer des résultats pour les contrôles qui utilisent la même règle sous-jacente AWS Config liée au service que les contrôles activés issus d'autres normes activées. Par exemple, si vous activez le Lambda.1contrôle dans la norme AWS Foundational Security Best Practices (FSBP), Security Hub CSPM crée la règle liée au service et génère généralement des résultats en quelques minutes. Ensuite, si vous activez le Lambda.1 contrôle dans le cadre de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), Security Hub CSPM peut mettre jusqu'à 24 heures à générer des résultats pour le contrôle, car celui-ci utilise la même règle liée au service.

Après la vérification initiale, le calendrier de chaque contrôle peut être périodique ou déclenché par des modifications. Pour un contrôle basé sur une AWS Config règle gérée, la description du contrôle inclut un lien vers la description de la règle dans le guide du AWS Config développeur. Cette description indique si la règle est déclenchée par des modifications ou périodique.

Contrôles de sécurité périodiques

Les contrôles de sécurité périodiques sont exécutés automatiquement dans les 12 ou 24 heures suivant la dernière exécution. Security Hub CSPM détermine la périodicité, et vous ne pouvez pas la modifier. Les contrôles périodiques reflètent une évaluation au moment où le contrôle est exécuté.

Si vous mettez à jour l'état du flux de travail d'un résultat de contrôle périodique, puis que, lors de la prochaine vérification, le statut de conformité du résultat reste le même, le statut du flux de travail

reste dans son état modifié. Par exemple, si vous ne parvenez pas à trouver le KMS.4contrôle (la AWS KMS keyrotation doit être activée), puis que vous y remédiez, Security Hub CSPM fait passer le statut du flux de travail de à. `NEW` `RESOLVED` Si vous désactivez la rotation des clés KMS avant la prochaine vérification périodique, l'état du résultat dans le flux de travail est conservé`RESOLVED`.

Les contrôles qui utilisent les fonctions Lambda personnalisées de Security Hub CSPM sont périodiques.

Change-triggered contrôles de sécurité

Change-triggered les contrôles de sécurité sont exécutés lorsque la ressource associée change d'état. AWS Configvous permet de choisir entre un enregistrement continu des modifications de l'état des ressources et un enregistrement quotidien. Si vous choisissez l'enregistrement quotidien, AWS Config fournit les données de configuration des ressources à la fin de chaque période de 24 heures en cas de modification de l'état des ressources. S'il n'y a aucune modification, aucune donnée n'est transmise. Cela peut retarder la génération des résultats du Security Hub CSPM jusqu'à ce qu'une période de 24 heures soit terminée. Quelle que soit la période d'enregistrement que vous avez choisie, Security Hub CSPM vérifie au moins une fois toutes les 24 heures qu'aucune mise à jour des ressources n'a AWS Config été manquée.

En général, Security Hub CSPM utilise des règles déclenchées par des modifications chaque fois que cela est possible. Pour qu'une ressource utilise une règle déclenchée par des modifications, elle doit prendre en charge les éléments AWS Config de configuration.

Génération et mise à jour des résultats de contrôle

AWSSecurity Hub CSPM génère et met à jour les résultats des contrôles lorsqu'il effectue des vérifications par rapport aux contrôles de sécurité. Les résultats des contrôles utilisent le format ASFF (AWSSecurity Finding Format).

Security Hub CSPM facture normalement chaque contrôle de sécurité effectué pour un contrôle. Toutefois, si plusieurs contrôles utilisent la même AWS Config règle, Security Hub CSPM ne facture qu'une seule fois pour chaque vérification effectuée par rapport à la règle. Par exemple, la AWS Config `iam-password-policy` règle est utilisée par plusieurs contrôles dans les normes CIS AWS Foundations Benchmark et AWS Foundational Security Best Practices. Chaque fois que Security Hub CSPM effectue une vérification par rapport à cette règle, il génère un résultat de contrôle distinct pour chaque contrôle associé, mais ne facture qu'une seule fois pour le contrôle.

Si la taille d'un résultat de contrôle dépasse le maximum de 240 Ko, Security Hub CSPM supprime l'`Resource.Details`objet du résultat. Pour les contrôles basés sur des AWS Config ressources, vous pouvez consulter les détails des ressources à l'aide de la AWS Config console.

Rubriques

- Conclusions de contrôle consolidées
- Génération, mise à jour et archivage des résultats des contrôles
- Automatisation et suppression des résultats de contrôle
- Détails de conformité pour les résultats des contrôles
- ProductFields détails relatifs aux résultats des contrôles
- Niveaux de gravité des résultats de contrôle

Conclusions de contrôle consolidées

Si les résultats de contrôle consolidés sont activés pour votre compte, Security Hub CSPM génère une seule découverte ou mise à jour des résultats pour chaque contrôle de sécurité d'un contrôle, même si un contrôle s'applique à plusieurs normes activées. Pour obtenir la liste des contrôles et des normes auxquelles ils s'appliquent, consultez leRéférence de contrôle pour Security Hub CSPM. Nous recommandons d'activer les résultats de contrôle consolidés afin de réduire le bruit de détection.

Si vous avez activé Security Hub CSPM Compte AWS avant le 23 février 2023, vous pouvez activer les résultats de contrôle consolidés en suivant les instructions fournies plus loin dans cette section. Si vous activez Security Hub CSPM le 23 février 2023 ou après cette date, les résultats de contrôle consolidés sont automatiquement activés pour votre compte.

Si vous utilisez l'intégration du Security Hub CSPM avec des comptes membres AWS Organizations ou si vous les invitez par le biais d'un processus d'invitation manuel, les résultats de contrôle consolidés ne sont activés pour les comptes membres que s'ils sont activés pour le compte administrateur. Si la fonctionnalité est désactivée pour le compte administrateur, elle est désactivée pour les comptes membres. Ce comportement s'applique aux comptes de membres nouveaux et existants. En outre, si l'administrateur utilise une configuration centralisée pour gérer le Security Hub CSPM pour plusieurs comptes, il ne peut pas utiliser de politiques de configuration centralisées pour activer ou désactiver les résultats de contrôle consolidés pour les comptes.

Si vous désactivez les résultats de contrôle consolidés pour votre compte, Security Hub CSPM génère ou met à jour un résultat de contrôle distinct pour chaque norme activée qui inclut un contrôle.

Par exemple, si vous activez quatre normes qui partagent un contrôle, vous recevez quatre résultats distincts après un contrôle de sécurité pour le contrôle. Si vous activez les résultats de contrôle consolidés, vous ne recevez qu'un seul résultat.

Lorsque vous activez les résultats de contrôle consolidés, Security Hub CSPM crée de nouveaux résultats indépendants des normes et archive les résultats standard d'origine. Certains champs et valeurs de recherche de contrôle vont changer, ce qui peut avoir un impact sur vos flux de travail existants. Pour plus d'informations sur ces modifications, consultezRésultats des contrôles consolidés — modifications de l'ASFF. L'activation des résultats de contrôle consolidés peut également affecter les résultats que les produits tiers intégrés reçoivent de Security Hub CSPM. Si vous utilisez la solution Automated Security Response on AWS v2.0.0, notez qu'elle prend en charge les résultats de contrôle consolidés.

Pour activer ou désactiver les résultats de contrôle consolidés, vous devez être connecté à un compte administrateur ou à un compte autonome.

> **Note**
>
> Une fois que vous avez activé les résultats de contrôle consolidés, Security Hub CSPM peut mettre jusqu'à 24 heures pour générer de nouveaux résultats consolidés et archiver les résultats standard existants. De même, après avoir désactivé les résultats de contrôle consolidés, Security Hub CSPM peut mettre jusqu'à 24 heures pour générer de nouveaux résultats basés sur des normes et archiver les résultats consolidés existants. Au cours de ces périodes, il est possible que vous constatiez un mélange de résultats indépendants des normes et de résultats basés sur les normes dans votre compte.

Security Hub CSPM console

Pour activer ou désactiver les résultats des contrôles consolidés

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Dans la section Contrôles, choisissez Modifier.
4. Utilisez le commutateur Consolidated control findings pour activer ou désactiver les résultats de contrôle consolidés.
5. Choisissez Enregistrer.

Security Hub CSPM API

Pour activer ou désactiver les résultats des contrôles consolidés par programmation, utilisez l'UpdateSecurityHubConfigurationAPI Security Hub CSPM. Ou, si vous utilisez leAWS CLI, exécutez la update-security-hub-configurationcommande.

Pour le `control-finding-generator` paramètre, spécifiez `SECURITY_CONTROL` pour activer les résultats de contrôle consolidés. Pour désactiver les résultats des contrôles consolidés, spécifiez`STANDARD_CONTROL`.

Par exemple, la AWS CLI commande suivante permet de consolider les résultats des contrôles.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

La AWS CLI commande suivante désactive les résultats de contrôle consolidés.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Génération, mise à jour et archivage des résultats des contrôles

Security Hub CSPM exécute des contrôles de sécurité selon un calendrier. La première fois que Security Hub CSPM effectue un contrôle de sécurité pour un contrôle, il génère un nouveau résultat pour chaque AWS ressource vérifiée par le contrôle. Chaque fois que Security Hub CSPM effectue ensuite un contrôle de sécurité pour le contrôle, il met à jour les résultats existants pour signaler les résultats du contrôle. Cela signifie que vous pouvez utiliser les données fournies par les résultats individuels pour suivre les changements de conformité pour des ressources spécifiques par rapport à des contrôles particuliers.

Par exemple, si le statut de conformité d'une ressource passe de `FAILED` à `PASSED` pour un contrôle particulier, Security Hub CSPM ne génère pas de nouveau résultat. Security Hub CSPM met plutôt à jour les résultats existants pour le contrôle et la ressource. Dans le résultat, Security Hub CSPM remplace la valeur du champ État de conformité (`Compliance.Status`) par. `PASSED` Security Hub CSPM met également à jour les valeurs des champs supplémentaires afin de refléter les résultats de la vérification, par exemple, l'étiquette de gravité, le statut du flux de travail et les horodatages qui indiquent la date à laquelle Security Hub CSPM a effectué la dernière vérification et mis à jour le résultat.

Lorsque vous signalez une modification de l'état de conformité, Security Hub CSPM peut mettre à jour l'un des champs suivants dans une constatation de contrôle :

- `Compliance.Status`— Le nouveau statut de conformité de la ressource pour le contrôle spécifié.
- `FindingProviderFields.Severity.Label`— La nouvelle représentation qualitative de la gravité du résultat, telle que `LOW`MEDIUM, ou`HIGH`.
- `FindingProviderFields.Severity.Original`— La nouvelle représentation quantitative de la gravité de la constatation, par exemple `0` pour une ressource conforme.
- `FirstObservedAt`— Lorsque le statut de conformité de la ressource a récemment changé.
- `LastObservedAt`— Lorsque Security Hub CSPM a récemment effectué le contrôle de sécurité pour le contrôle et la ressource spécifiés.
- `ProcessedAt`— Quand Security Hub CSPM a récemment commencé à traiter le résultat.
- `ProductFields.PreviousComplianceStatus`— L'état de conformité précédent (`Compliance.Status`) de la ressource pour le contrôle spécifié.
- `UpdatedAt`— Quand Security Hub CSPM a mis à jour le résultat pour la dernière fois.
- `Workflow.Status`— L'état de l'enquête sur le résultat, sur la base du nouveau statut de conformité de la ressource pour le contrôle spécifié.

La mise à jour d'un champ par Security Hub CSPM dépend principalement des résultats du dernier contrôle de sécurité concernant le contrôle et les ressources applicables. Par exemple, si le statut de conformité d'une ressource passe de `PASSED` à `FAILED` pour un contrôle particulier, Security Hub CSPM change le statut du flux de travail du résultat en. `NEW` Pour suivre les mises à jour des résultats individuels, vous pouvez consulter l'historique d'un résultat. Pour plus de détails sur les champs individuels des résultats, voir AWSSecurity Finding Format (ASFF).

Dans certains cas, Security Hub CSPM génère de nouveaux résultats pour des vérifications ultérieures par un contrôle, au lieu de mettre à jour les résultats existants. Cela peut se produire en cas de problème avec la AWS Config règle qui soutient un contrôle. Dans ce cas, Security Hub CSPM archive le résultat existant et génère un nouveau résultat pour chaque vérification. Dans les nouvelles découvertes, le statut de conformité est `NOT_AVAILABLE` et l'état de l'enregistrement est`ARCHIVED`. Une fois que vous avez résolu le problème lié à la AWS Config règle, Security Hub CSPM génère de nouvelles conclusions et commence à les mettre à jour afin de suivre les modifications ultérieures du statut de conformité des ressources individuelles.

Outre la génération et la mise à jour des résultats de contrôle, Security Hub CSPM archive automatiquement les résultats de contrôle qui répondent à certains critères. Security Hub CSPM

archive un résultat si le contrôle est désactivé, si la ressource spécifiée est supprimée ou si la ressource spécifiée n'existe plus. Il est possible qu'une ressource n'existe plus car le service associé n'est plus utilisé. Plus précisément, Security Hub CSPM archive automatiquement un résultat de contrôle si celui-ci répond à l'un des critères suivants :

- Le résultat n'a pas été mis à jour depuis 3 à 5 jours. Notez que l'archivage basé sur cette période est effectué dans la mesure du possible et n'est pas garanti.
- L'AWS Configévaluation associée renvoyée `NOT_APPLICABLE` pour l'état de conformité de la ressource spécifiée.

Pour déterminer si une recherche est archivée, vous pouvez vous référer au champ record state (`RecordState`) de la recherche. Si un résultat est archivé, la valeur de ce champ est`ARCHIVED`.

Security Hub CSPM stocke les résultats de contrôle archivés pendant 30 jours. Au bout de 30 jours, les résultats expirent et Security Hub CSPM les supprime définitivement. Pour déterminer si un résultat de contrôle archivé a expiré, Security Hub CSPM base son calcul sur la valeur du `UpdatedAt` champ du résultat.

Pour conserver les résultats de contrôle archivés pendant plus de 30 jours, vous pouvez les exporter vers un compartiment S3. Vous pouvez le faire en utilisant une action personnalisée avec une EventBridge règle Amazon. Pour de plus amples informations, veuillez consulter Utilisation à EventBridge des fins de réponse et de correction automatisées.

> **Note**
>
> Avant le 3 juillet 2025, Security Hub CSPM générait et mettait à jour les résultats de contrôle différemment lorsque le statut de conformité d'une ressource changeait pour un contrôle. Auparavant, Security Hub CSPM créait un nouveau résultat de contrôle et archivait le résultat existant pour une ressource. Par conséquent, vous pouvez avoir plusieurs résultats archivés pour un contrôle et une ressource particuliers jusqu'à leur expiration (après 30 jours).

Automatisation et suppression des résultats de contrôle

Vous pouvez utiliser les règles d'automatisation CSPM de Security Hub pour mettre à jour ou supprimer des résultats de contrôle spécifiques. Si vous supprimez un résultat, vous pouvez continuer à y accéder. Cependant, la suppression indique que vous pensez qu'aucune action n'est nécessaire pour remédier à la constatation.

En supprimant les résultats, vous pouvez réduire le bruit de recherche. Par exemple, vous pouvez supprimer les résultats de contrôle générés dans les comptes de test. Vous pouvez également supprimer les résultats liés à des ressources spécifiques. Pour en savoir plus sur la mise à jour ou la suppression automatique des résultats, consultezComprendre les règles d'automatisation dans Security Hub CSPM.

Les règles d'automatisation sont appropriées lorsque vous souhaitez mettre à jour ou supprimer des résultats de contrôle spécifiques. Toutefois, si un contrôle n'est pas pertinent pour votre organisation ou votre cas d'utilisation, nous vous recommandons de le désactiver. Si vous désactivez un contrôle, Security Hub CSPM n'effectue aucun contrôle de sécurité pour celui-ci et vous n'êtes pas facturé pour ce contrôle.

Détails de conformité pour les résultats des contrôles

Dans les résultats générés par les contrôles de sécurité pour les contrôles, l'objet de conformité et les champs du format ASFF (AWSSecurity Finding Format) fournissent des détails de conformité pour les ressources individuelles vérifiées par un contrôle. Cela inclut les informations suivantes :

- `AssociatedStandards`— Les normes activées dans lesquelles le contrôle est activé.
- `RelatedRequirements`— Les exigences associées pour le contrôle dans toutes les normes activées. Ces exigences découlent de cadres de sécurité tiers pour le contrôle, tels que la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) ou la norme NIST SP 800-171 révision 2.
- `SecurityControlId`— L'identifiant pour le contrôle des normes prises en charge par Security Hub CSPM.
- `Status`— Le résultat de la dernière vérification effectuée par Security Hub CSPM pour le contrôle. Les résultats des vérifications précédentes sont conservés dans l'historique des résultats.
- `StatusReasons`— Tableau répertoriant les raisons de la valeur spécifiée par le `Status` champ. Pour chaque raison, cela inclut un code de motif et une description.

Le tableau suivant répertorie les codes de motif et les descriptions qu'un résultat peut inclure dans le `StatusReasons` tableau. Les étapes de correction varient en fonction du contrôle qui a généré une constatation avec un code de motif spécifié. Pour consulter les instructions de correction relatives à un contrôle, reportez-vous auRéférence de contrôle pour Security Hub CSPM.

Code de motif	Statut de conformité	Description
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	Le CloudTrail parcours multirégional ne possède pas de filtre métrique valide.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Les filtres métriques ne sont pas présents pour le CloudTrail parcours multirégional.
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	Le compte ne dispose pas d'un CloudTrail parcours multirégional avec la configuration requise.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	Multi-Region CloudTrail les sentiers ne se trouvent pas dans la région actuelle.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	Aucune action d'alarme valide n'est présente.
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch les alarmes n'existent pas dans le compte.
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS Configle statut est `ConfigError`	AWS Configaccès refusé. Vérifiez qu'il AWS Config est activé et que des autorisations suffisantes ont été accordées.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Configa évalué vos ressources en fonction de la règle. La règle ne s'appliquait pas aux AWS ressources incluses dans son champ d'application, les ressources spécifiées ont été supprimées ou

Code de motif	Statut de conformité	Description
		les résultats de l'évaluation ont été supprimés.
`CONFIG_RECORDER_CUSTOM_ROLE`	`FAILED`(pour Config.1)	L'AWS Configenregistreur utilise un rôle IAM personnalisé au lieu du rôle AWS Config lié au service, et le paramètre `includeConfigServiceLinkedRoleCheck` personnalisé pour Config.1 n'est pas défini sur. `false`
`CONFIG_RECORDER_DISABLED`	`FAILED`(pour Config.1)	AWS Confign'est pas activé lorsque l'enregistreur de configuration est activé.
`CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES`	`FAILED`(pour Config.1)	AWS Confign'enregistre pas tous les types de ressources correspondant aux contrôles Security Hub CSPM activés. Activez l'enregistrement pour les ressources suivantes :*`Resources that aren't being recorded`*.

Code de motif	Statut de conformité	Description
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	Le statut de conformité est `NOT_AVAILABLE` dû au fait que le statut « Non applicable » a été AWS Config renvoyé. AWS Configne fournit pas la raison du statut. Voici quelques raisons pouvant expliquer le statut « Non applicable » : • La ressource a été supprimée du champ d'application de la AWS Config règle. • La AWS Config règle a été supprimée. • La ressource a été supprimée. • La logique des AWS Config règles peut produire un statut Non applicable.

Code de motif	Statut de conformité	Description
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Configle statut est `ConfigError`	Ce code de motif est utilisé pour plusieurs types d'erreur d'évaluation différents. La description fournit des informations sur la raison spécifique. Le type d'erreur peut être l'un des suivants : • Impossibilité d'effectuer l'évaluation en raison d'un manque d'autorisations. La description fournit l'autorisation spécifique manquante. • Valeur manquante ou non valide pour un paramètre. La description fournit le paramètre et les conditions requises pour la valeur du paramètre. • Erreur de lecture à partir d'un compartiment S3. La description identifie le compartiment et indique l'erreur spécifique. • AWSAbonnement manquant. • Un délai d'attente général pour l'évaluation. • Un compte suspendu.

Code de motif	Statut de conformité	Description
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS Configle statut est `ConfigError`	La AWS Config règle est en cours de création.
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Une erreur inconnue s'est produite.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	`FAILED`	Security Hub CSPM n'est pas en mesure d'effectuer une vérification par rapport à un environnement d'exécution Lambda personnalisé.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	Le résultat est dans un `WARNING` état car le compartiment S3 associé à cette règle se trouve dans une région ou un compte différent. Cette règle ne prend pas en charge les vérifications entre régions ou entre comptes. Il est recommandé de désactiver ce contrôle dans cette région ou ce compte. Exécutez-le uniquement dans la région ou le compte où se trouve la ressource.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	Les filtres métriques CloudWatch Logs ne disposent pas d'un abonnement Amazon SNS valide.

Code de motif	Statut de conformité	Description
SNS_TOPIC_CROSS_ACCOUNT	WARNING	Le résultat est en WARNING état. La rubrique SNS associée à cette règle appartient à un autre compte. Le compte courant ne peut pas obtenir les informations d'abonnement. Le compte propriétaire de la rubrique SNS doit accorder au compte actuel l'sns:ListSubscriptionsByTopic autorisation pour la rubrique SNS.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Le résultat est invalide WARNING car le sujet SNS associé à cette règle se trouve dans une autre région ou dans un autre compte. Cette règle ne prend pas en charge les vérifications entre régions ou entre comptes. Il est recommandé de désactiver ce contrôle dans cette région ou ce compte. Exécutez-le uniquement dans la région ou le compte où se trouve la ressource.
SNS_TOPIC_INVALID	FAILED	La rubrique SNS associée à cette règle n'est pas valide.
THROTTLING_ERROR	NOT_AVAILABLE	L'opération d'API pertinente a dépassé le taux autorisé.

ProductFields détails relatifs aux résultats des contrôles

Dans les résultats générés par les contrôles de sécurité pour les contrôles, l'ProductFieldsattribut du format ASFF (AWSSecurity Finding Format) peut inclure les champs suivants.

`ArchivalReasons:0/Description`

Décrit pourquoi Security Hub CSPM a archivé une découverte.

Par exemple, Security Hub CSPM archive les résultats existants lorsque vous désactivez un contrôle ou une norme, ou lorsque vous activez ou désactivez les résultats de contrôle consolidés.

`ArchivalReasons:0/ReasonCode`

Spécifie pourquoi Security Hub CSPM a archivé un résultat.

Par exemple, Security Hub CSPM archive les résultats existants lorsque vous désactivez un contrôle ou une norme, ou lorsque vous activez ou désactivez les résultats de contrôle consolidés.

`PreviousComplianceStatus`

État de conformité précédent (`Compliance.Status`) de la ressource pour le contrôle spécifié, à compter de la dernière mise à jour du résultat. Si le statut de conformité de la ressource n'a pas changé lors de la dernière mise à jour, cette valeur est identique à la valeur du `Compliance.Status` champ du résultat. Pour obtenir une liste des valeurs possibles, consultez Évaluation de l'état de conformité et de l'état du contrôle.

`StandardsGuideArn` ou `StandardsArn`

L'ARN de la norme associée au contrôle.

Pour la norme de référence AWS des fondations de la CEI, le champ est`StandardsGuideArn`. En ce qui concerne les normes PCI DSS et les meilleures pratiques de sécurité AWS fondamentales, le domaine est. `StandardsArn`

Ces champs sont supprimés au profit de `Compliance.AssociatedStandards` si vous activez les résultats de contrôle consolidés.

`StandardsGuideSubscriptionArn` ou `StandardsSubscriptionArn`

L'ARN de l'abonnement du compte à la norme.

Pour la norme de référence AWS des fondations de la CEI, le champ est`StandardsGuideSubscriptionArn`. En ce qui concerne les normes PCI

DSS et les meilleures pratiques de sécurité AWS fondamentales, le domaine est. `StandardsSubscriptionArn`

Ces champs sont supprimés si vous activez les résultats de contrôle consolidés.

`RuleId` ou `ControlId`

Identifiant du contrôle.

Pour la version 1.2.0 de la norme CIS AWS Foundations Benchmark, le champ est`RuleId`. Pour les autres normes, y compris les versions ultérieures de la norme de AWS référence de la Fondation CIS, le champ est`ControlId`.

Ces champs sont supprimés au profit de `Compliance.SecurityControlId` si vous activez les résultats de contrôle consolidés.

`RecommendationUrl`

URL contenant les informations de correction pour le contrôle. Ce champ est supprimé au profit de `Remediation.Recommendation.Url` si vous activez les résultats de contrôle consolidés.

`RelatedAWSResources:0/name`

Nom de la ressource associée à la découverte.

`RelatedAWSResource:0/type`

Type de ressource associé au contrôle.

`StandardsControlArn`

L'ARN du contrôle. Ce champ est supprimé si vous activez les résultats de contrôle consolidés.

`aws/securityhub/ProductName`

Pour les résultats de contrôle, le nom du produit est`Security Hub`.

`aws/securityhub/CompanyName`

Pour les résultats de contrôle, le nom de la société est`AWS`.

`aws/securityhub/annotation`

Description du problème découvert par le contrôle.

`aws/securityhub/FindingId`

Identifiant de la recherche.

Ce champ ne fait pas référence à une norme si vous activez les résultats de contrôle consolidés.

Niveaux de gravité des résultats de contrôle

La sévérité attribuée à un contrôle Security Hub CSPM indique l'importance de ce contrôle. La sévérité d'un contrôle détermine le label de gravité attribué aux résultats du contrôle.

Critères de sévérité

La sévérité d'un contrôle est déterminée sur la base d'une évaluation des critères suivants :

- Est-il difficile pour un auteur de menaces de tirer parti de la faiblesse de configuration associée au contrôle ? La difficulté est déterminée par le degré de sophistication ou de complexité requis pour utiliser la faiblesse afin de réaliser un scénario de menace.
- Quelle est la probabilité que cette faiblesse compromette vos ressources Comptes AWS ou celles de vos ressources ? La compromission de vos ressources Comptes AWS ou de vos ressources signifie que la confidentialité, l'intégrité ou la disponibilité de vos données ou de votre AWS infrastructure sont compromises d'une manière ou d'une autre. La probabilité d'une compromission indique la probabilité que le scénario de menace entraîne une interruption ou une violation de vos ressources Services AWS ou de vos ressources.

À titre d'exemple, considérez les faiblesses de configuration suivantes :

- Les clés d'accès des utilisateurs ne sont pas renouvelées tous les 90 jours.
- La clé utilisateur root IAM existe.

Il est tout aussi difficile pour un adversaire de tirer parti de ces deux faiblesses. Dans les deux cas, l'adversaire peut avoir recours au vol d'informations d'identification ou à une autre méthode pour obtenir une clé utilisateur. Ils peuvent ensuite l'utiliser pour accéder à vos ressources de manière non autorisée.

Cependant, le risque de compromission est beaucoup plus élevé si l'auteur de la menace obtient la clé d'accès de l'utilisateur root, car cela lui donne un meilleur accès. Par conséquent, la faiblesse de la clé de l'utilisateur root est plus grave.

La gravité ne tient pas compte de la criticité de la ressource sous-jacente. La criticité est le niveau d'importance des ressources associées à la découverte. Par exemple, une ressource associée à une application critique est plus critique qu'une ressource associée à des tests hors production. Pour saisir des informations sur la criticité des ressources, utilisez le `Criticality` champ du format ASFF (AWSSecurity Finding Format).

Le tableau suivant décrit la difficulté d'exploitation et le risque de compromission des étiquettes de sécurité.

	Compromis très probable	Compromis probable	Compromis peu probable	Compromis très peu probable
Très facile à exploiter	Critique	Critique	Élevée	Moyenne
Assez facile à exploiter	Critique	Élevée	Moyenne	Moyenne
Assez difficile à exploiter	Élevée	Moyenne	Moyenne	Faible
Très difficile à exploiter	Moyenne	Moyenne	Faible	Faible

Définitions de la gravité

Les étiquettes de gravité sont définies comme suit.

Critique — Le problème doit être résolu immédiatement pour éviter qu'il ne s'aggrave.

Par exemple, un compartiment S3 ouvert est considéré comme une résultat dont la gravité est critique. Étant donné que de nombreux acteurs de la menace recherchent des compartiments S3 ouverts, les données contenues dans les compartiments S3 exposés sont susceptibles d'être découvertes et d'être consultées par d'autres personnes.

En général, les ressources accessibles au public sont considérées comme des problèmes de sécurité critiques. Vous devez traiter les résultats critiques avec la plus grande urgence. Vous devez également tenir compte de l’importance de la ressource.

Élevé — Le problème doit être traité en priorité à court terme.

Par exemple, si un groupe de sécurité VPC par défaut est ouvert au trafic entrant et sortant, son niveau de gravité est considéré comme élevé. Il est assez facile pour un auteur de menaces de compromettre un VPC en utilisant cette méthode. Il est également probable que l'auteur de la menace soit en mesure de perturber ou d'exfiltrer les ressources une fois qu'elles se trouvent dans le VPC.

Security Hub CSPM vous recommande de traiter une constatation de gravité élevée comme une priorité à court terme. Vous devez prendre des mesures correctives immédiates. Vous devez également tenir compte de l’importance de la ressource.

Moyen — Le problème devrait être traité en priorité à moyen terme.

Par exemple, l'absence de chiffrement des données en transit est considérée comme une constatation de gravité moyenne. Une attaque sophistiquée de type « man-in-the-middle » est nécessaire pour tirer parti de cette faiblesse. En d'autres termes, c'est un peu difficile. Il est probable que certaines données soient compromises si le scénario de menace est réussi.

Security Hub CSPM vous recommande de rechercher la ressource impliquée dès que possible. Vous devez également tenir compte de l’importance de la ressource.

Faible — Le problème ne nécessite aucune action en soi.

Par exemple, le fait de ne pas recueillir d'informations médico-légales est considéré comme peu grave. Ce contrôle peut aider à prévenir de futurs compromis, mais l'absence de criminalistique ne mène pas directement à un compromis.

Il n’est pas nécessaire de prendre des mesures immédiates en cas de constatation de faible gravité, mais ces résultats peuvent fournir un contexte lorsque vous les mettez en corrélation avec d’autres problèmes.

Information — Aucune faiblesse de configuration n'a été détectée.

En d'autres termes, le statut est `PASSEDWARNING`, ou`NOT AVAILABLE`.

Aucune action spécifique n'est recommandée. Les résultats fournis à titre informatif aident les clients à démontrer qu'ils sont dans un état de conformité.

Évaluation de l'état de conformité et de l'état du contrôle

Le `Compliance.Status` champ du format de recherche de AWS sécurité décrit le résultat d'un résultat de contrôle. AWSSecurity Hub CSPM utilise l'état de conformité des résultats des contrôles pour déterminer un état de contrôle global. L'état du contrôle est affiché sur la page de détails d'un contrôle sur la console Security Hub CSPM.

Évaluation de l'état de conformité des résultats du Security Hub CSPM

L'état de conformité de chaque constatation se voit attribuer l'une des valeurs suivantes :

- PASSED— Indique que le contrôle a réussi le contrôle de sécurité pour le résultat. Cela définit automatiquement le Security Hub CSPM sur. Workflow.Status RESOLVED
- FAILED— Indique que le contrôle n'a pas réussi le contrôle de sécurité pour le résultat.
- WARNING— Indique que Security Hub CSPM ne peut pas déterminer si la ressource est dans un état PASSED ouFAILED. Par exemple, l'enregistrement AWS Config des ressources n'est pas activé pour le type de ressource correspondant.
- NOT_AVAILABLE— Indique que le contrôle ne peut pas être effectué car un serveur est défaillant, la ressource a été supprimée ou le résultat de l'AWS Configévaluation l'a étéNOT_APPLICABLE. Si le résultat de AWS Config l'évaluation est le casNOT_APPLICABLE, Security Hub CSPM archive automatiquement le résultat.

Si le statut de conformité d'une constatation passe de PASSED àFAILED, ou WARNINGNOT_AVAILABLE, et Workflow.Status était l'un NOTIFIED ou l'autreRESOLVED, Security Hub CSPM passe Workflow.Status automatiquement à. NEW

Si vous ne disposez pas de ressources correspondant à un contrôle, Security Hub CSPM produit un PASSED résultat au niveau du compte. Si vous avez une ressource correspondant à un contrôle mais que vous la supprimez ensuite, Security Hub CSPM crée une NOT_AVAILABLE recherche et l'archive immédiatement. Au bout de 18 heures, vous recevez un PASSED résultat car vous ne disposez plus des ressources correspondant au contrôle.

Dérivation du statut de contrôle à partir de l'état de conformité

Security Hub CSPM obtient un statut de contrôle global à partir de l'état de conformité des résultats des contrôles. Lors de la détermination de l'état du contrôle, Security Hub CSPM ignore les résultats contenant un RecordState de ARCHIVED et ceux contenant un de. Workflow.Status SUPPRESSED

L'une des valeurs suivantes est attribuée à l'état du contrôle :

- Réussi — Indique que le statut de conformité de tous les résultats est dePASSED.
- Echec — Indique qu'au moins un résultat a un statut de conformité deFAILED.
- Inconnu — Indique qu'au moins un résultat a un statut de conformité de WARNING ouNOT_AVAILABLE. Aucun résultat n'a un statut de conformité deFAILED.
- Aucune donnée — Indique qu'aucun résultat n'a été trouvé pour le contrôle. Par exemple, un contrôle nouvellement activé possède ce statut jusqu'à ce que Security Hub CSPM commence à

générer des résultats le concernant. Un contrôle possède également ce statut si tous ses résultats sont SUPPRESSED ou ne sont pas disponibles dans le courantRégion AWS.

- Désactivé — Indique que le contrôle est désactivé dans le compte courant et dans la région. Aucun contrôle de sécurité n'est actuellement effectué pour ce contrôle dans le compte courant et dans la région. Cependant, les résultats d'une commande désactivée peuvent avoir une valeur pour l'état de conformité jusqu'à 24 heures après la désactivation.

Pour un compte administrateur, le statut de contrôle reflète l'état de contrôle du compte administrateur et des comptes membres. Plus précisément, le statut général d'un contrôle apparaît comme Échec si le contrôle présente un ou plusieurs échecs trouvés dans le compte administrateur ou dans l'un des comptes membres. Si vous avez défini une région d'agrégation, le statut de contrôle dans la région d'agrégation reflète le statut de contrôle dans la région d'agrégation et les régions associées. Plus précisément, le statut général d'un contrôle apparaît comme Échec si le contrôle présente un ou plusieurs résultats d'échec dans la région d'agrégation ou dans l'une des régions liées.

Security Hub CSPM génère généralement l'état de contrôle initial dans les 30 minutes suivant votre première visite de la page Résumé ou de la page des normes de sécurité de la console Security Hub CSPM. L'enregistrement des AWS Config ressources doit être configuré pour que l'état du contrôle apparaisse. Une fois les statuts de contrôle générés pour la première fois, Security Hub CSPM les met à jour toutes les 24 heures en fonction des résultats des 24 heures précédentes. Un horodatage sur la page des détails du contrôle indique la date à laquelle l'état du contrôle a été mis à jour pour la dernière fois.

> **Note**
>
> Après avoir activé un contrôle pour la première fois, la génération des statuts de contrôle dans les régions de Chine et leAWS GovCloud (US) Region.

Calcul des scores de sécurité

Sur la console AWS Security Hub CSPM, la page Résumé et la page Contrôles affichent un score de sécurité récapitulatif pour toutes les normes que vous avez activées. Sur la page Normes de sécurité, Security Hub CSPM affiche également un score de sécurité compris entre 0 et 100 % pour chaque norme activée.

Lorsque vous activez Security Hub CSPM pour la première fois, Security Hub CSPM calcule le score de sécurité récapitulatif et les scores de sécurité standard dans les 30 minutes suivant votre première visite sur la page Résumé ou Normes de sécurité de la console. Les scores sont générés uniquement pour les standards qui sont activés lorsque vous visitez ces pages sur la console. De plus, l'enregistrement AWS Config des ressources doit être configuré pour que les scores apparaissent. Le score de sécurité récapitulatif est la moyenne des scores de sécurité standard. Pour consulter la liste des normes actuellement activées, vous pouvez utiliser le GetEnabledStandards fonctionnement de l'API CSPM Security Hub.

Après la première génération de scores, Security Hub CSPM met à jour les scores de sécurité toutes les 24 heures. Security Hub CSPM affiche un horodatage pour indiquer la date de dernière mise à jour d'un score de sécurité. Notez que la génération des premiers scores de sécurité peut prendre jusqu'à 24 heures dans les régions chinoises et AWS GovCloud (US) Regions.

Si vous activez les résultats des contrôles consolidés, la mise à jour de vos scores de sécurité peut prendre jusqu'à 24 heures. En outre, l'activation d'une nouvelle région d'agrégation ou la mise à jour des régions liées réinitialise les scores de sécurité existants. Security Hub CSPM peut mettre jusqu'à 24 heures pour générer de nouveaux scores de sécurité incluant les données des régions mises à jour.

Méthode de calcul des scores de sécurité

Les scores de sécurité représentent la proportion de contrôles réussis par rapport aux contrôles activés. Le score est affiché sous forme de pourcentage arrondi au nombre entier le plus proche.

Security Hub CSPM calcule un score de sécurité récapitulatif pour toutes vos normes activées. Security Hub CSPM calcule également un score de sécurité pour chaque norme activée. Aux fins du calcul du score, les contrôles activés incluent les contrôles dont le statut est Réussi, Échec et Inconnu. Les contrôles dont le statut est Aucune donnée sont exclus du calcul du score.

Security Hub CSPM ignore les résultats archivés et supprimés lors du calcul de l'état des contrôles. Cela peut avoir un impact sur les scores de sécurité. Par exemple, si vous supprimez tous les résultats qui ont échoué pour un contrôle, son statut devient Réussi, ce qui peut améliorer vos scores de sécurité. Pour plus d'informations sur l'état des contrôles, consultezÉvaluation de l'état de conformité et de l'état du contrôle.

Exemple de notation :

Standard	Contrôles réussis	Contrôles défaillants	Contrôles inconnus	Note standard
AWS Meilleures pratiques fondamentales en matière de sécurité v1.0.0	168	22	0	88 %
Indice de référence CIS AWS Foundations v1.4.0	8	29	0	22 %
Indice de référence CIS AWS Foundations v1.2.0	6	35	0	15 %
Publication spéciale 800-53 du NIST, révision 5	159	56	0	74 %
PCI DSS v3.2.1	28	17	0	62 %

Lors du calcul du score de sécurité récapitulatif, Security Hub CSPM ne compte chaque contrôle qu'une seule fois pour toutes les normes. Par exemple, si vous avez activé un contrôle qui s'applique à trois normes activées, il ne compte que comme un seul contrôle activé à des fins de notation.

Dans cet exemple, bien que le nombre total de contrôles activés dans l'ensemble des normes activées soit de 528, Security Hub CSPM ne compte chaque contrôle qu'une seule fois à des fins de notation. Le nombre de contrôles uniques activés est probablement inférieur à 528. Si nous supposons que le nombre de contrôles uniques activés est de 515 et que le nombre de contrôles uniques passés est de 357, le score récapitulatif est de 69 %. Ce score est calculé en divisant le nombre de contrôles uniques passés par le nombre de contrôles uniques activés.

Il se peut que votre score récapitulatif diffère du score de sécurité standard, même si vous n'avez activé qu'une seule norme sur votre compte dans la région actuelle. Cela peut se produire si vous êtes connecté à un compte administrateur et que des normes supplémentaires ou différentes normes sont activées sur les comptes membres. Cela peut également se produire si vous consultez le score depuis la région d'agrégation et que des normes supplémentaires ou différentes normes sont activées dans les régions liées.

Scores de sécurité pour les comptes administrateurs

Si vous êtes connecté à un compte administrateur, le score de sécurité récapitulatif et les scores standard tiennent compte des états de contrôle du compte administrateur et de tous les comptes membres.

Si le statut d'un contrôle est Échec, ne serait-ce que pour un seul compte membre, son statut est Échec dans le compte administrateur et a un impact sur les scores du compte administrateur.

Si vous êtes connecté à un compte administrateur et que vous consultez les scores dans une région d'agrégation, les scores de sécurité tiennent compte des statuts de contrôle de tous les comptes membres et de toutes les régions associées.

Scores de sécurité si vous avez défini une région d'agrégation

Si vous avez défini une agrégation Région AWS, le score de sécurité récapitulatif et les scores standard tiennent compte des états de contrôle dans tous les cas
Régions liées.

Si le statut d'un contrôle est Échec, ne serait-ce que dans une seule région liée, son statut est Échec dans la région d'agrégation et a un impact sur les scores de la région d'agrégation.

Si vous êtes connecté à un compte administrateur et que vous consultez les scores dans une région d'agrégation, les scores de sécurité tiennent compte des statuts de contrôle de tous les comptes membres et de toutes les régions associées.

Catégories de contrôle dans Security Hub CSPM

Une catégorie est attribuée à chaque contrôle. La catégorie d'un contrôle reflète la fonction de sécurité à laquelle le contrôle s'applique.

La valeur de la catégorie contient la catégorie, la sous-catégorie au sein de la catégorie et, éventuellement, un classificateur au sein de la sous-catégorie. Par exemple :

- Identifier > Inventaire

- Protection > Protection des données > Chiffrement des données en transit

Voici les descriptions des catégories, sous-catégories et classificateurs disponibles.

Identifier

Élaborer la compréhension organisationnelle pour gérer les risques liés à la cybersécurité pour les systèmes, les actifs, les données et les capacités.

Inventory

Le service a-t-il mis en œuvre les stratégies de balisage des ressources appropriées ? Les stratégies de balisage incluent-elles le propriétaire de la ressource ?

Quelles ressources le service utilise-t-il ? S’agit-il de ressources approuvées pour ce service ?

Disposez-vous d’une visibilité sur le stock approuvé ? Par exemple, utilisez-vous des services tels qu'Amazon EC2 Systems Manager et Service Catalog ?

Logging

Avez-vous activé en toute sécurité toutes les journalisations pertinentes pour le service ? Les exemples de fichiers journaux sont les suivants :

- Journaux de flux Amazon VPC
- Journaux d'accès Elastic Load Balancing
- CloudFront Journaux Amazon
- Amazon CloudWatch Logs
- Journalisation d'Amazon Relational Database Service
- Journaux d'indexation lents d'Amazon OpenSearch Service
- X-Ray traçage
- AWS Directory Servicejournaux
- AWS Configarticles
- Instantanés

Protection

Élaborer et mettre en œuvre les mesures de protection appropriées pour assurer la prestation des services d'infrastructure essentiels et des pratiques de codage sécurisées.

Gestion sécurisée des accès

- Le service applique-t-il les pratiques du moindre privilège dans ses politiques IAM ou de ressources ?
- Les mots de passe et les secrets sont-ils suffisamment complexes ? La rotation est-elle réalisée de façon appropriée ?
- Le service utilise-t-il l'authentification à plusieurs facteurs (MFA) ?
- Le service évite-t-il l'utilisateur root ?
- Les stratégies basées sur les ressources permet-elles l'accès du public ?

Configuration réseau sécurisée

- Le service empêche-t-il l'accès au réseau distant public et non sécurisé ?
- Le service utilise-t-il correctement les VPC ? Par exemple, des tâches doivent-elles s'exécuter dans des VPC ?
- Le service segmente-t-il et isole-t-il correctement les ressources sensibles ?

Protection des données

- Chiffrement des données au repos : le service crypte-t-il les données au repos ?
- Chiffrement des données en transit : le service crypte-t-il les données en transit ?
- Intégrité des données : le service valide-t-il l'intégrité des données ?
- Protection contre la suppression des données : le service protège-t-il les données contre toute suppression accidentelle ?
- Gestion et utilisation des données — Utilisez-vous des services tels qu'Amazon Macie pour suivre l'emplacement de vos données sensibles ?

Protection des API

- Le service utilise-t-il AWS PrivateLink pour protéger les opérations de l'API du service ?

Services de protection

- Les services de protection appropriés sont-ils en installés ? Fournissent-ils la couverture appropriée ?

Les services de protection vous aident à détourner les attaques et les compromissions qui sont dirigées vers le service. Les exemples de services de protection AWS incluentAWS Control Tower,, AWS WAFAWS Shield Advanced, Vanta, Secrets Manager, IAM Access Analyzer et. AWS Resource Access Manager

Développement sécurisé

Utilisez-vous des pratiques de codage sécurisées ?

Évitez-vous des vulnérabilités telles que le Top 10 du projet OWASP (Open Web Application Security Project) ?

Détection

Élaborer et mettre en œuvre les activités appropriées pour identifier la survenance d'un événement de cybersécurité.

Services de détection

Les services de détection appropriés sont-ils en place ?

Fournissent-ils la couverture appropriée ?

Les exemples de services de AWS détection incluent Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector, Amazon DetectiveAWS IoT Device Defender, Amazon CloudWatch Alarms et. AWS Trusted Advisor

Réponse

Élaborer et mettre en œuvre les activités appropriées pour prendre des mesures concernant un événement de cybersécurité détecté.

Actions de réponse

Répondez-vous rapidement aux événements de sécurité ?

Avez-vous des résultats critiques actifs ou de gravité élevée ?

Analyse scientifique

Pouvez-vous acquérir en toute sécurité des données d'analyse scientifique pour le service ? Par exemple, obtenez-vous des instantanés Amazon EBS associés à de véritables résultats positifs ?

Avez-vous créé un compte d'analyse scientifique ?

Récupération

Élaborer et mettre en œuvre les activités appropriées pour maintenir des plans de résilience et rétablir les capacités ou les services qui ont été compromis en raison d'un événement de cybersécurité.

Résilience

La configuration du service prend-elle en charge les basculements gracieux, la mise à l'échelle élastique et la haute disponibilité ?

Avez-vous établi des sauvegardes ?

Examiner les détails des contrôles dans Security Hub CSPM

La sélection d'un contrôle sur la page Contrôles ou la page de détails standard de la console Security Hub CSPM vous amène à une page contenant les détails du contrôle.

Le haut de la page des détails du contrôle indique l'état du contrôle. L'état du contrôle résume la performance d'un contrôle en fonction de l'état de conformité des résultats du contrôle. Security Hub CSPM génère généralement l'état de contrôle initial dans les 30 minutes suivant votre première visite sur la page de résumé ou sur la page des normes de sécurité de la console Security Hub CSPM. Les statuts ne sont disponibles que pour les contrôles qui sont activés lorsque vous visitez ces pages.

La page des détails des contrôles fournit également une ventilation de l'état de conformité des résultats des contrôles au cours des dernières 24 heures. Pour plus d'informations sur l'état des contrôles et l'état de conformité, consultezÉvaluation de l'état de conformité et de l'état du contrôle.

AWS Config l'enregistrement des ressources doit être configuré pour que l'état du contrôle apparaisse. Une fois les états de contrôle générés pour la première fois, Security Hub CSPM met à jour l'état des contrôles toutes les 24 heures en fonction des résultats des 24 heures précédentes.

Les comptes administrateur affichent un état de contrôle agrégé pour le compte administrateur et les comptes membres. Si vous avez défini une région d'agrégation, l'état du contrôle inclut les résultats de toutes les régions liées. Pour plus d'informations sur l'état des contrôles, consultezthe section called "État de conformité et statut de contrôle".

Vous pouvez également activer ou désactiver le contrôle depuis la page des détails du contrôle.

> **Note**
>
> Cela peut prendre jusqu'à 24 heures après l'activation d'un contrôle pour la génération des premiers statuts de contrôle dans les régions chinoises et. AWS GovCloud (US) Regions

L'onglet Normes et exigences répertorie les normes pour lesquelles un contrôle peut être activé et les exigences liées au contrôle issues de différents cadres de conformité.

L'onglet Vérifications répertorie les résultats actifs du contrôle au cours des dernières 24 heures. Les résultats des contrôles sont générés et mis à jour lorsque Security Hub CSPM effectue des contrôles de sécurité pour le contrôle. La liste de cet onglet n'inclut pas les résultats archivés.

Pour chaque découverte, la liste donne accès à des détails tels que l'état de conformité et les ressources associées. Vous pouvez également définir l'état du flux de travail pour chaque découverte et envoyer les résultats à des actions personnalisées. Pour de plus amples informations, veuillez consulter Examen et gestion des résultats des contrôles.

Affichage des détails d'un contrôle

Choisissez votre méthode d'accès préférée et suivez ces étapes pour consulter les détails d'un contrôle. Les détails s'appliquent au compte courant et à la région et incluent les suivants :

- Titre et description du contrôle.
- Lien vers les directives de remédiation en cas d'échec des contrôles.
- La sévérité du contrôle.
- État de la commande.

Sur la console, vous pouvez également consulter la liste des résultats récents concernant le contrôle. Pour ce faire par programmation, vous pouvez utiliser le GetFindings fonctionnement de l'API CSPM Security Hub.

Security Hub CSPM console

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

2. Choisissez Controls dans le volet de navigation.
3. Sélectionnez un contrôle.

Security Hub CSPM API

1. Exécutez `ListSecurityControlDefinitions` et fournissez un ou plusieurs ARN standard pour obtenir une liste des ID de contrôle pour cette norme. Pour obtenir des ARN standard, exécutez `DescribeStandards`. Si vous ne fournissez pas d'ARN standard, cette API renvoie tous les ID de contrôle CSPM de Security Hub. Cette API renvoie des identifiants de contrôle de sécurité indépendants des normes, et non les ID de contrôle standard qui existaient avant ces versions de fonctionnalités.

   Exemple de demande :

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Exécutez `BatchGetSecurityControls` pour obtenir des détails sur une ou plusieurs commandes du Compte AWS et en cours Région AWS.

   Exemple de demande :

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Exécutez la `list-security-control-definitions` commande et fournissez un ou plusieurs ARN standard pour obtenir une liste des ID de contrôle. Pour obtenir des ARN standard, exécutez la `describe-standards` commande. Si vous ne fournissez pas d'ARN standard, cette commande renvoie tous les ID de contrôle CSPM de Security Hub. Cette commande renvoie des ID de contrôle de sécurité indépendants des normes, et non les ID de contrôle standard qui existaient avant ces versions de fonctionnalités.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Exécutez la batch-get-security-controls commande pour obtenir des détails sur une ou plusieurs commandes du Compte AWS et en cours Région AWS.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Contrôles de filtrage et de tri dans Security Hub CSPM

Sur la console AWS Security Hub CSPM, vous pouvez utiliser la page Contrôles pour consulter un tableau des contrôles actuellement disponibles. Région AWS L'exception est une région d'agrégation. Si vous avez configuré une région d'agrégation et que vous vous connectez à cette région, la console affiche les commandes disponibles dans la région d'agrégation ou dans une ou plusieurs régions liées.

Pour vous concentrer sur un sous-ensemble de contrôles spécifique, vous pouvez trier et filtrer le tableau des contrôles. Les options Filtrer par situées à côté du tableau peuvent vous aider à vous concentrer rapidement sur ces sous-ensembles spécifiques :

- Tous les contrôles activés, qui sont des contrôles qui sont activés dans au moins une norme activée.
- Toutes les commandes désactivées, qui sont des commandes désactivées dans toutes les normes.
- Toutes les commandes activées qui ont un statut de contrôle spécifique, tel que Échec. L'option Aucune donnée affiche uniquement les contrôles qui ne contiennent actuellement aucun résultat. Pour plus d'informations sur l'état des contrôles, consultezÉvaluation de l'état de conformité et de l'état du contrôle.

Outre les options Filtrer par, vous pouvez filtrer le tableau en saisissant des critères de filtre dans la zone de contrôle du filtre située au-dessus du tableau. Par exemple, vous pouvez filtrer par ID de contrôle ou par niveau de gravité.

Par défaut, les contrôles dont le statut a échoué sont répertoriés en premier, par ordre décroissant de gravité. Vous pouvez modifier l'ordre de tri en choisissant un autre titre de colonne.

> **Tip**
>
> Si vous avez des flux de travail automatisés basés sur les résultats des contrôles, nous vous recommandons d'utiliser les champs `SecurityControlId` ou `SecurityControlArn` ASFF comme filtres, plutôt que les `Description` champs `Title` ou. Ces derniers champs peuvent être modifiés occasionnellement, alors que l'ID de contrôle et l'ARN sont des identifiants statiques.

Si vous êtes connecté à un compte administrateur CSPM de Security Hub, les contrôles activés incluent les contrôles qui sont activés dans au moins un compte membre. Si vous avez configuré une région d'agrégation, les contrôles activés incluent les contrôles qui sont activés dans au moins une région liée.

Si vous sélectionnez l'option à côté d'un contrôle activé, un panneau apparaît et affiche les normes dans lesquelles le contrôle est actuellement activé. Vous pouvez également voir les normes dans lesquelles le contrôle est actuellement désactivé. À partir de ce panneau, vous pouvez désactiver un contrôle dans toutes les normes. Pour de plus amples informations, veuillez consulter Désactivation des contrôles dans Security Hub CSPM. Pour les comptes d'administrateur, les informations du panneau reflètent les paramètres de tous vos comptes de membres.

Pour récupérer une liste de contrôles par programmation, vous pouvez utiliser le ListSecurityControlDefinitions fonctionnement de l'API CSPM Security Hub. Pour récupérer les détails des commandes individuelles, utilisez l'BatchGetSecurityControlsopération.

Comprendre les paramètres de contrôle dans Security Hub CSPM

Certains contrôles de AWS Security Hub CSPM utilisent des paramètres qui influent sur la manière dont le contrôle est évalué. Généralement, ces contrôles sont évalués par rapport aux valeurs de paramètres par défaut définies par Security Hub CSPM. Cependant, pour un sous-ensemble de ces contrôles, vous pouvez modifier les valeurs des paramètres. Lorsque vous modifiez la valeur d'un paramètre de contrôle, Security Hub CSPM commence à évaluer le contrôle par rapport à la valeur que vous spécifiez. Si la ressource sous-jacente au contrôle satisfait la valeur personnalisée, Security Hub CSPM génère un résultat. `PASSED` Si la ressource ne correspond pas à la valeur personnalisée, Security Hub CSPM génère un `FAILED` résultat.

En personnalisant les paramètres de contrôle, vous pouvez affiner les meilleures pratiques de sécurité recommandées et surveillées par Security Hub CSPM afin de les aligner sur les exigences

de votre entreprise et vos attentes en matière de sécurité. Au lieu de supprimer les résultats d'un contrôle, vous pouvez personnaliser un ou plusieurs de ses paramètres pour obtenir des résultats qui répondent à vos besoins de sécurité.

Voici quelques exemples de cas d'utilisation pour modifier les paramètres de contrôle et définir des valeurs personnalisées :

- [CloudWatch.16] — les groupes de CloudWatch journaux doivent être conservés pendant une période spécifiée

  Vous pouvez spécifier la durée de conservation.
- [IAM.7] — Les politiques de mots de passe pour les utilisateurs IAM doivent être configurées de manière robuste

  Vous pouvez spécifier des paramètres relatifs à la sécurité du mot de passe.
- [EC2.18] — Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés

  Vous pouvez spécifier quels ports sont autorisés à autoriser le trafic entrant sans restriction.
- [Lambda.5] — Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité

  Vous pouvez spécifier le nombre minimum de zones de disponibilité qui produisent un résultat positif.

Cette section décrit les éléments à prendre en compte lorsque vous modifiez des paramètres de contrôle.

Effet de la modification des valeurs des paramètres de contrôle

Lorsque vous modifiez la valeur d'un paramètre, vous déclenchez également un nouveau contrôle de sécurité qui évalue le contrôle en fonction de la nouvelle valeur. Security Hub CSPM génère ensuite de nouveaux résultats de contrôle en fonction de la nouvelle valeur. Lors des mises à jour périodiques des résultats des contrôles, Security Hub CSPM utilise également la nouvelle valeur de paramètre. Si vous modifiez les valeurs des paramètres d'un contrôle, mais que vous n'avez activé aucune norme incluant ce contrôle, Security Hub CSPM n'effectue aucun contrôle de sécurité à l'aide des nouvelles valeurs. Vous devez activer au moins une norme pertinente pour Security Hub CSPM afin d'évaluer le contrôle en fonction de la nouvelle valeur du paramètre.

Un contrôle peut comporter un ou plusieurs paramètres personnalisables. Les types de données possibles pour chaque paramètre de contrôle sont les suivants :

- Booléen
- Double
- Enum
- EnumList
- Entier
- IntegerList
- Chaîne
- StringList

Les valeurs de paramètres personnalisées s'appliquent à toutes les normes que vous avez activées. Vous ne pouvez pas personnaliser les paramètres d'un contrôle qui n'est pas pris en charge dans votre région actuelle. Pour une liste des limites régionales pour les contrôles individuels, consultezLimites régionales des contrôles CSPM du Security Hub.

Pour certains contrôles, les valeurs de paramètres acceptables doivent se situer dans une plage spécifiée pour être valides. Dans ces cas, Security Hub CSPM fournit la plage acceptable.

Security Hub CSPM choisit les valeurs de paramètres par défaut et peut parfois les mettre à jour. Une fois que vous avez personnalisé un paramètre de contrôle, sa valeur reste celle que vous avez spécifiée pour le paramètre, sauf si vous la modifiez. En d'autres termes, le paramètre arrête le suivi des mises à jour de la valeur CSPM par défaut de Security Hub, même si la valeur personnalisée du paramètre correspond à la valeur par défaut actuelle définie par Security Hub CSPM. Voici un exemple pour le contrôle [ACM.1] — ACM-issued Les certificats importés doivent être renouvelés après une période spécifiée :

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
```

```
    }
}
```

Dans l'exemple précédent, le `daysToExpiration` paramètre a une valeur personnalisée de`30`. La valeur par défaut actuelle pour ce paramètre est également`30`. Si Security Hub CSPM change la valeur par défaut en`14`, le paramètre de cet exemple ne suivra pas cette modification. Il conservera une valeur de`30`.

Si vous souhaitez suivre les mises à jour de la valeur CSPM par défaut de Security Hub pour un paramètre, définissez le `ValueType` champ sur `DEFAULT` plutôt que. `CUSTOM` Pour de plus amples informations, veuillez consulter Revenir aux paramètres de contrôle par défaut dans un seul compte et une seule région.

Contrôles prenant en charge les paramètres personnalisés

Pour obtenir la liste des contrôles de sécurité qui prennent en charge les paramètres personnalisés, consultez la page Contrôles de la console Security Hub CSPM ou le. Référence de contrôle pour Security Hub CSPM Pour récupérer cette liste par programmation, vous pouvez utiliser l'ListSecurityControlDefinitionsopération. Dans la réponse, l'`CustomizableProperties`objet indique quelles commandes prennent en charge les paramètres personnalisables.

Révision des valeurs actuelles des paramètres de contrôle

Il peut être utile de connaître la valeur actuelle d'un paramètre de contrôle avant de le modifier.

Vous pouvez consulter les valeurs actuelles des différents paramètres de contrôle dans votre compte. Si vous utilisez la configuration centralisée, l'administrateur CSPM délégué de AWS Security Hub peut également consulter les valeurs des paramètres spécifiées dans une politique de configuration.

Choisissez votre méthode préférée et suivez les étapes pour vérifier les valeurs actuelles des paramètres de contrôle.

Security Hub CSPM console

Pour consulter les valeurs actuelles des paramètres de contrôle (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Controls. Choisissez une commande.

3. Sélectionnez l'onglet Paramètres. Cet onglet affiche les valeurs des paramètres actuels du contrôle.

Security Hub CSPM API

Pour consulter les valeurs actuelles des paramètres de contrôle (API)

Invoquez l'BatchGetSecurityControlsAPI et fournissez un ou plusieurs ID de contrôle de sécurité ou ARN. L'`Parameters`objet de la réponse indique les valeurs de paramètres actuelles pour les contrôles spécifiés.

Par exemple, la AWS CLI commande suivante affiche les valeurs de paramètres actuelles pour `APIGatway.1`, `CloudWatch.15`, et`IAM.7`. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Choisissez votre méthode préférée pour afficher les valeurs de paramètres actuelles dans une politique de configuration centralisée.

Security Hub CSPM console

Pour consulter les valeurs actuelles des paramètres de contrôle dans une politique de configuration (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Connectez-vous à l'aide des informations d'identification du compte administrateur CSPM délégué de Security Hub dans la région d'origine.
2. Dans le volet de navigation, choisissez Paramètres et configuration.
3. Dans l'onglet Politiques, sélectionnez la politique de configuration, puis choisissez Afficher les détails. Les détails de la politique apparaissent alors, y compris les valeurs des paramètres actuels.

Security Hub CSPM API

Pour consulter les valeurs actuelles des paramètres de contrôle dans une politique de configuration (API)

1. Appelez l'GetConfigurationPolicyAPI depuis le compte administrateur délégué de la région d'origine.
2. Indiquez l'ARN ou l'ID de la politique de configuration dont vous souhaitez voir les détails. La réponse inclut les valeurs de paramètres actuelles.

Par exemple, la AWS CLI commande suivante récupère les valeurs actuelles des paramètres de contrôle dans la politique de configuration spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Les résultats de contrôle incluent également les valeurs actuelles des paramètres de contrôle. Dans leAWS Format de recherche de sécurité (ASFF), ces valeurs apparaissent dans le `Parameters` champ de l'`Compliance`objet. Pour consulter les résultats sur la console Security Hub CSPM, choisissez Findings dans le volet de navigation. Pour examiner les résultats par programmation, utilisez le GetFindings fonctionnement de l'API Security Hub CSPM.

Personnalisation des valeurs des paramètres de contrôle

Les instructions de personnalisation des paramètres de contrôle varient selon que vous utilisez ou non la configuration centralisée dans AWS Security Hub CSPM. La configuration centrale est une fonctionnalité que l'administrateur délégué de Security Hub CSPM peut utiliser pour configurer les fonctionnalités CSPM de Security Hub entre Régions AWS les comptes et les unités organisationnelles (UO).

Si votre organisation utilise une configuration centralisée, l'administrateur délégué peut créer des politiques de configuration qui incluent des paramètres de contrôle personnalisés. Ces politiques

peuvent être associées à des comptes membres et à des unités d'organisation gérés de manière centralisée, et elles prennent effet dans votre région d'origine et dans toutes les régions associées. L'administrateur délégué peut également désigner un ou plusieurs comptes comme étant autogérés, ce qui permet au propriétaire du compte de configurer ses propres paramètres séparément dans chaque région. Si votre organisation n'utilise pas la configuration centralisée, vous devez personnaliser les paramètres de contrôle séparément pour chaque compte et chaque région.

Nous vous recommandons d'utiliser la configuration centralisée car elle vous permet d'aligner les valeurs des paramètres de contrôle dans les différentes parties de votre organisation. Par exemple, tous vos comptes de test peuvent utiliser certaines valeurs de paramètres et tous les comptes de production peuvent utiliser des valeurs différentes.

Personnalisation des paramètres de contrôle dans plusieurs comptes et régions

Si vous êtes l'administrateur CSPM délégué de Security Hub pour une organisation qui utilise la configuration centralisée, choisissez votre méthode préférée et suivez les étapes pour personnaliser les paramètres de contrôle sur plusieurs comptes et régions.

Security Hub CSPM console

Pour personnaliser les valeurs des paramètres de contrôle dans plusieurs comptes et régions (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

   Assurez-vous d'être connecté à la région d'origine.
2. Dans le volet de navigation, choisissez Paramètres et configuration.
3. Choisissez l'onglet Politiques.
4. Pour créer une nouvelle politique de configuration incluant des paramètres personnalisés, choisissez Créer une politique. Pour spécifier des paramètres personnalisés dans une politique de configuration existante, sélectionnez la politique, puis choisissez Modifier.

   Pour créer une nouvelle politique de configuration avec des valeurs de paramètres de contrôle personnalisées

   1. Dans la section Politique personnalisée, choisissez les normes et contrôles de sécurité que vous souhaitez activer.
   2. Sélectionnez Personnaliser les paramètres de contrôle.

3. Sélectionnez un contrôle, puis spécifiez des valeurs personnalisées pour un ou plusieurs paramètres.
4. Pour personnaliser les paramètres d'un plus grand nombre de contrôles, choisissez Personnaliser le contrôle supplémentaire.
5. Dans la section Comptes, sélectionnez les comptes ou les unités d'organisation auxquels vous souhaitez appliquer la politique.
6. Choisissez Suivant.
7. Choisissez Créer une politique et appliquer. Dans votre région d'origine et dans toutes les régions liées, cette action remplace les paramètres de configuration existants des comptes et des unités d'organisation associés à cette politique de configuration. Les comptes et les unités d'organisation peuvent être associés à une politique de configuration par le biais d'une application directe ou d'un héritage auprès d'un parent.

Pour personnaliser les valeurs des paramètres de contrôle dans une politique de configuration existante

1. Dans la section Contrôles, sous Politique personnalisée, spécifiez les nouvelles valeurs de paramètres personnalisés que vous souhaitez.
2. Si c'est la première fois que vous personnalisez les paramètres de contrôle dans cette politique, sélectionnez Personnaliser les paramètres de contrôle, puis sélectionnez un contrôle à personnaliser. Pour personnaliser les paramètres d'un plus grand nombre de contrôles, choisissez Personnaliser le contrôle supplémentaire.
3. Dans la section Comptes, vérifiez les comptes ou les unités d'organisation auxquels vous souhaitez appliquer la politique.
4. Choisissez Suivant.
5. Passez en revue vos modifications et vérifiez qu'elles sont correctes. Lorsque vous avez terminé, choisissez Enregistrer la politique et appliquez. Dans votre région d'origine et dans toutes les régions liées, cette action remplace les paramètres de configuration existants des comptes et des unités d'organisation associés à cette politique de configuration. Les comptes et les unités d'organisation peuvent être associés à une politique de configuration par le biais d'une application directe ou d'un héritage auprès d'un parent.

Security Hub CSPM API

Pour personnaliser les valeurs des paramètres de contrôle dans plusieurs comptes et régions (API)

Pour créer une nouvelle politique de configuration avec des valeurs de paramètres de contrôle personnalisées

1. Appelez l'CreateConfigurationPolicyAPI depuis le compte d'administrateur délégué dans la région d'origine.
2. Pour l'`SecurityControlCustomParameters`objet, indiquez l'identifiant de chaque contrôle que vous souhaitez personnaliser.
3. Pour l'`Parameters`objet, indiquez le nom de chaque paramètre que vous souhaitez personnaliser. Pour chaque paramètre que vous personnalisez, `CUSTOM` indiquez`ValueType`. Pour`Value`, indiquez le type de données du paramètre et la valeur personnalisée. Le `Value` champ ne peut pas être vide quand `ValueType` c'est le cas`CUSTOM`. Si votre demande omet un paramètre pris en charge par le contrôle, ce paramètre conserve sa valeur actuelle. Vous pouvez trouver les paramètres, les types de données et les valeurs valides pris en charge pour un contrôle en appelant l'GetSecurityControlDefinitionAPI.

Pour personnaliser les valeurs des paramètres de contrôle dans une politique de configuration existante

1. Appelez l'UpdateConfigurationPolicyAPI depuis le compte d'administrateur délégué dans la région d'origine.
2. Pour le `Identifier` champ, indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique de configuration que vous souhaitez mettre à jour.
3. Pour l'`SecurityControlCustomParameters`objet, indiquez l'identifiant de chaque contrôle que vous souhaitez personnaliser.
4. Pour l'`Parameters`objet, indiquez le nom de chaque paramètre que vous souhaitez personnaliser. Pour chaque paramètre que vous personnalisez, `CUSTOM` indiquez`ValueType`. Pour`Value`, indiquez le type de données du paramètre et la valeur personnalisée. Si votre demande omet un paramètre pris en charge par le contrôle, ce paramètre conserve sa valeur actuelle. Vous pouvez trouver les paramètres, les types de données et les valeurs valides pris en charge pour un contrôle en appelant l'GetSecurityControlDefinitionAPI.

Par exemple, la AWS CLI commande suivante crée une nouvelle politique de configuration avec une valeur personnalisée pour le `daysToExpiration` paramètre de`ACM.1`. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Personnalisation des paramètres de contrôle dans un compte et une région uniques

Si vous n'utilisez pas la configuration centralisée ou si vous possédez un compte autogéré, vous pouvez personnaliser les paramètres de contrôle de votre compte dans une seule région à la fois.

Choisissez votre méthode préférée et suivez les étapes pour personnaliser les paramètres de contrôle. Vos modifications s'appliquent uniquement à votre compte dans la région actuelle. Pour personnaliser les paramètres de contrôle dans d'autres régions, répétez les étapes suivantes pour chaque compte et chaque région supplémentaires dans lesquels vous souhaitez personnaliser les paramètres. Le même contrôle peut utiliser différentes valeurs de paramètres dans différentes régions.

Security Hub CSPM console

Pour personnaliser les valeurs des paramètres de contrôle dans un compte et une région (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Controls. Dans le tableau, choisissez un contrôle qui prend en charge les paramètres personnalisés pour lesquels vous souhaitez modifier

les paramètres. La colonne Paramètres personnalisés indique quels contrôles prennent en charge les paramètres personnalisés.

3. Sur la page de détails du contrôle, choisissez l'onglet Paramètres, puis sélectionnez Modifier.
4. Spécifiez les valeurs de paramètres souhaitées.
5. Si vous le souhaitez, dans la section Motif du changement, sélectionnez la raison pour laquelle vous souhaitez personnaliser les paramètres.
6. Choisissez Enregistrer.

Security Hub CSPM API

Pour personnaliser les valeurs des paramètres de contrôle dans un compte et une région (API)

1. Invoquez l'UpdateSecurityControlAPI.
2. Pour`SecurityControlId`, indiquez l'ID du contrôle que vous souhaitez personnaliser.
3. Pour l'`Parameters`objet, indiquez le nom de chaque paramètre que vous souhaitez personnaliser. Pour chaque paramètre que vous personnalisez, `CUSTOM` indiquez`ValueType`. Pour`Value`, indiquez le type de données du paramètre et la valeur personnalisée. Si votre demande omet un paramètre pris en charge par le contrôle, ce paramètre conserve sa valeur actuelle. Vous pouvez trouver les paramètres, les types de données et les valeurs valides pris en charge pour un contrôle en appelant l'GetSecurityControlDefinitionAPI.
4. Facultativement, pour`LastUpdateReason`, indiquez la raison de la personnalisation des paramètres de contrôle.

Par exemple, la AWS CLI commande suivante définit une valeur personnalisée pour le `daysToExpiration` paramètre de`ACM.1`. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Revenir aux valeurs des paramètres de contrôle par défaut

Un paramètre de contrôle peut avoir une valeur par défaut définie par AWS Security Hub CSPM. Security Hub CSPM met parfois à jour la valeur par défaut d'un paramètre afin de refléter l'évolution des meilleures pratiques de sécurité. Si vous n'avez pas spécifié de valeur personnalisée pour un paramètre de contrôle, le contrôle suit automatiquement ces mises à jour et utilise la nouvelle valeur par défaut.

Vous pouvez revenir à l'utilisation des valeurs de paramètres par défaut pour un contrôle. Les instructions de retour varient selon que vous utilisez ou non la configuration centralisée dans Security Hub CSPM. La configuration centrale est une fonctionnalité que l'administrateur délégué de Security Hub CSPM peut utiliser pour configurer les fonctionnalités CSPM de Security Hub entre Régions AWS les comptes et les unités organisationnelles (UO).

> **Note**
>
> Tous les paramètres de contrôle n'ont pas de valeur CSPM par défaut pour Security Hub. Dans de tels cas, when `ValueType` est défini sur`DEFAULT`, il n'existe pas de valeur par défaut spécifique utilisée par Security Hub CSPM. Security Hub CSPM ignore plutôt le paramètre en l'absence de valeur personnalisée.

Revenir aux paramètres de contrôle par défaut dans plusieurs comptes et régions

Si vous utilisez la configuration centralisée, vous pouvez rétablir les paramètres de contrôle de plusieurs comptes et unités d'organisation gérés de manière centralisée dans la région d'origine et les régions associées.

Choisissez votre méthode préférée et suivez les étapes pour revenir aux valeurs de paramètres par défaut pour plusieurs comptes et régions à l'aide d'une configuration centralisée.

Security Hub CSPM console

Pour revenir aux valeurs des paramètres de contrôle par défaut dans plusieurs comptes et régions (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

Connectez-vous à l'aide des informations d'identification du compte administrateur CSPM délégué de Security Hub dans la région d'origine.

2. Dans le volet de navigation, choisissez Paramètres et configuration.
3. Choisissez l'onglet Politiques.
4. Sélectionnez une politique, puis choisissez Modifier.
5. Sous Politique personnalisée, la section Contrôles affiche la liste des contrôles pour lesquels vous avez spécifié des paramètres personnalisés.
6. Trouvez le contrôle qui possède une ou plusieurs valeurs de paramètres à rétablir. Choisissez ensuite Supprimer pour revenir aux valeurs par défaut.
7. Dans la section Comptes, vérifiez les comptes ou les unités d'organisation auxquels vous souhaitez appliquer la politique.
8. Choisissez Suivant.
9. Passez en revue vos modifications et vérifiez qu'elles sont correctes. Lorsque vous avez terminé, choisissez Enregistrer la politique et appliquez. Dans votre région d'origine et dans toutes les régions liées, cette action remplace les paramètres de configuration existants des comptes et des unités d'organisation associés à cette politique de configuration. Les comptes et les unités d'organisation peuvent être associés à une politique de configuration par le biais d'une application directe ou d'un héritage auprès d'un parent.

Security Hub CSPM API

Pour revenir aux valeurs des paramètres de contrôle par défaut dans plusieurs comptes et régions (API)

1. Appelez l'UpdateConfigurationPolicyAPI depuis le compte d'administrateur délégué dans la région d'origine.
2. Pour le `Identifier` champ, indiquez le nom de ressource Amazon (ARN) ou l'ID de la politique que vous souhaitez mettre à jour.
3. Pour l'`SecurityControlCustomParameters`objet, indiquez l'identifiant de chaque contrôle pour lequel vous souhaitez rétablir un ou plusieurs paramètres.
4. Dans l'`Parameters`objet, pour chaque paramètre que vous souhaitez rétablir, indiquez `DEFAULT` le `ValueType` champ. Quand `ValueType` est défini sur`DEFAULT`, vous n'avez pas besoin de fournir de valeur pour le `Value` champ. Si une valeur est incluse dans votre

demande, Security Hub CSPM l'ignore. Si votre demande omet un paramètre pris en charge par le contrôle, ce paramètre conserve sa valeur actuelle.

> **Warning**
>
> Si vous omettez un objet de contrôle `SecurityControlCustomParameters` dans le champ, Security Hub CSPM rétablit les valeurs par défaut de tous les paramètres personnalisés du contrôle. Une liste complètement vide permet de `SecurityControlCustomParameters` rétablir les valeurs par défaut des paramètres personnalisés de tous les contrôles.

Par exemple, la AWS CLI commande suivante rétablit la valeur par défaut du paramètre de `daysToExpiration` contrôle `ACM.1` pour dans la politique de configuration spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

Revenir aux paramètres de contrôle par défaut dans un seul compte et une seule région

Si vous n'utilisez pas la configuration centralisée ou si vous possédez un compte autogéré, vous pouvez revenir à l'utilisation des valeurs de paramètres par défaut pour votre compte dans une région à la fois.

Choisissez votre méthode préférée et suivez les étapes pour revenir aux valeurs de paramètres par défaut pour votre compte dans une seule région. Pour revenir aux valeurs de paramètres par défaut dans des régions supplémentaires, répétez ces étapes dans chaque région supplémentaire.

> **Note**
>
> Si vous désactivez Security Hub CSPM, vos paramètres de contrôle personnalisés sont réinitialisés. Si vous réactivez Security Hub CSPM ultérieurement, tous les contrôles utiliseront les valeurs de paramètres par défaut pour démarrer.

Security Hub CSPM console

Pour revenir aux valeurs des paramètres de contrôle par défaut dans un compte et une région (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Controls. Choisissez le contrôle pour lequel vous souhaitez rétablir les valeurs de paramètres par défaut.
3. `Parameters`Dans l'onglet, choisissez Personnalisé à côté d'un paramètre de contrôle. Choisissez ensuite Supprimer la personnalisation. Ce paramètre utilise désormais la valeur CSPM par défaut de Security Hub et suit les futures mises à jour à cette valeur.
4. Répétez l'étape précédente pour chaque valeur de paramètre que vous souhaitez rétablir.

Security Hub CSPM API

Pour revenir aux valeurs des paramètres de contrôle par défaut dans un compte et une région (API)

1. Invoquez l'UpdateSecurityControlAPI.
2. Pour`SecurityControlId`, indiquez l'ARN ou l'ID du contrôle dont vous souhaitez rétablir les paramètres.
3. Dans l'`Parameters`objet, pour chaque paramètre que vous souhaitez rétablir, indiquez `DEFAULT` le `ValueType` champ. Quand `ValueType` est défini sur`DEFAULT`, vous n'avez pas besoin de fournir de valeur pour le `Value` champ. Si une valeur est incluse dans votre demande, Security Hub CSPM l'ignore.

4. Facultativement, pour`LastUpdateReason`, indiquez la raison pour laquelle vous revenez aux valeurs de paramètres par défaut.

Par exemple, la AWS CLI commande suivante rétablit la valeur par défaut du paramètre `ACM.1` de `daysToExpiration` contrôle pour. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Vérification de l'état des modifications des paramètres de contrôle

Lorsque vous tentez de personnaliser un paramètre de contrôle ou de revenir à la valeur par défaut, vous pouvez vérifier si les modifications souhaitées ont été efficaces. Cela permet de garantir qu'un contrôle fonctionne comme prévu et fournit la valeur de sécurité souhaitée. Si la mise à jour d'un paramètre échoue, Security Hub CSPM conserve la valeur actuelle du paramètre.

Pour vérifier qu'une mise à jour des paramètres a été effectuée avec succès, vous pouvez consulter les détails du contrôle sur la console Security Hub CSPM. Sur la console, choisissez Controls dans le volet de navigation. Choisissez ensuite un contrôle pour afficher ses détails. L'onglet Paramètres indique l'état de la modification des paramètres.

Par programmation, si votre demande de mise à jour d'un paramètre est valide, la valeur du `UpdateStatus` champ est `UPDATING` une réponse à l'BatchGetSecurityControlsopération. Cela signifie que la mise à jour était valide, mais que tous les résultats n'incluent peut-être pas encore les valeurs de paramètres mises à jour. Lorsque la valeur de `UpdateState` passe à`READY`, Security Hub CSPM utilise les valeurs des paramètres de contrôle mises à jour lors de l'exécution des contrôles de sécurité du contrôle. Les résultats incluent les valeurs de paramètres mises à jour.

L'`UpdateSecurityControl`opération renvoie une `InvalidInputException` réponse pour les valeurs de paramètres non valides. La réponse fournit des détails supplémentaires sur la raison de l'échec. Par exemple, vous avez peut-être spécifié une valeur qui se situe en dehors de la plage valide pour un paramètre. Ou bien, vous avez peut-être spécifié une valeur qui n'utilise pas le type de données correct. Soumettez à nouveau votre demande avec une saisie valide.

Si une défaillance interne se produit lorsque vous tentez de mettre à jour la valeur d'un paramètre, Security Hub CSPM réessaie automatiquement si vous l'avez activée. AWS Config Pour de plus amples informations, veuillez consulter Considérations avant l'activation et la configuration AWS Config.

Examen et gestion des résultats des contrôles dans Security Hub CSPM

La page des détails du contrôle affiche la liste des résultats actifs pour un contrôle. La liste n'inclut pas les résultats archivés.

La page des détails du contrôle prend en charge l'agrégation entre régions. Si vous avez défini une région d'agrégation, l'état du contrôle et la liste des contrôles de sécurité figurant sur la page des détails du contrôle incluent les contrôles provenant de tous les liensRégions AWS.

La liste fournit des outils permettant de filtrer et de trier les résultats, afin que vous puissiez d'abord vous concentrer sur les résultats les plus urgents. Une constatation peut inclure des liens vers des informations détaillées sur les ressources dans la console de service correspondante. Pour les contrôles basés sur des AWS Config règles, vous pouvez consulter les détails de la règle.

Vous pouvez également utiliser l'API AWS Security Hub CSPM pour récupérer une liste des résultats et des détails des recherches.

Pour de plus amples informations, veuillez consulter Révision des détails et de l'historique des découvertes.

Pour refléter l'état actuel de votre enquête sur un résultat de contrôle, vous définissez le statut du flux de travail. Pour de plus amples informations, veuillez consulter the section called “Définition de l'état des résultats dans le flux de travail”.

Vous pouvez également envoyer les résultats CSPM sélectionnés du Security Hub à une action personnalisée sur Amazon. EventBridge Pour de plus amples informations, veuillez consulter the section called “Envoi de résultats à une action personnalisée”.

Rubriques

- Résultats des contrôles de filtrage et de tri
- Échantillons de résultats de contrôle

Résultats des contrôles de filtrage et de tri

La sélection d'un contrôle sur la page Contrôles de la console AWS Security Hub CSPM ou sur la page de détails d'une norme vous amène à la page des détails du contrôle.

La page des détails du contrôle indique le titre et la description du contrôle, l'état général du contrôle, ainsi qu'une liste des vérifications de sécurité effectuées pour le contrôle au cours des dernières 24 heures.

Utilisez les options Filtrer par situées à côté de la liste de contrôle pour vous concentrer rapidement sur les résultats présentant un statut de flux de travail ou un statut de conformité spécifique.

Outre les options Filtrer par, vous pouvez utiliser la case Ajouter un filtre pour filtrer la liste de contrôle en fonction d'autres champs, tels que l'Compte AWSID ou l'ID de ressource.

Par défaut, les résultats dont le statut de conformité est PASSED sont répertoriés en premier. Vous pouvez modifier le tri par défaut en choisissant une autre option dans les en-têtes de colonne.

Sur la page des détails du contrôle, vous pouvez choisir Télécharger pour télécharger la page actuelle des résultats du contrôle dans un fichier .csv.

Si vous filtrez la liste de recherche, le téléchargement inclut uniquement les commandes correspondant au filtre. Si vous sélectionnez des résultats spécifiques dans la liste, le téléchargement inclut uniquement les résultats sélectionnés.

Pour plus d'informations sur le filtrage des résultats, consultezFiltrage des résultats dans Security Hub CSPM.

Échantillons de résultats de contrôle

Les exemples suivants fournissent des exemples de résultats de contrôle CSPM de AWS Security Hub au format ASFF (AWSSecurity Finding Format). Le contenu des résultats de contrôle varie selon que vous avez activé ou non les résultats de contrôle consolidés.

Si vous activez les résultats de contrôle consolidés, Security Hub CSPM génère un résultat unique pour un contrôle, même si le contrôle s'applique à plusieurs normes activées. Si vous n'activez pas cette fonctionnalité, Security Hub CSPM génère un résultat de contrôle distinct pour chaque norme activée à laquelle s'applique un contrôle. Par exemple, si vous activez deux normes et qu'un contrôle s'applique aux deux, vous recevez deux résultats distincts pour le contrôle, un pour chaque norme. Si vous activez les résultats de contrôle consolidés, vous ne recevez qu'un seul résultat pour le contrôle. Pour de plus amples informations, veuillez consulter Conclusions de contrôle consolidées.

Les exemples présentés sur cette page fournissent des exemples pour les deux scénarios. Les exemples incluent : les résultats de contrôle pour les différentes normes CSPM de Security Hub lorsque les résultats de contrôle consolidés sont désactivés, et un résultat de contrôle pour plusieurs normes CSPM de Security Hub lorsque les résultats de contrôle consolidés sont activés.

Échantillons de résultats de contrôle

- Recherche d'échantillons pour leAWSNorme sur les meilleures pratiques de sécurité fondamentales
- Recherche d'échantillons pour le CISAWSFoundations Benchmark v5.0.0
- Recherche d'échantillons pour le CISAWSFoundations Benchmark v3.0.0
- Recherche d'échantillons pour le CISAWSFoundations Benchmark v1.4.0
- Recherche d'échantillons pour le CISAWSFoundations Benchmark v1.2.0
- Recherche d'échantillons pour la norme NIST SP 800-53 Revision 5
- Recherche d'échantillons pour la norme NIST SP 800-171 Revision 2
- Exemple de recherche pour la norme de sécurité des données de l'industrie des cartes de paiement v3.2.1
- Recherche d'échantillons pour leAWSNorme de balisage des ressources
- Recherche d'échantillons pour leAWS Control Towernorme de gestion des services
- Exemple de résultats consolidés pour plusieurs normes

> **Note**
>
> Les résultats des contrôles font référence à différents champs et valeurs dans les régions de Chine et les AWS GovCloud (US) régions. Pour de plus amples informations, veuillez consulter Impact de la consolidation sur les champs et les valeurs ASFF.

Recherche d'échantillons pour leAWSNorme sur les meilleures pratiques de sécurité fondamentales

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à la norme AWS Foundational Security Best Practices (FSBP). Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
```

```
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
```

```
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
```

```
}
```

Recherche d'échantillons pour le CISAWSFoundations Benchmark v5.0.0

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à CIS AWS Foundations Benchmark v5.0.0. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.


```
{
  "AwsAccountId": "123456789012",
  "CompanyName": "AWS",
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.7",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v5.0.0/5.1.1"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/5.0.0"
      }
    ]
  },
  "CreatedAt": "2025-10-10T17:04:00.952Z",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Product": 40,
      "Original": "MEDIUM"
    }
  },
  "FirstObservedAt": "2025-10-10T17:03:57.895Z",
  "GeneratorId": "cis-aws-foundations-benchmark/v/5.0.0/5.1.1",
  "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
```

```
  "LastObservedAt": "2025-10-14T05:22:28.667Z",
  "ProcessedAt": "2025-10-14T05:22:50.099Z",
  "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub",
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/5.0.0",
    "ControlId": "5.1.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2a99554f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-west-1:123456789012:control/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-1::product/aws/
securityhub/arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
    "PreviousComplianceStatus": "FAILED"
  },
  "ProductName": "Security Hub CSPM",
  "RecordState": "ACTIVE",
  "Region": "us-west-1",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "Resources": [
    {
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-west-1",
      "Type": "AwsAccount"
    }
  ],
  "SchemaVersion": "2018-10-08",
  "Severity": {
```

```
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM",
    "Product": 40
  },
  "Title": "5.1.1 EBS default encryption should be enabled",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "UpdatedAt": "2025-10-14T05:22:38.671Z",
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW"
}
```

Recherche d'échantillons pour le CISAWSFoundations Benchmark v3.0.0

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à CIS AWS Foundations Benchmark v3.0.0. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
```

```
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Recherche d'échantillons pour le CISAWSFoundations Benchmark v1.4.0

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à CIS AWS Foundations Benchmark v1.4.0. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
```

```
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrailis a web service that recordsAWSAPI calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies.AWS Key Management Service(KMS) is a managed service that helps create and
 control the encryption keys used to encrypt account data, and uses Hardware Security
 Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be
 configured to leverage server side encryption (SSE) andAWS KMScustomer created master
 keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be
 configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
```

```
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CISAWSFoundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
```

```
}
```

Recherche d'échantillons pour le CISAWSFoundations Benchmark v1.2.0

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à CIS AWS Foundations Benchmark v1.2.0. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service(KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
```

```
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
}
```

Recherche d'échantillons pour la norme NIST SP 800-53 Revision 5

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à la norme NIST SP 800-53 Revision 5. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
```

```
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult theAWSSecurity Hub CSPM
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Recherche d'échantillons pour la norme NIST SP 800-171 Revision 2

L'exemple suivant fournit un exemple de recherche pour un contrôle qui s'applique à la norme NIST SP 800-171 Revision 2. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
```

```
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-171/v/2.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
```

```
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
```

```
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}
```

Exemple de recherche pour la norme de sécurité des données de l'industrie des cartes de paiement v3.2.1

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v3.2.1. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest usingAWS
 KMSCMKs",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Recherche d'échantillons pour leAWSNorme de balisage des ressources

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à la norme AWS Resource Tagging. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
```

```
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
```

```
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
           },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Recherche d'échantillons pour leAWS Control Towernorme de gestion des services

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à la norme de AWS Control Tower gestion des services. Dans cet exemple, les résultats de contrôle consolidés sont désactivés.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
```

```
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Exemple de résultats consolidés pour plusieurs normes

L'exemple suivant fournit un exemple de résultat pour un contrôle qui s'applique à plusieurs normes activées. Dans cet exemple, les résultats de contrôle consolidés sont activés.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
```

```
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-DO-NOT-DELETE"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
```

```
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},
      { "StandardsId": "standards/pci-dss/v/3.2.1"},
      { "StandardsId": "standards/pci-dss/v/4.0.1"}
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```


Comprendre les intégrations dans Security Hub CSPM

AWS Security Hub CSPM peut ingérer les résultats de sécurité provenant de plusieurs Services AWS solutions de sécurité tierces AWS Partner Network prises en charge. Ces intégrations peuvent vous aider à obtenir une vision complète de la sécurité et de la conformité dans votre AWS environnement. Security Hub CSPM ingère les résultats des solutions intégrées et les convertit au format ASFF (AWS Security Finding Format).

> **Important**
>
> Pour les intégrations de produits pris en charge AWS et tiers, Security Hub CSPM reçoit et consolide les résultats générés uniquement une fois que vous avez activé Security Hub

CSPM pour votre. Comptes AWS Le service ne reçoit et ne consolide pas rétroactivement les résultats de sécurité générés avant que vous n'activiez Security Hub CSPM.

La page Intégrations de la console Security Hub CSPM permet d'accéder aux intégrations de produits disponibles AWS et tiers. L'API Security Hub CSPM propose également des opérations de gestion des intégrations.

Il se peut qu'une intégration ne soit pas disponible dans tous Régions AWS. Si une intégration n'est pas prise en charge dans la région à laquelle vous êtes actuellement connecté sur la console Security Hub CSPM, elle n'apparaît pas sur la page Intégrations de la console. Pour obtenir la liste des intégrations disponibles dans les régions de Chine et AWS GovCloud (US) Regions, consultezDisponibilité des intégrations par région.

Outre les Service AWS intégrations tierces intégrées, vous pouvez intégrer des produits de sécurité personnalisés à Security Hub CSPM. Vous pouvez ensuite envoyer les résultats de ces produits à Security Hub CSPM à l'aide de l'API Security Hub CSPM. Vous pouvez également utiliser l'API pour mettre à jour les résultats existants que Security Hub CSPM a reçus d'un produit de sécurité personnalisé.

Rubriques

- Consulter la liste des intégrations CSPM de Security Hub
- Faciliter le flux des résultats à partir de l'intégration d'un Security Hub CSPM
- Désactivation du flux de résultats provenant d'une intégration CSPM de Security Hub
- Affichage des résultats d'une intégration de Security Hub CSPM
- Service AWS intégrations avec Security Hub CSPM
- Third-party intégrations de produits avec Security Hub CSPM
- Intégrer Security Hub CSPM à des produits personnalisés

Consulter la liste des intégrations CSPM de Security Hub

Choisissez votre méthode préférée et suivez les étapes pour consulter la liste des intégrations dans AWS Security Hub CSPM ou les détails d'une intégration spécifique.

Security Hub CSPM console

Pour consulter les options et les détails de l'intégration (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation CSPM de Security Hub, sélectionnez Intégrations.

Sur la page Intégrations, les intégrations avec d'autres produits Services AWS sont répertoriées en premier, suivies des intégrations avec des produits tiers.

Pour chaque intégration, la page Intégrations fournit les informations suivantes :

- Nom de la société.
- Nom du produit.
- Description de l'intégration.
- Catégories auxquelles l'intégration s'applique.
- Comment activer l'intégration.
- État actuel de l'intégration.

Vous pouvez filtrer la liste en saisissant du texte dans les champs suivants :

- Nom de la société
- Nom du produit
- Description de l'intégration
- Catégories

Security Hub CSPM API

Pour passer en revue les options et les détails de l'intégration (API)

Pour obtenir la liste des intégrations, utilisez l'DescribeProductsopération. Si vous utilisez le AWS CLI, exécutez la describe-products commande.

Pour récupérer les détails d'une intégration de produit spécifique, utilisez le `ProductArn` paramètre pour spécifier l'Amazon Resource Name (ARN) de l'intégration.

Par exemple, la AWS CLI commande suivante permet d'obtenir des informations sur l'intégration de Security Hub CSPM à 3CoreSec.

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Faciliter le flux des résultats à partir de l'intégration d'un Security Hub CSPM

Sur la page Intégrations de la console AWS Security Hub CSPM, vous pouvez consulter les étapes requises pour activer chaque intégration.

Pour la plupart des intégrations avec d'autres Services AWS, la seule étape requise pour activer l'intégration est d'activer l'autre service. Les informations d'intégration incluent un lien vers la page d'accueil de l'autre service. Lorsque vous activez l'autre service, une autorisation au niveau des ressources qui permet à Security Hub CSPM de recevoir les résultats du service est automatiquement créée et appliquée.

Pour les intégrations de produits tiers, vous devrez peut-être acheter l'intégration auprès de AWS Marketplace, puis configurer l'intégration. Les informations d'intégration fournissent des liens permettant d'effectuer ces tâches.

Si plusieurs versions d'un produit sont disponibles AWS Marketplace, sélectionnez la version à laquelle vous souhaitez vous abonner, puis choisissez Continuer à vous abonner. Par exemple, certains produits proposent une version standard et une AWS GovCloud (US) version.

Lorsque vous activez l'intégration d'un produit, une stratégie de ressources est automatiquement attachée à l'abonnement de ce produit. Cette politique de ressources définit les autorisations dont Security Hub CSPM a besoin pour recevoir les résultats de ce produit.

Après avoir effectué les étapes préliminaires nécessaires à l'activation d'une intégration, vous pouvez désactiver et réactiver le flux des résultats de cette intégration. Sur la page Intégrations, pour les intégrations qui envoient des résultats, les informations d'état indiquent si vous acceptez actuellement des résultats.

Security Hub CSPM console

Pour activer le flux de résultats à partir d'une intégration (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation CSPM de Security Hub, sélectionnez Intégrations.
3. Pour les intégrations qui envoient des résultats, les informations d'état indiquent si Security Hub CSPM accepte actuellement les résultats de cette intégration.
4. Choisissez Accepter les résultats.

Security Hub CSPM API

Utilisez l'EnableImportFindingsForProductopération. Si vous utilisez le AWS CLI, exécutez la enable-import-findings-for-product commande. Pour permettre à Security Hub de recevoir les résultats d'une intégration, vous avez besoin de l'ARN du produit. Pour obtenir les ARN des intégrations disponibles, utilisez l'DescribeProductsopération. Si vous utilisez le AWS CLI, exécutez le describe-products.

Par exemple, la AWS CLI commande suivante permet à Security Hub CSPM de recevoir les résultats de l'intégration CrowdStrike Falçon. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Désactivation du flux de résultats provenant d'une intégration CSPM de Security Hub

Choisissez votre méthode préférée et suivez les étapes pour désactiver le flux de résultats provenant d'une intégration CSPM de AWS Security Hub.

Security Hub CSPM console

Pour désactiver le flux de résultats provenant d'une intégration (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

2. Dans le volet de navigation CSPM de Security Hub, sélectionnez Intégrations.
3. Pour les intégrations qui envoient des résultats, les informations d'état indiquent si Security Hub CSPM accepte actuellement les résultats de cette intégration.
4. Choisissez Arrêter d'accepter les résultats.

Security Hub CSPM API

Utilisez l'DisableImportFindingsForProductopération. Si vous utilisez le AWS CLI, exécutez la disable-import-findings-for-product commande. Pour désactiver le flux de résultats d'une intégration, vous avez besoin de l'ARN d'abonnement correspondant à l'intégration activée. Pour obtenir l'ARN de l'abonnement, utilisez l'ListEnabledProductsForImportopération. Si vous utilisez le AWS CLI, exécutez le list-enabled-products-for-import.

Par exemple, la AWS CLI commande suivante désactive le flux de résultats vers Security Hub CSPM à partir de l' CrowdStrike intégration Falçon. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Affichage des résultats d'une intégration de Security Hub CSPM

Lorsque vous commencez à accepter les résultats d'une intégration AWS Security Hub CSPM, la page Intégrations de la console Security Hub CSPM affiche le statut de l'intégration comme Acceptation des résultats. Pour consulter la liste des résultats de l'intégration, choisissez Voir les résultats.

La liste des résultats affiche les résultats actifs de l'intégration sélectionnée dont l'état du flux de travail est `NEW` ou `NOTIFIED`.

Si vous activez l'agrégation entre régions, dans la région d'agrégation, la liste inclut les résultats de la région d'agrégation et des régions liées dans lesquelles l'intégration est activée. Security Hub n'active pas automatiquement les intégrations en fonction de la configuration d'agrégation interrégionale.

Dans les autres régions, la liste des résultats d'une intégration ne contient que les résultats de la région actuelle.

Pour plus d'informations sur la configuration de l'agrégation entre régions, consultezthe section called "Agrégation des données entre les régions".

Dans la liste des résultats, vous pouvez effectuer les actions suivantes.

- Modifier les filtres et le regroupement pour la liste
- Afficher les détails des résultats individuels
- Mettre à jour l'état du flux de travail des résultats
- Envoyer les résultats à des actions personnalisées

Service AWS intégrations avec Security Hub CSPM

AWS Security Hub CSPM prend en charge les intégrations avec plusieurs autres. Services AWS Ces intégrations peuvent vous aider à obtenir une vision complète de la sécurité et de la conformité dans votre AWS environnement.

Sauf indication contraire ci-dessous, Service AWS les intégrations qui envoient des résultats à Security Hub CSPM sont activées automatiquement une fois que vous avez activé Security Hub CSPM et l'autre service. Les intégrations qui reçoivent les résultats de Security Hub CSPM peuvent nécessiter des étapes supplémentaires pour leur activation. Consultez les informations relatives à chaque intégration pour en savoir plus.

Certaines intégrations ne sont pas disponibles dans toutes Régions AWS. Sur la console Security Hub CSPM, aucune intégration n'apparaît sur la page Intégrations si elle n'est pas prise en charge dans la région actuelle. Pour obtenir la liste des intégrations disponibles dans les régions de Chine et AWS GovCloud (US) Regions, consultezDisponibilité des intégrations par région.

Vue d'ensemble de AWS intégrations de services avec Security Hub CSPM

Le tableau suivant fournit une vue d'ensemble des AWS services qui envoient des résultats à Security Hub CSPM ou reçoivent des résultats de Security Hub CSPM.

AWS Service intégré	Direction	
AWS Config	Envoie les résultats	
AWS Firewall Manager	Envoie les résultats	

AWS Service intégré	Direction	
Amazon GuardDuty	Envoie les résultats	
AWS Health	Envoie les résultats	
AWS Identity and Access Management Access Analyzer	Envoie les résultats	
Amazon Inspector	Envoie les résultats	
AWS IoT Device Defender	Envoie les résultats	
Amazon Macie	Envoie les résultats	
Amazon Route 53 Resolver Pare-feu DNS	Envoie les résultats	
AWS Systems Manager Gestionnaire de correctifs	Envoie les résultats	
AWS Audit Manager	Reçoit les résultats	
Amazon Q Developer dans les applications de chat	Reçoit les résultats	
Amazon Detective	Reçoit les résultats	
Amazon Security Lake	Reçoit les résultats	
AWS Systems Manager E xplorateur et OpsCenter	Reçoit et met à jour les résultats	
AWS Trusted Advisor	Reçoit les résultats	

Services AWS qui envoient les résultats au Security Hub CSPM

Les éléments suivants Services AWS s'intègrent à Security Hub CSPM et peuvent envoyer des résultats à ce dernier. Security Hub CSPM convertit les résultats au format AWS Security Finding.

AWS Config (Envoie les résultats)

AWS Config est un service qui vous permet d'évaluer, d'auditer et d'évaluer les configurations de vos AWS ressources. AWS Config surveille et enregistre en permanence les configurations de vos AWS ressources et vous permet d'automatiser l'évaluation des configurations enregistrées par rapport aux configurations souhaitées.

En utilisant l'intégration avec AWS Config, vous pouvez consulter les résultats des évaluations de règles AWS Config gérées et personnalisées sous forme de résultats dans Security Hub CSPM. Ces résultats peuvent être consultés conjointement avec d'autres résultats de Security Hub CSPM, fournissant un aperçu complet de votre posture de sécurité.

AWS Config utilise Amazon EventBridge pour envoyer des évaluations de AWS Config règles à Security Hub CSPM. Security Hub CSPM transforme les évaluations des règles en résultats conformes au format AWS Security Finding. Security Hub CSPM enrichit ensuite les résultats du mieux possible en obtenant plus d'informations sur les ressources concernées, telles que le nom de la ressource Amazon (ARN), les balises de ressources et la date de création.

Pour plus d'informations sur cette intégration, consultez les sections suivantes.

Comment ? AWS Config envoie les résultats au Security Hub CSPM

Toutes les données de Security Hub CSPM utilisent le format JSON standard ASFF. L'ASFF inclut des détails sur l'origine de la découverte, la ressource affectée et l'état actuel de la découverte. AWS Config envoie des évaluations de règles gérées et personnalisées à Security Hub CSPM via. EventBridge Security Hub CSPM transforme les évaluations des règles en résultats qui suivent l'ASFF et enrichit les résultats du mieux possible.

Types de résultats qui AWS Config envoie au Security Hub CSPM

Une fois l'intégration activée, AWS Config envoie les évaluations de toutes les règles AWS Config gérées et des règles personnalisées à Security Hub CSPM. Seules les évaluations effectuées après l'activation de Security Hub CSPM sont envoyées. Supposons, par exemple, qu'une évaluation de AWS Config règles révèle cinq ressources défaillantes. Si vous activez Security Hub CSPM après cette évaluation et que la règle révèle ensuite une sixième ressource défaillante, AWS Config envoie uniquement la sixième évaluation de ressource à Security Hub CSPM.

Les évaluations issues de AWS Config règles liées à des services, telles que celles utilisées pour vérifier les contrôles CSPM de Security Hub, sont exclues. L'exception concerne les résultats

générés par des règles liées à des services qui AWS Control Tower créent et gèrent dans. AWS Config L'inclusion de résultats pour ces règles permet de garantir que vos données de résultats incluent les résultats des contrôles proactifs effectués par AWS Control Tower.

Envoi AWS Config résultats pour Security Hub CSPM

Lorsque l'intégration est activée, Security Hub CSPM attribue automatiquement les autorisations nécessaires pour recevoir les résultats de. AWS Config Security Hub CSPM utilise des autorisations de niveau service à service qui vous permettent d'activer cette intégration en toute sécurité et d'importer des résultats depuis Amazon. AWS Config EventBridge

Latence pour l'envoi des résultats

Lorsque vous AWS Config créez une nouvelle découverte, vous pouvez généralement la consulter dans Security Hub CSPM dans un délai de cinq minutes.

Réessayer lorsque Security Hub CSPM n'est pas disponible

AWS Config envoie les résultats au Security Hub CSPM dans la mesure du possible via. EventBridge Lorsqu'un événement n'est pas transmis avec succès au Security Hub CSPM, une EventBridge nouvelle tentative de diffusion peut être effectuée pendant 24 heures ou 185 fois, selon la première éventualité.

Mettre à jour l'existant AWS Config résultats du Security Hub CSPM

Après avoir AWS Config envoyé un résultat à Security Hub CSPM, il peut envoyer des mises à jour du même résultat à Security Hub CSPM pour refléter des observations supplémentaires concernant l'activité de recherche. Les mises à jour ne sont envoyées que pour les `ComplianceChangeNotification` événements. Si aucun changement de conformité ne se produit, les mises à jour ne sont pas envoyées à Security Hub CSPM. Security Hub CSPM supprime les résultats 90 jours après la dernière mise à jour ou 90 jours après leur création si aucune mise à jour n'est effectuée.

Security Hub CSPM n'archive pas les résultats envoyés, AWS Config même si vous supprimez la ressource associée.

Régions dans lesquelles AWS Config des résultats existent

AWS Config les résultats se produisent sur une base régionale. AWS Config envoie les résultats au Security Hub CSPM de la région ou des régions où les résultats sont détectés.

Visualisation AWS Config résultats du Security Hub CSPM

Pour consulter vos AWS Config résultats, choisissez Findings dans le volet de navigation CSPM de Security Hub. Pour filtrer les résultats afin de n'afficher que AWS Config les résultats, choisissez Nom du produit dans la liste déroulante de la barre de recherche. Entrez Config, puis choisissez Appliquer.

Interprétation AWS Config recherche de noms dans Security Hub CSPM

Security Hub CSPM transforme les évaluations des AWS Config règles en résultats qui suivent le. AWS Format de recherche de sécurité (ASFF) AWS Config les évaluations de règles utilisent un modèle d'événement différent de celui de l'ASFF. Le tableau suivant met en correspondance les champs d'évaluation des AWS Config règles avec leur équivalent ASFF tels qu'ils apparaissent dans Security Hub CSPM.

Type de recherche d'évaluation des règles de configuration	Type de résultat ASFF	Valeur codée en dur
détail.aws AccountId	AwsAccountId	
détail.nouveau EvaluationResult.resultRecordedTime	CreatedAt	
détail.nouveau EvaluationResult.resultRecordedTime	UpdatedAt	
	ProductArn	<region>« arn ::securityhub : <partition>: : /config » product/aws
	ProductName	« Configuration »
	CompanyName	"AWS"
	Région	« eu-central-1"
configuration RuleArn	GeneratorId, ProductFields	
détail. ConfigRuleARN/finding/hash	Id	

Type de recherche d'évaluation des règles de configuration	Type de résultat ASFF	Valeur codée en dur
détail.config RuleName	Titre, ProductFields	
détail.config RuleName	Description	« Cette découverte est créée pour une modification de la conformité des ressources pour la règle de configuration : `${detail.ConfigRuleName}` »
Élément de configuration « ARN » ou ARN calculé par Security Hub CSPM	Ressources [i] .id	
Type de ressource détaillé	Ressources [i] .Type	"AwsS3Bucket"
	Ressources [i] .Partition	"aws"
	Ressources [i] .Région	« eu-central-1"
Élément de configuration « configuration »	Ressources [i]. Détails	
	SchemaVersion	« 08 octobre 2018 »
	Severity.Label	Voir « Interprétation de l'étiquette de gravité » ci-dessous
	Types	[« Vérifications du logiciel et de la configuration »]
détail.nouveau EvaluationResult.complianceType	Compliance.Status	« ÉCHEC », « NOT_AVAILABLE », « PASSÉ » ou « AVERTISSEMENT »

Type de recherche d'évaluation des règles de configuration	Type de résultat ASFF	Valeur codée en dur
	Workflow.Status	« RESOLVED » si un AWS Config résultat est généré avec Compliance.Status la valeur « PASSED », ou si le résultat Compliance.Status passe de « FAILED » à « PASSED ». Sinon, Workflow.Status ce sera « NOUVEAU ». Vous pouvez modifier cette valeur à l'aide de l'opération BatchUpdateFindings API.

Interpréter l'étiquette de gravité

Tous les résultats des évaluations des AWS Config règles ont une étiquette de gravité par défaut de MEDIUM dans l'ASFF. Vous pouvez mettre à jour l'étiquette de gravité d'un résultat à l'aide de l'opération `BatchUpdateFindings` API.

Constatation typique de AWS Config

Security Hub CSPM transforme les évaluations des AWS Config règles en résultats conformes à l'ASFF. Voici un exemple d'une constatation typique de AWS Config l'ASFF.

> **Note**
>
> Si la description comporte plus de 1 024 caractères, elle sera tronquée à 1 024 caractères et la mention « (tronquée) » sera ajoutée à la fin.

```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
```

```
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
```

```
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

Activation et configuration de l'intégration

Une fois que vous avez activé Security Hub CSPM, cette intégration est automatiquement activée. AWS Config commence immédiatement à envoyer les résultats au Security Hub CSPM.

Arrêt de la publication des résultats dans Security Hub CSPM

Pour arrêter d'envoyer des résultats à Security Hub CSPM, vous pouvez utiliser la console Security Hub CSPM ou l'API Security Hub CSPM.

Pour obtenir des instructions sur l'arrêt du flux de résultats, voirFaciliter le flux des résultats à partir de l'intégration d'un Security Hub CSPM.

AWS Firewall Manager (Envoie les résultats)

Firewall Manager envoie les résultats au Security Hub CSPM lorsqu'une politique de pare-feu d'applications Web (WAF) pour les ressources ou une règle de liste de contrôle d'accès Web (ACL Web) n'est pas conforme. Firewall Manager envoie également des résultats lorsqu' AWS Shield Advanced il ne protège pas les ressources ou lorsqu'une attaque est identifiée.

Une fois que vous avez activé Security Hub CSPM, cette intégration est automatiquement activée. Firewall Manager commence immédiatement à envoyer les résultats au Security Hub CSPM.

Pour en savoir plus sur l'intégration, consultez la page Intégrations de la console Security Hub CSPM.

Pour en savoir plus sur Firewall Manager, consultez le Guide du AWS WAF développeur .

Amazon GuardDuty (envoie des résultats)

GuardDuty envoie tous les types de résultats qu'il génère à Security Hub CSPM. Certains types de recherche comportent des prérequis, des exigences d'activation ou des limites régionales. Pour plus d'informations, consultez la section relative à la GuardDuty recherche de types dans le guide de GuardDuty l'utilisateur Amazon.

Les nouveaux résultats GuardDuty sont envoyés au Security Hub CSPM dans les cinq minutes. Les mises à jour des résultats sont envoyées en fonction du paramètre Résultats mis à jour pour Amazon EventBridge dans GuardDuty les paramètres.

Lorsque vous générez des GuardDuty exemples de résultats à l'aide de la page GuardDuty Paramètres, Security Hub CSPM reçoit les exemples de résultats et omet le préfixe `[Sample]` dans le type de résultat. Par exemple, le type de recherche d'échantillon GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` est affiché comme `Recon:IAMUser/ResourcePermissions` dans Security Hub CSPM.

Une fois que vous avez activé Security Hub CSPM, cette intégration est automatiquement activée. GuardDutycommence immédiatement à envoyer les résultats au Security Hub CSPM.

Pour plus d'informations sur l' GuardDuty intégration, consultez la section Intégration à AWS Security Hub CSPM dans le guide de l' GuardDuty utilisateur Amazon.

AWS Health (Envoie les résultats)

AWS Health fournit une visibilité continue sur les performances de vos ressources et sur la disponibilité de vos Services AWS données et Comptes AWS. Vous pouvez utiliser AWS Health les événements pour découvrir comment les modifications apportées aux services et aux ressources peuvent affecter les applications qui s'exécutent AWS.

L'intégration avec AWS Health n'utilise pas`BatchImportFindings`. AWS Health Utilise plutôt la messagerie d'événements service à service pour envoyer les résultats à Security Hub CSPM.

Pour plus d'informations sur l'intégration, consultez les sections suivantes.

Comment ? AWS Health envoie les résultats au Security Hub CSPM

Dans Security Hub CSPM, les problèmes de sécurité sont suivis en tant que findings (résultats). Certains résultats proviennent de problèmes détectés par d'autres AWS services ou par des partenaires tiers. Security Hub CSPM dispose également d'un ensemble de règles qu'il utilise pour détecter les problèmes de sécurité et générer des résultats.

Security Hub CSPM fournit des outils permettant de gérer les résultats provenant de toutes ces sources. Vous pouvez afficher et filtrer les listes de résultats et afficher les informations sur un résultat. Consultez Révision des détails et de l'historique des recherches dans Security Hub CSPM. Vous pouvez également suivre le statut d'une analyse dans un résultat. Consultez Configuration de l'état du flux de travail des résultats dans Security Hub CSPM.

Toutes les découvertes de Security Hub CSPM utilisent un format JSON standard appelé. AWS Format de recherche de sécurité (ASFF) L'ASFF inclut des informations sur la source du problème, les ressources concernées et l'état actuel de la découverte.

AWS Health est l'un des AWS services qui envoie les résultats au Security Hub CSPM.

Types de résultats qui AWS Health envoie au Security Hub CSPM

Une fois l'intégration activée, AWS Health envoie les résultats qui répondent à une ou plusieurs des spécifications répertoriées à Security Hub CSPM. Security Hub CSPM intègre les résultats dans le. AWS Format de recherche de sécurité (ASFF)

- Résultats contenant l'une des valeurs suivantes pour Service AWS :
  - `RISK`
  - `ABUSE`
  - `ACM`
  - `CLOUDHSM`
  - `CLOUDTRAIL`
  - `CONFIG`
  - `CONTROLTOWER`
  - `DETECTIVE`
  - `EVENTS`
  - `GUARDDUTY`
  - `IAM`
  - `INSPECTOR`
  - `KMS`
  - `MACIE`
  - `SES`
  - `SECURITYHUB`

- SHIELD
- SSO
- COGNITO
- IOTDEVICEDEFENDER
- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB

- Résultats obtenus avec les mots `securityabuse`, ou `certificate` AWS Health `typeCode` sur le terrain
- Constatations où se trouve le AWS Health service `risk` ou `abuse`

Envoi AWS Health résultats pour Security Hub CSPM

Lorsque vous choisissez d'accepter les résultats AWS Health, Security Hub CSPM attribue automatiquement les autorisations nécessaires pour recevoir les résultats. AWS Health Security Hub CSPM utilise des autorisations de niveau service à service qui vous offrent un moyen sûr et simple d'activer cette intégration et d'importer des résultats depuis AWS Health Amazon en votre

nom. EventBridge En choisissant Accepter les résultats, Security Hub CSPM est autorisé à utiliser les résultats de. AWS Health

Latence pour l'envoi des résultats

Lors de AWS Health la création d'une nouvelle découverte, celle-ci est généralement envoyée au Security Hub CSPM dans les cinq minutes.

Réessayer lorsque Security Hub CSPM n'est pas disponible

AWS Health envoie les résultats au Security Hub CSPM dans la mesure du possible via. EventBridge Lorsqu'un événement n'est pas transmis avec succès au Security Hub CSPM, EventBridge réessaie de l'envoyer pendant 24 heures.

Mise à jour des résultats existants dans Security Hub CSPM

Après avoir AWS Health envoyé un résultat à Security Hub CSPM, il peut envoyer des mises à jour du même résultat afin de refléter des observations supplémentaires concernant l'activité de recherche au Security Hub CSPM.

Régions dans lesquelles des résultats existent

Pour les événements mondiaux, AWS Health envoie les résultats au Security Hub CSPM dans us-east-1 (AWS partition), cn-northwest-1 (partition chinoise) et gov-us-west-1 (partition). GovCloud AWS Health envoie Region-specific des événements au Security Hub CSPM dans la ou les mêmes régions que celles où les événements se produisent.

Visualisation AWS Health résultats du Security Hub CSPM

Pour consulter vos AWS Health résultats dans Security Hub CSPM, choisissez Résultats dans le panneau de navigation. Pour filtrer les résultats afin de n'afficher que AWS Health les résultats, choisissez Santé dans le champ Nom du produit.

Interprétation AWS Health recherche de noms dans Security Hub CSPM

AWS Health envoie les résultats au Security Hub CSPM à l'aide du. AWS Format de recherche de sécurité (ASFF) AWS Health la recherche utilise un modèle d'événement différent de celui du format CSPM ASFF de Security Hub. Le tableau ci-dessous détaille tous les champs de AWS Health recherche avec leur équivalent ASFF tels qu'ils apparaissent dans Security Hub CSPM.

Type de découverte de santé	Type de résultat ASFF	Valeur codée en dur
compte	AwsAccountId	
Détail. Heure de début	CreatedAt	
détail de l'événement Descripti on.latestDescription	Description	
détail de l'événement TypeCode	GeneratorId	
Detail.eventArn (compte inclus) + hash de Detail.St artTime	Id	
<region>« arn:aws:securityhu b : : : /health » product/aws	ProductArn	
compte ou ResourceID	Ressources [i] .id	
	Ressources [i] .Type	« Autres »
	SchemaVersion	« 08 octobre 2018 »
	Severity.Label	Voir « Interprétation de l'étiquette de gravité » ci-dessous
« AWS Health - » detail.event TypeCode	Titre	
-	Types	[« Vérifications du logiciel et de la configuration »]
heure de l'événement	UpdatedAt	
URL de l'événement sur Health console	SourceUrl	

Interpréter l'étiquette de gravité

L'étiquette de gravité figurant dans le résultat de l'ASFF est déterminée selon la logique suivante :

- Gravité CRITIQUE si :
  - Le `service` champ de la AWS Health découverte a la valeur `Risk`
  - Le `typeCode` champ de la AWS Health découverte a la valeur `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - Le `typeCode` champ de la AWS Health découverte a la valeur `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - Le `typeCode` champ de la AWS Health découverte a la valeur `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  Gravité ÉLEVÉE si :
  - Le `service` champ de la AWS Health découverte a la valeur `Abuse`
  - Le `typeCode` champ de la AWS Health découverte contient la valeur `SECURITY_NOTIFICATION`
  - Le `typeCode` champ de la AWS Health découverte contient la valeur `ABUSE_DETECTION`

  Gravité MOYENNE si :
  - Le `service` champ du résultat est l'un des suivants :`ACM,,,,,,,,,,,ARTIFACT,AUDITMANAGER,,BACKUP,,CLOUDENDURE,CLOUDHSM,,CLOUDTRAIL,,CLWAF`
  - Le champ TypeCode de la AWS Health découverte contient la valeur `CERTIFICATE`
  - Le champ TypeCode de la AWS Health découverte contient la valeur `END_OF_SUPPORT`

Constatation typique de AWS Health

AWS Health envoie les résultats au Security Hub CSPM à l'aide du. AWS Format de recherche de sécurité (ASFF) Voici un exemple de résultat typique tiré de AWS Health.

> **Note**
>
> Si la description comporte plus de 1 024 caractères, elle sera tronquée à 1 024 caractères et la mention (tronquée) sera ajoutée à la fin.

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
```

```
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

Activation et configuration de l'intégration

Une fois que vous avez activé Security Hub CSPM, cette intégration est automatiquement activée. AWS Health commence immédiatement à envoyer les résultats au Security Hub CSPM.

Arrêt de la publication des résultats dans Security Hub CSPM

Pour arrêter d'envoyer des résultats à Security Hub CSPM, vous pouvez utiliser la console Security Hub CSPM ou l'API Security Hub CSPM.

Pour obtenir des instructions sur l'arrêt du flux de résultats, voirFaciliter le flux des résultats à partir de l'intégration d'un Security Hub CSPM.

AWS Identity and Access Management Access Analyzer (Envoie les résultats)

Avec IAM Access Analyzer, tous les résultats sont envoyés au Security Hub CSPM.

IAM Access Analyzer utilise un raisonnement logique pour analyser les politiques basées sur les ressources appliquées aux ressources prises en charge dans votre compte. IAM Access Analyzer génère un résultat lorsqu'il détecte une déclaration de politique qui permet à un responsable externe d'accéder à une ressource de votre compte.

Dans IAM Access Analyzer, seul le compte administrateur peut consulter les résultats des analyseurs qui s'appliquent à une organisation. Pour les analyseurs d'organisations, le champ

`AwsAccountId` ASFF reflète l'ID du compte administrateur. En dessous`ProductFields`, le `ResourceOwnerAccount` champ indique le compte dans lequel la découverte a été découverte. Si vous activez les analyseurs individuellement pour chaque compte, Security Hub CSPM génère plusieurs résultats, l'un identifiant l'identifiant du compte administrateur et l'autre identifiant l'ID du compte ressource.

Pour plus d'informations, consultez la section Intégration à AWS Security Hub CSPM dans le guide de l'utilisateur IAM.

Amazon Inspector (envoie les résultats)

Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos AWS charges de travail à la recherche de vulnérabilités. Amazon Inspector découvre et analyse automatiquement les instances Amazon EC2 et les images de conteneurs qui se trouvent dans l'Amazon Elastic Container Registry. L'analyse recherche des vulnérabilités logicielles et une exposition involontaire au réseau.

Une fois que vous avez activé Security Hub CSPM, cette intégration est automatiquement activée. Amazon Inspector commence immédiatement à envoyer toutes les conclusions qu'il génère à Security Hub CSPM.

Pour plus d'informations sur l'intégration, consultez la section Intégration à AWS Security Hub CSPM dans le guide de l'utilisateur d'Amazon Inspector.

Security Hub CSPM peut également recevoir les résultats d'Amazon Inspector Classic. Amazon Inspector Classic envoie les résultats au Security Hub CSPM qui sont générés lors de cycles d'évaluation pour tous les packages de règles pris en charge.

Pour plus d'informations sur l'intégration, consultez la section Intégration à AWS Security Hub CSPM dans le guide de l'utilisateur d'Amazon Inspector Classic.

Les résultats pour Amazon Inspector et Amazon Inspector Classic utilisent le même ARN du produit. Les résultats d'Amazon Inspector contiennent l'entrée suivante `ProductFields` :

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Les résultats de sécurité générés par Amazon Inspector Code Security ne sont pas disponibles pour cette intégration. Vous pouvez toutefois accéder à ces résultats spécifiques dans la console Amazon Inspector et via l'API Amazon Inspector.

AWS IoT Device Defender (Envoie les résultats)

AWS IoT Device Defender est un service de sécurité qui audite la configuration de vos appareils IoT, surveille les appareils connectés pour détecter les comportements anormaux et contribue à atténuer les risques de sécurité.

Après avoir activé Security Hub CSPM, rendez-vous sur la page Intégrations de la console Security Hub CSPM et choisissez Accepter les résultats pour l'audit, la détection ou les deux AWS IoT Device Defender . AWS IoT Device Defender Audit and Detect commence à envoyer tous les résultats au Security Hub CSPM.

AWS IoT Device Defender L'audit envoie des résumés des contrôles au Security Hub CSPM, qui contiennent des informations générales sur un type de contrôle d'audit et une tâche d'audit spécifiques. AWS IoT Device Defender Detect envoie les résultats des violations concernant l'apprentissage automatique (ML), les comportements statistiques et statiques à Security Hub CSPM. L'audit envoie également les mises à jour des résultats au Security Hub CSPM.

Pour plus d'informations sur cette intégration, consultez la section Intégration à AWS Security Hub CSPM dans le Guide du AWS IoT développeur.

Amazon Macie (envoie des résultats)

Amazon Macie est un service de sécurité des données qui découvre les données sensibles à l'aide du machine learning et de la correspondance de modèles, fournit une visibilité sur les risques liés à la sécurité des données et permet une protection automatisée contre ces risques. Une découverte de Macie peut indiquer qu'il existe une violation potentielle des règles ou que des données sensibles existent dans votre parc de données Amazon S3.

Une fois que vous avez activé Security Hub CSPM, Macie commence automatiquement à envoyer les résultats des politiques à Security Hub CSPM. Vous pouvez configurer l'intégration pour envoyer également les résultats de données sensibles à Security Hub CSPM.

Dans Security Hub CSPM, le type de recherche d'une politique ou de données sensibles est remplacé par une valeur compatible avec ASFF. Par exemple, le type de `Policy:IAMUser/S3BucketPublic` recherche dans Macie s'affiche comme `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` dans Security Hub CSPM.

Macie envoie également les échantillons de résultats générés au Security Hub CSPM. Pour les résultats des échantillons, le nom de la ressource affectée est `macie-sample-finding-bucket` et la valeur du `Sample` champ est`true`.

Pour plus d'informations, consultez la section Évaluation des résultats de Macie à l'aide de Security Hub dans le guide de l'utilisateur Amazon Macie.

Amazon Route 53 Resolver Pare-feu DNS (envoie les résultats)

Grâce au pare-feu Amazon Route 53 Resolver DNS, vous pouvez filtrer et réguler le trafic DNS sortant pour votre cloud privé virtuel (VPC). Pour ce faire, créez des collections réutilisables de règles de filtrage dans les groupes de règles du pare-feu DNS, associez les groupes de règles à votre VPC, puis surveillez l'activité dans les journaux et les mesures du pare-feu DNS. En fonction de l'activité, vous pouvez ajuster le comportement du pare-feu DNS. Le pare-feu DNS est une fonctionnalité de Route 53 Resolver.

Le pare-feu DNS Route 53 Resolver peut envoyer plusieurs types de résultats à Security Hub CSPM :

- Résultats relatifs aux requêtes bloquées ou alertées pour les domaines associés aux listes de domaines AWS gérés, qui sont des listes de domaines AWS gérées.
- Résultats relatifs aux requêtes bloquées ou alertées pour les domaines associés à une liste de domaines personnalisée que vous définissez.
- Résultats relatifs aux requêtes bloquées ou alertées par DNS Firewall Advanced, une fonctionnalité de résolution Route 53 capable de détecter les requêtes associées à des menaces DNS avancées telles que les algorithmes de génération de domaines (DGA) et le tunneling DNS.

Une fois que vous avez activé Security Hub CSPM et le pare-feu DNS du résolveur Route 53, le pare-feu DNS commence automatiquement à envoyer les résultats pour les listes de domaines AWS gérés et le pare-feu DNS avancé à Security Hub CSPM. Pour envoyer également les résultats d'une liste de domaines personnalisée à Security Hub CSPM, activez manuellement l'intégration dans Security Hub CSPM.

Dans Security Hub CSPM, tous les résultats du pare-feu DNS du résolveur Route 53 sont du type suivant :. `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Pour plus d'informations, consultez la section Envoyer les résultats du pare-feu DNS du résolveur Route 53 à Security Hub dans le guide du développeur Amazon Route 53.

AWS Systems Manager Patch Manager (envoie les résultats)

AWS Systems Manager Patch Manager envoie les résultats à Security Hub CSPM lorsque les instances de la flotte d'un client ne sont pas conformes à sa norme de conformité des correctifs.

Le Gestionnaire de correctifs automatise le processus d'application des correctifs de sécurité et d'autres types de mise à jour sur les instances gérées.

Une fois que vous avez activé Security Hub CSPM, cette intégration est automatiquement activée. Systems Manager Patch Manager commence immédiatement à envoyer les résultats au Security Hub CSPM.

Pour plus d'informations sur l'utilisation de Patch Manager, consultez AWS Systems Manager Patch Manager dans le Guide de AWS Systems Manager l'utilisateur.

AWS services qui reçoivent les résultats du Security Hub CSPM

Les AWS services suivants sont intégrés à Security Hub CSPM et reçoivent les résultats de Security Hub CSPM. Lorsque cela est indiqué, le service intégré peut également mettre à jour les résultats. Dans ce cas, la recherche des mises à jour que vous effectuez dans le service intégré sera également reflétée dans Security Hub CSPM.

AWS Audit Manager (Reçoit les résultats)

AWS Audit Manager reçoit les résultats du Security Hub CSPM. Ces résultats aident les utilisateurs d'Audit Manager à se préparer aux audits.

Pour en savoir plus sur Audit Manager, consultez le Guide de l'utilisateur d'AWS Audit Manager . AWS Les contrôles Security Hub CSPM sont pris en charge par AWS Audit Manager des listes de contrôles pour lesquels Security Hub CSPM envoie les résultats à Audit Manager.

Amazon Q Developer dans les applications de chat (reçoit les résultats)

Amazon Q Developer dans les applications de chat est un agent interactif qui vous aide à surveiller et à interagir avec vos AWS ressources sur vos chaînes Slack et les salons de discussion Amazon Chime.

Amazon Q Developer dans les applications de chat reçoit les résultats de Security Hub CSPM.

Pour en savoir plus sur l'intégration d'Amazon Q Developer in chat applications avec Security Hub CSPM, consultez la présentation de l'intégration de Security Hub CSPM dans le Guide de l'administrateur Amazon Q Developer in chat applications.

Amazon Detective (reçoit les résultats)

Detective collecte automatiquement les données des journaux de vos AWS ressources et utilise l'apprentissage automatique, l'analyse statistique et la théorie des graphes pour vous aider à visualiser et à mener des enquêtes de sécurité plus rapides et plus efficaces.

L'intégration de Security Hub CSPM à Detective vous permet de passer des GuardDuty résultats obtenus par Amazon dans Security Hub CSPM à Detective. Vous pouvez ensuite utiliser les outils Detective et les visualisations pour les étudier. L'intégration ne nécessite aucune configuration supplémentaire dans Security Hub CSPM ou Detective.

Pour les résultats provenant d'autres personnes Services AWS, le panneau des détails de la découverte de la console Security Hub CSPM comprend une sous-section Enquêter dans Detective. Cette sous-section contient un lien vers Detective où vous pouvez approfondir le problème de sécurité signalé par la découverte. Vous pouvez également créer un graphique de comportement dans Detective sur la base des résultats du Security Hub CSPM afin de mener des enquêtes plus efficaces. Pour plus d'informations, consultez les résultats AWS de sécurité dans le guide d'administration d'Amazon Detective.

Si l'agrégation interrégionale est activée, lorsque vous quittez la région d'agrégation, Detective ouvre dans la région d'origine du résultat.

Si un lien ne fonctionne pas et que vous souhaitez accéder à des conseils de dépannage, veuillez consulter la page relative au dépannage.

Amazon Security Lake (reçoit les résultats)

Security Lake est un service de lac de données de sécurité entièrement géré. Vous pouvez utiliser Security Lake pour centraliser automatiquement les données de sécurité provenant de sources cloud, locales et personnalisées dans un lac de données stocké sur votre compte. Les abonnés peuvent utiliser les données de Security Lake à des fins d'investigation et d'analyse de cas.

Pour activer cette intégration, vous devez activer les deux services et ajouter Security Hub CSPM comme source dans la console Security Lake, l'API Security Lake ou. AWS CLI Une fois ces étapes terminées, Security Hub CSPM commence à envoyer tous les résultats à Security Lake.

Security Lake normalise automatiquement les résultats du Security Hub CSPM et les convertit en un schéma open source standardisé appelé Open Cybersecurity Schema Framework (OCSF). Dans Security Lake, vous pouvez ajouter un ou plusieurs abonnés pour consulter les résultats du Security Hub CSPM.

Pour plus d'informations sur cette intégration, notamment des instructions sur l'ajout de Security Hub CSPM en tant que source et la création d'abonnés, consultez la section Intégration à AWS Security Hub CSPM dans le guide de l'utilisateur d'Amazon Security Lake.

AWS Systems Manager Explorer et OpsCenter (reçoit et met à jour les résultats)

AWS Systems Manager Explorez et OpsCenter recevez les résultats de Security Hub CSPM, puis mettez-les à jour dans Security Hub CSPM.

Explorer vous fournit un tableau de bord personnalisable qui fournit des informations et des analyses clés sur la santé opérationnelle et les performances de votre AWS environnement.

OpsCenter vous fournit un emplacement central pour visualiser, étudier et résoudre les tâches opérationnelles.

Pour plus d'informations sur Explorer et OpsCenter, consultez la section Gestion des opérations dans le Guide de AWS Systems Manager l'utilisateur.

AWS Trusted Advisor (Reçoit les résultats)

Trusted Advisor s'appuie sur les meilleures pratiques apprises au service de centaines de milliers de AWS clients. Trusted Advisor inspecte votre AWS environnement, puis formule des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité.

Lorsque vous activez Security Hub CSPM à la fois Trusted Advisor , l'intégration est automatiquement mise à jour.

Security Hub CSPM envoie les résultats de ses contrôles des meilleures pratiques AWS de sécurité fondamentales à. Trusted Advisor

Pour plus d'informations sur l'intégration de Security Hub CSPM avec Trusted Advisor, consultez la section Affichage des contrôles CSPM AWS de Security Hub AWS Trusted Advisor dans le Guide de l'utilisateur du AWS support.

Third-party intégrations de produits avec Security Hub CSPM

AWS Security Hub CSPM s'intègre à plusieurs produits partenaires tiers. Une intégration peut effectuer une ou plusieurs des actions suivantes :

- Envoyer les résultats qu'il génère au Security Hub CSPM
- Recevez les résultats du Security Hub CSPM
- Mettre à jour les résultats dans Security Hub CSPM

Les intégrations qui envoient les résultats au Security Hub CSPM possèdent un Amazon Resource Name (ARN).

Il se peut qu'une intégration ne soit pas disponible dans tous Régions AWS. Si une intégration n'est pas prise en charge dans la région à laquelle vous êtes actuellement connecté sur la console Security Hub CSPM, elle n'apparaît pas sur la page Intégrations de la console. Pour obtenir la liste des intégrations disponibles dans les régions de Chine et AWS GovCloud (US) Regions, consultezDisponibilité des intégrations par région.

Si vous disposez d'une solution de sécurité et souhaitez devenir partenaire de Security Hub CSPM, envoyez un e-mail à < `securityhub-partners@amazon.com.` > Pour plus d'informations, consultez le Guide d'intégration des partenaires.

Présentation des intégrations tierces avec Security Hub CSPM

Le tableau suivant fournit une vue d'ensemble des intégrations tierces qui peuvent envoyer des résultats à Security Hub CSPM ou recevoir des résultats de Security Hub CSPM.

Integration	Direction	ARN (le cas échéant)
3CORESec – 3CORESec NTA	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	Envoie les résultats	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`

Integration	Direction	ARN (le cas échéant)
Aqua Security – Aqua Cloud Native Security Platform	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench`
Armor – Armor Anywhere	Envoie les résultats	`arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere`
AttackIQ – AttackIQ	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform`
Barracuda Networks – Cloud Security Guardian	Envoie les résultats	`arn:aws:securityhub: <REGION>:151784055945:product/barracuda/cloudsecurityguardian`
BigID – BigID Enterprise	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise`
Blue Hexagon – Blue Hexagon forAWS	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Integration	Direction	ARN (le cas échéant)
Check Point – CloudGuard IaaS	Envoie les résultats	arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	Envoie les résultats	arn:aws:securityhub: *<REGION>*:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	Envoie les résultats	arn:aws:securityhub: *<REGION>*::product/claroty/xdome
Cloud Storage Security—Antivirus for Amazon S3	Envoie les résultats	arn:aws:securityhub: *<REGION>*::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	Envoie les résultats	arn:aws:securityhub: *<REGION>*::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	Envoie les résultats	arn:aws:securityhub: *<REGION>*:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	Envoie les résultats	arn:aws:securityhub: *<REGION>*:749430749651:product/cyberark/cyberark-pta

Integration	Direction	ARN (le cas échéant)
Data Theorem – Data Theorem	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`
Drata	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Envoie les résultats	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Envoie les résultats	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Envoie les résultats	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Integration	Direction	ARN (le cas échéant)
Fugue – Fugue	Envoie les résultats	arn:aws:securityhub: <REGION>::product/fugue/fugue
Guardicore – Centra 4.0	Envoie les résultats	arn:aws:securityhub: <REGION>::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	Envoie les résultats	arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	Envoie les résultats	arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	Envoie les résultats	arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	Envoie les résultats	arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer
Lacework – Lacework	Envoie les résultats	arn:aws:securityhub: <REGION>::product/lacework/lacework

Integration	Direction	ARN (le cas échéant)
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`
NETSCOUT – NETSCOUT Cyber Investigator	Envoie les résultats	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`
Palo Alto Networks – Prisma Cloud Compute	Envoie les résultats	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Envoie les résultats	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/prowler/prowler`

Integration	Direction	ARN (le cas échéant)
Qualys – Vulnerability Management	Envoie les résultats	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Envoie les résultats	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`
SentinelOne – SentinelOne	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	Envoie les résultats	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Envoie les résultats	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`

Integration	Direction	ARN (le cas échéant)
Sumo Logic – Machine Data Analytics	Envoie les résultats	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`
Symantec – Cloud Workload Protection	Envoie les résultats	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Envoie les résultats	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`
Trend Micro – Cloud One	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Envoie les résultats	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Envoie les résultats	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Reçoit et met à jour les résultats	Non applicable

Integration	Direction	ARN (le cas échéant)
Atlassian - Jira Service Management Cloud	Reçoit et met à jour les résultats	Non applicable
Atlassian – Opsgenie	Reçoit les résultats	Non applicable
Dynatrace	Reçoit les résultats	Non applicable
Elastic	Reçoit les résultats	Non applicable
Fortinet – FortiCNP	Reçoit les résultats	Non applicable
IBM – QRadar	Reçoit les résultats	Non applicable
Logz.io Cloud SIEM	Reçoit les résultats	Non applicable
MetricStream	Reçoit les résultats	Non applicable
MicroFocus – MicroFocus Arcsight	Reçoit les résultats	Non applicable
New Relic Vulnerability Management	Reçoit les résultats	Non applicable
PagerDuty – PagerDuty	Reçoit les résultats	Non applicable
Palo Alto Networks – Cortex XSOAR	Reçoit les résultats	Non applicable
Palo Alto Networks – VM-Series	Reçoit les résultats	Non applicable
Rackspace Technology – Cloud Native Security	Reçoit les résultats	Non applicable
Rapid7 – InsightConnect	Reçoit les résultats	Non applicable
RSA – RSA Archer	Reçoit les résultats	Non applicable

Integration	Direction	ARN (le cas échéant)
ServiceNow – ITSM	Reçoit et met à jour les résultats	Non applicable
Slack – Slack	Reçoit les résultats	Non applicable
Splunk – Splunk Enterprise	Reçoit les résultats	Non applicable
Splunk – Splunk Phantom	Reçoit les résultats	Non applicable
ThreatModeler	Reçoit les résultats	Non applicable
Trellix – Trellix Helix	Reçoit les résultats	Non applicable
Caveonix – Caveonix Cloud	Envoie et reçoit les résultats	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	Envoie et reçoit les résultats	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Envoie et reçoit les résultats	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Envoie et reçoit les résultats	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Envoie et reçoit les résultats	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Third-party intégrations qui envoient les résultats au Security Hub CSPM

Les intégrations de produits partenaires tiers suivantes peuvent envoyer des résultats à Security Hub CSPM. Security Hub CSPM transforme les résultats au format AWS Security Finding.

3 cœurs SEC – 3 cœurs SEC NTA

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESecfournit des services de détection gérés à la fois sur site et pour les AWS systèmes. Leur intégration à Security Hub CSPM offre une visibilité sur les menaces telles que les malwares, l'augmentation des privilèges, les mouvements latéraux et une segmentation réseau incorrecte.

Lien vers le produit

Documentation destinée aux partenaires

Alert Logic – Gestion des menaces sans SIEM

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Bénéficiez du niveau de couverture adéquat : visibilité des vulnérabilités et des actifs, détection des menaces et gestion des incidents AWS WAF, et options assignées aux analystes du SOC.

Lien vers le produit

Documentation destinée aux partenaires

Aqua Security – Aqua Cloud Native Security Platform

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)assure la sécurité du cycle de vie complet des applications basées sur des conteneurs et sans serveur, de votre CI/CD pipeline aux environnements de production d'exécution.

Lien vers le produit

Documentation destinée aux partenaires

Aqua Security – Kube-bench

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-benchest un outil open source qui exécute le benchmark Kubernetes du Center for Internet Security (CIS) par rapport à votre environnement.

Lien vers le produit

Documentation destinée aux partenaires

Armor – Armor Anywhere

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywherefournit une sécurité et une conformité gérées pour AWS.

Lien vers le produit

Documentation destinée aux partenaires

AttackIQ – AttackIQ

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformémule un véritable comportement contradictoire conformément au cadre MITRE ATT&CK pour vous aider à valider et à améliorer votre posture de sécurité globale.

Lien vers le produit

Documentation destinée aux partenaires

Barracuda Networks – Cloud Security Guardian

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentryaide les entreprises à rester en sécurité lors de la création d'applications et du transfert des charges de travail vers le cloud public.

AWS Lien vers le marché

Lien vers le produit

BigID – BigID Enterprise

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

Il BigID Enterprise Privacy Management Platform aide les entreprises à gérer et à protéger les données sensibles (PII) sur l'ensemble de leurs systèmes.

Lien vers le produit

Documentation destinée aux partenaires

Hexagone bleu – Hexagone bleu for AWS

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagonest une plateforme de détection des menaces en temps réel. Il utilise des principes d'apprentissage profond pour détecter les menaces connues et inconnues, notamment les malwares et les anomalies du réseau.

AWS Lien vers le marché

Documentation destinée aux partenaires

Point de contrôle – CloudGuard IaaS

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuardétend facilement la sécurité complète de prévention des menaces AWS tout en protégeant les actifs dans le cloud.

Lien vers le produit

Documentation destinée aux partenaires

Point de contrôle – CloudGuard Gestion de la posture

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Une plateforme SaaS qui assure une sécurité réseau cloud vérifiable, une protection IAM avancée, ainsi qu'une conformité et une gouvernance complètes.

Lien vers le produit

Documentation destinée aux partenaires

Clarté – Dôme

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomeaide les entreprises à sécuriser leurs systèmes cyberphysiques via l'Internet des objets étendu (XIoT) dans les environnements industriels (OT), de santé (IoMT) et d'entreprise (IoT).

Lien vers le produit

Documentation destinée aux partenaires

Sécurité du stockage dans le cloud – Antivirus pour Amazon S3

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securityfournit une analyse antivirus et anti-malware native du cloud pour les objets Amazon S3.

Antivirus for Amazon S3 propose des analyses planifiées et en temps réel des objets et des fichiers dans Amazon S3 pour détecter les programmes malveillants et les menaces. Il fournit une visibilité et une solution pour les fichiers problématiques et infectés.

Lien vers le produit

Documentation destinée aux partenaires

Sécurité du contraste — Contrast Assess

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assessest un outil IAST qui permet de détecter les vulnérabilités en temps réel dans les applications Web, les API et les microservices. Contrast Assesss'intègre à Security Hub CSPM pour fournir une visibilité et une réponse centralisées pour toutes vos charges de travail.

Lien vers le produit

Documentation destinée aux partenaires

CrowdStrike – CrowdStrike Faucon

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Le capteur CrowdStrike Falcon unique et léger unifie l'antivirus de nouvelle génération, la détection et la réponse des terminaux, ainsi que la 24/7 gestion de la recherche via le cloud.

AWS Lien vers le marché

Documentation destinée aux partenaires

CyberArk – Privileged Threat Analytics

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analyticscollectez, détectez, alertez et répondez aux activités et comportements à haut risque des comptes privilégiés afin de contenir les attaques en cours.

Lien vers le produit

Documentation destinée aux partenaires

Théorème des données – Théorème des données

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremanalyse en permanence les applications Web, les API et les ressources cloud à la recherche de failles de sécurité et de confidentialité des données afin de prévenir les violations de AppSec données.

Lien vers le produit

Documentation destinée aux partenaires

Drata

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataest une plateforme d'automatisation de la conformité qui vous aide à atteindre et à maintenir la conformité avec divers cadres, tels que SOC2, ISO et GDPR. L'intégration entre Drata et Security Hub CSPM vous permet de centraliser vos résultats de sécurité en un seul endroit.

AWS Lien vers le marché

Documentation destinée aux partenaires

Forcepoint – Forcepoint CASB

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBvous permet de découvrir l'utilisation des applications cloud, d'analyser les risques et d'appliquer les contrôles appropriés pour les applications SaaS et personnalisées.

Lien vers le produit

Documentation destinée aux partenaires

Forcepoint – Passerelle de sécurité Forcepoint Cloud

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gatewayest un service de sécurité cloud convergent qui fournit visibilité, contrôle et protection contre les menaces aux utilisateurs et aux données, où qu'ils se trouvent.

Lien vers le produit

Documentation destinée aux partenaires

Forcepoint – Forcepoint DLP

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPrépond aux risques centrés sur l'humain en offrant visibilité et contrôle partout où travaillent vos employés et où se trouvent vos données.

Lien vers le produit

Documentation destinée aux partenaires

Forcepoint – Forcepoint NGFW

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWvous permet de connecter votre AWS environnement au réseau de votre entreprise avec l'évolutivité, la protection et les informations nécessaires pour gérer votre réseau et répondre aux menaces.

Lien vers le produit

Documentation destinée aux partenaires

Fugue – Fugue

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueest une plateforme cloud native évolutive et sans agent qui automatise la validation continue des environnements d'infrastructure en tant que code et d'exécution dans le cloud en utilisant les mêmes politiques.

Lien vers le produit

Documentation destinée aux partenaires

Guardicore – Centra 4.0

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centrafournit la visualisation des flux, la microsegmentation et la détection des violations pour les charges de travail dans les centres de données et les clouds modernes.

Lien vers le produit

Documentation destinée aux partenaires

HackerOne – Renseignements sur les vulnérabilités

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

La HackerOne plateforme travaille en partenariat avec la communauté mondiale des hackers pour découvrir les problèmes de sécurité les plus pertinents. Vulnerability Intelligencepermet à votre

organisation d'aller au-delà de la numérisation automatique. Il partage des vulnérabilités que des pirates HackerOne éthiques ont validées et ont proposé des étapes pour les reproduire.

AWS lien vers le marché

Documentation destinée aux partenaires

J Frog – Radiographie

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xrayest un outil universel d'analyse de la composition logicielle (SCA) de sécurité des applications qui analyse en permanence les fichiers binaires pour détecter la conformité des licences et les failles de sécurité afin que vous puissiez gérer une chaîne d'approvisionnement logicielle sécurisée.

AWS Lien vers le marché

Documentation destinée aux partenaires

Réseaux Juniper – Pare-feu vSRX de nouvelle génération

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'Le pare-feu virtuel de nouvelle génération vSRX fournit un pare-feu virtuel complet basé sur le cloud avec une sécurité avancée, une mise en réseau sécurisée SD-WAN et robuste et une automatisation intégrée.

AWS Lien vers le marché

Documentation destinée aux partenaires

Lien vers le produit

k9 Sécurité – Analyseur d'accès

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securityvous avertit lorsque des changements d'accès importants se produisent dans votre Gestion des identités et des accès AWS compte. Aveck9 Security, vous pouvez comprendre l'accès des utilisateurs et des rôles IAM aux données critiques Services AWS et à vos données.

k9 Securityest conçu pour une livraison continue, vous permettant d'opérationnaliser l'IAM grâce à des audits d'accès exploitables et à une automatisation simple des politiques pour AWS CDK et Terraform.

Lien vers le produit

Documentation destinée aux partenaires

Dentelle – Dentelle

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Laceworkest la plateforme de sécurité axée sur les données pour le cloud. La plateforme de sécurité cloud Lacework automatise la sécurité du cloud à grande échelle afin que vous puissiez innover rapidement et en toute sécurité.

Lien vers le produit

Documentation destinée aux partenaires

McAfee – Plateforme de protection des applications natives MVISION Cloud (CNAPP)

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)propose la gestion de la posture de sécurité dans le cloud (CSPM) et la plateforme de protection de la charge de travail dans le cloud (CWPP) pour votre environnement. AWS

Lien vers le produit

Documentation destinée aux partenaires

NETSCOUT – Cyberenquêteur NETSCOUT

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigatorest une plateforme d'analyse des menaces réseau, d'investigation des risques et d'analyse forensique à l'échelle de l'entreprise qui contribue à réduire l'impact des cybermenaces sur les entreprises.

Lien vers le produit

Documentation destinée aux partenaires

Plateforme de sécurité Orca Cloud

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Il Orca Cloud Security Platform identifie, hiérarchise et corrige les risques et les problèmes de conformité sur l'ensemble de votre parc cloud. Orca'sPrivilégiant les agents, la AI-driven plateforme offre une couverture complète en détectant les vulnérabilités, les mauvaises configurations, les mouvements latéraux, les risques liés aux API, les données sensibles, les événements et comportements anormaux et les identités trop permissives.

Orcas'intègre à Security Hub CSPM pour intégrer une télémétrie de sécurité cloud approfondie dans Security Hub CSPM. Orca, à l'aide de sa SideScanning technologie, hiérarchise les risques liés à l'infrastructure cloud, aux charges de travail, aux applications, aux données, aux API, aux identités, etc.

Lien vers le produit

Documentation destinée aux partenaires

Palo Alto Networks – Informatique en nuage Prisma

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Computeest une plateforme de cybersécurité native du cloud qui protège les machines virtuelles, les conteneurs et les plateformes sans serveur.

Lien vers le produit

Documentation destinée aux partenaires

Palo Alto Networks – Prisma Cloud Enterprise

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Protège votre AWS déploiement grâce à des analyses de sécurité dans le cloud, à une détection avancée des menaces et à une surveillance de la conformité.

Lien vers le produit

Documentation destinée aux partenaires

Plérion – Plateforme de sécurité dans le cloud

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerionest une plateforme de sécurité cloud dotée d'une approche unique axée sur les menaces et les risques qui propose des mesures préventives, de détection et de correction sur l'ensemble de vos charges de travail. L'intégration entre Security Hub CSPM Plerion et Security Hub permet aux clients de centraliser leurs résultats de sécurité et d'y donner suite en un seul endroit.

AWS Lien vers le marché

Documentation destinée aux partenaires

Rondeur – Rondeur

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowlerest un outil de sécurité open source permettant d'effectuer AWS des contrôles liés aux meilleures pratiques de sécurité, au renforcement et à la surveillance continue.

Lien vers le produit

Documentation destinée aux partenaires

Qualys – Vulnerability Management

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)analyse et identifie en permanence les vulnérabilités, protégeant ainsi vos actifs.

Lien vers le produit

Documentation destinée aux partenaires

Rapid7 – InsightVM

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVMfournit une gestion des vulnérabilités pour les environnements modernes, vous permettant de détecter, de hiérarchiser et de corriger efficacement les vulnérabilités.

Lien vers le produit

Documentation destinée aux partenaires

SentinelOne – SentinelOne

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOneest une plateforme autonome de détection et de réponse étendues (XDR) qui englobe AI-powered la prévention, la détection, la réponse et la recherche sur les terminaux, les conteneurs, les charges de travail cloud et les appareils IoT.

AWS Lien vers le marché

Lien vers le produit

Snyk

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snykfournit une plate-forme de sécurité qui analyse les composants de l'application pour détecter les risques de sécurité liés aux charges de travail exécutées sur AWS. Ces risques sont envoyés au Security Hub CSPM sous forme de résultats, ce qui permet aux développeurs et aux équipes de sécurité de les visualiser et de les hiérarchiser, ainsi que le reste de leurs résultats de AWS sécurité.

AWS Lien vers le marché

Documentation destinée aux partenaires

Sécurité Sonrai – Sonari Dig

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digsurveille et corrige les erreurs de configuration du cloud et les violations des politiques, afin que vous puissiez améliorer votre niveau de sécurité et de conformité.

Lien vers le produit

Documentation destinée aux partenaires

Sophos – Server Protection

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectiondéfend les applications et les données critiques au cœur de votre organisation, à l'aide de techniques complètes de défense en profondeur.

Lien vers le produit

StackRox – StackRox Sécurité Kubernetes

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRoxaide les entreprises à sécuriser leurs déploiements de conteneurs et de Kubernetes à grande échelle en appliquant leurs politiques de conformité et de sécurité tout au long du cycle de vie des conteneurs : création, déploiement et exécution.

Lien vers le produit

Documentation destinée aux partenaires

Sumo Logic – Machine Data Analytics

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logicest une plateforme sécurisée d'analyse des données machine qui permet aux équipes de développement et des opérations de sécurité de créer, d'exécuter et de sécuriser leurs AWS applications.

Lien vers le produit

Documentation destinée aux partenaires

Symantec – Cloud Workload Protection

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protectionfournit une protection complète à vos instances Amazon EC2 avec un antimalware, une prévention des intrusions et une surveillance de l'intégrité des fichiers.

Lien vers le produit

Documentation destinée aux partenaires

Tenable – Tenable.io

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Identifier, rechercher et hiérarchiser avec précision les vulnérabilités. Géré dans le cloud.

Lien vers le produit

Documentation destinée aux partenaires

Trend Micro – Cloud 1

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud Onefournit les bonnes informations de sécurité aux équipes au bon moment et au bon endroit. Cette intégration envoie les résultats de sécurité au Security Hub CSPM en temps réel, améliorant ainsi la visibilité de vos AWS ressources et des détails des Trend Micro Cloud One événements dans Security Hub CSPM.

AWS Lien vers le marché

Documentation destinée aux partenaires

Vectra – Cognito Detect

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectratransforme la cybersécurité en appliquant une IA avancée pour détecter les cyberattaquants cachés et y répondre avant qu'ils ne volent ou ne causent des dommages.

AWS Lien vers le marché

Documentation destinée aux partenaires

Wiz – Sécurité Wiz

Type d'intégration : Envoyer

ARN du produit : `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizanalyse en permanence les configurations, les vulnérabilités, les réseaux, les paramètres IAM, les secrets, etc. concernant vos Comptes AWS utilisateurs et vos charges de travail afin de découvrir les problèmes critiques qui représentent un risque réel. Intégrez Wiz à Security Hub CSPM pour visualiser et résoudre les problèmes détectés par Wiz depuis la console Security Hub CSPM.

AWS Lien vers le marché

Documentation destinée aux partenaires

Third-party intégrations qui reçoivent les résultats du Security Hub CSPM

Les intégrations de produits partenaires tiers suivantes peuvent recevoir des résultats de Security Hub CSPM. Le cas échéant, le produit peut également mettre à jour les résultats. Dans ce cas, les mises à jour que vous apportez aux résultats du produit partenaire sont également reflétées dans Security Hub CSPM.

Atlassian - Gestion des services Jira

Type d'intégration : réception et mise à jour

Le Connecteur AWS Service Management formulaire Jira envoie les résultats du Security Hub CSPM à. Jira Jirades problèmes sont créés sur la base des résultats. Lorsque les Jira problèmes sont mis à jour, les résultats correspondants sont mis à jour dans Security Hub CSPM.

L'intégration ne prend en charge que Jira Server et Jira Data Center.

Pour un aperçu de l'intégration et de son fonctionnement, regardez la vidéo AWS Security Hub CSPM — Intégration bidirectionnelle avec. Atlassian Jira Service Management

Lien vers le produit

Documentation destinée aux partenaires

Atlassian - Jira Service Management Cloud

Type d'intégration : réception et mise à jour

Jira Service Management Cloudest le composant cloud de Jira Service Management.

Le Connecteur AWS Service Management formulaire Jira envoie les résultats du Security Hub CSPM à. Jira Les résultats déclenchent la création de problèmes dansJira Service Management Cloud. Lorsque vous mettez à jour ces problèmes dansJira Service Management Cloud, les résultats correspondants sont également mis à jour dans Security Hub CSPM.

Lien vers le produit

Documentation destinée aux partenaires

Atlassian – Opsgénie

Type d'intégration : Réception

Opsgenieest une solution moderne de gestion des incidents permettant de gérer des services permanents, permettant aux équipes de développement et d'exploitation de planifier les interruptions de service et de garder le contrôle en cas d'incidents.

L'intégration à Security Hub CSPM garantit que les incidents critiques liés à la sécurité sont acheminés vers les équipes appropriées pour une résolution immédiate.

Lien vers le produit

Documentation destinée aux partenaires

Dynatrace

Type d'intégration : Réception

L'Dynatraceintégration avec Security Hub CSPM permet d'unifier, de visualiser et d'automatiser les résultats de sécurité entre les outils et les environnements. L'ajout Dynatrace d'un contexte d'exécution aux résultats de sécurité permet une hiérarchisation plus intelligente, contribue à réduire le bruit généré par les alertes et permet à vos DevSecOps équipes de se concentrer sur la résolution efficace des problèmes critiques qui affectent vos environnements de production et vos applications.

Lien vers le produit

Documentation destinée aux partenaires

Elasticité

Type d'intégration : Réception

Elasticdéveloppe des solutions basées sur la recherche pour la sécurité, l'observabilité et la recherche. Grâce à l'intégration de Security Hub CSPM, Elastic ingère les résultats et les informations de Security Hub CSPM par programmation, les normalise à des fins de corrélation et d'analyse, et présente des tableaux de bord et des détections unifiés, permettant un triage et une investigation plus rapides sans déployer d'agents. Elastic Security

Lien vers le produit

Documentation destinée aux partenaires

Fortinet – pour TICNP

Type d'intégration : Réception

FortiCNPest un produit Cloud Native Protection qui regroupe les résultats de sécurité en informations exploitables et hiérarchise les informations de sécurité en fonction du score de risque afin de réduire la fatigue liée aux alertes et d'accélérer les mesures correctives.

AWS Lien vers le marché

Documentation destinée aux partenaires

IBM – QRadar

Type d'intégration : Réception

IBM QRadarLe SIEM permet aux équipes de sécurité de détecter, de hiérarchiser, d'étudier et de répondre aux menaces de manière rapide et précise.

Lien vers le produit

Documentation destinée aux partenaires

Logz.io SIEM dans le cloud

Type d'intégration : Réception

Logz.ioest un fournisseur Cloud SIEM qui fournit une corrélation avancée des données de journal et d'événements pour aider les équipes de sécurité à détecter, analyser et répondre aux menaces de sécurité en temps réel.

Lien vers le produit

Documentation destinée aux partenaires

MetricStream – CyberGRC

Type d'intégration : Réception

MetricStream CyberGRCvous aide à gérer, mesurer et atténuer les risques de cybersécurité. En recevant les résultats de Security Hub CSPM, vous CyberGRC bénéficiez d'une meilleure visibilité sur ces risques, ce qui vous permet de hiérarchiser les investissements en cybersécurité et de vous conformer aux politiques informatiques.

AWS Lien vers le marché

Lien vers le produit

MicroFocus – MicroFocus Viseur à arc

Type d'intégration : Réception

ArcSightaccélère la détection efficace des menaces et la réponse en temps réel, en intégrant la corrélation des événements et des analyses supervisées et non supervisées à l'automatisation et à l'orchestration des réponses.

Lien vers le produit

Documentation destinée aux partenaires

Gestion des vulnérabilités de New Relic

Type d'intégration : Réception

New Relic Vulnerability Managementreçoit les résultats de sécurité du Security Hub CSPM, afin que vous puissiez obtenir une vue centralisée de la sécurité ainsi qu'une télémétrie des performances en contexte sur l'ensemble de votre stack.

AWS Lien vers le marché

Documentation destinée aux partenaires

PagerDuty – PagerDuty

Type d'intégration : Réception

La plateforme de gestion des opérations PagerDuty numériques permet aux équipes d'atténuer de manière proactive les problèmes qui ont un impact sur les clients en transformant automatiquement tout signal en informations et en actions appropriées.

AWS les utilisateurs peuvent utiliser l'PagerDutyensemble d' AWS intégrations pour faire évoluer leurs environnements AWS et leurs environnements hybrides en toute confiance.

Associé aux alertes de sécurité agrégées et organisées de Security Hub CSPM, il PagerDuty permet aux équipes d'automatiser leur processus de réponse aux menaces et de mettre en place rapidement des actions personnalisées pour prévenir les problèmes potentiels.

PagerDutyles utilisateurs qui entreprennent un projet de migration vers le cloud peuvent agir rapidement, tout en réduisant l'impact des problèmes survenant tout au long du cycle de vie de la migration.

Lien vers le produit

Documentation destinée aux partenaires

Palo Alto Networks – Cortex XSOAR

Type d'intégration : Réception

Cortex XSOARest une plateforme SOAR (Security Orchestration, Automation, and Response) qui s'intègre à l'ensemble de votre gamme de produits de sécurité pour accélérer la réponse aux incidents et les opérations de sécurité.

Lien vers le produit

Documentation destinée aux partenaires

Palo Alto Networks – VM-Series

Type d'intégration : Réception

Palo Alto VM-SeriesL'intégration à Security Hub CSPM collecte des informations sur les menaces et les envoie au pare-feu de VM-Series nouvelle génération sous forme de mise à jour automatique de la politique de sécurité qui bloque les activités malveillantes des adresses IP.

Lien vers le produit

Documentation destinée aux partenaires

Technologie Rackspace – Sécurité du cloud natif

Type d'intégration : Réception

Rackspace Technology fournit des services de sécurité gérés en plus des produits de AWS sécurité natifs pour une surveillance 24 h/24, 7 j/7 et 365 j/7 par le Rackspace SOC, une analyse avancée et la correction des menaces.

Lien vers le produit

Rapid7 – InsightConnect

Type d'intégration : Réception

Rapid7 InsightConnectest une solution d'orchestration et d'automatisation de la sécurité qui permet à votre équipe d'optimiser les opérations du SOC avec peu ou pas de code.

Lien vers le produit

Documentation destinée aux partenaires

RSA – Archer RSA

Type d'intégration : Réception

RSA ArcherLa gestion des risques informatiques et de sécurité vous permet de déterminer quels actifs sont essentiels pour votre entreprise, d'établir et de communiquer des politiques et des normes de sécurité, de détecter les attaques et d'y répondre, d'identifier et de corriger les failles de sécurité et d'établir des bonnes pratiques claires en matière de gestion des risques informatiques.

Lien vers le produit

Documentation destinée aux partenaires

ServiceNow – ITSM

Type d'intégration : réception et mise à jour

L'ServiceNowintégration avec Security Hub CSPM permet de visualiser les résultats de sécurité du Security Hub CSPM. ServiceNow ITSM Vous pouvez également configurer ServiceNow pour créer automatiquement un incident ou un problème lorsqu'il reçoit un résultat de Security Hub CSPM.

Toute mise à jour de ces incidents et problèmes entraîne la mise à jour des résultats dans Security Hub CSPM.

Pour un aperçu de l'intégration et de son fonctionnement, regardez la vidéo AWS Security Hub CSPM - Intégration bidirectionnelle avec. ServiceNow ITSM

Lien vers le produit

Documentation destinée aux partenaires

Slack – Slack

Type d'intégration : Réception

Slackest une couche de la pile technologique de l'entreprise qui réunit les personnes, les données et les applications. Il s'agit d'un endroit unique où les personnes peuvent travailler ensemble efficacement, trouver des informations importantes et accéder à des centaines de milliers d'applications et de services essentiels pour faire de leur mieux.

Lien vers le produit

Documentation destinée aux partenaires

Splunk – Splunk Enterprise

Type d'intégration : Réception

Splunkutilise Amazon CloudWatch Events pour recueillir les résultats de Security Hub CSPM. Envoyez vos données à Splunk pour bénéficier d'analyses de sécurité avancées et d'un SIEM.

Lien vers le produit

Documentation destinée aux partenaires

Splunk – Splunk Phantom

Type d'intégration : Réception

Avec l'Splunk Phantomapplication pour AWS Security Hub CSPM, les résultats sont envoyés Phantom pour un enrichissement automatique du contexte avec des informations supplémentaires sur les menaces ou pour effectuer des actions de réponse automatisées.

Lien vers le produit

Documentation destinée aux partenaires

ThreatModeler

Type d'intégration : Réception

ThreatModelerest une solution automatisée de modélisation des menaces qui sécurise et fait évoluer le cycle de développement des logiciels d'entreprise et du cloud.

Lien vers le produit

Documentation destinée aux partenaires

Trellix – Hélice Trellix

Type d'intégration : Réception

Trellix Helixest une plateforme d'opérations de sécurité hébergée dans le cloud qui permet aux entreprises de prendre le contrôle de tout incident, de l'alerte à la résolution.

Lien vers le produit

Documentation destinée aux partenaires

Third-party intégrations qui envoient des résultats à Security Hub CSPM et en reçoivent

Les intégrations de produits partenaires tiers suivantes peuvent envoyer des résultats à Security Hub CSPM et en recevoir des résultats.

Caveonix – Nuage de Cavéonix

Type d'intégration : Envoyer et recevoir

ARN du produit : `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

La Caveonix AI-powered plateforme automatise la visibilité, l'évaluation et l'atténuation dans les clouds hybrides, couvrant les services natifs du cloud, les machines virtuelles et les conteneurs. Intégré à AWS Security Hub CSPM, il Caveonix fusionne les AWS données et les analyses avancées pour obtenir des informations sur les alertes de sécurité et la conformité.

AWS Lien vers le marché

Documentation destinée aux partenaires

Cloud Custodian – Cloud Custodian

Type d'intégration : Envoyer et recevoir

ARN du produit : `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodianpermet aux utilisateurs d'être bien gérés dans le cloud. Le DSL YAML simple permet de définir facilement des règles pour permettre une infrastructure cloud bien gérée, à la fois sécurisée et optimisée en termes de coûts.

Lien vers le produit

Documentation destinée aux partenaires

DisruptOps, Inc. – DisruptOPS

Type d'intégration : Envoyer et recevoir

ARN du produit : `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

La DisruptOps Security Operations Platform aide les entreprises à appliquer les meilleures pratiques de sécurité dans leur cloud grâce à l'utilisation de garde-corps automatisés.

Lien vers le produit

Documentation destinée aux partenaires

Kion

Type d'intégration : Envoyer et recevoir

ARN du produit : `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(anciennement cloudtamer.io) est une solution complète de gouvernance du cloud pour. AWSKiondonne aux parties prenantes une visibilité sur les opérations du cloud et aide les utilisateurs du cloud à gérer les comptes, à contrôler le budget et les coûts et à garantir une conformité continue.

Lien vers le produit

Documentation destinée aux partenaires

Turbot – Turbot

Type d'intégration : Envoyer et recevoir

ARN du produit : `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotgarantit que votre infrastructure cloud est sécurisée, conforme, évolutive et optimisée en termes de coûts.

Lien vers le produit

Documentation destinée aux partenaires

Intégrer Security Hub CSPM à des produits personnalisés

Outre les résultats générés par des AWS services intégrés et des produits tiers, AWS Security Hub CSPM peut utiliser les résultats générés par d'autres produits de sécurité personnalisés.

Vous pouvez envoyer ces résultats à Security Hub CSPM en utilisant l'API BatchImportFindings Security Hub CSPM. Vous pouvez utiliser la même opération pour mettre à jour les résultats des produits personnalisés que vous avez déjà envoyés à Security Hub CSPM.

Lorsque vous configurez l'intégration personnalisée, suivez les instructions et les listes de contrôle fournies dans le Guide d'intégration des partenaires CSPM de Security Hub.

Exigences et recommandations pour les intégrations de produits personnalisées

Avant de pouvoir appeler correctement l'opération d'`BatchImportFindings`API, vous devez activer Security Hub CSPM.

Vous devez également fournir des informations de recherche pour le produit personnalisé à l'aide duthe section called "Format de recherche : ASFF". Consultez les exigences et recommandations suivantes pour les intégrations de produits personnalisées :

Définition de l'ARN du produit

Lorsque vous activez Security Hub CSPM, un produit Amazon Resource Name (ARN) par défaut pour Security Hub CSPM est généré sur votre compte actuel.

Le format de l'ARN de ce produit est le suivant : `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. Par exemple, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Utilisez l'ARN de ce produit comme valeur de l'attribut `ProductArn` lorsque vous appelez l'opération d'API `BatchImportFindings`.

Définition du nom de l'entreprise et du produit

Vous pouvez les utiliser `BatchImportFindings` pour définir un nom de société et un nom de produit préférés pour l'intégration personnalisée qui envoie les résultats à Security Hub CSPM.

Les noms que vous avez spécifiés remplacent le nom de l'entreprise et le nom du produit préconfigurés, appelés respectivement nom personnel et nom par défaut, et apparaissent dans la console Security Hub CSPM et dans le JSON de chaque résultat. Consultez BatchImportFindings pour trouver des prestataires.

Définition des ID de résultat

Vous devez fournir, gérer et incrémenter vos propres ID de résultat à l'aide de l'attribut `Id`.

Chaque nouvelle découverte doit avoir un identifiant de découverte unique. Si le produit personnalisé envoie plusieurs résultats avec le même identifiant de recherche, Security Hub CSPM ne traite que le premier résultat.

Définition de l'ID de compte

Vous devez spécifier votre propre ID de compte à l'aide de l'attribut `AwsAccountId`.

Définition des dates de création et de mise à jour

Vous devez fournir vos propres horodatages pour les attributs `CreatedAt` et `UpdatedAt`.

Importation de résultats à partir de produits personnalisés

En plus d'envoyer de nouveaux résultats provenant de produits personnalisés, vous pouvez également utiliser l'opération d'API `BatchImportFindings` pour mettre à jour les résultats existants provenant de produits personnalisés.

Pour mettre à jour les résultats existants, utilisez l'ID de résultat existant (attribut `Id`). Renvoyez le résultat complet avec les informations appropriées mises à jour dans la demande, y compris un horodatage `UpdatedAt` modifié.

Exemples d'intégrations personnalisées

Vous pouvez utiliser les exemples d'intégrations de produits personnalisés suivants comme guide pour créer vos propres solutions personnalisées :

Envoi des résultats des Chef InSpec scans au Security Hub CSPM

Vous pouvez créer un CloudFormation modèle qui exécute une analyse de Chef InSpec conformité, puis envoie les résultats à Security Hub CSPM.

Pour plus de détails, consultez la section Surveillance continue de la conformité avec Chef InSpecAWS Security Hub CSPM.

Envoi des vulnérabilités de conteneurs détectées par Trivy Security Hub CSPM

Vous pouvez créer un CloudFormation modèle qui permet de scanner AquaSecurity Trivy les conteneurs à la recherche de vulnérabilités, puis d'envoyer les résultats de ces vulnérabilités à Security Hub CSPM.

Pour plus de détails, consultez Comment créer un CI/CD pipeline pour l'analyse des vulnérabilités des conteneurs avec TrivyAWS Security Hub CSPM.

Intégration du Security Hub CSPM à Microsoft Azure

Pour surveiller vos ressources Microsoft Azure, vous pouvez intégrer Microsoft Azure à AWS Security Hub CSPM. Security Hub CSPM active ensuite automatiquement les contrôles de gestion de posture pour votre environnement Azure et génère des résultats sur votre environnement. Plus précisément, le service vous fournit les services suivants :

> **Note**
>
> Vous pouvez gérer les normes et les contrôles Azure à l'aide de la console Security Hub CSPM, des API et. AWS CloudFormation La fonctionnalité de configuration centrale du Security Hub CSPM n'est pas prise en charge par les normes Azure.

- Résultats ASFF — Security Hub CSPM génère des résultats au format ASFF (AWS Security Finding Format) pour les contrôles de posture qu'il effectue pour vos ressources Azure.
- CIS Microsoft Azure Foundations Benchmark v4.0 — Contrôles de conformité automatisés par rapport à la norme CIS Azure v4.0. Cette norme inclut les contrôles d'identité, de mise en réseau, de stockage, de journalisation et de base de données.
- Meilleures pratiques de base Azure : détection automatique des erreurs de configuration des ressources Azure sur la base des meilleures pratiques de AWS sécurité répertoriées concernant la sécurité du réseau, la gestion des identités, la protection des données et la journalisation.
- Gestion de la posture : évaluation continue des configurations des ressources Azure par rapport aux meilleures pratiques de sécurité et aux normes de conformité, avec 122 contrôles pour les deux normes.
- Per-provider scores de sécurité — Séparez les scores de sécurité pour Azure AWS et pour que vous puissiez suivre chaque environnement indépendamment.

Pour créer l'intégration, vous devez connecter votre environnement Azure à Security Hub CSPM en suivant le processus suivant :

> **Note**
>
> Les normes Azure diffèrent des AWS normes sur les points suivants :
>
> - Les normes Azure ne nécessitent pas de AWS Config prérequis manuels. Contrairement aux AWS cas où CSPM-only les clients ont besoin d'un enregistreur géré par le client, les normes Azure utilisent automatiquement un enregistreur interne lié à un service.
> - Les normes Azure utilisent toujours des règles de configuration internes liées aux services. AWS les standards n'utilisent les règles de configuration liées aux services que lorsque Security Hub est également activé.

1. Vous configurez votre environnement Azure avec un enregistrement d'application, des informations d'identification d'identité fédérées, des attributions de rôles Azure et une infrastructure Event Hub.
2. À l'aide de la console Security Hub CSPM, vous créez un connecteur pour l'intégration. Vous spécifiez votre identifiant de locataire Azure, votre identifiant de client d'application et votre étendue de surveillance.
3. AWS Config collecte les données de configuration des ressources à partir de votre environnement Azure.

   AWS Config est utilisé en interne pour collecter les données de configuration des ressources. Contrairement à AWS la gestion des postures, pour laquelle vous devez explicitement activer AWS Config et payer pour l'enregistrement, la gestion des postures Azure s'en charge AWS Config automatiquement. Vous n'avez pas besoin d'activer AWS Config séparément, de configurer un enregistreur ou de payer séparément pour AWS Config l'utilisation. Ces coûts sont inclus dans la tarification de votre Security Hub CSPM.
4. Security Hub CSPM commence à recevoir les données de configuration des ressources et les événements du journal d'activité de votre environnement Azure.
5. Security Hub CSPM génère des résultats de gestion de posture concernant votre environnement Azure.

Comment ? AWS Config est utilisé

AWS Config est utilisé en interne pour collecter les données de configuration des ressources et détecter les modifications dans votre environnement Azure. Le connecteur gère cela automatiquement. Vous n'avez pas besoin de l'activer AWS Config séparément, de configurer un enregistreur ou de payer pour AWS Config l'utilisation. Ces coûts sont inclus dans la tarification CSPM de votre Security Hub pour les ressources Azure.

Service-linked connecteurs et connecteurs gérés par le client

Security Hub CSPM prend en charge deux types de connecteurs :

Service-linked connecteur (SLC)

Créé automatiquement lorsque vous configurez l'intégration Azure dans Security Hub. L'étendue d'un connecteur lié à un service correspond toujours à celle définie dans votre connecteur Security Hub. Vous ne pouvez pas modifier directement l'étendue d'un connecteur lié à un service ; modifiez plutôt l'étendue dans Security Hub. Security Hub gère le cycle de vie des connecteurs liés aux services en votre nom.

Customer-managed connecteur (CMC)

Créé directement dans la console Security Hub CSPM sur la page Intégrations. Utilisez un connecteur géré par le client lorsque vous souhaitez utiliser Security Hub CSPM indépendamment de Security Hub, ou lorsque vous avez besoin d'une portée différente de celle de votre connecteur Security Hub. Lorsque les deux types existent, l'étendue du connecteur lié au service doit toujours être égale ou supérieure à celle du connecteur géré par le client.

> **Note**
>
> Contrairement à Security Hub, Security Hub CSPM ne propose pas de sélection par fonctionnalité pour les connecteurs Azure. Lorsque vous créez un connecteur dans Security Hub CSPM, toutes les fonctionnalités de gestion de posture sont activées ensemble.

Pour plus d'informations sur l'estimation et le calcul des coûts liés à l'intégration de Security Hub CSPM à Azure, consultez la section Tarification AWS de Security Hub CSPM.

Rubriques

- Conditions préalables à l'intégration de Security Hub CSPM à Microsoft Azure
- Configuration de Microsoft Azure pour l'intégrer à Security Hub CSPM
- Configuration du Security Hub CSPM pour l'intégrer à Microsoft Azure
- Suppression d'un connecteur Microsoft Azure dans Security Hub CSPM

Conditions préalables à l'intégration de Security Hub CSPM à Microsoft Azure

Avant d'intégrer Microsoft Azure à AWS Security Hub CSPM, effectuez les tâches suivantes dans votre environnement AWS et dans celui d'Azure. Cela permet de garantir que vous et Security Hub CSPM disposez des ressources et des autorisations dont vous avez besoin pour surveiller vos ressources Azure.

Rubriques

- Prérequis pour AWS
- Conditions requises pour Microsoft Azure

Prérequis pour AWS

Vérifiez que vous avez les éléments suivants dans votre Compte AWS :

AWS Security Hub CSPM activé

Security Hub CSPM doit être activé dans le connecteur Compte AWS et à l' Région AWS endroit où vous souhaitez créer le connecteur.

Autorisations IAM sur console

Le principal IAM qui crée le connecteur doit disposer des autorisations suivantes :

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

Fédération d'identité sortante IAM activée

Vous devez activer la fédération d'identité sortante IAM dans votre. Compte AWS Cette fonctionnalité permet aux AWS services de s'authentifier auprès de fournisseurs d'identité

externes (tels que Microsoft Entra ID) à l'aide d'informations d'identification fédérées plutôt que de secrets de longue durée.

Après avoir activé la fédération des identités sortantes, notez l'URL de l'émetteur du jeton. Cette URL suit le format suivant :

```
https://uuid.tokens.sts.global.api.aws
```

Vous aurez besoin de cette URL pour configurer les informations d'identification fédérées dans Azure.

Conditions requises pour Microsoft Azure

Vérifiez que vous disposez des éléments suivants dans votre environnement Azure :

Locataire Azure

Vous devez disposer d'un client Azure dans le cloud commercial Azure. Azure Government et Azure Chine ne sont pas pris en charge.

Disponibilité du journal Microsoft Entra ID

L'enregistrement des ressources nécessite les journaux d'audit Microsoft Graph et les journaux de connexion de votre client Microsoft Entra ID. Certains journaux Microsoft Entra ID nécessitent une licence Microsoft Entra ID P1 ou P2.

Si le locataire ne dispose pas des journaux requis, l'enregistrement des ressources peut signaler des défaillances partielles. L'enregistrement de l'application et les attributions de rôles Azure ne fournissent pas de données de journal manquantes.

Rôle d'administrateur global

La personne qui configure l'environnement Azure doit avoir le rôle d'administrateur global dans Microsoft Entra ID. Ce rôle est requis pour enregistrer les applications, accorder le consentement de l'administrateur aux autorisations de l'API Microsoft Graph, attribuer des rôles RBAC dans le cadre du groupe de gestion racine du locataire et configurer les paramètres de diagnostic pour les journaux d'audit Entra ID.

> **Note**
>
> Dans de nombreuses organisations, l'administrateur global Azure et l'administrateur AWS de sécurité sont des personnes différentes. La configuration d'Azure peut être réalisée indépendamment à l'aide du script de configuration généré.

Enregistrement de l'application Azure

Vous devez enregistrer une application dans Microsoft Entra ID. Cette application sert d'identité qui AWS permet de s'authentifier auprès de votre environnement Azure à l'aide d'informations d'identification fédérées. Aucun secret client n'est requis.

Hub d'événements Azure

Vous devez créer un espace de noms Azure Event Hub et une instance Event Hub pour recevoir les événements du journal d'activité et du journal d'audit Entra ID. Le script de configuration automatise cette création.

Autorisations relatives à l'API Microsoft Graph

L'application enregistrée nécessite les autorisations d'API Microsoft Graph suivantes (type d'application, nécessite le consentement de l'administrateur) :

- `Directory.Read.All`— Lisez les données du répertoire, y compris les utilisateurs, les groupes et les principaux de service.
- `AuditLog.Read.All`— Lisez les événements du journal d'audit d'Entra ID.
- `Policy.Read.All`— Lisez les politiques de l'organisation et les configurations d'accès conditionnel.

Rôle Azure RBAC Reader

Le rôle de lecteur doit être attribué au principal du service dans le cadre du groupe de gestion racine du locataire. Cela accorde un accès en lecture seule à toutes les ressources Azure pour tous les abonnements du locataire.

Une fois ces tâches terminées, vous êtes prêt à configurer votre environnement Azure.

Configuration de Microsoft Azure pour l'intégrer à Security Hub CSPM

Après avoir effectué les tâches préalables, vous pouvez configurer votre environnement Microsoft Azure pour prendre en charge l'intégration avec AWS Security Hub CSPM. Pour vous y aider, la

console Security Hub CSPM génère un script de configuration personnalisé en fonction de votre configuration.

Pour générer le script, procédez comme suit :

1. Ouvrez la console Security Hub CSPM.
2. Dans le volet de navigation, choisissez Intégrations.
3. Choisissez Créer un connecteur Azure.
4. Terminez la configuration du connecteur (ID du locataire, étendue et nom), puis copiez le script de configuration généré.

Pour exécuter le script, utilisez l'interface de ligne de commande Azure et authentifiez-vous avec un compte d'administrateur global (`az login`).

Lorsque vous exécutez le script, il exécute une série de tâches. Les sections suivantes décrivent chaque tâche exécutée par le script. Si votre organisation restreint l'exécution des scripts, vous pouvez effectuer ces tâches manuellement, en vous servant de cette rubrique comme guide. Après avoir configuré votre environnement Azure, vous pouvez configurer Security Hub CSPM pour l'intégrer à Azure.

> **Note**
>
> Un seul enregistrement d'application Azure est partagé entre les services AWS de sécurité. Si vous utilisez également Security Hub ou Amazon Inspector pour Azure, ils utilisent le même enregistrement d'application. Il n'est pas nécessaire de créer des inscriptions distinctes pour chaque AWS service.

Tâches

- Étape 1 : enregistrer une application Azure
- Étape 2 : Création d'un responsable de service
- Étape 3 : Configuration des informations d'identification fédérées
- Étape 4 : Attribuer le rôle de lecteur
- Étape 5 : Configuration des autorisations de l'API Microsoft Graph
- Étape 6 : configurer Azure Event Hub

- Étape 7 : Configuration du journal d'activité et exportation du journal d'audit Entra ID

Étape 1 : enregistrer une application Azure

Enregistrez une nouvelle application dans Microsoft Entra ID. Cette application sert d'identité AWS utilisée pour s'authentifier auprès de votre environnement Azure à l'aide d'informations d'identification fédérées. Aucun secret client n'est requis.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Notez l'ID de l'application (client) de la sortie (l'`appId`attribut). Vous fournirez cette valeur lors de la création du connecteur dans la console Security Hub CSPM.

Étape 2 : Création d'un responsable de service

Créez un principal de service pour l'application enregistrée. Vous utilisez les attributions de rôles Azure pour accorder des autorisations au responsable du service. Le responsable du service exécute des actions dans votre environnement Azure.

```
$ az ad sp create --id application-client-id
```

Où se *`application-client-id`* trouve l'ID de l'application (client) de l'étape précédente.

Étape 3 : Configuration des informations d'identification fédérées

Configurez les informations d'identification fédérées sur l'application pour AWS permettre l'authentification sans secret client. Cela permet d'établir une relation de confiance OIDC entre AWS et Azure. Aucun secret ou identifiant de longue durée n'est stocké.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "AWSConfigFederation",
    "issuer": "token-issuer-url",
    "subject": "arn:aws:iam::account-id:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "Federation for AWS Config third-party cloud resource discovery"
  }'
```

Valeurs clés :

- Émetteur : URL de l'émetteur de votre jeton provenant de l'IAM Outbound Identity Federation. Cela suit le format`https://uuid.tokens.sts.global.api.aws`.
- Objet : l'ARN du rôle `AWSServiceRoleForConfigThirdParty` lié au service dans votre. Compte AWS AWS crée automatiquement ce rôle lié à un service lors de la configuration du connecteur.
- Audience — `api://AzureADTokenExchange` (valeur standard pour la fédération des identités de la charge de travail).

Étape 4 : Attribuer le rôle de lecteur

Attribuez le rôle de lecteur au responsable du service à la racine (`/`). Cela permet d'accéder en lecture seule à toutes les ressources Azure pour tous les abonnements du locataire.

> **Attribuer Reader à la portée racine**
>
> Assurez-vous d'attribuer le rôle Reader à la portée racine (`/`), et non à l'étendue du groupe de gestion racine du locataire. Security Hub CSPM lit les ressources d'attribution de rôles Azure à tous les niveaux, y compris les attributions définies à la racine du locataire. Une attribution Reader au niveau du groupe de gestion racine ne couvre pas les affectations dont la portée est limitée. Sans elle`/`, les lectures échouent avec une erreur d'autorisation et le connecteur peut entrer dans un état dégradé.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

> **Root-scope l'affectation nécessite un accès élevé**
>
> L'attribution d'un rôle à la portée racine (`/`) nécessite un accès élevé. Si l'attribution d'un rôle échoue, vérifiez que la gestion des accès pour les ressources Azure est définie sur Oui dans Microsoft Entra ID > Propriétés. Déconnectez-vous puis reconnectez-vous pour actualiser votre jeton.

⚠ Supprimer l'élévation temporaire de la racine

L'activation de la gestion des accès pour les ressources Azure confère à l'administrateur connecté le rôle d'administrateur de l'accès utilisateur à la racine (/), qui peut gérer l'accès à tous les abonnements et groupes de gestion du locataire. Une fois l'intégration terminée, redéfinissez Gestion de l'accès pour les ressources Azure sur Non dans Microsoft Entra ID > Propriétés, enregistrez et déconnectez-vous afin que cette élévation ne reste pas active.

Étape 5 : Configuration des autorisations de l'API Microsoft Graph

Accordez les autorisations d'API Microsoft Graph suivantes (type d'application) à l'application, puis accordez le consentement de l'administrateur :

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Étape 6 : configurer Azure Event Hub

AWS Config utilise un Azure Event Hub pour recevoir des notifications en temps quasi réel concernant les modifications de configuration des ressources dans votre environnement Azure. Le script de configuration crée l'infrastructure Event Hub et l'étiquette à des fins de découverte.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 1 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Après avoir créé l'Event Hub, balisez l'espace de noms à découvrir et attribuez le rôle de récepteur de données :

```
$ az tag create \
  --resource-id namespace-resource-id \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> Dans le format tag`AWSConfig-account-id-region`, *`account-id`* il s'agit de votre Compte AWS identifiant à 12 chiffres et *`region`* de l' Région AWS endroit où vous créez

le connecteur (par exemple,`us-east-1`). Ces valeurs identifient Compte AWS la région propriétaire de cette intégration d'Event Hub.

Configuration des touches :

- Namespace SKU — Standard (obligatoire pour les groupes de consommateurs).
- Nom du hub d'événements —`activitylog`.
- Groupe de consommateurs —`AWSConfig`.
- Tag — `AWSConfig-`*`account-id`*`-`*`region`* avec valeur`activitylog`. Ce tag permet AWS Config de découvrir automatiquement l'Event Hub.
- Attribution de rôle : récepteur de données Azure Event Hubs dans l'espace de noms.

Étape 7 : Configuration du journal d'activité et exportation du journal d'audit Entra ID

Configurez Azure pour exporter les journaux d'activité et les journaux d'audit d'Entra ID vers l'Event Hub.

Exportation du journal d'activité :

Configurez les paramètres de diagnostic de chaque abonnement pour exporter les journaux d'activité vers l'Event Hub. Le script de configuration le configure automatiquement pour tous les abonnements surveillés. Les journaux d'activité capturent l'activité au niveau de l'abonnement, y compris les attributions de rôles et les modifications de ressources.

Exportation du journal d'audit Entra ID :

Configurez les paramètres de diagnostic sur Microsoft Entra ID pour exporter les journaux d'audit vers le même Event Hub. Accédez à Microsoft Entra ID > Surveillance > Paramètres de diagnostic > Ajouter un paramètre de diagnostic. Activez-les AuditLogs et acheminez-les vers votre Event Hub.

Exportation continue de Microsoft Defender pour Cloud (facultatif) :

Pour transmettre les alertes de sécurité de Defender for Cloud à Security Hub CSPM, configurez l'exportation continue vers votre Event Hub. Dans le portail Azure, accédez à Microsoft Defender pour Cloud > Paramètres d'environnement > sélectionnez Abonnement > Exportation continue. Sélectionnez Event Hub comme cible d'exportation et choisissez votre espace de noms Event Hub. Activez les alertes de sécurité comme type de données d'exportation.

Configuration des événements de données Amazon Inspector (facultatif) :

Si vous envisagez d'utiliser Amazon Inspector pour l'analyse des machines virtuelles Azure, une configuration supplémentaire des événements de données est requise. Pour plus d'informations sur la configuration Inspector-specific des événements de données, consultez la documentation Amazon Inspector pour l'intégration d'Azure.

Configuration du Security Hub CSPM pour l'intégrer à Microsoft Azure

Après avoir effectué les tâches prérequises et configuré votre environnement Microsoft Azure, vous pouvez configurer AWS Security Hub CSPM pour l'intégrer à Azure. Pour configurer Security Hub CSPM afin de l'intégrer à Azure, vous devez créer un connecteur. Après avoir créé le connecteur, les événements suivants se produisent :

1. Security Hub CSPM valide les informations d'identification Azure et la connectivité à votre environnement Azure. Ce processus peut prendre plusieurs minutes.
2. AWS Config commence à découvrir et à enregistrer les données de configuration pour vos ressources Azure.
3. Security Hub CSPM commence à générer des résultats de gestion de posture pour vos ressources Azure une fois la collecte des données sur les ressources terminée.

> **Note**
>
> Si vous avez déjà créé un connecteur dans Security Hub, un connecteur lié à un service a été automatiquement créé dans Security Hub CSPM. Il n'est pas nécessaire de créer un connecteur distinct géré par le client, sauf si vous avez besoin d'une portée différente.

Rubriques

- Création d'un connecteur Azure
- Normes et contrôles habilitants
- Ajuster l'étendue d'un connecteur Azure
- Vérifier l'état d'un connecteur Azure
- Résoudre les problèmes liés à un connecteur Azure
- Comment Security Hub CSPM gère les identificateurs de ressources

- Contrôles disponibles pour Azure

Création d'un connecteur Azure

Pour créer un connecteur Microsoft Azure pour votre environnement, effectuez les étapes suivantes à l'aide de la console AWS Security Hub CSPM ou de l'API.

1. Ouvrez la console Security Hub CSPM.
2. Dans le volet de navigation, choisissez Intégrations.
3. Choisissez Create Azure connector.
4. Pour Azure Tenant ID, entrez votre identifiant de locataire Azure Active Directory.
5. Pour Application (ID client), entrez l'ID d'application pour l'enregistrement de l'application Azure que vous avez créée.
6. Configurez les paramètres supplémentaires et l'étendue du connecteur en procédant comme suit :

   - Dans Nom, entrez un nom unique pour le connecteur. Le nom peut contenir jusqu'à 50 caractères alphanumériques et inclure des tirets (-).

     > **Important**
     >
     > Les noms et les descriptions sont utilisés pour identifier votre contenu, et nous vous recommandons de ne pas y inclure d'informations sensibles, confidentielles ou personnellement identifiables (PII).

   - Dans Description, entrez éventuellement une brève description du connecteur. La description peut contenir jusqu'à 200 caractères.
   - Pour les abonnements, choisissez Tous les abonnements pour surveiller tous les abonnements actuels et futurs du locataire, ou Abonnements spécifiques pour surveiller uniquement les abonnements que vous spécifiez. Si vous choisissez de ne surveiller que des abonnements spécifiques, entrez l'identifiant de chacun d'entre eux.
   - Pour Régions, choisissez les régions Azure dans lesquelles vos ressources sont déployées.

     > **Note**
     >
     > Les contrôles qui évaluent les ressources Microsoft Entra ID et Microsoft Graph nécessitent que l'étendue de la région mondiale soit incluse dans votre configuration

d'intégration. Si vous sélectionnez uniquement des régions Azure spécifiques, ces contrôles ne généreront pas de résultats.

7. Vérifiez votre configuration et choisissez Create connector.

Après avoir créé le connecteur, Security Hub CSPM valide vos informations d'identification Azure et commence à découvrir les ressources. Le connecteur devrait afficher le statut Actif dans un délai de 2 à 5 minutes.

Normes et contrôles habilitants

Après avoir créé le connecteur, vous devez activer les normes de sécurité Azure pour commencer à générer des résultats. Pour des informations générales sur l'activation des normes et la gestion des contrôles, voir Activation des normes et Activation et désactivation des contrôles.

Normes disponibles

- CIS Microsoft Azure Foundations Benchmark v4.0 - Un benchmark de sécurité largement adopté qui définit les meilleures pratiques pour sécuriser les environnements Azure. Chaque contrôle évalue un aspect spécifique de votre configuration Azure (par exemple, le chiffrement du compte de stockage, les règles du groupe de sécurité réseau, les paramètres d'identité et d'accès).
- Meilleures pratiques de base Azure : évalue les ressources Azure pour détecter les risques d'exposition en corrélant l'accessibilité du réseau, l'accès public et les indicateurs de données sensibles. Génère des résultats de type exposition qui mettent en évidence les ressources présentant un risque élevé.

Les normes Azure disposent de leur propre ensemble de contrôles, distinct AWS des contrôles. Il n'existe aucun contrôle inter-cloud qui évalue à la fois les ressources Azure AWS et celles d'Azure en une seule vérification.

Activation d'une norme

Vous pouvez activer les normes Azure via la console Security Hub CSPM ou via le. API/CLI Accédez à Standards dans la console Security Hub CSPM et activez la norme souhaitée. Vous pouvez également utiliser la CLI :

```
$ aws securityhub batch-enable-standards \
  --standards-subscription-requests '[{"StandardsArn": "Standard-ARN"}]' \
```

```
  --region your-aws-region
```

> **Note**
>
> Vous pouvez activer les normes Azure avant ou après la création du connecteur ; elles ne sont pas couplées. Cependant, les résultats ne seront générés que lorsque le connecteur et la norme seront actifs et que les données sur les ressources auront été collectées.

Gestion des contrôles individuels

Une fois qu'une norme est activée (généralement en quelques secondes), vous pouvez afficher et gérer les contrôles individuels :

- Afficher les contrôles : utilisez la console Security Hub CSPM (Standards > sélectionnez standard > Contrôles) ou l'`list-standards-control-associations`API.
- Désactiver un contrôle : si un contrôle spécifique n'est pas applicable à votre environnement, vous pouvez le désactiver.
- Configurer des paramètres personnalisés : certains contrôles acceptent des paramètres d'entrée personnalisés (par exemple, les seuils de longueur des mots de passe). Ils peuvent être configurés par le biais de l'`update-security-control`API.

Remarques importantes

- Les normes Azure s'appliquent de manière uniforme sur l'ensemble du périmètre de votre connecteur. Vous ne pouvez pas activer différentes normes ou contrôles pour différents abonnements Azure au sein du même connecteur.
- Les contrôles dépendent de la disponibilité des données sur les ressources. Chaque contrôle évalue un type de ressource Azure spécifique. S'il n' AWS Config a pas encore collecté de données de configuration pour un type de ressource particulier, le contrôle générera une recherche PASS par défaut pour ces ressources. Ces résultats PASS par défaut seront automatiquement mis à jour pour donner lieu à des évaluations précises à mesure que les données sur les ressources arriveront. Ne considérez pas les scores de conformité initiaux comme exacts tant que la collecte des données sur les ressources n'est pas terminée.
- Les paramètres d'entrée personnalisés pour les contrôles de sécurité peuvent être configurés avant même de créer un connecteur. Ils sont conservés indépendamment.

- Les contrôles évaluant les paramètres au niveau de l'abonnement (par exemple, les plans Microsoft Defender, les alertes du journal d'activité) produisent un résultat par abonnement Azure plutôt que par ressource individuelle.
- Les normes multicloud ne peuvent pas être incluses dans les politiques de configuration centrale. Vous devez gérer l'activation standard d'Azure indépendamment dans chaque groupe Compte AWS . Région AWS

Ajuster l'étendue d'un connecteur Azure

Après avoir créé un connecteur Microsoft Azure, vous pouvez ajuster l'étendue du connecteur en modifiant les abonnements Azure ou les régions Azure qu'il surveille. Si vous ajustez l'étendue, la plupart des types de modifications prennent effet dans un délai d'environ 15 minutes.

Avant de régler la portée, notez les points suivants :

- L'étendue d'un connecteur géré par le client ne peut pas dépasser celle d'un connecteur lié à un service existant dans le même compte et dans la même région.
- Lorsque vous étendez le champ d'application, Security Hub CSPM commence à générer des résultats pour les nouvelles ressources après avoir AWS Config collecté leurs données de configuration.
- Lorsque vous réduisez la portée, les résultats existants concernant les ressources supprimées passent à l'état archivé.

Vérifier l'état d'un connecteur Azure

Vous pouvez vérifier l'état d'un connecteur Microsoft Azure à tout moment. Accédez à Intégrations dans la console Security Hub CSPM et vérifiez que le statut de votre connecteur est actif.

Les premiers résultats apparaissent généralement dans les 15 à 30 minutes suivant la fin de la collecte des données sur les ressources.

> **Note**
>
> L'état de santé du connecteur est finalement constant. Lorsqu'un problème d'autorisation ou de configuration survient, le statut du connecteur passe rapidement à Dégradé avec un message exploitable. Cependant, une fois le problème résolu, le statut peut prendre jusqu'à 24 heures pour revenir à Connecté.

- Un statut Dégradé après une correction récente n'indique pas nécessairement un problème persistant.
- Pour une visibilité en temps réel des échecs d'enregistrement, vérifiez les CloudWatch métriques dans l'espace de noms.

Résoudre les problèmes liés à un connecteur Azure

Si vous rencontrez des problèmes avec votre connecteur, utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants.

L'état du connecteur est défectueux

Ce problème se produit généralement si les informations d'identification fédérées ne sont pas correctement configurées dans Azure.

Pour résoudre ce problème, vérifiez que l'URL de l'émetteur du jeton et l'ARN du sujet figurant dans vos informations d'identification fédérées Azure correspondent à vos. Compte AWS

Aucun résultat après 30 minutes

Ce problème peut se produire si Event Hub ne reçoit pas les journaux d'activité ou si aucune norme n'est activée.

Pour résoudre ce problème, vérifiez que l'espace de noms Event Hub est correctement balisé (`AWSConfig-`*`account-id`*`-`*`region`*`=activitylog`), que le groupe de `AWSConfig` consommateurs existe, que le rôle de récepteur de données est attribué et qu'au moins une norme Azure est activée.

Impossible d'enregistrer certaines ressources Azure

L'erreur peut se produire pour l'une des raisons suivantes :

- L'environnement Azure ne répond pas aux conditions requises pour l'enregistrement des ressources.
- L'enregistrement de l'application ne nécessite pas le consentement de l'administrateur pour les autorisations de l'API Microsoft Graph.
- L'attribution du rôle de lecteur ne couvre pas toutes les étendues requises.
- Le locataire de l'identifiant Microsoft Entra ne dispose pas des données de journal requises.

Pour corriger l'erreur, procédez comme suit :

1. Pour vérifier que votre environnement répond à toutes les exigences, consultez les conditions préalables pour Microsoft Azure.
2. Vérifiez que l'enregistrement de l'application dispose des autorisations requises pour l'API Microsoft Graph avec le consentement de l'administrateur.
3. Vérifiez que le principal du service a le rôle de lecteur dans le cadre du groupe de gestion racine du locataire.

Le connecteur reste dans le statut En attente

Ce problème peut se produire si l'enregistrement de l'application Azure est mal configuré.

Pour résoudre ce problème, vérifiez que l'URL de l'émetteur des informations d'identification fédérées et l'identifiant du sujet correspondent à vos. Compte AWS Vérifiez également que le consentement de l'administrateur a été accordé pour toutes les autorisations requises pour l'API Microsoft Graph.

Comment Security Hub CSPM gère les identificateurs de ressources

En activant votre intégration Azure pour AWS Security Hub CSPM, les identifiants de ressources d'autres fournisseurs de cloud seront stockés dans AWS Security AWS Config Hub CSPM et dans d'autres AWS services (selon les besoins) sous forme de métadonnées liées à la gestion des données de configuration des ressources correspondantes collectées auprès des autres fournisseurs de cloud. Ces identifiants de ressources ne constituent pas votre contenu, et nous vous recommandons de ne pas y inclure d'informations sensibles, confidentielles ou permettant de vous identifier personnellement.

Les identifiants suivants issus de votre environnement cloud connecté sont stockés et utilisés pour fournir des AWS fonctionnalités de sécurité multicloud :

- Identifiants de ressources : ID de locataire Azure, ID d'abonnement, emplacement (région), ID de ressource (ID ou noms de groupes de ressources, fournisseur de ressources, type de ressource)

Les relations entre ces identifiants, notamment la façon dont les ressources sont liées les unes aux autres et la manière dont les résultats sont liés aux ressources, sont également stockées sous forme de métadonnées de service. AWS utilise ces identifiants pour la corrélation des ressources, l'association des résultats aux ressources, la journalisation des opérations des services et la déduplication.

Contrôles disponibles pour Azure

Après avoir activé les normes Azure, les 122 contrôles suivants évaluent vos ressources Azure. Les contrôles sont répartis selon deux normes :

- CIS Microsoft Azure Foundations Benchmark v4.0 — 96 contrôles mappés à des sections CIS spécifiques
- Meilleures pratiques de base d'Azure : 26 contrôles couvrant les meilleures pratiques de sécurité supplémentaires

> **Note**
>
> Les contrôles qui évaluent les ressources Microsoft Entra ID et Microsoft Graph nécessitent que l'étendue de la région mondiale soit incluse dans votre configuration d'intégration.

Contrôles Azure disponibles

Titre du contrôle	Type de ressource	Standard
Les applications Azure Container pour lesquelles l'identité gérée est activée doivent bénéficier du moindre privilège	`microsoft.app/containerapps`	Bonnes pratiques de base d'Azure
Azure Container Apps ne doit pas transmettre les informations d'identification du SDK Azure en tant que variables d'environnement	`microsoft.app/containerapps`	Bonnes pratiques de base d'Azure
L'entrée externe ne doit pas être activée dans Azure Container Apps	`microsoft.app/containerapps`	Bonnes pratiques de base d'Azure
Les environnements Azure Container App ne doivent pas bénéficier d'un accès NSG illimité	`microsoft.app/containerapps`	Bonnes pratiques de base d'Azure

Titre du contrôle	Type de ressource	Standard
Les environnements gérés par Azure Container App ne doivent pas avoir d'adresse IP publique activée	`microsoft.app/managedenvironments`	Bonnes pratiques de base d'Azure
Les attributions de rôles Azure ne doivent pas accorder un accès administrateur étendu pendant la durée de l'abonnement	`microsoft.authorization/roleassignments`	Bonnes pratiques de base d'Azure
Les attributions de rôles Azure ne doivent pas octroyer le rôle d'administrateur d'accès utilisateur	`microsoft.authorization/roleassignments`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les définitions de rôles personnalisés Azure ne doivent pas comporter d'autorisations administratives génériques	`microsoft.authorization/roledefinitions`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Le mode d'application des attributions de politiques Microsoft Cloud Security Benchmark doit être activé	`microsoft.authorization/policyassignments`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les clusters Azure Kubernetes Service (AKS) ne doivent pas disposer de serveurs d'API accessibles au public sans restrictions d'adresse IP	`microsoft.containerservice/managedclusters`	Bonnes pratiques de base d'Azure
Les clusters Azure Kubernetes Service (AKS) doivent chiffrer les secrets Kubernetes au repos	`microsoft.containerservice/managedclusters`	Bonnes pratiques de base d'Azure
Les clusters Azure Kubernetes Service (AKS) doivent exécuter une version de Kubernetes prise en charge	`microsoft.containerservice/managedclusters`	Bonnes pratiques de base d'Azure

Titre du contrôle	Type de ressource	Standard
La sauvegarde continue des comptes Azure Cosmos DB doit être activée	`microsoft.documentdb/databaseaccounts`	Bonnes pratiques de base d'Azure
L'accès au réseau public doit être désactivé pour les serveurs flexibles Azure Database pour MySQL	`microsoft.dbformysql/flexibleservers`	Bonnes pratiques de base d'Azure
Les espaces de travail Azure Databricks doivent être déployés dans un réseau virtuel géré par le client	`microsoft.databricks/workspaces`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
La livraison des journaux de diagnostic doit être configurée dans les espaces de travail Azure Databricks	`microsoft.databricks/workspaces`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les espaces de travail Azure Databricks doivent utiliser des clés gérées par le client pour le chiffrement des disques gérés	`microsoft.databricks/workspaces`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'autorisation relatives à l'identifiant Microsoft Entra devraient interdire aux utilisateurs par défaut d'enregistrer des applications	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les paramètres de sécurité par défaut d'Azure Entra ID doivent être activés	`microsoft.graph/policies/identitysecuritydefaultsenforcementpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les locataires de Microsoft Entra doivent disposer d'une politique d'accès conditionnel qui bloque l'accès depuis des zones géographiques interdites	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les locataires de Microsoft Entra doivent disposer d'une politique d'accès conditionnel qui bloque le flux d'authentification par code de l'appareil.	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'accès conditionnel Azure doivent exiger le MFA pour tous les utilisateurs	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les locataires de Microsoft Entra devraient exiger une authentification multifactorielle pour les connexions risquées via une politique d'accès conditionnel	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les locataires Azure doivent avoir besoin du MFA via un accès conditionnel pour l'API Azure Service Management	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Au moins une politique d'accès conditionnel doit exiger le MFA pour les portails d'administration Microsoft	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'autorisation de Microsoft Entra devraient empêcher les utilisateurs non administrateurs de créer des locataires	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques relatives aux méthodes d'authentification Microsoft Entra ID doivent définir la période de reconfirmation sur une valeur différente de zéro	`microsoft.graph/policies/authenticationmethodspolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'autorisation de Microsoft Entra devraient restreindre le consentement des utilisateurs pour les applications	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les politiques d'autorisation Azure doivent restreindre le consentement des utilisateurs aux applications d'éditeur vérifiées	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'autorisation de Microsoft Entra devraient restreindre l'accès des utilisateurs invités à leurs propres objets de répertoire	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'autorisation Azure doivent limiter les invitations d'invités aux rôles d'administrateur uniquement	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les politiques d'autorisation Azure devraient limiter la création de groupes de sécurité aux administrateurs	`microsoft.graph/policies/authorizationpolicy`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les locataires de Microsoft Entra doivent exiger une authentification multifactorielle pour enregistrer ou connecter des appareils	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les rôles de répertoire Microsoft Entra ID doivent comporter entre 2 et 4 administrateurs globaux	`microsoft.graph/directoryrole`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les paramètres du groupe Azure Entra ID devraient limiter la création de groupes aux administrateurs	`microsoft.graph/organization`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent avoir un paramètre de diagnostic configuré pour les journaux d'activité	`microsoft.insights/diagnosticsettings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les abonnements Azure doivent comporter une alerte de journal d'activité pour créer une attribution de politique	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte dans le journal d'activité pour la suppression de l'attribution de politiques	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activité pour créer ou mettre à jour les opérations du groupe de sécurité réseau	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activité pour la suppression du groupe de sécurité réseau	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activité pour créer ou mettre à jour une solution de sécurité	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activité pour la suppression de la solution de sécurité	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activité pour la création ou la mise à jour des règles de pare-feu de SQL Server	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les abonnements Azure doivent comporter une alerte dans le journal d'activité pour la suppression des règles de pare-feu de SQL Server	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activit é configurée pour les opérations de création ou de mise à jour d'adresses IP publiques	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte de journal d'activit é pour la suppression d'adresses IP publiques	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent comporter une alerte dans le journal d'activité pour les incidents liés à Service Health	`microsoft.insights/activitylogalerts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent avoir au moins un composant Application Insights configuré	`microsoft.insights/components`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Azure Key Vaults doit avoir une protectio n contre la suppression et la purge logicielles activées	`microsoft.keyvault/vaults`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Le contrôle d'accès basé sur les rôles doit être activé dans Azure Key Vaults	`microsoft.keyvault/vaults`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'accès au réseau public d'Azure Key Vaults doit être désactivé lors de l'utilisa tion de points de terminaison privés	`microsoft.keyvault/vaults`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Azure Key Vaults doit utiliser des points de terminaison privés	`microsoft.keyvault/vaults`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
La protection contre la purge doit être activée dans Azure Key Vaults	`microsoft.keyvault/vaults`	Bonnes pratiques de base d'Azure
Azure Key Vaults doit restreindre l'accès au réseau	`microsoft.keyvault/vaults`	Bonnes pratiques de base d'Azure
La AuditEvent journalisation doit être activée dans Azure Key Vaults	`microsoft.keyvault/vaults`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les clés Azure Key Vault dans les coffres-forts RBAC doivent avoir une date d'expiration définie	`microsoft.keyvault/vaults/keys`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les clés Azure Key Vault dans les coffres-forts non RBAC doivent avoir une date d'expiration définie	`microsoft.keyvault/vaults/keys`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les secrets Azure Key Vault dans les RBAC-enabled coffres-forts doivent avoir une date d'expiration définie	`microsoft.keyvault/vaults/secrets`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les secrets Azure Key Vault dans les coffres-forts non RBAC doivent avoir une date d'expiration définie	`microsoft.keyvault/vaults/secrets`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
La rotation automatique des clés Azure Key Vault doit être activée	`microsoft.keyvault/vaults/keys`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les groupes de sécurité réseau Azure doivent restreindre l'accès RDP entrant depuis Internet	`microsoft.network/networksecuritygroups`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les groupes de sécurité réseau Azure doivent restreindre l'accès UDP entrant depuis Internet	`microsoft.network/networksecuritygroups`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les groupes de sécurité du réseau Azure doivent restreindre l'accès HTTP entrant depuis Internet	`microsoft.network/networksecuritygroups`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les sous-réseaux Azure Application Gateway ne doivent pas avoir un accès NSG illimité	`microsoft.network/networksecuritygroups`	Bonnes pratiques de base d'Azure
Les groupes de sécurité réseau Azure doivent disposer d'une règle de refus de tout explicite	`microsoft.network/networksecuritygroups`	Bonnes pratiques de base d'Azure
Les groupes de sécurité réseau Azure ne doivent pas autoriser l'accès entrant illimité aux ports restreints	`microsoft.network/networksecuritygroups`	Bonnes pratiques de base d'Azure
La journalisation des flux réseau virtuels doit être activée dans les journaux de flux Azure Network Watcher et les analyses de trafic envoyées à Log Analytics	`microsoft.network/networkwatchers/flowlogs`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les groupes de sécurité du réseau Azure doivent restreindre l'accès SSH depuis Internet	`microsoft.network/networksecuritygroups`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent avoir au moins un hôte Azure Bastion	`microsoft.network/bastionhosts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour serveurs doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les machines doivent disposer d'une solution d'évaluation des vulnérabilités saine déployée dans Microsoft Defender for Cloud	`microsoft.security/assessments`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'intégration de la protection des terminaux à Microsoft Defender for Cloud doit être activée sur les abonnements Azure	`microsoft.security/settings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les abonnements Azure doivent être dotés d'une fonction d'analyse sans agent pour les machines activée dans Microsoft Defender pour serveurs	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
La surveillance de l'intégrité des fichiers doit être activée dans Defender pour serveurs sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender for Containers doit être activé sur l'abonnement Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender for Storage doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender for App Service doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour Azure Cosmos DB doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Microsoft Defender pour les bases de données relationnelles open source doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour les bases de données SQL Azure doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour les serveurs SQL sur machines doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour Key Vault doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour Resource Manager doit être activé sur les abonnements Azure	`microsoft.security/pricings`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les évaluations des mises à jour du système des machines virtuelles doivent être signalées comme saines par Microsoft Defender for Cloud	`microsoft.security/assessments`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les contacts de sécurité de Microsoft Defender for Cloud doivent informer le propriétaire (rôle du propriétaire) des alertes	`microsoft.security/securitycontacts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les contacts de sécurité de Microsoft Defender for Cloud doivent avoir une adresse e-mail supplémentaire configuré e	`microsoft.security/securitycontacts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les notifications par e-mail d'alerte doivent être activées pour les contacts de sécurité Azure avec une sévérité minimale suffisamment inclusive	`microsoft.security/securitycontacts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les notifications par e-mail relatives au chemin d'attaque doivent être activées pour les contacts de sécurité Azure et configurer un niveau de risque	`microsoft.security/securitycontacts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Microsoft Defender pour l'IoT doit être activé sur les abonnements Azure	`microsoft.security/iotsecuritysolutions`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'accès au réseau public doit être désactivé sur les serveurs Azure SQL	`microsoft.sql/servers`	Bonnes pratiques de base d'Azure
Un administrateur Azure Active Directory doit être configuré sur les serveurs SQL	`microsoft.sql/servers`	Bonnes pratiques de base d'Azure
La sauvegarde géo-redondante des bases de données Azure SQL doit être activée	`microsoft.sql/servers/databases`	Bonnes pratiques de base d'Azure
Les serveurs Azure SQL ne doivent pas utiliser les noms de compte d'administrateur par défaut	`microsoft.sql/servers`	Bonnes pratiques de base d'Azure
La mise à niveau automatique des versions mineures des instances gérées Azure SQL doit être activée	`microsoft.sql/managedinstances`	Bonnes pratiques de base d'Azure
Les comptes Azure Storage doivent utiliser des clés gérées par le client pour le chiffrement	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
La suppression logicielle des services de fichiers du compte Azure Storage doit être activée pour les partages de fichiers	`microsoft.storage/storageaccounts/fileservices`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les partages de fichiers du compte Azure Storage devraient limiter les versions du protocole SMB à SMB 3.1.1	`microsoft.storage/storageaccounts/fileservices`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent utiliser un algorithme de chiffrement des canaux SMB sécurisé pour les partages de fichiers	`microsoft.storage/storageaccounts/fileservices`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Un rappel de rotation des clés doit être configuré pour les comptes Azure Storage	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'accès aux clés partagées doit être désactivé pour les comptes Azure Storage	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent utiliser des points de terminaison privés pour l'accès	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'accès au réseau public doit être désactivé pour les comptes Azure Storage	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'accès au réseau par défaut des comptes Azure Storage doit être défini pour être refusé	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes de stockage doivent être autorisés par défaut par Microsoft Entra sur le portail Azure	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
Les comptes Azure Storage doivent nécessiter un transfert sécurisé	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent permettre aux services Azure fiables de contourner les règles du réseau	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent être configurés avec la version TLS minimale requise	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
La réplication entre locataires doit être désactivée sur les comptes Azure Storage	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
L'accès anonyme aux blob doit être désactivé pour les comptes Azure Storage	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent limiter la suppression permanente des blob	`microsoft.storage/storageaccounts/blobservices`	Bonnes pratiques de base d'Azure
Les comptes de stockage Azure contenant des journaux d'activité doivent être chiffrés à l'aide d'une clé gérée par le client	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les services blob du compte Azure Storage doivent avoir la suppression logicielle des blob activée	`microsoft.storage/storageaccounts/blobservices`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
La gestion des versions des services blob du compte Azure Storage doit être activée	`microsoft.storage/storageaccounts/blobservices`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Titre du contrôle	Type de ressource	Standard
La suppression progressive des blob et des conteneurs doit être activée pour les services blob du compte Azure Storage	`microsoft.storage/storageaccounts/blobservices`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Un verrou de suppression d'Azure Resource Manager doit être appliqué aux comptes Azure Storage	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent être dotés d'un verrou de gestion ReadOnly des ressources	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les comptes Azure Storage doivent utiliser un stockage géo-redondant	`microsoft.storage/storageaccounts`	Benchmark Microsoft Azure Foundations du CIS, version 4.0
Les applications Azure Function doivent restreindre l'accès administratif	`microsoft.web/sites/config`	Bonnes pratiques de base d'Azure
Azure Functions ne doit pas autoriser l'invocation anonyme d'un déclencheur HTTP	`microsoft.web/sites/functions`	Bonnes pratiques de base d'Azure
Les applications Web et les applications fonctionnelles Azure App Service ne doivent pas utiliser de versions d'exécution non prises en charge	`microsoft.web/sites`	Bonnes pratiques de base d'Azure
Les applications Azure Function sur les plans Premium ou Dedicated doivent être intégrées à un réseau virtuel	`microsoft.web/sites`	Bonnes pratiques de base d'Azure
Les journaux HTTP des applications Web Azure App Service doivent être activés dans les paramètres de diagnostic	`microsoft.web/sites`	Benchmark Microsoft Azure Foundations du CIS, version 4.0

Suppression d'un connecteur Microsoft Azure dans Security Hub CSPM

Après avoir créé un connecteur Microsoft Azure dans AWS Security Hub CSPM, vous pouvez le supprimer à tout moment. Si vous supprimez un connecteur, Security Hub CSPM arrête d'effectuer des vérifications de gestion de posture et de surveillance des vulnérabilités pour votre environnement Azure. Security Hub CSPM cesse également de générer de nouvelles informations sur votre environnement. Vos résultats existants sont conservés pendant 90 jours. L'inventaire des ressources reste tel qu'il était lorsque le connecteur a été supprimé et est supprimé au bout de 90 jours.

Lorsque vous supprimez un connecteur, tenez compte des points suivants :

- Security Hub CSPM ne supprime pas l'enregistrement de l'application Azure ni l'infrastructure Event Hub dans votre environnement Azure. Vous devez les supprimer manuellement, directement dans Microsoft Azure. Pour savoir comment procéder, consultez la section Supprimer une application dans la documentation Microsoft Azure.
- S'il s'agit d'un connecteur géré par le client et qu'un connecteur lié à un service existe également, la suppression du connecteur géré par le client n'affecte pas le connecteur lié au service. Security Hub CSPM continue de recevoir les résultats de gestion de la posture via le connecteur lié au service.
- Les résultats existants passent à l'état archivé dans un délai de 3 à 5 jours et sont supprimés après la période de conservation de 90 jours.

Pour supprimer un connecteur Azure

1. Ouvrez la console Security Hub CSPM.
2. Dans le volet de navigation, choisissez Intégrations.
3. Sélectionnez votre connecteur.
4. Sélectionnez Delete (Supprimer).
5. Lorsque vous y êtes invité, confirmez que vous souhaitez supprimer le connecteur.

Après la suppression, vous pouvez éventuellement nettoyer les ressources Azure créées lors de l'installation :

- Supprimez l'enregistrement de l'application dans Microsoft Entra ID.
- Supprimez l'espace de noms et le groupe de ressources Event Hub.

- Supprimez les paramètres de diagnostic qui exportent les journaux d'activité et les journaux d'audit Entra ID.

Création et mise à jour des résultats dans Security Hub CSPM

Dans AWS Security Hub CSPM, une découverte est un enregistrement observable d'un contrôle de sécurité ou d'une détection liée à la sécurité. Une découverte peut provenir de l'une des sources suivantes :

- Un contrôle de sécurité pour un contrôle dans Security Hub CSPM.
- Une intégration avec un autre Service AWS.
- Une intégration avec un produit tiers.
- Une intégration personnalisée.

Security Hub CSPM normalise les résultats provenant de toutes les sources dans une syntaxe et un format standard appelés AWS Security Finding Format (ASFF). Pour des informations détaillées sur ce format, y compris la description des différents champs ASFF, consultezAWS Format de recherche de sécurité (ASFF). Si vous activez l'agrégation entre régions, Security Hub CSPM regroupe également automatiquement les résultats nouveaux et mis à jour de toutes les régions liées vers une région d'agrégation que vous spécifiez. Pour de plus amples informations, veuillez consulter Comprendre l'agrégation entre régions dans Security Hub CSPM.

Une fois qu'un résultat a été créé, il peut être mis à jour comme suit :

- Un fournisseur de recherche peut utiliser le BatchImportFindings fonctionnement de l'API CSPM Security Hub pour mettre à jour les informations générales relatives à la découverte. Les fournisseurs de résultats ne peuvent mettre à jour que les résultats qu'ils ont créés.
- Un client peut utiliser la console Security Hub CSPM ou utiliser l'BatchUpdateFindingsAPI Security Hub CSPM pour mettre à jour l'état de l'enquête sur la découverte. L'`BatchUpdateFindings`opération peut également être utilisée par un SIEM, une billetterie, une gestion des incidents, un SOAR ou tout autre type d'outil pour le compte d'un client.

Pour réduire le bruit des recherches et rationaliser le suivi et l'analyse des résultats individuels, Security Hub CSPM supprime automatiquement les résultats qui n'ont pas été mis à jour récemment. Le calendrier avec lequel Security Hub CSPM effectue cette opération dépend du fait qu'une découverte est active ou archivée :

- Une découverte active est une découverte dont l'état d'enregistrement est (`RecordState`)`ACTIVE`. Security Hub CSPM conserve les résultats actifs pendant 90 jours. Si un résultat actif n'a pas été mis à jour pendant 90 jours, il expire et Security Hub CSPM le supprime définitivement.
- Une découverte archivée est une découverte dont l'état d'enregistrement est (`RecordState`)`ARCHIVED`. Security Hub CSPM conserve les résultats archivés pendant 30 jours. Si une découverte archivée n'a pas été mise à jour pendant 30 jours, elle expire et Security Hub CSPM la supprime définitivement.

Pour les résultats de contrôle, qui sont des résultats que Security Hub CSPM génère à partir des contrôles de sécurité, Security Hub CSPM détermine si un résultat a expiré en fonction de la valeur du `UpdatedAt` champ du résultat. Si cette valeur remonte à plus de 90 jours pour un résultat actif, Security Hub CSPM supprime définitivement le résultat. Si cette valeur remonte à plus de 30 jours pour un résultat archivé, Security Hub CSPM supprime définitivement le résultat.

Pour tous les autres types de résultats, Security Hub CSPM détermine si un résultat a expiré en fonction des valeurs des `UpdatedAt` champs `ProcessedAt` et du résultat. Security Hub CSPM compare les valeurs de ces champs et détermine laquelle est la plus récente. Si la valeur la plus récente remonte à plus de 90 jours pour un résultat actif, Security Hub CSPM supprime définitivement le résultat. Si la valeur la plus récente remonte à plus de 30 jours pour une découverte archivée, Security Hub CSPM supprime définitivement la découverte. Les fournisseurs de recherche peuvent modifier la valeur du `UpdatedAt` champ d'un ou de plusieurs résultats en utilisant le BatchImportFindings fonctionnement de l'API CSPM Security Hub.

Pour une conservation à long terme des résultats, vous pouvez les exporter vers un compartiment S3. Vous pouvez le faire en utilisant une action personnalisée avec une EventBridge règle Amazon. Pour de plus amples informations, veuillez consulter Utilisation à EventBridge des fins de réponse et de correction automatisées.

Rubriques

- BatchImportFindings pour trouver des prestataires
- BatchUpdateFindings pour les clients
- Révision des détails et de l'historique des recherches dans Security Hub CSPM
- Filtrage des résultats dans Security Hub CSPM
- Regroupement des résultats dans Security Hub CSPM
- Configuration de l'état du flux de travail des résultats dans Security Hub CSPM

- Envoi des résultats à une action CSPM personnalisée de Security Hub
- AWS Format de recherche de sécurité (ASFF)

BatchImportFindings pour trouver des prestataires

La recherche de fournisseurs peut utiliser cette BatchImportFindings opération pour créer de nouvelles découvertes dans AWS Security Hub CSPM. Ils peuvent également utiliser cette opération pour mettre à jour les résultats qu'ils ont créés. Les fournisseurs de recherche ne peuvent pas mettre à jour les résultats qu'ils n'ont pas créés.

Les clients, les SIEM, la billetterie, le SOAR et d'autres types d'outils doivent utiliser cette BatchUpdateFindings opération pour effectuer des mises à jour liées à leur enquête sur les résultats de la recherche de fournisseurs. Pour de plus amples informations, veuillez consulter the section called "BatchUpdateFindings pour les clients".

Lorsque Security Hub CSPM reçoit une `BatchImportFindings` demande de création ou de mise à jour d'une découverte, il génère automatiquement un Security Hub Findings - Imported événement sur Amazon. EventBridge Vous pouvez prendre des mesures automatisées lors de cet événement. Pour de plus amples informations, veuillez consulter the section called "Réponse et remédiation automatisées".

Conditions préalables pour l'utilisation du **`BatchImportFindings`**.

`BatchImportFindings`doit être appelé par l'une des personnes suivantes :

- Le compte associé aux résultats. L'identifiant du compte associé doit correspondre à la valeur de l'`AwsAccountId`attribut pour la découverte.
- Un compte autorisé en tant qu'intégration officielle d'un partenaire Security Hub CSPM.

Security Hub CSPM peut uniquement accepter la recherche de mises à jour pour les comptes sur lesquels Security Hub CSPM est activé. Le fournisseur de résultats doit également être activé. Si Security Hub CSPM est désactivé ou si l'intégration du fournisseur de recherche n'est pas activée, les résultats sont renvoyés dans la `FailedFindings` liste, avec une `InvalidAccess` erreur.

Déterminer s'il faut créer ou mettre à jour un résultat

Pour déterminer s'il faut créer ou mettre à jour une découverte, Security Hub CSPM vérifie le `ID` champ. Si la valeur de `ID` ne correspond pas à un résultat existant, Security Hub CSPM crée un nouveau résultat.

S'il `ID` correspond à un résultat existant, Security Hub CSPM vérifie le `UpdatedAt` champ pour la mise à jour et procède comme suit :

- Si `UpdatedAt` la mise à jour correspond ou survient avant `UpdatedAt` la découverte existante, Security Hub CSPM ignore la demande de mise à jour.
- Si `UpdatedAt` la mise à jour se produit après `UpdatedAt` la découverte existante, Security Hub CSPM met à jour la découverte existante.

Restrictions concernant la recherche de mises à jour avec **`BatchImportFindings`**

Les fournisseurs de recherche ne peuvent pas être utilisés `BatchImportFindings` pour mettre à jour les attributs suivants d'une recherche existante :

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM ignore tout contenu fourni dans une `BatchImportFindings` demande pour ces attributs. Les clients ou les entités agissant en leur nom (tels que les outils de billetterie) peuvent utiliser `BatchUpdateFindings` pour mettre à jour ces attributs.

Mise à jour des résultats avec FindingProviderFields

Les fournisseurs de recherche ne doivent pas non plus être utilisés `BatchImportFindings` pour mettre à jour les attributs de niveau supérieur suivants dans le AWS Security Finding Format (ASFF) :

- `Confidence`
- `Criticality`
- `RelatedFindings`

- `Severity`
- `Types`

La recherche de fournisseurs doit plutôt utiliser l'`FindingProviderFields`objet pour fournir des valeurs pour ces attributs.

Exemple

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Pour les `BatchImportFindings` demandes, Security Hub CSPM gère les valeurs des attributs de niveau supérieur et de la manière `FindingProviderFields` suivante.

(Préféré) **`BatchImportFindings`** fournit une valeur pour un attribut dans **`FindingProviderFields`**, mais ne fournit pas de valeur pour l'attribut de niveau supérieur correspondant.

> Par exemple, `BatchImportFindings` fournit`FindingProviderFields.Confidence`, mais ne fournit pas`Confidence`. Il s'agit de l'option préférée pour les `BatchImportFindings` demandes.
>
> Security Hub CSPM met à jour la valeur de l'attribut dans. `FindingProviderFields`
>
> Il réplique la valeur vers l'attribut de niveau supérieur uniquement si l'attribut n'a pas déjà été mis à jour par. `BatchUpdateFindings`

`BatchImportFindings`fournit une valeur pour un attribut de niveau supérieur, mais ne fournit pas de valeur pour l'attribut correspondant dans**`FindingProviderFields`**.

Par exemple, `BatchImportFindings` fournit`Confidence`, mais ne fournit pas`FindingProviderFields.Confidence`.

Security Hub CSPM utilise la valeur pour mettre à jour l'attribut dans. `FindingProviderFields` Il remplace toute valeur existante.

Security Hub CSPM met à jour l'attribut de niveau supérieur uniquement s'il n'a pas déjà été mis à jour par. `BatchUpdateFindings`

`BatchImportFindings`fournit une valeur à la fois pour un attribut de niveau supérieur et pour l'attribut correspondant dans**`FindingProviderFields`**.

Par exemple, `BatchImportFindings` fournit à la fois `Confidence` et`FindingProviderFields.Confidence`.

Pour une nouvelle découverte, Security Hub CSPM utilise la valeur in `FindingProviderFields` pour renseigner à la fois l'attribut de niveau supérieur et l'attribut correspondant. `FindingProviderFields` Il n'utilise pas la valeur d'attribut de niveau supérieur fournie.

Pour une découverte existante, Security Hub CSPM utilise les deux valeurs. Cependant, il met à jour la valeur de l'attribut de niveau supérieur uniquement si l'attribut n'a pas déjà été mis à jour par`BatchUpdateFindings`.

BatchUpdateFindings pour les clients

AWS Les clients de Security Hub CSPM et les entités agissant en leur nom peuvent utiliser cette BatchUpdateFindings opération pour mettre à jour les informations relatives au traitement des résultats de Security Hub CSPM provenant de la recherche de fournisseurs. En tant que client, vous pouvez utiliser cette opération directement. Les outils SIEM, de billetterie, de gestion des incidents et de SOAR peuvent également utiliser cette opération pour le compte d'un client.

Vous ne pouvez pas utiliser cette `BatchUpdateFindings` opération pour créer de nouveaux résultats. Vous pouvez toutefois l'utiliser pour mettre à jour jusqu'à 100 résultats existants à la fois. Dans une `BatchUpdateFindings` demande, vous spécifiez les résultats à mettre à jour, les champs ASFF (AWS Security Finding Format) à mettre à jour pour les résultats et les nouvelles

valeurs des champs. Security Hub CSPM met ensuite à jour les résultats comme indiqué dans votre demande. Ce processus peut prendre plusieurs minutes. Si vous mettez à jour les résultats à l'aide de cette `BatchUpdateFindings` opération, vos mises à jour n'affectent pas les valeurs existantes pour le `UpdatedAt` champ des résultats.

Lorsque Security Hub CSPM reçoit une `BatchUpdateFindings` demande de mise à jour d'une découverte, il génère automatiquement un Security Hub Findings – Imported événement sur Amazon. EventBridge Vous pouvez éventuellement utiliser cet événement pour prendre des mesures automatisées sur le résultat spécifié. Pour de plus amples informations, veuillez consulter the section called “Réponse et remédiation automatisées”.

Champs disponibles pour BatchUpdateFindings

Si vous êtes connecté à un compte administrateur CSPM de Security Hub, vous pouvez l'utiliser `BatchUpdateFindings` pour mettre à jour les résultats générés par le compte administrateur ou les comptes des membres. Les comptes des membres peuvent être utilisés `BatchUpdateFindings` pour mettre à jour les résultats pour leur compte uniquement.

Les clients peuvent utiliser `BatchUpdateFindings` pour mettre à jour les champs et objets suivants :

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Configuration de l'accès à BatchUpdateFindings

Vous pouvez configurer des politiques Gestion des identités et des accès AWS (IAM) pour restreindre l'accès à l'utilisation pour mettre `BatchUpdateFindings` à jour les champs de recherche et les valeurs des champs.

Dans une instruction à laquelle restreindre l'accès`BatchUpdateFindings`, utilisez les valeurs suivantes :

- `Action` est `securityhub:BatchUpdateFindings`
- `Effect` est `Deny`
- En `Condition` effet, vous pouvez refuser une `BatchUpdateFindings` demande pour les raisons suivantes :
  - La découverte inclut un domaine spécifique.
  - La découverte inclut une valeur de champ spécifique.

Clés de condition

Il s'agit des clés de condition permettant de restreindre l'accès à`BatchUpdateFindings`.

Champ ASFF

La clé de condition pour un champ ASFF est la suivante :

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Remplacez *<fieldName>* par le champ ASFF. Lorsque vous configurez l'accès à`BatchUpdateFindings`, incluez un ou plusieurs champs ASFF spécifiques dans votre politique IAM plutôt qu'un champ au niveau du parent. Par exemple, pour restreindre l'accès au `Workflow.Status` champ, vous devez inclure `securityhub:ASFFSyntaxPath/Workflow.Status` dans votre politique plutôt que le champ au `Workflow` niveau du parent.

Interdire toutes les mises à jour d'un champ

Pour empêcher un utilisateur de mettre à jour un champ spécifique, utilisez une condition comme celle-ci :

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
                }
}
```

Par exemple, l'instruction suivante indique qu'elle ne `BatchUpdateFindings` peut pas être utilisée pour mettre à jour le `Workflow.Status` champ des résultats.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Interdire des valeurs de champ spécifiques

Pour empêcher un utilisateur de définir une valeur spécifique pour un champ, utilisez une condition comme celle-ci :

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
               }
}
```

Par exemple, l'instruction suivante indique qu'il n'est pas `BatchUpdateFindings` possible de l'utiliser `Workflow.Status` pour définir sur`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Vous pouvez également fournir une liste de valeurs qui ne sont pas autorisées.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Par exemple, l'instruction suivante indique qu'il n'est pas `BatchUpdateFindings` possible de définir l'un `RESOLVED` ou `Workflow.Status` l'autre de ces paramètres`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Révision des détails et de l'historique des recherches dans Security Hub CSPM

Dans AWS Security Hub CSPM, une découverte est un enregistrement observable d'un contrôle de sécurité ou d'une détection liée à la sécurité. Security Hub CSPM génère un résultat lorsqu'il effectue un contrôle de sécurité et lorsqu'il ingère un résultat provenant d'un produit intégré Service AWS ou tiers. Chaque découverte inclut un historique des modifications et d'autres détails, tels qu'un indice de gravité et des informations sur les ressources affectées.

Vous pouvez consulter l'historique et d'autres détails des résultats individuels sur la console Security Hub CSPM ou par programmation à l'aide de l'API Security Hub CSPM ou du. AWS CLI

Pour vous aider à rationaliser votre analyse, la console Security Hub CSPM affiche un panneau de recherche lorsque vous choisissez un résultat spécifique. Le panneau comprend différents menus et onglets permettant de consulter les détails spécifiques d'une découverte.

Menu d'actions

Dans ce menu, vous pouvez consulter le JSON complet d'une découverte ou ajouter des notes. Une constatation ne peut être associée qu'à une seule note à la fois. Ce menu propose également des options permettant de définir l'état du flux de travail d'une recherche ou d'envoyer une recherche à une action personnalisée sur Amazon EventBridge.

Menu Enquêter

Dans ce menu, vous pouvez rechercher une découverte dans Amazon Detective. Detective extrait des entités, telles que les adresses IP et AWS les utilisateurs, à partir d'une découverte et visualise leur activité. Vous pouvez utiliser l'activité de l'entité comme point de départ pour étudier la cause et l'impact d'une découverte.

Onglet Overview (Présentation)

Cet onglet fournit un résumé d'une constatation. Par exemple, vous pouvez déterminer quand un résultat a été créé et mis à jour pour la dernière fois, dans quel compte il existe et quelle est la source du résultat. Pour les résultats des contrôles, cet onglet affiche également le nom de la AWS Config règle associée et un lien vers les instructions de correction figurant dans la documentation CSPM de Security Hub.

Dans la capture d'écran Ressources de l'onglet Vue d'ensemble, vous pouvez obtenir un bref aperçu des ressources impliquées dans une découverte. Pour certaines ressources, cela inclut une option de ressource ouverte, qui renvoie directement à une ressource affectée sur la Service AWS console correspondante. L'instantané de l'historique montre jusqu'à deux modifications apportées à la découverte à la date la plus récente pour laquelle l'historique est suivi. Par exemple, si vous avez effectué une modification hier et une autre aujourd'hui, l'instantané montre la modification d'aujourd'hui. Pour consulter les entrées précédentes, passez à l'onglet Historique.

La ligne Conformité s'agrandit pour afficher plus de détails. Par exemple, si un contrôle inclut des paramètres, vous pouvez consulter les valeurs de paramètres que Security Hub CSPM utilise actuellement lors des contrôles de sécurité du contrôle.

Onglet Ressources

Cet onglet fournit des informations sur les ressources impliquées dans une découverte. Si vous êtes connecté au compte qui possède une ressource, vous pouvez consulter la ressource dans la Service AWS console appropriée. Si vous n'êtes pas le propriétaire d'une ressource, cet onglet affiche l' Compte AWS identifiant du propriétaire.

La ligne Détails affiche les détails spécifiques à la ressource dans une découverte. Il affiche la ResourceDetails section de la découverte au format JSON.

La ligne Balises affiche les clés et les valeurs des balises qui sont attribuées aux ressources impliquées dans une recherche. Les ressources prises en charge par le GetResources fonctionnement de l'API de Groupes de ressources AWS balisage peuvent être balisées. Security Hub CSPM appelle cette opération en utilisant un rôle lié à un service lors du traitement des résultats nouveaux ou mis à jour, et récupère les balises de ressource si le `Resource.Id` champ AWS Security Finding Format (ASFF) est renseigné avec l'ARN d'une ressource. Security Hub CSPM ignore les ID de ressources non valides. Pour plus d'informations sur l'inclusion de balises de ressources dans les résultats, consultezÉtiquettes.

Onglet Historique

Cet onglet permet de suivre l'historique d'une découverte. L'historique des recherches est disponible pour les résultats actifs et archivés. Il fournit une trace immuable des modifications apportées à une découverte au fil du temps, y compris le champ ASFF modifié, la date à laquelle la modification s'est produite et par quel utilisateur. Chaque page de l'onglet affiche jusqu'à 20 modifications. Les modifications les plus récentes sont affichées en premier.

Pour les résultats actifs, l'historique des recherches est disponible pour une durée maximale de 90 jours. Pour les résultats archivés, l'historique des recherches est disponible pendant 30 jours maximum. L'historique de recherche inclut les modifications apportées manuellement ou automatiquement par les règles d'automatisation CSPM de Security Hub. Il n'inclut pas les modifications apportées aux champs d'horodatage de niveau supérieur, tels que les champs et. `CreatedAt` `UpdatedAt`

Si vous êtes connecté à un compte administrateur CSPM de Security Hub, la recherche de l'historique concerne le compte administrateur et tous les comptes membres.

Onglet Menaces

Cet onglet inclut les données provenant des ProcessDetails objets Action Malware, et de l'ASFF, notamment le type de menace et le fait qu'une ressource soit la cible ou l'acteur. Ces informations s'appliquent généralement aux résultats provenant d'Amazon GuardDuty.

onglet Vulnérabilités

Cet onglet affiche les données de l'Vulnerabilityobjet de l'ASFF, notamment s'il existe des exploits ou des correctifs disponibles associés à une découverte. Ces informations s'appliquent généralement aux résultats provenant d'Amazon Inspector.

Les lignes de chaque onglet incluent une option de copie ou de filtre. Par exemple, si vous ouvrez le panneau correspondant à un résultat dont le statut du flux de travail est Notifié, vous pouvez choisir l'option de filtre à côté de la ligne État du flux de travail. Si vous choisissez Afficher tous les résultats avec cette valeur, Security Hub CSPM filtre le tableau des résultats et affiche uniquement les résultats ayant le même statut de flux de travail.

Révision des détails et de l'historique des découvertes

Choisissez votre méthode préférée et suivez les étapes pour vérifier la recherche de détails dans Security Hub CSPM.

Si vous activez l'agrégation interrégionale et que vous vous connectez à la région d'agrégation, la recherche de données inclut les données de la région d'agrégation et des régions liées. Dans les autres régions, la recherche de données est spécifique à cette région uniquement. Pour plus d'informations sur l'agrégation entre régions, consultezthe section called "Agrégation des données entre les régions".

Security Hub CSPM console

Révision des détails et de l'historique des découvertes

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Pour afficher une liste de résultats, effectuez l'une des opérations suivantes :
   - Dans le volet de navigation, choisissez Conclusions. Ajoutez des filtres de recherche si nécessaire pour affiner la liste des résultats.
   - Dans le panneau de navigation, choisissez Insights. Choisissez un aperçu. Ensuite, dans la liste des résultats, choisissez un résultat d'analyse.
   - Dans le volet de navigation, choisissez Intégrations. Choisissez Afficher les résultats pour une intégration.
   - Dans le volet de navigation, choisissez Controls.
3. Choisissez une découverte. Le panneau de recherche affiche les détails de la découverte.
4. Dans le panneau de recherche, effectuez l'une des opérations suivantes :
   - Pour consulter les détails spécifiques de la découverte, choisissez un onglet.
   - Pour agir sur cette découverte, choisissez une option dans le menu Actions.
   - Pour étudier la découverte dans Amazon Detective, choisissez une option Enquêter.

> **Note**
>
> Si vous vous intégrez à un compte membre AWS Organizations et que vous êtes connecté à celui-ci, le panneau de recherche inclut le nom du compte. Pour les comptes de membres qui sont invités manuellement, plutôt que par le biais des organisations, le panneau de recherche inclut uniquement l'identifiant du compte.

Security Hub CSPM API

Utilisez le GetFindings fonctionnement de l'API Security Hub CSPM ou, si vous utilisez le AWS CLI, exécutez la get-findings commande. Vous pouvez fournir une ou plusieurs valeurs pour le `Filters` paramètre afin d'affiner les résultats à récupérer.

Si le volume de résultats est trop important, vous pouvez utiliser le `MaxResults` paramètre pour limiter les résultats à un certain nombre et le `NextToken` paramètre pour paginer les résultats. Utilisez le `SortCriteria` paramètre pour trier les résultats selon un champ spécifique.

Par exemple, la AWS CLI commande suivante extrait les résultats qui correspondent aux critères de filtre spécifiés et trie les résultats par ordre décroissant par `LastObservedAt` champ. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

Pour consulter l'historique des recherches, utilisez l'GetFindingHistoryopération. Si vous utilisez le AWS CLI, exécutez la get-finding-history commande. Identifiez la découverte pour laquelle vous souhaitez obtenir un historique à l'aide `ProductArn` des `Id` champs et. Pour obtenir des informations sur ces champs, consultez AwsSecurityFindingIdentifier. Chaque demande ne peut récupérer l'historique que pour une seule découverte.

Par exemple, la AWS CLI commande suivante récupère l'historique de la découverte spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub get-finding-history \
```

```
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Utilisez l'applet de commande `Get-SHUBFinding`. Renseignez éventuellement le `Filter` paramètre pour affiner les résultats à récupérer.

Par exemple, l'applet de commande suivante extrait les résultats correspondant aux filtres spécifiés.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Si vous filtrez les résultats par `CompanyName` ou`ProductName`, Security Hub CSPM utilise les valeurs qui font partie de l'objet `ProductFields` ASFF. Security Hub CSPM n'utilise pas les champs et de niveau supérieur. `CompanyName` `ProductName`

Filtrage des résultats dans Security Hub CSPM

AWS Security Hub CSPM génère ses propres résultats à partir des contrôles de sécurité et reçoit les résultats des produits intégrés. Vous pouvez afficher une liste des résultats sur les pages Résultats, Intégrations et Informations de la console Security Hub CSPM. Vous pouvez ajouter des filtres pour affiner une liste de recherche afin qu'elle soit adaptée à votre organisation ou à votre cas d'utilisation.

Pour plus d'informations sur le filtrage des résultats pour un contrôle de sécurité spécifique, consultezthe section called "Résultats des contrôles de filtrage et de tri". Les informations de cette page s'appliquent aux pages Résultats , Informations et Intégrations.

Filtres par défaut pour la recherche de listes

Par défaut, les listes de recherche de la console Security Hub CSPM sont filtrées en fonction des `Workflow.Status` champs `RecordState` et du AWS Security Finding Format (ASFF). Cela s'ajoute aux filtres pour un aperçu ou une intégration spécifique.

L'état de l'enregistrement indique si une recherche est active ou archivée. Par défaut, une liste de résultats affiche uniquement les résultats actifs. Un fournisseur de recherche peut archiver une découverte si elle n'est plus active ou importante. Security Hub CSPM archive également automatiquement les résultats des contrôles si la ressource associée est supprimée.

L'état du flux de travail indique l'état d'une enquête sur un résultat. Par défaut, une liste de résultats affiche uniquement ceux dont l'état du flux de travail est `NEW` ou `NOTIFIED`. Vous pouvez mettre à jour l'état du flux de travail d'une découverte.

Instructions pour ajouter des filtres

Vous pouvez filtrer une liste de recherche selon un maximum de dix attributs. Pour chaque attribut, vous pouvez fournir jusqu'à 20 valeurs de filtre.

Lors du filtrage de la liste de recherche, Security Hub CSPM applique une `AND` logique à l'ensemble de filtres. Un résultat ne correspond que s'il correspond à tous les filtres fournis. Par exemple, si vous ajoutez GuardDuty un filtre pour le nom du produit et `AwsS3Bucket` un filtre pour le type de ressource, Security Hub CSPM affiche les résultats qui correspondent à ces deux critères.

Security Hub CSPM applique une `OR` logique aux filtres qui utilisent le même attribut mais des valeurs différentes. Par exemple, si vous ajoutez Amazon Inspector GuardDuty et Amazon Inspector comme valeurs de filtre pour le nom du produit, Security Hub CSPM affiche les résultats générés par Amazon Inspector GuardDuty ou par Amazon Inspector.

Pour ajouter des filtres à une liste de résultats (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Pour afficher la liste des résultats, effectuez l'une des actions suivantes dans le volet de navigation :

   - Choisissez Résultats.
   - Choisissez Informations. Choisissez un aperçu. Ensuite, dans la liste des résultats, choisissez un résultat d'analyse.

- Choisissez Integrations (Intégrations). Choisissez Afficher les résultats pour une intégration.

3. Dans la zone Ajouter des filtres, sélectionnez un ou plusieurs champs selon lesquels filtrer.

   Lorsque vous filtrez par nom de société ou nom de produit, la console utilise le niveau supérieur `CompanyName` et `ProductName` les champs du AWS Security Finding Format (ASFF). L'API utilise les valeurs qui sont imbriquées sous`ProductFields`.

4. Choisissez le type de correspondance de filtre.

   Pour un filtre de chaînes, vous pouvez choisir l'une des options suivantes :

   - est — Trouvez une valeur qui correspond exactement à la valeur du filtre.
   - commence par : recherchez une valeur qui commence par la valeur du filtre.
   - n'est pas : recherchez une valeur qui ne correspond pas à la valeur du filtre.
   - ne commence pas par : recherchez une valeur qui ne commence pas par la valeur du filtre.

   Pour le champ Balises de ressources, vous pouvez filtrer en fonction de clés ou de valeurs spécifiques.

   Pour un filtre numérique, vous pouvez choisir de fournir un numéro unique (Simple) ou une plage de nombres (Plage).

   Pour un filtre de date ou d'heure, vous pouvez choisir de fournir une durée à partir de la date et de l'heure actuelles (fenêtre déroulante) ou une plage de dates spécifique (plage fixe).

   L'ajout de plusieurs filtres entraîne les interactions suivantes :

   - est et commence par des filtres joints par OR. Une valeur correspond si elle contient l'une des valeurs de filtre. Par exemple, si vous spécifiez que l'étiquette de gravité est CRITIQUE et que l'étiquette de gravité est ÉLEVÉE, les résultats incluent à la fois des valeurs critiques et des valeurs de gravité élevées.
   - n'est pas et ne commence pas par des filtres joints par ET. Une valeur correspond uniquement si elle ne contient aucune de ces valeurs de filtre. Par exemple, si vous spécifiez que l'étiquette de gravité n'est pas FAIBLE et que l'étiquette de gravité n'est pas MOYENNE, les résultats n'incluent pas les résultats de gravité faible ou moyenne.

   Si vous avez un filtre is sur un champ, vous ne pouvez pas avoir de filtre is not ou a ne commence pas par un filtre sur le même champ.

5. Spécifiez la valeur du filtre. Pour les filtres de chaînes, la valeur du filtre fait la distinction entre majuscules et minuscules.
6. Cliquez sur Appliquer.

   Pour un filtre existant, vous pouvez modifier le type ou la valeur de correspondance du filtre. Dans une liste de recherche filtrée, choisissez le filtre. Dans la zone Modifier le filtre, choisissez le nouveau type ou la nouvelle valeur de correspondance, puis choisissez Appliquer.

   Pour supprimer un filtre, cliquez sur l'icône X. La liste est mise à jour automatiquement pour refléter les modifications.

Regroupement des résultats dans Security Hub CSPM

Vous pouvez regrouper les résultats dans AWS Security Hub CSPM en fonction des valeurs d'un attribut sélectionné.

Lorsque vous regroupez les résultats, la liste des résultats est remplacée par une liste de valeurs pour l'attribut sélectionné dans les résultats correspondants. Pour chaque valeur, la liste affiche le nombre de résultats correspondants.

Par exemple, si vous regroupez les résultats par Compte AWS identifiant, une liste d'identifiants de compte s'affiche, avec le nombre de résultats correspondants pour chaque compte.

Security Hub CSPM peut afficher jusqu'à 100 valeurs pour un attribut sélectionné. S'il y a plus de 100 valeurs, seules les 100 premières s'affichent.

Lorsque vous choisissez une valeur d'attribut, Security Hub CSPM affiche la liste des résultats correspondants pour cette valeur.

Pour regrouper les résultats dans une liste de résultats (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Pour afficher la liste des résultats, effectuez l'une des actions suivantes dans le volet de navigation :

   - Choisissez Résultats.
   - Choisissez Informations. Choisissez un aperçu. Ensuite, dans la liste des résultats, choisissez un résultat d'analyse.

- Choisissez Integrations (Intégrations). Choisissez Afficher les résultats pour une intégration.

3. Dans la liste déroulante Regrouper par, choisissez l'attribut à utiliser pour le regroupement.

   Pour supprimer un attribut de regroupement, cliquez sur l'icône x. Lorsque vous supprimez l'attribut de regroupement, la liste passe de la liste des valeurs des attributs à une liste de résultats.

Configuration de l'état du flux de travail des résultats dans Security Hub CSPM

L'état du flux de travail permet de suivre la progression de votre enquête sur une découverte. L'état du flux de travail est spécifique à une découverte individuelle et n'affecte pas la génération de nouvelles découvertes. Par exemple, si vous modifiez le statut du flux de travail d'une découverte sur `SUPPRESSED` ou`RESOLVED`, votre modification n'empêche pas Security Hub CSPM de générer une nouvelle découverte pour le même problème.

L'état du flux de travail d'une découverte peut prendre l'une des valeurs suivantes.

NOUVEAU

État initial d'un résultat avant que vous ne l'examiniez.

Les résultats qui sont ingérés à partir d'intégrés Services AWS, tels que AWS Config, ont `NEW` pour statut initial.

Security Hub CSPM réinitialise également l'état du flux de travail de l'un `NOTIFIED` ou l'autre `RESOLVED` à `NEW` dans les cas suivants :

- `RecordState`passe de `ARCHIVED` à`ACTIVE`.
- `Compliance.Status`passe de `PASSED` à `FAILED``WARNING`, ou`NOT_AVAILABLE`.

Ces modifications impliquent la nécessité d'une enquête supplémentaire.

NOTIFIÉ

Indique que vous avez informé le propriétaire de la ressource du problème de sécurité. Vous pouvez utiliser cet état lorsque vous n'êtes pas le propriétaire de la ressource et que vous avez besoin de son intervention pour résoudre un problème de sécurité.

Si l'une des situations suivantes se produit, l'état du flux de travail passe automatiquement de `NOTIFIED` à `NEW` :

- `RecordState`passe de `ARCHIVED` à`ACTIVE`.
- `Compliance.Status`passe de `PASSED` à `FAILED`, `WARNING`, ou`NOT_AVAILABLE`.

SUPPRIMÉ

Indique que vous avez examiné le résultat et que vous ne pensez pas qu'une action soit nécessaire.

L'état du flux de travail d'une `SUPPRESSED` découverte ne change pas s'il `RecordState` passe de `ARCHIVED` à`ACTIVE`.

RÉSOLU

Le résultat a été examiné et corrigé. Il est maintenant considéré comme résolu.

Le résultat demeure `RESOLVED` sauf si l'une des situations suivantes se produit :

- `RecordState`passe de `ARCHIVED` à`ACTIVE`.
- `Compliance.Status`passe de `PASSED` à `FAILED`, `WARNING`, ou`NOT_AVAILABLE`.

Dans ces cas, l'état du flux de travail est automatiquement réinitialisé à`NEW`.

Pour les résultats des contrôles, si `Compliance.Status` c'est le cas`PASSED`, Security Hub CSPM définit automatiquement l'état du flux de travail sur. `RESOLVED`

Définition de l'état des résultats dans le flux de travail

Pour modifier l'état du flux de travail d'un ou de plusieurs résultats, vous pouvez utiliser la console Security Hub CSPM ou l'API Security Hub CSPM. Si vous modifiez l'état du flux de travail d'une découverte, notez que le traitement de votre demande et la mise à jour de la découverte par Security Hub CSPM peuvent prendre plusieurs minutes.

> **Tip**
>
> Vous pouvez également modifier automatiquement l'état des résultats du flux de travail à l'aide de règles d'automatisation. Grâce aux règles d'automatisation, vous configurez Security Hub CSPM pour mettre à jour automatiquement l'état des résultats du flux de travail en fonction des critères que vous spécifiez. Pour de plus amples informations, veuillez consulter Comprendre les règles d'automatisation dans Security Hub CSPM.

Pour modifier l'état du flux de travail d'un ou de plusieurs résultats, choisissez votre méthode préférée et suivez les étapes.

Security Hub CSPM console

Pour modifier l'état des résultats du flux de travail

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, effectuez l'une des opérations suivantes pour afficher un tableau des résultats :
   - Choisissez Findings.
   - Choisissez Informations. Choisissez ensuite un aperçu. Dans les résultats d'analyse, choisissez un résultat.
   - Choisissez Integrations (Intégrations). Ensuite, dans la section consacrée à l'intégration, choisissez Voir les résultats.
   - Choisissez Normes de sécurité. Ensuite, dans la section relative à la norme, choisissez Afficher les résultats. Dans le tableau des contrôles, choisissez un contrôle pour afficher les résultats du contrôle.
3. Dans le tableau des résultats, cochez la case correspondant à chaque résultat dont vous souhaitez modifier l'état du flux de travail.
4. En haut de la page, choisissez État du flux de travail, puis choisissez le nouveau statut du flux de travail pour les résultats sélectionnés.
5. Dans la boîte de dialogue Définir l'état du flux de travail, entrez éventuellement une note détaillant la raison de la modification de l'état du flux de travail. Choisissez ensuite Définir le statut.

Security Hub CSPM API

Utilisez l'BatchUpdateFindingsopération. Fournissez à la fois l'identifiant et l'ARN du produit qui a généré le résultat. Vous pouvez obtenir ces informations en utilisant l'GetFindingsopération.

AWS CLI

Exécutez la commande batch-update-findings. Fournissez à la fois l'identifiant et l'ARN du produit qui a généré le résultat. Vous pouvez obtenir ces informations en exécutant la commande get-findings.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Exemple

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Envoi des résultats à une action CSPM personnalisée de Security Hub

Vous pouvez créer des actions personnalisées AWS Security Hub CSPM pour automatiser Security Hub CSPM avec Amazon. EventBridge Pour les actions personnalisées, le type d'événement est Security Hub Findings - Custom Action. Après avoir configuré une action personnalisée, vous pouvez lui envoyer des résultats. Pour de plus amples informations et pour obtenir des instructions complètes sur la création des actions personnalisées, veuillez consulter the section called "Réponse et remédiation automatisées".

Pour envoyer les résultats à une action personnalisée (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Pour afficher une liste de résultats, effectuez l'une des opérations suivantes :
   - Dans le volet de navigation CSPM de Security Hub, choisissez Findings.
   - Dans le volet de navigation CSPM de Security Hub, choisissez Insights. Choisissez un aperçu. Ensuite, dans la liste des résultats, choisissez un résultat d'analyse.
   - Dans le volet de navigation CSPM de Security Hub, choisissez Intégrations. Choisissez Afficher les résultats pour une intégration.
   - Dans le volet de navigation CSPM de Security Hub, sélectionnez Normes de sécurité. Choisissez Afficher les résultats pour afficher la liste des commandes. Choisissez ensuite le nom du contrôle.
3. Dans la liste des résultats, cochez la case correspondant à chaque résultat à envoyer à l'action personnalisée.

Vous pouvez envoyer jusqu'à 20 résultats à la fois.

4. Pour Actions, choisissez l'action personnalisée.

AWS Format de recherche de sécurité (ASFF)

AWS Security Hub CSPM utilise et regroupe les résultats de produits intégrés Services AWS et tiers. Security Hub CSPM traite ces résultats à l'aide d'un format de résultats standard appelé AWS Security Finding Format (ASFF), qui élimine le besoin de longs efforts de conversion des données.

Cette page fournit un aperçu complet du JSON pour une recherche au format ASFF (AWS Security Finding Format). Le format provient du schéma https://json-schema.org/ JSON. Choisissez le nom d'un objet lié pour consulter un exemple de découverte pour cet objet. La comparaison des résultats de votre Security Hub CSPM avec les ressources et les exemples présentés ici peut vous aider à interpréter vos résultats.

Pour une description des attributs ASFF individuels, reportez-vous aux sections the section called "Attributs ASFF de premier niveau requis" etthe section called "Attributs ASFF de niveau supérieur facultatifs".

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
```

```
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "ServiceName": "string"
       },
       "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
       },
       "NetworkConnectionAction": {
        "Blocked": boolean,
        "ConnectionDirection": "string",
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "Protocol": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
```

```
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "RemotePortDetails": {
         "Port": number,
         "PortName": "string"
        }
       },
       "PortProbeAction": {
        "Blocked": boolean,
        "PortProbeDetails": [{
         "LocalIpDetails": {
          "IpAddressV4": "string"
         },
         "LocalPortDetails": {
          "Port": number,
          "PortName": "string"
         },
         "RemoteIpDetails": {
          "City": {
           "CityName": "string"
          },
          "Country": {
           "CountryCode": "string",
           "CountryName": "string"
          },
          "GeoLocation": {
           "Lat": number,
           "Lon": number
          },
          "IpAddressV4": "string",
          "Organization": {
           "Asn": number,
           "AsnOrg": "string",
           "Isp": "string",
           "Org": "string"
          }
         }
        }]
       }
      },
      "AwsAccountId": "string",
```

```
      "AwsAccountName": "string",
      "CompanyName": "string",
      "Compliance": {
       "AssociatedStandards": [{
        "StandardsId": "string"
       }],
       "RelatedRequirements": ["string"],
       "SecurityControlId": "string",
       "SecurityControlParameters": [
        {
         "Name": "string",
         "Value": ["string"]
        }
      ],
       "Status": "string",
       "StatusReasons": [
        {
         "Description": "string",
         "ReasonCode": "string"
        }
       ]
      },
      "Confidence": number,
      "CreatedAt": "string",
      "Criticality": number,
      "Description": "string",
      "Detection": {
       "Sequence": {
        "Uid": "string",
        "Actors": [{
         "Id": "string",
         "Session": {
          "Uid": "string",
          "MfAStatus": "string",
          "CreatedTime": "string",
          "Issuer": "string"
         },
         "User": {
          "CredentialUid": "string",
          "Name": "string",
          "Type": "string",
          "Uid": "string",
          "Account": {
           "Uid": "string",
```

```
          "Name": "string"
         }
        }
       }],
       "Endpoints": [{
        "Id": "string",
        "Ip": "string",
        "Domain": "string",
        "Port": number,
        "Location": {
         "City": "string",
         "Country": "string",
         "Lat": number,
         "Lon": number
        },
        "AutonomousSystem": {
         "Name": "string",
         "Number": number
        },
        "Connection": {
         "Direction": "string"
        }
       }],
       "Signals": [{
        "Id": "string",
        "Title": "string",
        "ActorIds": ["string"],
        "Count": number,
        "FirstSeenAt": number,
        "SignalIndicators": [
         {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
         },
         {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
         }
        ],
        "LastSeenAt": number,
        "Name": "string",
        "ResourceIds": ["string"],
```

```
        "Type": "string"
       }],
       "SequenceIndicators": [
        {
         "Key": "string",
         "Title": "string",
         "Values": ["string"]
        },
        {
         "Key": "string",
         "Title": "string",
         "Values": ["string"]
        }
       ]
      }
     },
     "FindingProviderFields": {
      "Confidence": number,
      "Criticality": number,
      "RelatedFindings": [{
       "ProductArn": "string",
       "Id": "string"
      }],
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Types": ["string"]
     },
     "FirstObservedAt": "string",
     "GeneratorId": "string",
     "Id": "string",
     "LastObservedAt": "string",
     "Malware": [{
      "Name": "string",
      "Path": "string",
      "State": "string",
      "Type": "string"
     }],
     "Network": {
      "DestinationDomain": "string",
      "DestinationIpV4": "string",
      "DestinationIpV6": "string",
```

```
      "DestinationPort": number,
      "Direction": "string",
      "OpenPortRange": {
       "Begin": integer,
       "End": integer
      },
      "Protocol": "string",
      "SourceDomain": "string",
      "SourceIpV4": "string",
      "SourceIpV6": "string",
      "SourceMac": "string",
      "SourcePort": number
     },
     "NetworkPath": [{
      "ComponentId": "string",
      "ComponentType": "string",
      "Egress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
```

```
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
     },
     "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
     },
     "ProductArn": "string",
     "ProductFields": {
      "string": "string"
     },
     "ProductName": "string",
     "RecordState": "string",
     "Region": "string",
     "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
     }],
```

```
      "Remediation": {
       "Recommendation": {
        "Text": "string",
        "Url": "string"
       }
      },
      "Resources": [{
       "ApplicationArn": "string",
       "ApplicationName": "string",
       "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
         "AdditionalOccurrences": boolean,
         "CustomDataIdentifiers": {
          "Detections": [{
           "Arn": "string",
           "Count": integer,
           "Name": "string",
           "Occurrences": {
            "Cells": [{
             "CellReference": "string",
             "Column": integer,
             "ColumnName": "string",
             "Row": integer
            }],
            "LineRanges": [{
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            }],
            "OffsetRanges": [{
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            }],
            "Pages": [{
             "LineRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
             },
             "OffsetRange": {
              "End": integer,
              "Start": integer,
```

```
            "StartColumn": integer
           },
           "PageNumber": integer
          }],
          "Records": [{
           "JsonPath": "string",
           "RecordIndex": integer
          }]
         }
        }],
        "TotalCount": integer
       },
       "MimeType": "string",
       "SensitiveData": [{
        "Category": "string",
        "Detections": [{
         "Count": integer,
         "Occurrences": {
          "Cells": [{
           "CellReference": "string",
           "Column": integer,
           "ColumnName": "string",
           "Row": integer
          }],
          "LineRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "OffsetRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "Pages": [{
           "LineRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           },
           "OffsetRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
```

```
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
         "General": boolean,
         "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
         "DayOfWeek": "string",
```

```
          "TimeOfDay": "string",
          "TimeZone": "string"
         },
         "PubliclyAccessible": boolean,
         "SecurityGroups": [
          "string"
         ],
         "StorageType": "string",
         "SubnetIds": [
          "string",
          "string"
         ],
         "Users": [{
          "Username": "string"
         }]
        },
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
         "Name": "string",
         "Version": "string"
        },
        "AwsApiGatewayStage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
```

```
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
         "HttpMethod": "string",
         "LoggingLevel": "string",
         "MetricsEnabled": boolean,
         "RequireAuthorizationForCacheControl": boolean,
         "ResourcePath": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number,
         "UnauthorizedCacheControlHeaderStrategy": "string"
        }],
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
         "string": "string"
        },
        "WebAclArn": "string"
       },
       "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
```

```
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
```

```
          },
          {
           "AuthenticationType": "string"
          }
          ],
          "ApiId": "string",
          "Arn": "string",
          "AuthenticationType": "string",
          "Id": "string",
          "LogConfig": {
           "CloudWatchLogsRoleArn": "string",
           "ExcludeVerboseContent": boolean,
           "FieldLogLevel": "string"
          },
          "Name": "string",
          "XrayEnabled": boolean
         }
        },
        "AwsAthenaWorkGroup": {
         "Description": "string",
         "Name": "string",
         "WorkgroupConfiguration": {
          "ResultConfiguration": {
           "EncryptionConfiguration": {
            "EncryptionOption": "string",
            "KmsKey": "string"
           }
          }
         },
         "State": "string"
        },
        "AwsAutoScalingAutoScalingGroup": {
         "AvailabilityZones": [{
          "Value": "string"
         }],
         "CreatedTime": "string",
         "HealthCheckGracePeriod": integer,
         "HealthCheckType": "string",
         "LaunchConfigurationName": "string",
         "LoadBalancerNames": ["string"],
         "LaunchTemplate": {
                        "LaunchTemplateId": "string",
                        "LaunchTemplateName": "string",
                        "Version": "string"
```

```
                },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
```

```
        },
        "ImageId": "string",
        "InstanceMonitoring": {
         "Enabled": boolean
        },
        "InstanceType": "string",
        "KernelId": "string",
        "KeyName": "string",
        "LaunchConfigurationName": "string",
        "MetadataOptions": {
         "HttpEndPoint": "string",
         "HttpPutReponseHopLimit": number,
         "HttpTokens": "string"
        },
        "PlacementTenancy": "string",
        "RamdiskId": "string",
        "SecurityGroups": ["string"],
        "SpotPrice": "string",
        "UserData": "string"
       },
       "AwsBackupBackupPlan": {
        "BackupPlan": {
         "AdvancedBackupSettings": [{
          "BackupOptions": {
           "WindowsVSS":"string"
          },
          "ResourceType":"string"
         }],
         "BackupPlanName": "string",
         "BackupPlanRule": [{
          "CompletionWindowMinutes": integer,
          "CopyActions": [{
           "DestinationBackupVaultArn": "string",
           "Lifecycle": {
            "DeleteAfterDays": integer,
            "MoveToColdStorageAfterDays": integer
           }
          }],
          "Lifecycle": {
           "DeleteAfterDays": integer
          },
          "RuleName": "string",
          "ScheduleExpression": "string",
          "StartWindowMinutes": integer,
```

```
          "TargetBackupVault": "string"
         }]
        },
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "VersionId": "string"
      },
       "AwsBackupBackupVault": {
        "AccessPolicy": {
         "Statement": [{
          "Action": ["string"],
          "Effect": "string",
          "Principal": {
           "AWS": "string"
          },
          "Resource": "string"
         }],
         "Version": "string"
        },
        "BackupVaultArn": "string",
        "BackupVaultName": "string",
        "EncryptionKeyArn": "string",
        "Notifications": {
         "BackupVaultEvents": ["string"],
         "SNSTopicArn": "string"
        }
       },
       "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
        "CalculatedLifecycle": {
         "DeleteAt": "string",
         "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
```

```
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
         "DeleteAfterDays": integer,
         "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
       },
       "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
         "Name": "string",
         "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
```

```
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
```

```
        "OutputValue": "string"
       }],
       "RoleArn": "string",
       "StackId": "string",
       "StackName": "string",
       "StackStatus": "string",
       "StackStatusReason": "string",
       "TimeoutInMinutes": number
      },
      "AwsCloudFrontDistribution": {
       "CacheBehaviors": {
        "Items": [{
         "ViewerProtocolPolicy": "string"
        }]
       },
       "DefaultCacheBehavior": {
        "ViewerProtocolPolicy": "string"
       },
       "DefaultRootObject": "string",
       "DomainName": "string",
       "Etag": "string",
       "LastModifiedTime": "string",
       "Logging": {
        "Bucket": "string",
        "Enabled": boolean,
        "IncludeCookies": boolean,
        "Prefix": "string"
       },
       "OriginGroups": {
        "Items": [{
         "FailoverCriteria": {
          "StatusCodes": {
           "Items": [number],
           "Quantity": number
          }
         }
        }]
       },
       "Origins": {
        "Items": [{
         "CustomOriginConfig": {
          "HttpPort": number,
          "HttpsPort": number,
          "OriginKeepaliveTimeout": number,
```

```
          "OriginProtocolPolicy": "string",
          "OriginReadTimeout": number,
          "OriginSslProtocols": {
           "Items": ["string"],
           "Quantity": number
          }
         },
         "DomainName": "string",
         "Id": "string",
         "OriginPath": "string",
         "S3OriginConfig": {
          "OriginAccessIdentity": "string"
         }
        }]
       },
       "Status": "string",
       "ViewerCertificate": {
        "AcmCertificateArn": "string",
        "Certificate": "string",
        "CertificateSource": "string",
        "CloudFrontDefaultCertificate": boolean,
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
       "HomeRegion": "string",
       "IncludeGlobalServiceEvents": boolean,
       "IsMultiRegionTrail": boolean,
       "IsOrganizationTrail": boolean,
       "KmsKeyId": "string",
       "LogFileValidationEnabled": boolean,
       "Name": "string",
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "SnsTopicArn": "string",
       "SnsTopicName": "string",
       "TrailArn": "string"
      },
```

```
      "AwsCloudWatchAlarm": {
       "ActionsEnabled": boolean,
       "AlarmActions": ["string"],
       "AlarmArn": "string",
       "AlarmConfigurationUpdatedTimestamp": "string",
       "AlarmDescription": "string",
       "AlarmName": "string",
       "ComparisonOperator": "string",
       "DatapointsToAlarm": number,
       "Dimensions": [{
        "Name": "string",
        "Value": "string"
       }],
       "EvaluateLowSampleCountPercentile": "string",
       "EvaluationPeriods": number,
       "ExtendedStatistic": "string",
       "InsufficientDataActions": ["string"],
       "MetricName": "string",
       "Namespace": "string",
       "OkActions": ["string"],
       "Period": number,
       "Statistic": "string",
       "Threshold": number,
       "ThresholdMetricId": "string",
       "TreatMissingData": "string",
       "Unit": "string"
      },
      "AwsCodeBuildProject": {
       "Artifacts": [{
        "ArtifactIdentifier": "string",
        "EncryptionDisabled": boolean,
        "Location": "string",
        "Name": "string",
        "NamespaceType": "string",
        "OverrideArtifactName": boolean,
        "Packaging": "string",
        "Path": "string",
        "Type": "string"
       }],
       "SecondaryArtifacts": [{
                   "ArtifactIdentifier": "string",
                   "Type": "string",
                   "Location": "string",
                   "Name": "string",
```

```
                "NamespaceType": "string",
                "Packaging": "string",
                "Path": "string",
                "EncryptionDisabled": boolean,
                "OverrideArtifactName": boolean
            }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
         "Type": "string"
        },
        "LogsConfig": {
         "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
```

```
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
      }
    },
    "AwsDmsEndpoint": {
      "CertificateArn": "string",
      "DatabaseName": "string",
      "EndpointArn": "string",
      "EndpointIdentifier": "string",
      "EndpointType": "string",
      "EngineName": "string",
      "KmsKeyId": "string",
      "Port": integer,
      "ServerName": "string",
      "SslMode": "string",
      "Username": "string"
    },
    "AwsDmsReplicationInstance": {
      "AllocatedStorage": integer,
      "AutoMinorVersionUpgrade": boolean,
      "AvailabilityZone": "string",
      "EngineVersion": "string",
      "KmsKeyId": "string",
      "MultiAZ": boolean,
      "PreferredMaintenanceWindow": "string",
      "PubliclyAccessible": boolean,
      "ReplicationInstanceClass": "string",
      "ReplicationInstanceIdentifier": "string",
      "ReplicationSubnetGroup": {
          "ReplicationSubnetGroupIdentifier": "string"
      },
      "VpcSecurityGroups": [
          {
              "VpcSecurityGroupId": "string"
          }
      ]
    },
    "AwsDmsReplicationTask": {
      "CdcStartPosition": "string",
      "Id": "string",
      "MigrationType": "string",
      "ReplicationInstanceArn": "string",
      "ReplicationTaskIdentifier": "string",
      "ReplicationTaskSettings": {
```

```
        "string": "string"
       },
       "SourceEndpointArn": "string",
       "TableMappings": {
        "string": "string"
       },
       "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
       "AttributeDefinitions": [{
        "AttributeName": "string",
        "AttributeType": "string"
       }],
       "BillingModeSummary": {
        "BillingMode": "string",
        "LastUpdateToPayPerRequestDateTime": "string"
       },
       "CreationDateTime": "string",
       "DeletionProtectionEnabled": boolean,
       "GlobalSecondaryIndexes": [{
        "Backfilling": boolean,
        "IndexArn": "string",
        "IndexName": "string",
        "IndexSizeBytes": number,
        "IndexStatus": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        },
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        }
       }],
       "GlobalTableVersion": "string",
       "ItemCount": number,
```

```
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
         }],
         "KmsMasterKeyId": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         },
         "RegionName": "string",
         "ReplicaStatus": "string",
         "ReplicaStatusDescription": "string"
        }],
        "RestoreSummary": {
         "RestoreDateTime": "string",
         "RestoreInProgress": boolean,
         "SourceBackupArn": "string",
```

```
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
```

```
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
      },
      "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
          "HttpEndpoint": "string",
          "HttpProtocolIpv6": "string",
          "HttpPutResponseHopLimit": number,
          "HttpTokens": "string",
          "InstanceMetadataTags": "string"
        },
        "Monitoring": {
          "State": "string"
        },
        "NetworkInterfaces": [{
          "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
      },
      "AwsEc2LaunchTemplate": {
```

```
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
         "Monitoring": {
          "Enabled": boolean
         },
         "NetworkInterfaces": [{
          "AssociatePublicIpAddress" : boolean
         }]
        },
        "LaunchTemplateName": "string",
        "LicenseSpecifications": ["string"],
        "SecurityGroupIds": ["string"],
        "SecurityGroups": ["string"],
        "TagSpecifications": ["string"]
       },
       "AwsEc2NetworkAcl": {
        "Associations": [{
         "NetworkAclAssociationId": "string",
         "NetworkAclId": "string",
         "SubnetId": "string"
        }],
        "Entries": [{
         "CidrBlock": "string",
         "Egress": boolean,
         "IcmpTypeCode": {
```

```
          "Code": number,
          "Type": number
         },
         "Ipv6CidrBlock": "string",
         "PortRange": {
          "From": number,
          "To": number
         },
         "Protocol": "string",
         "RuleAction": "string",
         "RuleNumber": number
        }],
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2NetworkInterface": {
        "Attachment": {
         "AttachmentId": "string",
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "DeviceIndex": number,
         "InstanceId": "string",
         "InstanceOwnerId": "string",
         "Status": "string"
        },
        "Ipv6Addresses": [{
         "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
         "GroupName": "string"
        }],
        "SourceDestCheck": boolean
       },
       "AwsEc2RouteTable": {
```

```
        "AssociationSet": [{
         "AssociationState": {
          "State": "string"
         },
         "Main": boolean,
         "RouteTableAssociationId": "string",
         "RouteTableId": "string"
        }],
        "PropogatingVgwSet": [],
        "RouteTableId": "string",
        "RouteSet": [
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         },
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
       "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
```

```
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": boolean,
        "AvailabilityZone": "string",
        "AvailabilityZoneId": "string",
        "AvailableIpAddressCount": number,
        "CidrBlock": "string",
        "DefaultForAz": boolean,
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "Ipv6CidrBlock": "string",
         "CidrBlockState": "string"
        }],
```

```
        "MapPublicIpOnLaunch": boolean,
        "OwnerId": "string",
        "State": "string",
        "SubnetArn": "string",
        "SubnetId": "string",
        "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
        "AmazonSideAsn": number,
        "AssociationDefaultRouteTableId": "string",
        "AutoAcceptSharedAttachments": "string",
        "DefaultRouteTableAssociation": "string",
        "DefaultRouteTablePropagation": "string",
        "Description": "string",
        "DnsSupport": "string",
        "Id": "string",
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
        "Attachments": [{
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "InstanceId": "string",
          "Status": "string"
        }],
        "CreateTime": "string",
        "DeviceName": "string",
        "Encrypted": boolean,
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
```

```
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "CidrBlockState": "string",
         "Ipv6CidrBlock": "string"
        }],
        "State": "string"
       },
       "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
```

```
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
       "ImageScanningConfiguration": {
        "ScanOnPush": boolean
       },
       "ImageTagMutability": "string",
       "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
       },
       "RepositoryName": "string",
       "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
```

```
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
         "Name": "string",
         "Value": "string"
        }],
        "Configuration": {
         "ExecuteCommandConfiguration": {
          "KmsKeyId": "string",
          "LogConfiguration": {
           "CloudWatchEncryptionEnabled": boolean,
           "CloudWatchLogGroupName": "string",
           "S3BucketName": "string",
           "S3EncryptionEnabled": boolean,
           "S3KeyPrefix": "string"
          },
          "Logging": "string"
         }
        },
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
```

```
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
         "MaximumPercent": number,
         "MinimumHealthyPercent": number
        },
        "DeploymentController": {
         "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
```

```
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
```

```
        "DnsServers": ["string"],
        "DockerLabels": {
         "string": "string"
        },
        "DockerSecurityOptions": ["string"],
        "EntryPoint": ["string"],
        "Environment": [{
         "Name": "string",
         "Value": "string"
        }],
        "EnvironmentFiles": [{
         "Type": "string",
         "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
         "Hostname": "string",
         "IpAddress": "string"
        }],
        "FirelensConfiguration": {
         "Options": {
          "string": "string"
         },
         "Type": "string"
        },
        "HealthCheck": {
         "Command": ["string"],
         "Interval": number,
         "Retries": number,
         "StartPeriod": number,
         "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
```

```
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
         "HostPort": number,
         "Protocol": "string"
        }],
        "Privileged": boolean,
        "PseudoTerminal": boolean,
        "ReadonlyRootFilesystem": boolean,
        "RepositoryCredentials": {
         "CredentialsParameter": "string"
        },
        "ResourceRequirements": [{
         "Type": "string",
         "Value": "string"
```

```
        }],
        "Secrets": [{
         "Name": "string",
         "ValueFrom": "string"
        }],
        "StartTimeout": number,
        "StopTimeout": number,
        "SystemControls": [{
         "Namespace": "string",
         "Value": "string"
        }],
        "Ulimits": [{
         "HardLimit": number,
         "Name": "string",
         "SoftLimit": number
        }],
        "User": "string",
        "VolumesFrom": [{
         "ReadOnly": boolean,
         "SourceContainer": "string"
        }],
        "WorkingDirectory": "string"
       }],
       "Cpu": "string",
       "ExecutionRoleArn": "string",
       "Family": "string",
       "InferenceAccelerators": [{
        "DeviceName": "string",
        "DeviceType": "string"
       }],
       "IpcMode": "string",
       "Memory": "string",
       "NetworkMode": "string",
       "PidMode": "string",
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "ProxyConfiguration": {
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
```

```
        "Type": "string"
       },
       "RequiresCompatibilities": ["string"],
       "Status": "string",
       "TaskRoleArn": "string",
       "Volumes": [{
        "DockerVolumeConfiguration": {
         "Autoprovision": boolean,
         "Driver": "string",
         "DriverOpts": {
          "string": "string"
         },
         "Labels": {
          "string": "string"
         },
         "Scope": "string"
        },
        "EfsVolumeConfiguration": {
         "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
         },
         "FilesystemId": "string",
         "RootDirectory": "string",
         "TransitEncryption": "string",
         "TransitEncryptionPort": number
        },
        "Host": {
         "SourcePath": "string"
        },
        "Name": "string"
       }]
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
```

```
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
```

```
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
         "string": "string"
        }
       },
       "DomainEndpointOptions": {
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "ElasticsearchClusterConfig": {
        "DedicatedMasterCount": number,
        "DedicatedMasterEnabled": boolean,
        "DedicatedMasterType": "string",
        "InstanceCount": number,
        "InstanceType": "string",
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
       "ElasticsearchVersion": "string",
       "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
       },
```

```
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VPCOptions": {
         "AvailabilityZones": [
          "string"
         ],
         "SecurityGroupIds": [
          "string"
         ],
         "SubnetIds": [
          "string"
         ],
         "VPCId": "string"
        }
       },
       "AwsElbLoadBalancer": {
        "AvailabilityZones": ["string"],
        "BackendServerDescriptions": [{
         "InstancePort": number,
         "PolicyNames": ["string"]
```

```
        }],
        "CanonicalHostedZoneName": "string",
        "CanonicalHostedZoneNameID": "string",
        "CreatedTime": "string",
        "DnsName": "string",
        "HealthCheck": {
         "HealthyThreshold": number,
         "Interval": number,
         "Target": "string",
         "Timeout": number,
         "UnhealthyThreshold": number
        },
        "Instances": [{
         "InstanceId": "string"
        }],
        "ListenerDescriptions": [{
         "Listener": {
          "InstancePort": number,
          "InstanceProtocol": "string",
          "LoadBalancerPort": number,
          "Protocol": "string",
          "SslCertificateId": "string"
         },
         "PolicyNames": ["string"]
        }],
        "LoadBalancerAttributes": {
         "AccessLog": {
          "EmitInterval": number,
          "Enabled": boolean,
          "S3BucketName": "string",
          "S3BucketPrefix": "string"
         },
         "ConnectionDraining": {
          "Enabled": boolean,
          "Timeout": number
         },
         "ConnectionSettings": {
          "IdleTimeout": number
         },
         "CrossZoneLoadBalancing": {
          "Enabled": boolean
         },
         "AdditionalAttributes": [{
                        "Key": "string",
```

```
                    "Value": "string"
                }]
      },
      "LoadBalancerName": "string",
      "Policies": {
       "AppCookieStickinessPolicies": [{
        "CookieName": "string",
        "PolicyName": "string"
       }],
       "LbCookieStickinessPolicies": [{
        "CookieExpirationPeriod": number,
        "PolicyName": "string"
       }],
       "OtherPolicies": ["string"]
      },
      "Scheme": "string",
      "SecurityGroups": ["string"],
      "SourceSecurityGroup": {
       "GroupName": "string",
       "OwnerAlias": "string"
      },
      "Subnets": ["string"],
      "VpcId": "string"
     },
     "AwsElbv2LoadBalancer": {
      "AvailabilityZones": {
       "SubnetId": "string",
       "ZoneName": "string"
      },
      "CanonicalHostedZoneId": "string",
      "CreatedTime": "string",
      "DNSName": "string",
      "IpAddressType": "string",
      "LoadBalancerAttributes": [{
       "Key": "string",
       "Value": "string"
      }],
      "Scheme": "string",
      "SecurityGroups": ["string"],
      "State": {
       "Code": "string",
       "Reason": "string"
      },
      "Type": "string",
```

```
        "VpcId": "string"
      },
      "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
      },
      "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
```

```
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
         "CloudTrail": {
          "Status": "string"
         },
         "DnsLogs": {
          "Status": "string"
         },
         "FlowLogs": {
          "Status": "string"
         },
         "S3Logs": {
          "Status": "string"
         },
         "Kubernetes": {
          "AuditLogs": {
           "Status": "string"
          }
         },
         "MalwareProtection": {
          "ScanEc2InstanceWithFindings": {
           "EbsVolumes": {
            "Status": "string"
           }
          },
          "ServiceRole": "string"
         }
        }
       },
       "AwsIamAccessKey": {
        "AccessKeyId": "string",
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
```

```
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
        }
       },
       "Status": "string"
      },
      "AwsIamGroup": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupId": "string",
       "GroupName": "string",
       "GroupPolicyList": [{
        "PolicyName": "string"
       }],
       "Path": "string"
      },
      "AwsIamPolicy": {
       "AttachmentCount": number,
       "CreateDate": "string",
       "DefaultVersionId": "string",
       "Description": "string",
       "IsAttachable": boolean,
       "Path": "string",
       "PermissionsBoundaryUsageCount": number,
       "PolicyId": "string",
       "PolicyName": "string",
       "PolicyVersionList": [{
        "CreateDate": "string",
        "IsDefaultVersion": boolean,
        "VersionId": "string"
       }],
       "UpdateDate": "string"
      },
      "AwsIamRole": {
       "AssumeRolePolicyDocument": "string",
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
```

```
        "CreateDate": "string",
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
```

```
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
         },
         "Error": {
          "ErrorCode": "string",
          "Message": "string"
         }
```

```
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
         "CodeSize": number
        },
        "PackageType": "string",
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
        },
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
       "AwsMskCluster": {
        "ClusterInfo": {
         "ClientAuthentication": {
          "Sasl": {
           "Scram": {
            "Enabled": boolean
           },
           "Iam": {
            "Enabled": boolean
           }
          },
          "Tls": {
```

```
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
```

```
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
       "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
       "Description": "string",
       "RuleGroup": {
        "RulesSource": {
         "RulesSourceList": {
          "GeneratedRulesType": "string",
          "Targets": ["string"],
          "TargetTypes": ["string"]
         },
         "RulesString": "string",
         "StatefulRules": [{
          "Action": "string",
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
```

```
          }],
          "StatelessRulesAndCustomActions": {
           "CustomActions": [{
            "ActionDefinition": {
             "PublishMetricAction": {
              "Dimensions": [{
               "Value": "string"
              }]
             }
            },
            "ActionName": "string"
           }],
           "StatelessRules": [{
            "Priority": number,
            "RuleDefinition": {
             "Actions": ["string"],
             "MatchAttributes": {
              "DestinationPorts": [{
               "FromPort": number,
               "ToPort": number
              }],
              "Destinations": [{
               "AddressDefinition": "string"
              }],
              "Protocols": [number],
              "SourcePorts": [{
               "FromPort": number,
               "ToPort": number
              }],
              "Sources": [{
               "AddressDefinition": "string"
              }],
              "TcpFlags": [{
               "Flags": ["string"],
               "Masks": ["string"]
              }]
             }
            }
           }]
          }
         },
         "RuleVariables": {
          "IpSets": {
           "Definition": ["string"]
```

```
          },
          "PortSets": {
           "Definition": ["string"]
          }
         }
        },
        "RuleGroupArn": "string",
        "RuleGroupId": "string",
        "RuleGroupName": "string",
        "Type": "string"
       },
       "AwsOpenSearchServiceDomain": {
        "AccessPolicies": "string",
        "AdvancedSecurityOptions": {
         "Enabled": boolean,
         "InternalUserDatabaseEnabled": boolean,
         "MasterUserOptions": {
          "MasterUserArn": "string",
          "MasterUserName": "string",
          "MasterUserPassword": "string"
         }
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
```

```
        },
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "EngineVersion": "string",
        "Id": "string",
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "OptionalDeployment": boolean,
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VpcOptions": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        }
       },
       "AwsRdsDbCluster": {
```

```
        "ActivityStreamStatus": "string",
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
         "DbClusterOptionGroupName": "string",
         "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
```

```
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
```

```
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
```

```
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
```

```
          "Value": "string"
         }],
         "StorageType": "string"
        },
        "PerformanceInsightsEnabled": boolean,
        "PerformanceInsightsKmsKeyId": "string",
        "PerformanceInsightsRetentionPeriod": number,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
        "ReadReplicaDBInstanceIdentifiers": ["string"],
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
         "Normal": boolean,
         "Status": "string",
         "StatusType": "string"
        }],
        "StorageEncrypted": boolean,
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
         "Ec2SecurityGroupName": "string",
         "Ec2SecurityGroupOwnerId": "string",
         "Status": "string"
        }],
        "IpRanges": [{
```

```
        "CidrIp": "string",
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "OptionGroupName": "string",
       "PercentProgress": integer,
       "Port": integer,
       "ProcessorFeatures": [],
       "SnapshotCreateTime": "string",
       "SnapshotType": "string",
       "SourceDbSnapshotIdentifier": "string",
       "SourceRegion": "string",
       "Status": "string",
       "StorageType": "string",
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
       "CustomerAwsId": "string",
       "CustSubscriptionId": "string",
       "Enabled": boolean,
       "EventCategoriesList": ["string"],
       "EventSubscriptionArn": "string",
       "SnsTopicArn": "string",
       "SourceIdsList": ["string"],
       "SourceType": "string",
```

```
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
            "ParameterApplyErrorDescription": "string",
            "ParameterApplyStatus": "string",
            "ParameterName": "string"
          }],
          "ParameterApplyStatus": "string",
          "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
          "ClusterSecurityGroupName": "string",
          "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
          "DestinationRegion": "string",
          "ManualSnapshotRetentionPeriod": number,
          "RetentionPeriod": number,
          "SnapshotCopyGrantName": "string"
        },
        "ClusterStatus": "string",
        "ClusterSubnetGroupName": "string",
        "ClusterVersion": "string",
        "DBName": "string",
        "DeferredMaintenanceWindows": [{
          "DeferMaintenanceEndTime": "string",
          "DeferMaintenanceIdentifier": "string",
          "DeferMaintenanceStartTime": "string"
```

```
        }],
        "ElasticIpStatus": {
         "ElasticIp": "string",
         "Status": "string"
        },
        "ElasticResizeNumberOfNodeOptions": "string",
        "Encrypted": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number
        },
        "EnhancedVpcRouting": boolean,
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
```

```
        "EncryptionType": "string",
        "EnhancedVpcRouting": boolean,
        "MaintenanceTrackName": "string",
        "MasterUserPassword": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PubliclyAccessible": "string"
       },
       "PreferredMaintenanceWindow": "string",
       "PubliclyAccessible": boolean,
       "ResizeInfo": {
        "AllowCancelResize": boolean,
        "ResizeType": "string"
       },
       "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": number,
        "ElapsedTimeInSeconds": number,
        "EstimatedTimeToCompletionInSeconds": number,
        "ProgressInMegaBytes": number,
        "SnapshotSizeInMegaBytes": number,
        "Status": "string"
       },
       "SnapshotScheduleIdentifier": "string",
       "SnapshotScheduleState": "string",
       "VpcId": "string",
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRoute53HostedZone": {
       "HostedZone": {
        "Id": "string",
        "Name": "string",
        "Config": {
         "Comment": "string"
        }
       },
       "NameServers": ["string"],
       "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
         "CloudWatchLogsLogGroupArn": "string",
         "Id": "string",
         "HostedZoneId": "string"
```

```
        }
       },
       "Vpcs": [
        {
         "Id": "string",
         "Region": "string"
        }
       ]
      },
      "AwsS3AccessPoint": {
       "AccessPointArn": "string",
       "Alias": "string",
       "Bucket": "string",
       "BucketAccountId": "string",
       "Name": "string",
       "NetworkOrigin": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "VpcConfiguration": {
        "VpcId": "string"
       }
      },
      "AwsS3AccountPublicAccessBlock": {
       "BlockPublicAcls": boolean,
       "BlockPublicPolicy": boolean,
       "IgnorePublicAcls": boolean,
       "RestrictPublicBuckets": boolean
      },
      "AwsS3Bucket": {
       "AccessControlList": "string",
       "BucketLifecycleConfiguration": {
        "Rules": [{
         "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": number
         },
         "ExpirationDate": "string",
         "ExpirationInDays": number,
         "ExpiredObjectDeleteMarker": boolean,
         "Filter": {
          "Predicate": {
```

```
          "Operands": [{
            "Prefix": "string",
            "Type": "string"
           },
           {
            "Tag": {
             "Key": "string",
             "Value": "string"
            },
            "Type": "string"
           }
          ],
          "Type": "string"
         }
        },
        "Id": "string",
        "NoncurrentVersionExpirationInDays": number,
        "NoncurrentVersionTransitions": [{
         "Days": number,
         "StorageClass": "string"
        }],
        "Prefix": "string",
        "Status": "string",
        "Transitions": [{
         "Date": "string",
         "Days": number,
         "StorageClass": "string"
        }]
       }]
      },
      "BucketLoggingConfiguration": {
       "DestinationBucketName": "string",
       "LogFilePrefix": "string"
      },
      "BucketName": "string",
      "BucketNotificationConfiguration": {
       "Configurations": [{
        "Destination": "string",
        "Events": ["string"],
        "Filter": {
         "S3KeyFilter": {
          "FilterRules": [{
           "Name": "string",
           "Value": "string"
```

```
          }]
         }
        },
        "Type": "string"
       }]
      },
      "BucketVersioningConfiguration": {
       "IsMfaDeleteEnabled": boolean,
       "Status": "string"
      },
      "BucketWebsiteConfiguration": {
       "ErrorDocument": "string",
       "IndexDocumentSuffix": "string",
       "RedirectAllRequestsTo": {
        "HostName": "string",
        "Protocol": "string"
       },
       "RoutingRules": [{
        "Condition": {
         "HttpErrorCodeReturnedEquals": "string",
         "KeyPrefixEquals": "string"
        },
        "Redirect": {
         "HostName": "string",
         "HttpRedirectCode": "string",
         "Protocol": "string",
         "ReplaceKeyPrefixWith": "string",
         "ReplaceKeyWith": "string"
        }
       }]
      },
      "CreatedAt": "string",
      "ObjectLockConfiguration": {
       "ObjectLockEnabled": "string",
       "Rule": {
        "DefaultRetention": {
         "Days": integer,
         "Mode": "string",
         "Years": integer
        }
       }
      },
      "OwnerAccountId": "string",
      "OwnerId": "string",
```

```
        "OwnerName": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
       },
       "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
         "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
       },
       "AwsSecretsManagerSecret": {
```

```
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
         "AutomaticallyAfterDays": integer
        }
       },
       "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
```

```
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
         }
        }
       },
       "AwsStepFunctionStateMachine": {
        "StateMachineArn": "string",
        "Name": "string",
        "Status": "string",
        "RoleArn": "string",
        "Type": "string",
        "LoggingConfiguration": {
         "Level": "string",
         "IncludeExecutionData": boolean
        },
        "TracingConfiguration": {
         "Enabled": boolean
        }
       },
       "AwsWafRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
```

```
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
      },
      "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
      },
      "AwsWafRegionalRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
          "Action": {
            "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string"
        }]
      },
      "AwsWafRegionalWebAcl": {
        "DefaultAction": "string",
        "MetricName" : "string",
        "Name": "string",
        "RulesList" : [{
          "Action": {
            "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string",
          "ExcludedRules": [{
            "ExclusionType": "string",
            "RuleId": "string"
```

```
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
```

```
          },
          {
          "Name": "string",
          "Value": "string"
          }
         ]
        }
       }
       },
       "Name": "string",
       "Priority": number,
       "VisibilityConfig": {
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string",
        "SampledRequestsEnabled": boolean
       }
      }],
      "VisibilityConfig": {
       "CloudWatchMetricsEnabled": boolean,
       "MetricName": "string",
       "SampledRequestsEnabled": boolean
      }
     },
     "AwsWafWebAcl": {
      "DefaultAction": "string",
      "Name": "string",
      "Rules": [{
       "Action": {
        "Type": "string"
       },
       "ExcludedRules": [{
        "RuleId": "string"
       }],
       "OverrideAction": {
        "Type": "string"
       },
       "Priority": number,
       "RuleId": "string",
       "Type": "string"
      }],
      "WebAclId": "string"
     },
     "AwsWafv2WebAcl": {
      "Arn": "string",
```

```
        "Capacity": number,
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
          }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "SampledRequestsEnabled": boolean,
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "CodeRepository": {
        "CodeSecurityIntegrationArn": "string",
        "ProjectName": "string",
        "ProviderType": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
```

```
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
         "Name": "string",
         "MountPath": "string"
        }]
       },
       "Other": {
        "string": "string"
       },
       "Id": "string",
       "Partition": "string",
       "Region": "string",
       "ResourceRole": "string",
       "Tags": {
        "string": "string"
       },
       "Type": "string"
      }],
      "SchemaVersion": "string",
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Sample": boolean,
      "SourceUrl": "string",
      "Threats": [{
       "FilePaths": [{
        "FileName": "string",
        "FilePath": "string",
        "Hash": "string",
        "ResourceId": "string"
       }],
       "ItemCount": number,
       "Name": "string",
       "Severity": "string"
      }],
      "ThreatIntelIndicators": [{
       "Category": "string",
       "LastObservedAt": "string",
```

```
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
     "Vulnerabilities": [{
      "CodeVulnerabilities": [{
       "Cwes": [
        "string",
        "string"
       ],
       "FilePath": {
        "EndLine": integer,
        "FileName": "string",
        "FilePath": "string",
        "StartLine": integer
       },
       "SourceArn":"string"
      }],
      "Cvss": [{
       "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
       }],
       "BaseScore": number,
       "BaseVector": "string",
       "Source": "string",
       "Version": "string"
      }],
      "EpssScore": number,
      "ExploitAvailable": "string",
      "FixAvailable": "string",
      "Id": "string",
      "LastKnownExploitAt": "string",
      "ReferenceUrls": ["string"],
      "RelatedVulnerabilities": ["string"],
      "Vendor": {
```

```
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
       "VulnerablePackages": [{
        "Architecture": "string",
        "Epoch": "string",
        "FilePath": "string",
        "FixedInVersion": "string",
        "Name": "string",
        "PackageManager": "string",
        "Release": "string",
        "Remediation": "string",
        "SourceLayerArn": "string",
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

Impact de la consolidation sur les champs et les valeurs ASFF

AWS Security Hub CSPM propose deux types de consolidation des contrôles :

- Vue des contrôles consolidés — Avec ce type de consolidation, chaque contrôle possède un identifiant unique pour toutes les normes. En outre, sur la console Security Hub CSPM, la page Contrôles affiche tous les contrôles, toutes normes confondues.
- Résultats de contrôle consolidés : avec ce type de consolidation, Security Hub CSPM produit un résultat unique pour un contrôle, même si le contrôle s'applique à plusieurs normes activées. Cela peut réduire le bruit de détection.

Vous ne pouvez ni activer ni désactiver l'affichage des contrôles consolidés. Les résultats de contrôle consolidés sont activés par défaut si vous activez Security Hub CSPM le 23 février 2023 ou après cette date. Sinon, elle est désactivée par défaut. Toutefois, pour les organisations, les résultats des

contrôles consolidés sont activés pour les comptes membres de Security Hub CSPM uniquement s'ils sont activés pour le compte administrateur. Pour en savoir plus sur les résultats des contrôles consolidés, consultezGénération et mise à jour des résultats de contrôle.

Les deux types de consolidation affectent les champs et les valeurs des résultats de contrôle dans leAWS Format de recherche de sécurité (ASFF).

Rubriques

- Vue consolidée des contrôles — modifications de l'ASFF
- Résultats des contrôles consolidés — modifications de l'ASFF
- Identifiants des générateurs avant et après l'obtention de résultats de contrôle consolidés
- L'impact de la consolidation sur les identifiants et titres de contrôle
- Mise à jour des workflows pour la consolidation

Vue consolidée des contrôles — modifications de l'ASFF

La fonction d'affichage des contrôles consolidés a introduit les modifications suivantes dans les champs et les valeurs des résultats des contrôles dans l'ASFF. Si vos flux de travail ne reposent pas sur les valeurs de ces champs ASFF, aucune action n'est requise. Si vos flux de travail s'appuient sur des valeurs spécifiques pour ces champs, mettez à jour vos flux de travail pour utiliser les valeurs actuelles.

Champ ASFF	Valeur de l'échantillon avant la vue des contrôles consolidés	Exemple de valeur après affichage des contrôles consolidés et description de la modification
Compliance.SecurityControlId	Non applicable (nouveau champ)	EC2.2 Introduit un identifiant de contrôle unique pour toutes les normes. `ProductFields.RuleId` fournit toujours l'identifiant de contrôle standard pour les contrôles CIS v1.2.0. `ProductFields.Cont`

Champ ASFF	Valeur de l'échantillon avant la vue des contrôles consolidés	Exemple de valeur après affichage des contrôles consolidés et description de la modification
		`rolId` fournit toujours l'identifiant de contrôle basé sur la norme pour les contrôles dans d'autres normes.
Compliance.AssociatedStandards	Non applicable (nouveau champ)	[{» StandardsId « :" standards /aws -foundational-security- best- /1.0.0 «}] practices/v Indique les normes dans lesquelles un contrôle est activé.
ProductFields.ArchivalReasons:0/Description	Non applicable (nouveau champ)	« Le résultat est dans un état ARCHIVÉ car les résultats des contrôles consolidés ont été activés ou désactivés. Cela entraîne l'archivage des résultats dans l'état précédent lorsque de nouveaux résultats sont générés. » Décrit pourquoi Security Hub CSPM a archivé les résultats existants.
ProductFields.ArchivalReasons:0/ReasonCode	Non applicable (nouveau champ)	« MISE À JOUR CONSOLIDÉE DES RÉSULTATS DE CONTRÔLE » Explique la raison pour laquelle Security Hub CSPM a archivé les résultats existants.

Champ ASFF	Valeur de l'échantillon avant la vue des contrôles consolidés	Exemple de valeur après affichage des contrôles consolidés et description de la modification
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Ce champ ne fait plus référence à une norme.
Remediation.Recommendation.Text	« Pour savoir comment résoudre ce problème, consultez la documentation PCI AWS DSS du Security Hub CSPM. »	« Pour savoir comment corriger ce problème, consultez la documentation des contrôles CSPM de AWS Security Hub. » Ce champ ne fait plus référence à une norme.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Ce champ ne fait plus référence à une norme.

Résultats des contrôles consolidés — modifications de l'ASFF

Si vous activez les résultats de contrôle consolidés, vous pourriez être concerné par les modifications suivantes apportées aux champs et aux valeurs des résultats de contrôle dans l'ASFF. Ces modifications s'ajoutent à celles introduites par la fonction d'affichage des contrôles consolidés. Si vos flux de travail ne reposent pas sur les valeurs de ces champs ASFF, aucune action n'est requise. Si vos flux de travail s'appuient sur des valeurs spécifiques pour ces champs, mettez à jour vos flux de travail pour utiliser les valeurs actuelles.

> **Tip**
>
> Si vous utilisez la solution Automated Security Response on AWS v2.0.0, notez qu'elle prend en charge les résultats des contrôles consolidés. Cela signifie que vous pouvez maintenir vos flux de travail actuels si vous activez les résultats de contrôle consolidés.

Champ ASFF	Exemple de valeur avant d'activer les résultats de contrôle consolidés	Exemple de valeur après activation des résultats de contrôle consolidés et description de la modification
GeneratorId	aws-foundational-security-best- /1.0. practices/v 0/Config1.	sécurité- control/Config 1. Ce champ ne fait plus référence à une norme.
Titre	PCI.Config.1 AWS Config doit être activé	AWS Config doit être activé Ce champ ne fait plus référence aux informations spécifiques à la norme.
Id	arn:aws:securityhub:eu-central- 1:123456789012 : - /3.2. subscription/pci dss/v 1/PCI. IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central- 1:123456789012:security-. control/iam 9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 Ce champ ne fait plus référence à une norme.
ProductFields.ControlId	PCI.EC2.2	Supprimé. Voir à `Compliance.SecurityControlId` la place. Ce champ est supprimé au profit d'un identifiant de contrôle unique, indépendant des normes.

Champ ASFF	Exemple de valeur avant d'activer les résultats de contrôle consolidés	Exemple de valeur après activation des résultats de contrôle consolidés et description de la modification
ProductFields.RuleId	1.3	Supprimé. Voir à `Compliance.SecurityControlId` la place. Ce champ est supprimé au profit d'un identifiant de contrôle unique, indépendant des normes.
Description	Ce contrôle PCI DSS vérifie s'il AWS Config est activé dans le compte courant et dans la région.	Ce AWS contrôle vérifie si elle AWS Config est activée dans le compte courant et dans la région. Ce champ ne fait plus référence à une norme.

Sévérité	« Gravité » : {
	
	« Produit » : 90,
	
	« Label » : « CRITIQUE »,
	
	« Normalisé » : 90,
	
	« Original » : « CRITIQUE »
	
	}
		« Gravité » : {
		
		« Label » : « CRITIQUE »,
		
		« Normalisé » : 90,
		
		« Original » : « CRITIQUE »
		
		}
		
		Security Hub CSPM n'utilise plus le champ Produit pour décrire la gravité d'une découverte.

Types	[« Logiciel, configuration Checks/Industry et réglementation Standards/PCI-DSS »]	[« Logiciels, configuration Checks/Industry et normes réglementaires »] Ce champ ne fait plus référence à une norme.

Champ ASFF	Exemple de valeur avant d'activer les résultats de contrôle consolidés	Exemple de valeur après activation des résultats de contrôle consolidés et description de la modification
Compliance.Related Requirements	[« PCI DSS 10.5.2", « PCI DSS 11,5 POUCES », « CIS AWS Foundations 2.5"]	[« PCI DSS v3.2. 1/105,2 pouces, « PCI DSS v3.2. 1/111,5 pouces, « CIS AWS Foundations Benchmark v1.2. 0/20,5 pouces] Ce champ affiche les exigences associées à toutes les normes activées.
CreatedAt	05-05-05 T08:18:13.138Z	25/09/24 T08:18:13.138Z Le format reste le même, mais la valeur est réinitialisée lorsque vous activez les résultats de contrôle consolidés.
FirstObservedAt	05/05/07 T08:18:13.138Z	28-09-22 T08:18:13.138Z Le format reste le même, mais la valeur est réinitialisée lorsque vous activez les résultats de contrôle consolidés.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Supprimé. Voir à `Remediation.Recommendation.Url` la place.
ProductFields.StandardsArn	arn:aws:securityhub : : : -foundational-security-best- /1.0.0 standards/aws practices/v	Supprimé. Voir à `Compliance.AssociatedStandards` la place.

Champ ASFF	Exemple de valeur avant d'activer les résultats de contrôle consolidés	Exemple de valeur après activation des résultats de contrôle consolidés et description de la modification
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012 : -foundational-security-best- /1.0. control/aws practices/v 0/Config1.	Supprimé. Security Hub CSPM génère un résultat pour un contrôle de sécurité entre les normes.
ProductFields.StandardsGuideArn	arn:aws:securityhub : : : -aws-foundations- /1.2.0 ruleset/cis benchmark/v	Supprimé. Voir à `Compliance.AssociatedStandards` la place.
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub : us-east-2:123456789012 : -aws-foundations- /1.2.0 subscription/cis benchmark/v	Supprimé. Security Hub CSPM génère un résultat pour un contrôle de sécurité entre les normes.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012 : -foundational-security-best- /1.0.0 subscription/aws practices/v	Supprimé. Security Hub CSPM génère un résultat pour un contrôle de sécurité entre les normes.
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east-1 : : /:aws:securityhub:us-east-1:123456789012 : -foundational-security-best- /1.0. product/aws securityhub/arn subscription/aws practices/v 0/Config. 1/finding /751c2173-7372-4e12-8656-a5210dfb1d67	arn:aws:securityhub:us-east-1 : : /:aws:securityhub:us-east-1:123456789012:security-. product/aws securityhub/arn control/Config 1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 Ce champ ne fait plus référence à une norme.

Valeurs des champs ASFF fournis par le client après l'activation des résultats de contrôle consolidés

Si vous activez les résultats de contrôle consolidés, Security Hub CSPM génère un résultat pour toutes les normes et archive les résultats originaux (résultats distincts pour chaque norme).

Les mises à jour que vous avez apportées aux résultats d'origine à l'aide de la console Security Hub CSPM ou l'BatchUpdateFindingsopération ne seront pas conservées dans les nouveaux résultats. Si nécessaire, vous pouvez récupérer ces données en vous référant aux résultats archivés. Pour consulter les résultats archivés, vous pouvez utiliser la page Résultats de la console Security Hub CSPM et définir le filtre d'état des enregistrements sur ARCHIVÉ. Vous pouvez également utiliser le GetFindings fonctionnement de l'API CSPM Security Hub.

Customer-provided Champ ASFF	Description du changement après activation des résultats de contrôle consolidés
Fiabilité	Rétablit l'état vide.
Criticité	Rétablit l'état vide.
Remarque	Rétablit l'état vide.
RelatedFindings	Rétablit l'état vide.
Sévérité	Sévérité par défaut du résultat (correspond à la sévérité du contrôle).
Types	Rétablit une valeur indépendante de la norme.
UserDefinedFields	Rétablit l'état vide.
VerificationState	Rétablit l'état vide.
Flux de travail	Les nouveaux résultats ayant échoué ont une valeur par défaut de`NEW`. Les nouveaux résultats transmis ont une valeur par défaut de`RESOLVED`.

Identifiants des générateurs avant et après l'obtention de résultats de contrôle consolidés

Le tableau suivant répertorie les modifications apportées aux valeurs d'ID de générateur pour les contrôles lorsque vous activez les résultats de contrôle consolidés. Ces modifications s'appliquent aux contrôles pris en charge par Security Hub CSPM à compter du 15 février 2023.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,1	sécurité- control/CloudWatch 1.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,10	sécurité - control/IAM 1.6
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,11	sécurité - control/IAM 1.7
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,12	sécurité- control/IAM 4.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,13	sécurité- 9control/IAM.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,14	sécurité- 6control/IAM.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,16	sécurité- control/IAM 2.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,2	sécurité- control/IAM 5.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,20	sécurité - control/IAM 1.8
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,22	sécurité- control/IAM 1.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,3	sécurité- 8control/IAM.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,4	sécurité- control/IAM 3.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,5	sécurité- control/IAM 1.1
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,6	sécurité- control/IAM 1.2
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,7	sécurité- control/IAM 1.3
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,8	sécurité- control/IAM 1.4
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,9	sécurité - control/IAM 1.5
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.1	sécurité- control/CloudTrail 1.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,2	sécurité- control/CloudTrail 4.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,3	sécurité- 6control/CloudTrail.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,4	sécurité- control/CloudTrail 5.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,5	sécurité- control/Config 1.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,6	sécurité- 7control/CloudTrail.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,7	sécurité- control/CloudTrail 2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,8	sécurité- control/KMS 4.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2,9	sécurité- 6control/EC2.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,1	sécurité- control/CloudWatch 2.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,2	sécurité- control/CloudWatch 3.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,3	sécurité- control/CloudWatch 1.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,4	sécurité- control/CloudWatch 4.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,5	sécurité- control/CloudWatch 5.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,6	sécurité- 6control/CloudWatch.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,7	sécurité - 7control/CloudWatch.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,8	sécurité - 8control/CloudWatch.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,9	sécurité - 9control/CloudWatch.
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,10	sécurité - control/CloudWatch 1.0

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,11	sécurité- control/CloudWatch 1.1
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,12	sécurité- control/CloudWatch 1.2
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,13	sécurité- control/CloudWatch 1.3
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3,14	sécurité- control/CloudWatch 1.4
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/4,1	sécurité- control/EC2 1.3
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/4,2	sécurité- control/EC2 1.4
arn:aws:securityhub : : : -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/4,3	sécurité- control/EC2 2.
fondations cis-aws-/1.4. benchmark/v 0/11,0	sécurité- control/IAM 5.
fondations cis-aws-/1.4. benchmark/v 0/11,4	sécurité- control/IAM 3.
fondations cis-aws-/1.4. benchmark/v 0/11,6	sécurité- control/IAM 1.
fondations cis-aws-/1.4. benchmark/v 0/11,7	sécurité - control/IAM 1.8
fondations cis-aws-/1.4. benchmark/v 0/14.	sécurité- control/IAM 4.
fondations cis-aws-/1.4. benchmark/v 0/15.	sécurité - 9control/IAM.
fondations cis-aws-/1.4. benchmark/v 0/16.	sécurité- 6control/IAM.
fondations cis-aws-/1.4. benchmark/v 0/17,7	sécurité- control/CloudWatch 1.
fondations cis-aws-/1.4. benchmark/v 0/18,8	sécurité - control/IAM 1.5

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
fondations cis-aws-/1.4. benchmark/v 0/19.	sécurité - control/IAM 1.6
fondations cis-aws-/1.4. benchmark/v 0/21.1.2	sécurité- control/S3 5.
fondations cis-aws-/1.4. benchmark/v 0/21.5.1	sécurité- control/S3 1.
fondations cis-aws-/1.4. benchmark/v 0/21.5.2	sécurité - 8control/S3.
fondations cis-aws-/1.4. benchmark/v 0/22.1.1	sécurité - 7control/EC2.
fondations cis-aws-/1.4. benchmark/v 0/23.1	sécurité- control/RDS 3.
fondations cis-aws-/1.4. benchmark/v 0/31.	sécurité- control/CloudTrail 1.
fondations cis-aws-/1.4. benchmark/v 0/32.	sécurité- control/CloudTrail 4.
fondations cis-aws-/1.4. benchmark/v 0/34.	sécurité- control/CloudTrail 5.
fondations cis-aws-/1.4. benchmark/v 0/35.	sécurité- control/Config 1.
fondations cis-aws-/1.4. benchmark/v 0/36.	sécurité - 9control/S3.
fondations cis-aws-/1.4. benchmark/v 0/37,7	sécurité- control/CloudTrail 2.
fondations cis-aws-/1.4. benchmark/v 0/38,8	sécurité- control/KMS 4.
fondations cis-aws-/1.4. benchmark/v 0/39.	sécurité- 6control/EC2.
fondations cis-aws-/1.4. benchmark/v 0/43.	sécurité- control/CloudWatch 1.
fondations cis-aws-/1.4. benchmark/v 0/44.	sécurité- control/CloudWatch 4.
fondations cis-aws-/1.4. benchmark/v 0/45.	sécurité- control/CloudWatch 5.
fondations cis-aws-/1.4. benchmark/v 0/46.	sécurité- 6control/CloudWatch.
fondations cis-aws-/1.4. benchmark/v 0/47,7	sécurité - 7control/CloudWatch.
fondations cis-aws-/1.4. benchmark/v 0/48,8	sécurité- 8control/CloudWatch.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
fondations cis-aws-/1.4. benchmark/v 0/49.	sécurité- 9control/CloudWatch.
fondations cis-aws-/1.4. benchmark/v 0/41,0	sécurité - control/CloudWatch 1.0
fondations cis-aws-/1.4. benchmark/v 0/41.1	sécurité- control/CloudWatch 1.1
fondations cis-aws-/1.4. benchmark/v 0/41.2	sécurité- control/CloudWatch 1.2
fondations cis-aws-/1.4. benchmark/v 0/41,3	sécurité- control/CloudWatch 1.3
fondations cis-aws-/1.4. benchmark/v 0/41,4	sécurité- control/CloudWatch 1.4
fondations cis-aws-/1.4. benchmark/v 0/51.	sécurité - control/EC2 2.1
fondations cis-aws-/1.4. benchmark/v 0/53.	sécurité- control/EC2 2.
aws-foundational-security-best- /1.0. practices/v 0/Account1.	sécurité- control/Account 1.
aws-foundational-security-best- /1.0. practices/v 0/ACM1.	sécurité- control/ACM 1.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway1.	sécurité- control/APIGateway 1.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway2.	sécurité- control/APIGateway 2.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway3.	sécurité- control/APIGateway 3.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway4.	sécurité- control/APIGateway 4.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway5.	sécurité- control/APIGateway 5.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/APIGateway8.	sécurité- 8control/APIGateway.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway9.	sécurité- 9control/APIGateway.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling1.	sécurité- control/AutoScaling 1.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling2.	sécurité- control/AutoScaling 2.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling3.	sécurité- control/AutoScaling 3.
aws-foundational-security-best- /1.0. practices/v 0/Autoscaling5.	sécurité- control/Autoscaling 5.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling6.	sécurité- 6control/AutoScaling.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling9.	sécurité- 9control/AutoScaling.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront1.	sécurité- control/CloudFront 1.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront3.	sécurité- control/CloudFront 3.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront4.	sécurité- control/CloudFront 4.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront5.	sécurité- control/CloudFront 5.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/CloudFront6.	sécurité- 6control/CloudFront.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront7,7	sécurité- 7control/CloudFront.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront8.	sécurité- 8control/CloudFront.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront9.	sécurité- 9control/CloudFront.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront1,0	sécurité - control/CloudFront 1.0
aws-foundational-security-best- /1.0. practices/v 0/CloudFront1.2	sécurité- control/CloudFront 1.2
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail1.	sécurité- control/CloudTrail 1.
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail2.	sécurité- control/CloudTrail 2.
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail4.	sécurité- control/CloudTrail 4.
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail5.	sécurité- control/CloudTrail 5.
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild1.	sécurité- control/CodeBuild 1.
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild2.	sécurité- control/CodeBuild 2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild3.	sécurité- control/CodeBuild 3.
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild4.	sécurité- control/CodeBuild 4.
aws-foundational-security-best- /1.0. practices/v 0/Config1.	sécurité- control/Config 1.
aws-foundational-security-best- /1.0. practices/v 0/DMS1.	sécurité- control/DMS 1.
aws-foundational-security-best- /1.0. practices/v 0/DynamoDB1.	sécurité- control/DynamoDB 1.
aws-foundational-security-best- /1.0. practices/v 0/DynamoDB2.	sécurité- control/DynamoDB 2.
aws-foundational-security-best- /1.0. practices/v 0/DynamoDB3.	sécurité- control/DynamoDB 3.
aws-foundational-security-best- /1.0. practices/v 0/EC21.	sécurité- control/EC2 1.
aws-foundational-security-best- /1.0. practices/v 0/EC23.	sécurité- control/EC2 3.
aws-foundational-security-best- /1.0. practices/v 0/EC24.	sécurité- control/EC2 4.
aws-foundational-security-best- /1.0. practices/v 0/EC26.	sécurité- 6control/EC2.
aws-foundational-security-best- /1.0. practices/v 0/EC27,7	sécurité- 7control/EC2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/EC28.	sécurité- 8control/EC2.
aws-foundational-security-best- /1.0. practices/v 0/EC29.	sécurité- 9control/EC2.
aws-foundational-security-best- /1.0. practices/v 0/EC21,0	sécurité - control/EC2 1.0
aws-foundational-security-best- /1.0. practices/v 0/EC21,5	sécurité - control/EC2 1.5
aws-foundational-security-best- /1.0. practices/v 0/EC21,6	sécurité - control/EC2 1.6
aws-foundational-security-best- /1.0. practices/v 0/EC21,7	sécurité - control/EC2 1.7
aws-foundational-security-best- /1.0. practices/v 0/EC21,8	sécurité - control/EC2 1.8
aws-foundational-security-best- /1.0. practices/v 0/EC21,9	sécurité- control/EC2 1.9
aws-foundational-security-best- /1.0. practices/v 0/EC22.	sécurité- control/EC2 2.
aws-foundational-security-best- /1.0. practices/v 0/EC22,0	sécurité - control/EC2 2.0
aws-foundational-security-best- /1.0. practices/v 0/EC22,1	sécurité - control/EC2 2.1
aws-foundational-security-best- /1.0. practices/v 0/EC22,3	sécurité- control/EC2 2.3

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/EC22,4	sécurité - control/EC2 2.4
aws-foundational-security-best- /1.0. practices/v 0/EC22,5	sécurité - control/EC2 2.5
aws-foundational-security-best- /1.0. practices/v 0/ECR1.	sécurité- control/ECR 1.
aws-foundational-security-best- /1.0. practices/v 0/ECR2.	sécurité- control/ECR 2.
aws-foundational-security-best- /1.0. practices/v 0/ECR3.	sécurité- control/ECR 3.
aws-foundational-security-best- /1.0. practices/v 0/ECS1,0	sécurité - control/ECS 1.0
aws-foundational-security-best- /1.0. practices/v 0/ECS1.2	sécurité- control/ECS 1.2
aws-foundational-security-best- /1.0. practices/v 0/ECS2.	sécurité- control/ECS 2.
aws-foundational-security-best- /1.0. practices/v 0/ECS3.	sécurité- control/ECS 3.
aws-foundational-security-best- /1.0. practices/v 0/ECS4.	sécurité- control/ECS 4.
aws-foundational-security-best- /1.0. practices/v 0/ECS5.	sécurité- control/ECS 5.
aws-foundational-security-best- /1.0. practices/v 0/ECS8.	sécurité- 8control/ECS.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/EFS1.	sécurité- control/EFS 1.
aws-foundational-security-best- /1.0. practices/v 0/EFS2.	sécurité- control/EFS 2.
aws-foundational-security-best- /1.0. practices/v 0/EFS3.	sécurité- control/EFS 3.
aws-foundational-security-best- /1.0. practices/v 0/EFS4.	sécurité- control/EFS 4.
aws-foundational-security-best- /1.0. practices/v 0/EKS2.	sécurité- control/EKS 2.
aws-foundational-security-best- /1.0. practices/v 0/ElasticBeanstalk1.	sécurité- control/ElasticBeanstalk 1.
aws-foundational-security-best- /1.0. practices/v 0/ElasticBeanstalk2.	sécurité- control/ElasticBeanstalk 2.
aws-foundational-security-best- /1.0. practices/v 0/ELBv21.	sécurité- control/ELB 1.
aws-foundational-security-best- /1.0. practices/v 0/ELB2.	sécurité- control/ELB 2.
aws-foundational-security-best- /1.0. practices/v 0/ELB3.	sécurité- control/ELB 3.
aws-foundational-security-best- /1.0. practices/v 0/ELB4.	sécurité- control/ELB 4.
aws-foundational-security-best- /1.0. practices/v 0/ELB5.	sécurité- control/ELB 5.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/ELB6.	sécurité- 6control/ELB.
aws-foundational-security-best- /1.0. practices/v 0/ELB7,7	sécurité- 7control/ELB.
aws-foundational-security-best- /1.0. practices/v 0/ELB8.	sécurité- 8control/ELB.
aws-foundational-security-best- /1.0. practices/v 0/ELB9.	sécurité- 9control/ELB.
aws-foundational-security-best- /1.0. practices/v 0/ELB1,0	sécurité - control/ELB 1.0
aws-foundational-security-best- /1.0. practices/v 0/ELB1.1	sécurité- control/ELB 1.1
aws-foundational-security-best- /1.0. practices/v 0/ELB1.2	sécurité- control/ELB 1.2
aws-foundational-security-best- /1.0. practices/v 0/ELB1,3	sécurité- control/ELB 1.3
aws-foundational-security-best- /1.0. practices/v 0/ELB1,4	sécurité- control/ELB 1.4
aws-foundational-security-best- /1.0. practices/v 0/EMR1.	sécurité- control/EMR 1.
aws-foundational-security-best- /1.0. practices/ v 0/ES1.	sécurité- control/ES 1.
aws-foundational-security-best- /1.0. practices/ v 0/ES2.	sécurité- control/ES 2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/ v 0/ES3.	sécurité- control/ES 3.
aws-foundational-security-best- /1.0. practices/ v 0/ES4.	sécurité- control/ES 4.
aws-foundational-security-best- /1.0. practices/ v 0/ES5.	sécurité- control/ES 5.
aws-foundational-security-best- /1.0. practices/ v 0/ES6.	sécurité- 6control/ES.
aws-foundational-security-best- /1.0. practices/v 0/ES7,7	sécurité- 7control/ES.
aws-foundational-security-best- /1.0. practices/ v 0/ES8.	sécurité- 8control/ES.
aws-foundational-security-best- /1.0. practices/v 0/GuardDuty1.	sécurité- control/GuardDuty 1.
aws-foundational-security-best- /1.0. practices/v 0/IAM1.	sécurité- control/IAM 1.
aws-foundational-security-best- /1.0. practices/v 0/IAM2.	sécurité- control/IAM 2.
aws-foundational-security-best- /1.0. practices/v 0/IAM2,1	sécurité - control/IAM 2.1
aws-foundational-security-best- /1.0. practices/v 0/IAM3.	sécurité- control/IAM 3.
aws-foundational-security-best- /1.0. practices/v 0/IAM4.	sécurité- control/IAM 4.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/IAM5.	sécurité- control/IAM 5.
aws-foundational-security-best- /1.0. practices/v 0/IAM6.	sécurité- 6control/IAM.
aws-foundational-security-best- /1.0. practices/v 0/IAM7,7	sécurité- 7control/IAM.
aws-foundational-security-best- /1.0. practices/v 0/IAM8.	sécurité- 8control/IAM.
aws-foundational-security-best- /1.0. practices/v 0/Kinesis1.	sécurité- control/Kinesis 1.
aws-foundational-security-best- /1.0. practices/v 0/KMS1.	sécurité- control/KMS 1.
aws-foundational-security-best- /1.0. practices/v 0/KMS2.	sécurité- control/KMS 2.
aws-foundational-security-best- /1.0. practices/v 0/KMS3.	sécurité- control/KMS 3.
aws-foundational-security-best- /1.0. practices/v 0/Lambda1.	sécurité- control/Lambda 1.
aws-foundational-security-best- /1.0. practices/v 0/Lambda2.	sécurité- control/Lambda 2.
aws-foundational-security-best- /1.0. practices/v 0/Lambda5.	sécurité- control/Lambda 5.
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall3.	sécurité- control/NetworkFirewall 3.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall4.	sécurité- control/NetworkFirewall 4.
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall5.	sécurité- control/NetworkFirewall 5.
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall6.	sécurité- 6control/NetworkFirewall.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch1.	sécurité- control/Opensearch 1.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch2.	sécurité- control/Opensearch 2.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch3.	sécurité- control/Opensearch 3.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch4.	sécurité- control/Opensearch 4.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch5.	sécurité- control/Opensearch 5.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch6.	sécurité- 6control/Opensearch.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch7,7	sécurité- 7control/Opensearch.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch8.	sécurité- 8control/Opensearch.
aws-foundational-security-best- /1.0. practices/v 0/RDS1.	sécurité- control/RDS 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/RDS1,0	sécurité - control/RDS 1.0
aws-foundational-security-best- /1.0. practices/v 0/RDS1.1	sécurité- control/RDS 1.1
aws-foundational-security-best- /1.0. practices/v 0/RDS1.2	sécurité- control/RDS 1.2
aws-foundational-security-best- /1.0. practices/v 0/RDS1,3	sécurité- control/RDS 1.3
aws-foundational-security-best- /1.0. practices/v 0/RDS1,4	sécurité- control/RDS 1.4
aws-foundational-security-best- /1.0. practices/v 0/RDS1,5	sécurité - control/RDS 1.5
aws-foundational-security-best- /1.0. practices/v 0/RDS1,6	sécurité - control/RDS 1.6
aws-foundational-security-best- /1.0. practices/v 0/RDS1,7	sécurité - control/RDS 1.7
aws-foundational-security-best- /1.0. practices/v 0/RDS1,9	sécurité- control/RDS 1.9
aws-foundational-security-best- /1.0. practices/v 0/RDS2.	sécurité- control/RDS 2.
aws-foundational-security-best- /1.0. practices/v 0/RDS2,0	sécurité - control/RDS 2.0
aws-foundational-security-best- /1.0. practices/v 0/RDS2,1	sécurité - control/RDS 2.1

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/RDS2,2	sécurité - control/RDS 2.2
aws-foundational-security-best- /1.0. practices/v 0/RDS2,3	sécurité- control/RDS 2.3
aws-foundational-security-best- /1.0. practices/v 0/RDS2,4	sécurité - control/RDS 2.4
aws-foundational-security-best- /1.0. practices/v 0/RDS2,5	sécurité - control/RDS 2.5
aws-foundational-security-best- /1.0. practices/v 0/RDS3.	sécurité- control/RDS 3.
aws-foundational-security-best- /1.0. practices/v 0/RDS4.	sécurité- control/RDS 4.
aws-foundational-security-best- /1.0. practices/v 0/RDS5.	sécurité- control/RDS 5.
aws-foundational-security-best- /1.0. practices/v 0/RDS6.	sécurité- 6control/RDS.
aws-foundational-security-best- /1.0. practices/v 0/RDS7,7	sécurité- 7control/RDS.
aws-foundational-security-best- /1.0. practices/v 0/RDS8.	sécurité- 8control/RDS.
aws-foundational-security-best- /1.0. practices/v 0/RDS9.	sécurité- 9control/RDS.
aws-foundational-security-best- /1.0. practices/v 0/Redshift1.	sécurité- control/Redshift 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/Redshift2.	sécurité- control/Redshift 2.
aws-foundational-security-best- /1.0. practices/v 0/Redshift3.	sécurité- control/Redshift 3.
aws-foundational-security-best- /1.0. practices/v 0/Redshift4.	sécurité- control/Redshift 4.
aws-foundational-security-best- /1.0. practices/v 0/Redshift6.	sécurité- 6control/Redshift.
aws-foundational-security-best- /1.0. practices/v 0/Redshift7,7	sécurité- 7control/Redshift.
aws-foundational-security-best- /1.0. practices/v 0/Redshift8.	sécurité- 8control/Redshift.
aws-foundational-security-best- /1.0. practices/ v 0/S31.	sécurité- control/S3 1.
aws-foundational-security-best- /1.0. practices/v 0/S31.2	sécurité- control/S3 1.2
aws-foundational-security-best- /1.0. practices/v 0/S31,3	sécurité- control/S3 1.3
aws-foundational-security-best- /1.0. practices/ v 0/S32.	sécurité- control/S3 2.
aws-foundational-security-best- /1.0. practices/ v 0/S33.	sécurité- control/S3 3.
aws-foundational-security-best- /1.0. practices/ v 0/S35.	sécurité- control/S3 5.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/ v 0/S36.	sécurité- 6control/S3.
aws-foundational-security-best- /1.0. practices/ v 0/S38.	sécurité- 8control/S3.
aws-foundational-security-best- /1.0. practices/ v 0/S39.	sécurité- 9control/S3.
aws-foundational-security-best- /1.0. practices/v 0/SageMaker1.	sécurité- control/SageMaker 1.
aws-foundational-security-best- /1.0. practices/v 0/SageMaker2.	sécurité- control/SageMaker 2.
aws-foundational-security-best- /1.0. practices/v 0/SageMaker3.	sécurité- control/SageMaker 3.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager1.	sécurité- control/SecretsManager 1.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager2.	sécurité- control/SecretsManager 2.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager3.	sécurité- control/SecretsManager 3.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager4.	sécurité- control/SecretsManager 4.
aws-foundational-security-best- /1.0. practices/v 0/SQS1.	sécurité- control/SQS 1.
aws-foundational-security-best- /1.0. practices/v 0/SSM1.	sécurité- control/SSM 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
aws-foundational-security-best- /1.0. practices/v 0/SSM2.	sécurité- control/SSM 2.
aws-foundational-security-best- /1.0. practices/v 0/SSM3.	sécurité- control/SSM 3.
aws-foundational-security-best- /1.0. practices/v 0/SSM4.	sécurité- control/SSM 4.
aws-foundational-security-best- /1.0. practices/v 0/WAF1.	sécurité- control/WAF 1.
aws-foundational-security-best- /1.0. practices/v 0/WAF2.	sécurité- control/WAF 2.
aws-foundational-security-best- /1.0. practices/v 0/WAF3.	sécurité- control/WAF 3.
aws-foundational-security-best- /1.0. practices/v 0/WAF4.	sécurité- control/WAF 4.
aws-foundational-security-best- /1.0. practices/v 0/WAF6.	sécurité- 6control/WAF.
aws-foundational-security-best- /1.0. practices/v 0/WAF7,7	sécurité- 7control/WAF.
aws-foundational-security-best- /1.0. practices/v 0/WAF8.	sécurité- 8control/WAF.
aws-foundational-security-best- /1.0. practices/v 0/WAF1,0	sécurité - control/WAF 1.0
pci- /3.2. dss/v 1/PCI. AutoScaling.1	sécurité- control/AutoScaling 1.
pci-3/3.2. dss/v 1/PCI. CloudTrail.1	sécurité- control/CloudTrail 2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
pci-3/3.2. dss/v 1/PCI. CloudTrail.2	sécurité- control/CloudTrail 3.
pci- /3.2. dss/v 1/PCI. CloudTrail.3	sécurité- control/CloudTrail 4.
pci-3/3.2. dss/v 1/PCI. CloudTrail.4	sécurité- control/CloudTrail 5.
pci-3/3.2. dss/v 1/PCI. CodeBuild.1	sécurité- control/CodeBuild 1.
pci-3/3.2. dss/v 1/PCI. CodeBuild.2	sécurité- control/CodeBuild 2.
pci-3/3.2. dss/v 1/PCI. Config.1	sécurité- control/Config 1.
pci-3/3.2. dss/v 1/PCI. CW.1	sécurité- control/CloudWatch 1.
pci-3/3.2. dss/v 1/PCI. DMS.1	sécurité- control/DMS 1.
pci-3/3.2. dss/v 1/PCI. EC2.1	sécurité- control/EC2 1.
pci-3/3.2. dss/v 1/PCI. EC2.2	sécurité- control/EC2 2.
pci-3/3.2. dss/v 1/PCI. EC2.4	sécurité- control/EC2 1.2
pci-3/3.2. dss/v 1/PCI. EC2.5	sécurité- control/EC2 1.3
pci-3/3.2. dss/v 1/PCI. EC2.6	sécurité- 6control/EC2.
pci-3/3.2. dss/v 1/PCI. ELBv2.1	sécurité- control/ELB 1.
pci-3/3.2. dss/v 1/PCI. ES.1	sécurité- control/ES 2.
pci-3/3.2. dss/v 1/PCI. ES.2	sécurité- control/ES 1.
pci-3/3.2. dss/v 1/PCI. GuardDuty.1	sécurité- control/GuardDuty 1.
pci-3/3.2. dss/v 1/PCI. IAM.1	sécurité- control/IAM 4.
pci-3/3.2. dss/v 1/PCI. IAM.2	sécurité- control/IAM 2.
pci-3/3.2. dss/v 1/PCI. IAM.3	sécurité- control/IAM 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
pci-3/3.2. dss/v 1/PCI. IAM.4	sécurité- 6control/IAM.
pci-3/3.2. dss/v 1/PCI. IAM.5	sécurité - 9control/IAM.
pci-3/3.2. dss/v 1/PCI. IAM.6	sécurité- control/IAM 1.9
pci-3/3.2. dss/v 1/PCI. IAM.7	sécurité - 8control/IAM.
pci-3/3.2. dss/v 1/PCI. IAM.8	sécurité - control/IAM 1.0
pci- /3.2. dss/v 1/PCI. KMS.1	sécurité- control/KMS 4.
pci-3/3.2. dss/v 1/PCI. Lambda.1	sécurité- control/Lambda 1.
pci-3/3.2. dss/v 1/PCI. Lambda.2	sécurité- control/Lambda 3.
pci- /3.2. dss/v 1/PCI. Opensearch.1	sécurité- control/Opensearch 2.
pci-3/3.2. dss/v 1/PCI. Opensearch.2	sécurité- control/Opensearch 1.
pci-3/3.2. dss/v 1/PCI. RDS.1	sécurité- control/RDS 1.
pci-3/3.2. dss/v 1/PCI. RDS.2	sécurité- control/RDS 2.
pci-3/3.2. dss/v 1/PCI. Redshift.1	sécurité- control/Redshift 1.
pci-3/3.2. dss/v 1/PCI. S3.1	sécurité- control/S3 3.
pci- /3.2. dss/v 1/PCI. S3.2	sécurité- control/S3 2.
pci-3/3.2. dss/v 1/PCI. S3.3	sécurité - 7control/S3.
pci-3/3.2. dss/v 1/PCI. S3.5	sécurité- control/S3 5.
pci-3/3.2. dss/v 1/PCI. S3.6	sécurité- control/S3 1.
pci-3/3.2. dss/v 1/PCI. SageMaker.1	sécurité- control/SageMaker 1.
pci-3/3.2. dss/v 1/PCI. SSM.1	sécurité- control/SSM 2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
pci-3/3.2. dss/v 1/PCI. SSM.2	sécurité- control/SSM 3.
pci- /3.2. dss/v 1/PCI. SSM.3	sécurité- control/SSM 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/ACM1.	sécurité- control/ACM 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/APIGateway1.	sécurité- control/APIGateway 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/APIGateway2.	sécurité- control/APIGateway 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/APIGateway3.	sécurité- control/APIGateway 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/APIGateway4.	sécurité- control/APIGateway 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/APIGateway5.	sécurité- control/APIGateway 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/AutoScaling1.	sécurité- control/AutoScaling 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/AutoScaling2.	sécurité- control/AutoScaling 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/AutoScaling3.	sécurité- control/AutoScaling 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/AutoScaling4.	sécurité- control/AutoScaling 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/Autoscaling5.	sécurité- control/Autoscaling 5.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/AutoScaling6.	sécurité- 6control/AutoScaling.
contrôle AWS géré par les services- /1.0. tower/ v 0/AutoScaling9.	sécurité- 9control/AutoScaling.
contrôle AWS géré par les services- /1.0. tower/ v 0/CloudTrail1.	sécurité- control/CloudTrail 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/CloudTrail2.	sécurité- control/CloudTrail 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/CloudTrail4.	sécurité- control/CloudTrail 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/CloudTrail5.	sécurité- control/CloudTrail 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/CodeBuild1.	sécurité- control/CodeBuild 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/CodeBuild2.	sécurité- control/CodeBuild 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/CodeBuild4.	sécurité- control/CodeBuild 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/CodeBuild5.	sécurité- control/CodeBuild 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/DMS1.	sécurité- control/DMS 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/DynamoDB1.	sécurité- control/DynamoDB 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/DynamoDB2.	sécurité- control/DynamoDB 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21.	sécurité- control/EC2 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC22.	sécurité- control/EC2 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC23.	sécurité- control/EC2 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC24.	sécurité- control/EC2 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC26.	sécurité- 6control/EC2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC27,7	sécurité- 7control/EC2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC28.	sécurité- 8control/EC2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC29.	sécurité- 9control/EC2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21,0	sécurité - control/EC2 1.0
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21,5	sécurité - control/EC2 1.5
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21,6	sécurité - control/EC2 1.6

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21,7	sécurité - control/EC2 1.7
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21,8	sécurité - control/EC2 1.8
contrôle AWS géré par les services- /1.0. tower/ v 0/EC21,9	sécurité- control/EC2 1.9
contrôle AWS géré par les services- /1.0. tower/ v 0/EC22,0	sécurité - control/EC2 2.0
contrôle AWS géré par les services- /1.0. tower/ v 0/EC22,1	sécurité - control/EC2 2.1
contrôle AWS géré par les services- /1.0. tower/ v 0/EC22,2	sécurité - control/EC2 2.2
contrôle AWS géré par les services- /1.0. tower/ v 0/ECR1.	sécurité- control/ECR 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECR2.	sécurité- control/ECR 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECR3.	sécurité- control/ECR 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS2.	sécurité- control/ECS 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS3.	sécurité- control/ECS 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS4.	sécurité- control/ECS 4.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS5.	sécurité- control/ECS 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS8.	sécurité- 8control/ECS.
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS1,0	sécurité - control/ECS 1.0
contrôle AWS géré par les services- /1.0. tower/ v 0/ECS1.2	sécurité- control/ECS 1.2
contrôle AWS géré par les services- /1.0. tower/ v 0/EFS1.	sécurité- control/EFS 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/EFS2.	sécurité- control/EFS 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/EFS3.	sécurité- control/EFS 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/EFS4.	sécurité- control/EFS 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/EKS2.	sécurité- control/EKS 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB2.	sécurité- control/ELB 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB3.	sécurité- control/ELB 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB4.	sécurité- control/ELB 4.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB5.	sécurité- control/ELB 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB6.	sécurité- 6control/ELB.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB7,7	sécurité- 7control/ELB.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB8.	sécurité- 8control/ELB.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB9.	sécurité- 9control/ELB.
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB1,0	sécurité - control/ELB 1.0
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB1.2	sécurité- control/ELB 1.2
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB1,3	sécurité- control/ELB 1.3
contrôle AWS géré par les services- /1.0. tower/ v 0/ELB1,4	sécurité- control/ELB 1.4
contrôle AWS géré par les services- /1.0. tower/ v 0/ELBv21.	sécurité- control/ELBv2 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/EMR1.	sécurité- control/EMR 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES1.	sécurité- control/ES 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/ES2.	sécurité- control/ES 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES3.	sécurité- control/ES 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES4.	sécurité- control/ES 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES5.	sécurité- control/ES 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES6.	sécurité- 6control/ES.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES7,7	sécurité- 7control/ES.
contrôle AWS géré par les services- /1.0. tower/ v 0/ES8.	sécurité- 8control/ES.
contrôle AWS géré par les services- /1.0. tower/ v 0/ElasticBeanstalk1.	sécurité- control/ElasticBeanstalk 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/ElasticBeanstalk2.	sécurité- control/ElasticBeanstalk 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/GuardDuty1.	sécurité- control/GuardDuty 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM1.	sécurité- control/IAM 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM2.	sécurité- control/IAM 2.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM3.	sécurité- control/IAM 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM4.	sécurité- control/IAM 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM5.	sécurité- control/IAM 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM6.	sécurité- 6control/IAM.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM7,7	sécurité- 7control/IAM.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM8.	sécurité- 8control/IAM.
contrôle AWS géré par les services- /1.0. tower/ v 0/IAM2,1	sécurité - control/IAM 2.1
contrôle AWS géré par les services- /1.0. tower/ v 0/Kinesis1.	sécurité- control/Kinesis 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/KMS1.	sécurité- control/KMS 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/KMS2.	sécurité- control/KMS 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/KMS3.	sécurité- control/KMS 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/Lambda1.	sécurité- control/Lambda 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/Lambda2.	sécurité- control/Lambda 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/Lambda5.	sécurité- control/Lambda 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/NetworkFirewall3.	sécurité- control/NetworkFirewall 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/NetworkFirewall4.	sécurité- control/NetworkFirewall 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/NetworkFirewall5.	sécurité- control/NetworkFirewall 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/NetworkFirewall6.	sécurité- 6control/NetworkFirewall.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch1.	sécurité- control/Opensearch 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch2.	sécurité- control/Opensearch 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch3.	sécurité- control/Opensearch 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch4.	sécurité- control/Opensearch 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch5.	sécurité- control/Opensearch 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch6.	sécurité- 6control/Opensearch.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch7,7	sécurité- 7control/Opensearch.
contrôle AWS géré par les services- /1.0. tower/ v 0/Opensearch8.	sécurité- 8control/Opensearch.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS1.	sécurité- control/RDS 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS2.	sécurité- control/RDS 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS3.	sécurité- control/RDS 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS4.	sécurité- control/RDS 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS5.	sécurité- control/RDS 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS6.	sécurité- 6control/RDS.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS8.	sécurité- 8control/RDS.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS9.	sécurité- 9control/RDS.
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS1,0	sécurité - control/RDS 1.0
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS1.1	sécurité- control/RDS 1.1

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS1,3	sécurité- control/RDS 1.3
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS1,7	sécurité - control/RDS 1.7
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS1,9	sécurité- control/RDS 1.9
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS2,0	sécurité - control/RDS 2.0
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS2,1	sécurité - control/RDS 2.1
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS2,2	sécurité - control/RDS 2.2
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS2,3	sécurité- control/RDS 2.3
contrôle AWS géré par les services- /1.0. tower/ v 0/RDS2,5	sécurité - control/RDS 2.5
contrôle AWS géré par les services- /1.0. tower/ v 0/Redshift1.	sécurité- control/Redshift 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/Redshift2.	sécurité- control/Redshift 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/Redshift4.	sécurité- control/Redshift 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/Redshift6.	sécurité- 6control/Redshift.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/Redshift7,7	sécurité- 7control/Redshift.
contrôle AWS géré par les services- /1.0. tower/ v 0/Redshift8.	sécurité- 8control/Redshift.
contrôle AWS géré par les services- /1.0. tower/ v 0/S31.	sécurité- control/S3 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/S32.	sécurité- control/S3 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/S33.	sécurité- control/S3 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/S35.	sécurité- control/S3 5.
contrôle AWS géré par les services- /1.0. tower/ v 0/S36.	sécurité- 6control/S3.
contrôle AWS géré par les services- /1.0. tower/ v 0/S38.	sécurité- 8control/S3.
contrôle AWS géré par les services- /1.0. tower/ v 0/S39.	sécurité- 9control/S3.
contrôle AWS géré par les services- /1.0. tower/ v 0/S31.2	sécurité- control/S3 1.2
contrôle AWS géré par les services- /1.0. tower/ v 0/S31,3	sécurité- control/S3 1.3
contrôle AWS géré par les services- /1.0. tower/ v 0/SageMaker1.	sécurité- control/SageMaker 1.

GeneratorID avant d'activer les résultats de contrôle consolidés	GeneratorID après activation des résultats de contrôle consolidés
contrôle AWS géré par les services- /1.0. tower/ v 0/SecretsManager1.	sécurité- control/SecretsManager 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/SecretsManager2.	sécurité- control/SecretsManager 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/SecretsManager3.	sécurité- control/SecretsManager 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/SecretsManager4.	sécurité- control/SecretsManager 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/SQS1.	sécurité- control/SQS 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/SSM1.	sécurité- control/SSM 1.
contrôle AWS géré par les services- /1.0. tower/ v 0/SSM2.	sécurité- control/SSM 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/SSM3.	sécurité- control/SSM 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/SSM4.	sécurité- control/SSM 4.
contrôle AWS géré par les services- /1.0. tower/ v 0/WAF2.	sécurité- control/WAF 2.
contrôle AWS géré par les services- /1.0. tower/ v 0/WAF3.	sécurité- control/WAF 3.
contrôle AWS géré par les services- /1.0. tower/ v 0/WAF4.	sécurité- control/WAF 4.

L'impact de la consolidation sur les identifiants et titres de contrôle

L'affichage des contrôles consolidés et les résultats des contrôles consolidés normalisent les identifiants et les titres des contrôles selon les normes. Les termes ID de contrôle de sécurité et titre du contrôle de sécurité font référence à ces valeurs indépendantes des normes.

La console Security Hub CSPM affiche des identifiants de contrôle de sécurité et des titres de contrôle de sécurité indépendants des normes, que les résultats des contrôles consolidés soient activés ou désactivés pour votre compte. Toutefois, les résultats du Security Hub CSPM contiennent des titres de contrôle spécifiques aux normes, pour PCI DSS et CIS v1.2.0, si les résultats de contrôle consolidés sont désactivés pour votre compte. En outre, les résultats du Security Hub CSPM contiennent l'ID de contrôle et l'ID de contrôle de sécurité spécifiques à la norme. Pour des exemples de l'impact de la consolidation sur les résultats des contrôles, voirÉchantillons de résultats de contrôle.

Pour les contrôles qui font partie de la norme de AWS Control Tower gestion des services, le préfixe `CT.` est supprimé de l'identifiant et du titre du contrôle dans les résultats lorsque les résultats des contrôles consolidés sont activés.

Pour désactiver un contrôle de sécurité dans Security Hub CSPM, vous devez désactiver tous les contrôles standard qui correspondent au contrôle de sécurité. Le tableau suivant montre le mappage des ID et titres de contrôle de sécurité avec les ID et titres de contrôle spécifiques à la norme. Les identifiants et les titres des contrôles qui appartiennent à la norme FSBP (AWS Foundational Security Best Practices) sont déjà indépendants des normes. Pour une mise en correspondance des contrôles avec les exigences de Center for Internet Security (CIS) v3.0.0, consultez. Mise en correspondance des contrôles avec les exigences du CIS dans chaque version Pour exécuter vos propres scripts sur ce tableau, vous pouvez le télécharger sous forme de fichier .csv.

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.2.0	1.1 Évitez d'utiliser l'utilisateur root	[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »
CIS v1.2.0	1.10 Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe	[IAM.16] Assurez-vous que la politique de mot de passe IAM

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
		empêche la réutilisation des mots de passe
CIS v1.2.0	1.11 Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans les 90 jours ou moins	[IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
CIS v1.2.0	1.12 Assurez-vous qu'aucune clé d'accès utilisateur root n'existe	[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
CIS v1.2.0	1.13 Assurez-vous que le MFA est activé pour l'utilisateur root	[IAM.9] La MFA doit être activée pour l'utilisateur root
CIS v1.2.0	1.14 Assurez-vous que l'authent ification multifacteur matérielle est activée pour l'utilisateur root	[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
CIS v1.2.0	1.16 Assurez-vous que les politique s IAM ne sont associées qu'aux groupes ou aux rôles	[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
CIS v1.2.0	1.2 Assurez-vous que l'authent ification multifacteur (MFA) est activée pour tous les utilisateurs IAM disposant d'un mot de passe de console	[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
CIS v1.2.0	1.20 Assurez-vous qu'un rôle de soutien a été créé pour gérer les incidents avec Support	[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
CIS v1.2.0	1.22 Assurez-vous que les politique s IAM qui autorisent des privilèges administratifs complets « * : * » ne sont pas créées	[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administr atifs « * » complets

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.2.0	1.3 Vérifier que les informations d'identification inutilisées depuis 90 jours ou plus sont désactivées	[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
CIS v1.2.0	1.4 Vérifier que les clés d'accès font l'objet d'une rotation tous les 90 jours ou moins	[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
CIS v1.2.0	1.5 Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule	[IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
CIS v1.2.0	1.6 Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule	[IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
CIS v1.2.0	1.7 Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole	[IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
CIS v1.2.0	1.8 Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre	[IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
CIS v1.2.0	1.9 Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus	[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.2.0	2.1 Assurez-vous que CloudTrail c'est activé dans toutes les régions	[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture
CIS v1.2.0	2.2 Assurez-vous que la validation du fichier CloudTrail journal est activée	[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée
CIS v1.2.0	2.3 Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	[CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
CIS v1.2.0	2.4 Assurez-vous que les CloudTrail sentiers sont intégrés aux CloudWatch journaux	[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs
CIS v1.2.0	2.5 Assurez-vous que AWS Config c'est activé	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources
CIS v1.2.0	2.6 Assurez-vous que la journalisation de l'accès au compartiment S3 est activée sur le compartiment CloudTrail S3	[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
CIS v1.2.0	2.7 Assurez-vous que CloudTrail les journaux sont chiffrés au repos à l'aide des KMS CMK	[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé
CIS v1.2.0	2.8 Vérifier que la rotation des clés CMK créées par le client est activée	[KMS.4]AWS KMSla rotation des touches doit être activée

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.2.0	2.9 Vérifier que la journalisation de flux VPC est activée dans tous les VPC	[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC
CIS v1.2.0	3.1 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les appels d'API non autorisés	[CloudWatch.2] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les appels d'API non autorisés
CIS v1.2.0	3.10 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les modifications des groupes de sécurité	[CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité
CIS v1.2.0	3.11 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les modifications des listes de contrôle d'accès réseau (ACL réseau)	[CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)
CIS v1.2.0	3.12 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les modifications des passerelles réseau	[CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau
CIS v1.2.0	3.13 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les modifications des tables de routage	[CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage
CIS v1.2.0	3.14 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les modifications de VPC	[CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.2.0	3.2 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la connexion à la console de gestion sans MFA	[CloudWatch.3] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la connexion à la console de gestion sans MFA
CIS v1.2.0	3.3 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour l'utilisation de l'utilisa teur root	[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »
CIS v1.2.0	3.4 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM	[CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modificat ions de la politique IAM
CIS v1.2.0	3.5 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration	[CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modificat ions CloudTrail de configuration
CIS v1.2.0	3.6 Assurez-vous qu'un filtre de mesure du journal et une alarme existent en cas Console de gestion AWS d'échec d'authentification	[CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authent ification
CIS v1.2.0	3.7 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour la désactivation ou la suppressi on planifiée des clés CMK créées par le client	[CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.2.0	3.8 Vérifier qu'il existe un filtre de métrique et une alarme de journaux pour les modifications de stratégies de compartiments S3	[CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3
CIS v1.2.0	3.9 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications AWS Config de configuration	[CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration
CIS v1.2.0	4.1 Assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée depuis la version 0.0.0. 0/0 vers le port 22	[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22
CIS v1.2.0	4.2 Assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée depuis la version 0.0.0. 0/0 vers le port 3389	[EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
CIS v1.2.0	4.3 Vérifier que le groupe de sécurité par défaut de chaque VPC restreint l'ensemble du trafic	[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant
CIS v1.4.0	1.10 Assurez-vous que l'authentification multifacteur (MFA) est activée pour tous les utilisateurs IAM disposant d'un mot de passe de console	[IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
CIS v1.4.0	1.14 Assurez-vous que les clés d'accès sont changées tous les 90 jours ou moins	[IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.4.0	1.16 Assurez-vous que les politiques IAM qui autorisent des privilèges administratifs complets « * : * » ne sont pas associées	[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
CIS v1.4.0	1.17 Assurez-vous qu'un rôle de soutien a été créé pour gérer les incidents avec Support	[IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
CIS v1.4.0	1.4 Assurez-vous qu'aucune clé d'accès au compte utilisateur root n'existe	[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
CIS v1.4.0	1.5 Assurez-vous que le MFA est activé pour le compte utilisateur root	[IAM.9] La MFA doit être activée pour l'utilisateur root
CIS v1.4.0	1.6 Assurez-vous que l'authentification multifacteur matérielle est activée pour le compte utilisateur root	[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
CIS v1.4.0	1.7 Éliminer l'utilisation de l'utilisateur root pour les tâches administratives et quotidiennes	[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »
CIS v1.4.0	1.8 Assurez-vous que la politique de mot de passe IAM exige une longueur minimale de 14 ou plus	[IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
CIS v1.4.0	1.9 Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe	[IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.4.0	2.1.2 Assurez-vous que la politique de compartiment S3 est définie pour refuser les requêtes HTTP	[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS
CIS v1.4.0	2.1.5.1 Le paramètre S3 Block Public Access doit être activé	[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés
CIS v1.4.0	2.1.5.2 Le paramètre S3 Block Public Access doit être activé au niveau du bucket	[S3.8] Les compartiments S3 à usage général devraient bloquer l'accès public
CIS v1.4.0	2.2.1 Assurez-vous que le chiffrement des volumes EBS est activé	[EC2.7] Le chiffrement par défaut d'EBS doit être activé
CIS v1.4.0	2.3.1 Assurez-vous que le chiffrement est activé pour les instances RDS	[RDS.3] Les instances de base de données RDS doivent avoir le chiffrement au repos activé
CIS v1.4.0	3.1 Assurez-vous qu' CloudTrail il est activé dans toutes les régions	[CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture
CIS v1.4.0	3.2 Assurez-vous que la validation du fichier CloudTrail journal est activée	[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée
CIS v1.4.0	3.4 Assurez-vous que les CloudTrail sentiers sont intégrés aux CloudWatch journaux	[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs
CIS v1.4.0	3.5 Assurez-vous que AWS Config c'est activé dans toutes les régions	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.4.0	3.6 Assurez-vous que la journalisation de l'accès au compartiment S3 est activée sur le compartiment CloudTrail S3	[CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
CIS v1.4.0	3.7 Assurez-vous que CloudTrail les journaux sont chiffrés au repos à l'aide des KMS CMK	[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé
CIS v1.4.0	3.8 Assurez-vous que la rotation des CMK créés par les clients est activée	[KMS.4]AWS KMSla rotation des touches doit être activée
CIS v1.4.0	3.9 Assurez-vous que la journalisation des flux VPC est activée dans tous les VPC	[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC
CIS v1.4.0	4.4 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM	[CloudWatch.4] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique IAM
CIS v1.4.0	4.5 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration	[CloudWatch.5] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications CloudTrail de configuration
CIS v1.4.0	4.6 Assurez-vous qu'un filtre de mesure du journal et une alarme existent en cas Console de gestion AWS d'échec d'authentification	[CloudWatch.6] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour Console de gestion AWS échecs d'authentification

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.4.0	4.7 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour désactiver ou planifier la suppression des CMK créées par le client	[CloudWatch.7] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour la désactivation ou la suppression planifiée des clés gérées par le client
CIS v1.4.0	4.8 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3	[CloudWatch.8] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la politique du compartiment S3
CIS v1.4.0	4.9 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications AWS Config de configuration	[CloudWatch.9] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour AWS Config modifications de configuration
CIS v1.4.0	4.10 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications des groupes de sécurité	[CloudWatch.10] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au groupe de sécurité
CIS v1.4.0	4.11 Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès au réseau (NACL)	[CloudWatch.11] Assurez-vous qu'un filtre métrique de journal et une alarme existent pour les modifications apportées aux listes de contrôle d'accès réseau (NACL)
CIS v1.4.0	4.12 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau	[CloudWatch.12] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées aux passerelles réseau

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
CIS v1.4.0	4.13 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage	[CloudWatch.13] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications de la table de routage
CIS v1.4.0	4.14 Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC	[CloudWatch.14] Assurez-vous qu'un filtre de mesure du journal et une alarme existent pour les modifications apportées au VPC
CIS v1.4.0	5.1 Assurez-vous qu'aucune ACL réseau n'autorise l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration du serveur distant	[EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
CIS v1.4.0	5.3 Assurez-vous que le groupe de sécurité par défaut de chaque VPC limite l'ensemble du trafic	[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant
PCI DSS v3.2.1	PCI.AutoScaling.1 Les groupes de dimensionnement automatique associés à un équilibreur de charge doivent utiliser des contrôles de santé de l'équilibreur de charge	[AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail les journaux doivent être chiffrés au repos à l'aide de AWS KMS CMK	[CloudTrail.2] CloudTrail doit avoir le chiffrement au repos activé
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail doit être activé	[CloudTrail.3] Au moins une CloudTrail piste doit être activée
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail la validation des fichiers journaux doit être activée	[CloudTrail.4] la validation du fichier CloudTrail journal doit être activée

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail les sentiers doivent être intégrés à Amazon CloudWatch Logs	[CloudTrail.5] les CloudTrail sentiers doivent être intégrés à Amazon CloudWatch Logs
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub ou les URL du référentiel source Bitbucket doivent utiliser OAuth	[CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild les variables d'environnement du projet ne doivent pas contenir d'informations d'identification en texte clair	[CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
PCI DSS v3.2.1	PCI.Config.1 AWS Config doit être activé	[Config.1] AWS Config doit être activé et utiliser le rôle lié au service pour l'enregistrement des ressources
PCI DSS v3.2.1	PCI.CW.1 Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »	[CloudWatch.1] Un filtre de mesure du journal et une alarme devraient exister pour l'utilisation de l'utilisateur « root »
PCI DSS v3.2.1	PCI.DMS.1 Les instances de réplication du service de migration de base de données ne doivent pas être publiques	[DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques
PCI DSS v3.2.1	PCI.EC2.1 Les instantanés EBS ne doivent pas être restaurables publiquement	[EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement
PCI DSS v3.2.1	PCI.EC2.2 Le groupe de sécurité par défaut du VPC doit interdire le trafic entrant et sortant	[EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
PCI DSS v3.2.1	PCI.EC2.4 Les EIP EC2 non utilisés doivent être supprimés	[EC2.12] Les EIP Amazon EC2 non utilisés doivent être supprimés
PCI DSS v3.2.1	PCI.EC2.5 Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers le port 22	[EC2.13] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 22
PCI DSS v3.2.1	PCI.EC2.6 La journalisation des flux VPC doit être activée dans tous les VPC	[EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC
PCI DSS v3.2.1	PCI.ELBv2.1 L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS	[ELB.1] L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS
PCI DSS v3.2.1	PCI.ES.1 Les domaines Elasticse arch doivent se trouver dans un VPC	[ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public
PCI DSS v3.2.1	PCI.ES.2 Les domaines Elasticse arch doivent avoir le chiffrement au repos activé	[ES.1] Le chiffrement au repos doit être activé pour les domaines Elasticsearch
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty doit être activé	[GuardDuty.1] GuardDuty doit être activé
PCI DSS v3.2.1	PCI.IAM.1 La clé d'accès de l'utilisa teur root IAM ne doit pas exister	[IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
PCI DSS v3.2.1	PCI.IAM.2 Les utilisateurs IAM ne doivent pas être associés à des politiques IAM	[IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
PCI DSS v3.2.1	PCI.IAM.3 Les politiques IAM ne doivent pas autoriser la totalité des privilèges administratifs « * »	[IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
PCI DSS v3.2.1	PCI.IAM.4 L'authentification multifacteur matérielle doit être activée pour l'utilisateur root	[IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
PCI DSS v3.2.1	PCI.IAM.5 Le MFA virtuel doit être activé pour l'utilisateur root	[IAM.9] La MFA doit être activée pour l'utilisateur root
PCI DSS v3.2.1	PCI.IAM.6 Le MFA doit être activé pour tous les utilisateurs IAM	[IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
PCI DSS v3.2.1	PCI.IAM.7 Les informations d'identification utilisateur IAM doivent être désactivées si elles ne sont pas utilisées dans un délai prédéfini	[IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
PCI DSS v3.2.1	PCI.IAM.8 Les politiques de mot de passe pour les utilisateurs IAM doivent être configurées de manière robuste	[IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
PCI DSS v3.2.1	PCI.KMS.1 La rotation de la clé principale du client (CMK) doit être activée	[KMS.4]AWS KMSla rotation des touches doit être activée
PCI DSS v3.2.1	PCI.Lambda.1 Les fonctions Lambda devraient interdire l'accès public	[Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public
PCI DSS v3.2.1	PCI.Lambda.2 Les fonctions Lambda doivent se trouver dans un VPC	[Lambda.3] Les fonctions Lambda doivent se trouver dans un VPC

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch les domaines doivent se trouver dans un VPC	[Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
PCI DSS v3.2.1	PCI.Opensearch.2 Les instantanés EBS ne doivent pas être restaurables publiquement	[Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
PCI DSS v3.2.1	PCI.RDS.1 L'instantané RDS doit être privé	[RDS.1] L'instantané RDS doit être privé
PCI DSS v3.2.1	PCI.RDS.2 Les instances de base de données RDS doivent interdire l'accès public	[RDS.2] Les instances de base de données RDS doivent interdire l'accès public, comme le détermine la PubliclyAccessible configuration
PCI DSS v3.2.1	PCI.Redshift.1 Les clusters Amazon Redshift devraient interdire l'accès public	[Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public
PCI DSS v3.2.1	PCI.S3.1 Les compartiments S3 devraient interdire l'accès public à l'écriture	[S3.3] Les compartiments S3 à usage général devraient bloquer l'accès public à l'écriture
PCI DSS v3.2.1	PCI.S3.2 Les compartiments S3 devraient interdire l'accès public en lecture	[S3.2] Les compartiments S3 à usage général devraient bloquer l'accès public en lecture
PCI DSS v3.2.1	PCI.S3.3 La réplication entre régions doit être activée pour les compartim ents S3	[S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
PCI DSS v3.2.1	PCI.S3.5 Les compartiments S3 devraient nécessiter des requêtes pour utiliser Secure Socket Layer	[S3.5] Les compartiments S3 à usage général devraient nécessiter des demandes d'utilisation du protocole TLS

Standard	Identifiant et titre de contrôle standard	Identifiant et titre du contrôle de sécurité
PCI DSS v3.2.1	PCI.S3.6 Le paramètre S3 Block Public Access doit être activé	[S3.1] Les paramètres de blocage de l'accès public aux compartiments S3 à usage général doivent être activés
PCI DSS v3.2.1	PCI.SageMaker.1 Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet	[SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
PCI DSS v3.2.1	PCI.SSM.1 Les instances EC2 gérées par Systems Manager doivent avoir un statut de conformité des correctifs de COMPLIANT après l'installation d'un correctif	[SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
PCI DSS v3.2.1	PCI.SSM.2 Les instances EC2 gérées par Systems Manager doivent avoir un statut de conformité d'association de COMPLIANT	[SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT
PCI DSS v3.2.1	PCI.SSM.3 Les instances EC2 doivent être gérées par AWS Systems Manager	[SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager

Mise à jour des workflows pour la consolidation

Si vos flux de travail ne dépendent pas du format spécifique des champs des résultats de contrôle, aucune action n'est requise.

Si vos flux de travail reposent sur le format spécifique d'un ou de plusieurs champs des résultats de contrôle, comme indiqué dans les tableaux précédents, vous devez mettre à jour vos flux de travail. Par exemple, si vous avez créé une EventBridge règle Amazon qui a déclenché une action pour un ID de contrôle spécifique, par exemple en invoquant une AWS Lambda fonction si l'ID de contrôle est égal à CIS 2.7, mettez à jour la règle à utiliser CloudTrail.2, qui est la valeur du `Compliance.SecurityControlId` champ pour ce contrôle.

Si vous avez créé des informations personnalisées qui utilisent l'un des champs ou valeurs modifiés, mettez à jour ces informations pour utiliser les nouveaux champs ou valeurs.

Attributs ASFF de premier niveau requis

Les attributs de niveau supérieur suivants du AWS Security Finding Format (ASFF) sont requis pour toutes les découvertes dans Security Hub CSPM. Pour plus d'informations sur ces attributs, consultez le AwsSecurityFinding document de référence de l'API AWS Security Hub.

AwsAccountId

L' Compte AWS identifiant auquel s'applique le résultat.

Exemple

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indique quand le problème de sécurité potentiel ou l'événement détecté par une découverte a été créé.

Exemple

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Description

Description de la conclusion. Ce champ peut contenir un texte réutilisable non spécifique ou des détails spécifiques à l'instance de la conclusion.

Pour les résultats de contrôle générés par Security Hub CSPM, ce champ fournit une description du contrôle.

Ce champ ne fait référence à aucune norme si vous activez les résultats de contrôle consolidés.

Exemple

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

Identifiant de la solution de composant spécifique (une unité de logique discrète) ayant généré une conclusion.

Pour les résultats de contrôle générés par Security Hub CSPM, ce champ ne fait référence à aucune norme si vous activez les résultats de contrôle consolidés.

Exemple

```
"GeneratorId": "security-control/Config.1"
```

Id

Identifiant du produit pour une conclusion. Pour les résultats de contrôle générés par Security Hub CSPM, ce champ fournit le nom de ressource Amazon (ARN) du résultat.

Ce champ ne fait référence à aucune norme si vous activez les résultats de contrôle consolidés.

Exemple

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

Le nom de ressource Amazon (ARN) généré par Security Hub CSPM qui identifie de manière unique un produit de résultats tiers après son enregistrement auprès de Security Hub CSPM.

Le format de ce champ est `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Pour Services AWS ceux qui sont intégrés à Security Hub CSPM, le `company-id` doit être `aws` « » et le nom du service public `product-id` doit être le nom du service AWS public. Comme AWS les produits et services ne sont pas associés à un compte, la `account-id` section de l'ARN est vide. Services AWS qui ne sont pas encore intégrés à Security Hub CSPM sont considérés comme des produits tiers.
- Pour les produits publics, `company-id` et `product-id` doivent être les valeurs d'ID spécifiées au moment de l'inscription.
- Pour les produits privés, `company-id` doit être l'ID de compte. Le `product-id` doit être le mot réservé « par défaut » ou l'ID qui a été spécifié au moment de l'inscription.

Exemple

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Ressources

Le `Resources` tableau d'objets fournit un ensemble de types de données de ressources qui décrivent les AWS ressources auxquelles la découverte fait référence. Pour plus de détails sur les champs qu'un `Resources` objet peut contenir, notamment ceux qui sont obligatoires, consultez le document Resource de référence AWS de l'API Security Hub. Pour des exemples d'`Resources`objets spécifiques Services AWS, consultezRessources Objet ASFF.

Exemple

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
```

```
                    "Occurrences": {
                        "LineRanges": [
                            {
                                "Start": 1,
                                "End": 10,
                                "StartColumn": 20
                            }
                        ],
                        "Pages": [],
                        "Records": [],
                        "Cells": []
                    }
                },
                {
                    "Count": 59,
                    "Type": "EMAIL_ADDRESS",
                    "Occurrences": {
                        "Pages": [
                            {
                                "PageNumber": 1,
                                "OffsetRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                 },
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
```

```
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                         "Records": [
                             {
                                 "RecordIndex": 1,
                                 "JsonPath": "$.ssn.value"
                             }
                         ]
                     }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
             {
                 "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                 "Name": "1712be25e7c7f53c731fe464f1c869b8",
                 "Count": 2
             }
        ],
        "TotalCount": 2
    }
  }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
```

```
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

La version de schéma pour laquelle une conclusion est mise en forme. La valeur de ce champ doit être l'une des versions publiées officiellement identifiée par AWS. Dans la version actuelle, la version du schéma du AWS Security Finding Format est`2018-10-08`.

Exemple

```
"SchemaVersion": "2018-10-08"
```

Sévérité

Définit l'importance d'une découverte. Pour plus de détails sur cet objet, consultez `Severity` la référence de AWS Security Hub l'API.

`Severity`est à la fois un objet de premier niveau dans une découverte et imbriqué sous l'`FindingProviderFields`objet.

La valeur de l'`Severity`objet de niveau supérieur pour une découverte doit être mise à jour uniquement à l'aide de l'`BatchUpdateFindings`API.

Pour fournir des informations de gravité, les fournisseurs de recherche doivent mettre à jour l'`Severity`objet sous `FindingProviderFields` lors de l'envoi d'une demande d'`BatchImportFindings`API.
Si une `BatchImportFindings` demande de nouvelle découverte fournit uniquement `Label` ou uniquement`Normalized`, Security Hub CSPM renseigne automatiquement la valeur de l'autre champ.
Les `Original` champs `Product` et peuvent également être renseignés.

Si l'`Finding.Severity`objet de niveau supérieur est présent mais n'`Finding.FindingProviderFields`est pas présent, Security Hub CSPM crée l'`FindingProviderFields.Severity`objet et y copie l'intégralité`Finding.Severity object`. Cela garantit que les informations d'origine fournies par le fournisseur sont conservées dans la `FindingProviderFields.Severity` structure, même si l'`Severity`objet de niveau supérieur est remplacé.

La gravité du résultat ne tient pas compte de la sévérité des actifs en cause ou de la ressource sous-jacente. La sévérité est définie comme le niveau d'importance des ressources associées au résultat Par exemple, une ressource associée à une application critique présente une criticité plus élevée qu'une ressource associée à des tests hors production. Pour saisir des informations sur la sévérité des ressources, utilisez le champ `Criticality`.

Nous vous recommandons d'utiliser les conseils suivants lorsque vous traduisez les scores de gravité natifs des résultats en valeur de `Severity.Label` dans l'ASFF.

- `INFORMATIONAL`— Cette catégorie peut inclure la découverte d'une `PASSEDWARNING`, d'une `NOT AVAILABLE` vérification ou d'une identification de données sensibles.
- `LOW`— Des résultats qui pourraient donner lieu à de futurs compromis. Par exemple, cette catégorie peut inclure des vulnérabilités, des faiblesses de configuration et des mots de passe exposés.
- `MEDIUM`— Des résultats qui indiquent un compromis actif, mais rien n'indique qu'un adversaire a atteint ses objectifs. Par exemple, cette catégorie peut inclure les activités malveillantes, les activités de piratage et la détection de comportements inhabituels.

- `HIGH`ou `CRITICAL` — Des résultats indiquant qu'un adversaire a atteint ses objectifs, tels qu'une perte ou une compromission de données actives ou un déni de service.

Exemple

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Titre

Titre de la conclusion. Ce champ peut contenir un texte réutilisable non spécifique ou des détails spécifiques à cette instance de la conclusion.

Pour les résultats du contrôle, ce champ fournit le titre du contrôle. Ce champ ne fait référence à aucune norme si vous activez les résultats de contrôle consolidés.

Exemple

```
"Title": "AWS Config should be enabled"
```

Types

Un ou plusieurs types de résultats au format *namespace*/*category*/*classifier* qui classent un résultat. Ce champ ne fait référence à aucune norme si vous activez les résultats de contrôle consolidés.

`Types`doit être mis à jour uniquement à l'aide de l'`BatchUpdateFindings`API.

Pour trouver des fournisseurs qui souhaitent fournir une valeur pour, vous `Types` devez utiliser l'`Types`attribut ci-dessous `FindingProviderFields`.

Dans la liste suivante, les puces de premier niveau sont des espaces de noms, les puces de deuxième niveau sont des catégories et les puces de troisième niveau sont des classificateurs. Nous recommandons aux fournisseurs de recherche d'utiliser des espaces de noms définis pour faciliter le tri et le regroupement des résultats. Les catégories et les classificateurs définis peuvent également être utilisés, mais ne sont pas obligatoires. Seul l'espace de noms Vérifications de logiciels et de configuration contient des classificateurs définis.

Vous pouvez définir un chemin partiel pour namespace/category /classifier. Par exemple, les types de recherche suivants sont tous valides :

- TTP
- TTPs/Defense Évasion
- TTPs/Defense Evasion/CloudTrailStopped

Les catégories de tactiques, techniques et procédures (TTP) de la liste suivante correspondent à la matrice MITRE ATT&CK MatrixTM. L'espace de noms Comportements inhabituels reflète les comportements inhabituels généraux, tels que les anomalies statistiques générales, et n'est pas aligné sur un TTP spécifique. Toutefois, vous pouvez classer une conclusion avec les comportements inhabituels et les types de conclusions TTP.

Liste des espaces de noms, des catégories et des classificateurs :

- Vérifications de logiciels et de configuration
  - Vulnérabilités
    - CVE
  - AWS Meilleures pratiques en matière de sécurité
    - Joignabilité de réseau
    - Analyse du comportement d'exécution
  - Secteur d'activité et normes réglementaires
    - AWS Meilleures pratiques fondamentales en matière de sécurité
    - CIS Host Hardening Benchmarks
    - Indice de référence AWS des fondations CIS
    - PCI-DSS
    - Contrôles de la Cloud Security Alliance
    - Contrôles ISO 90001
    - Contrôles ISO 27001
    - Contrôles ISO 27017
    - Contrôles ISO 27018
    - SOC 1
    - SOC 2

    - Contrôles HIPAA (États-Unis)
    - Contrôles NIST 800-53 (États-Unis)
    - Contrôles NIST PPC (États-Unis)
    - Contrôles IRAP (Australie)
    - K-ISMS Controls (Corée)
    - Contrôles MTCS (Singapour)
    - Contrôles FISC (Japon)
    - Contrôles de la loi My Number Act (Japon)
    - Contrôles ENS (Espagne)
    - Contrôles Cyber Essentials Plus (Royaume-Uni)
    - G-Cloud Controls (Royaume-Uni)
    - Contrôles C5 (Allemagne)
    - IT-Grundschutz Controls (Allemagne)
    - Contrôles PIBR (Europe)
    - Contrôles TISAX (Europe)
  - Gestion des correctifs
- TTP
  - Accès initial
  - Exécution
  - Persistance
  - Escalade de privilèges
  - Évasion de défense
  - Accès via les informations d'identification
  - Découverte
  - Mouvement latéral
  - Collection
  - Commande et contrôle
- Effets
  - Exposition de données
  - Exfiltration de données

  - Destruction des données
  - Protection contre les attaques par déni de service
  - Consommation des ressources
- Comportements inhabituels
  - Application
  - Débit réseau
  - Adresse IP
  - Utilisateur
  - MV
  - Conteneur
  - sans serveur
  - Processus
  - Base de données
  - Données
- Définition des données sensibles
  - PII
  - Mots de passe
  - Juridique
  - Services financiers
  - Sécurité
  - Entreprise

Exemple

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

Indique la date à laquelle le fournisseur de recherche a mis à jour l'enregistrement de recherche pour la dernière fois.

Cet horodatage reflète l'heure à laquelle l'enregistrement de recherche a été mis à jour pour la dernière fois ou pour la dernière fois. Par conséquent, il peut différer de l'`LastObservedAt`horodatage, qui indique la date à laquelle l'événement ou la vulnérabilité a été observé pour la dernière fois ou pour la dernière fois.

Lorsque vous mettez à jour l'enregistrement de la conclusion, vous devez mettre à jour cet horodatage avec l'horodatage actuel. Lors de la création d'un enregistrement de recherche, les `UpdatedAt` horodatages `CreatedAt` et doivent être identiques. Après une mise à jour de l'enregistrement de recherche, la valeur de ce champ doit être plus récente que toutes les valeurs précédentes qu'il contenait.

Notez que cette `BatchUpdateFindings` opération `UpdatedAt` ne peut pas être mise à jour. Vous ne pouvez le mettre à jour qu'en utilisant `BatchImportFindings` operation.

Exemple

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Attributs ASFF de niveau supérieur facultatifs

Les attributs de niveau supérieur suivants du AWS Security Finding Format (ASFF) sont facultatifs pour les résultats dans Security Hub CSPM. Pour plus d'informations sur ces attributs, consultez le AwsSecurityFinding document de référence de l'API AWS Security Hub.

Action

L'`Action`objet fournit des détails sur une action qui affecte ou a été effectuée sur une ressource.

Exemple

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
```

```
                },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                    "GeoLocation": {
                        "Lon": 0,
                        "Lat": 0
                    },
                    "Organization": {
                        "AsnOrg": "ExampleASO",
                        "Org": "ExampleOrg",
                        "Isp": "ExampleISP",
                        "Asn": 64496
                    }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

Le Compte AWS nom auquel s'applique le résultat.

Exemple

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Le nom de l'entreprise du produit à l'origine de la découverte. Pour les résultats basés sur les contrôles, l'entreprise l'est AWS.

Security Hub CSPM renseigne cet attribut automatiquement pour chaque découverte. Vous ne pouvez pas le mettre à jour à l'aide de `BatchImportFindings` ou `BatchUpdateFindings`. L'exception à cette règle est lorsque vous utilisez une intégration personnalisée. Consultez the section called "Intégrations de produits personnalisées".

Lorsque vous utilisez la console Security Hub CSPM pour filtrer les résultats par nom de société, vous utilisez cet attribut. Lorsque vous utilisez l'API Security Hub CSPM pour filtrer les résultats par nom de société, vous utilisez l'`aws/securityhub/CompanyName`attribut ci-dessous. `ProductFields` Security Hub CSPM ne synchronise pas ces deux attributs.

Exemple

```
"CompanyName": "AWS"
```

Conformité d'

L'`Compliance`objet fournit généralement des détails sur une constatation de contrôle, tels que les normes applicables et l'état de la vérification de contrôle.

Exemple

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
```

```
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub CSPM a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Fiabilité

Probabilité qu'un résultat identifie avec précision le comportement ou le problème qu'il était censé identifier.

`Confidence`ne doit être mis à jour qu'à l'aide de `BatchUpdateFindings`.

Pour trouver des fournisseurs qui souhaitent fournir une valeur pour, vous `Confidence` devez utiliser l'`Confidence`attribut ci-dessous`FindingProviderFields`. Consultez the section called "Mise à jour des résultats avec FindingProviderFields".

`Confidence`est noté sur une base de 0 à 100 à l'aide d'une échelle de ratios. 0 signifie 0 % de confiance et 100 signifie 100 % de confiance. Par exemple, une détection d'exfiltration de données basée sur un écart statistique du trafic réseau est peu fiable car une exfiltration réelle n'a pas été vérifiée.

Exemple

```
"Confidence": 42
```

Criticité

Le niveau d'importance attribué aux ressources associées à une découverte.

`Criticality`ne doit être mis à jour qu'en appelant l'opération `BatchUpdateFindings` API. Ne mettez pas à jour cet objet avec `BatchImportFindings`.

Pour trouver des fournisseurs qui souhaitent fournir une valeur pour, vous `Criticality` devez utiliser l'`Criticality`attribut ci-dessous`FindingProviderFields`. Consultez the section called "Mise à jour des résultats avec FindingProviderFields".

`Criticality`est noté sur une base de 0 à 100, en utilisant une échelle de ratio qui ne prend en charge que les entiers entiers. Un score de 0 signifie que les ressources sous-jacentes ne sont pas critiques, et un score de 100 est réservé aux ressources les plus critiques.

Pour chaque ressource, tenez compte des points suivants lors de l'attribution `Criticality` :

- La ressource concernée contient-elle des données sensibles (par exemple, un compartiment S3 avec des informations personnelles) ?
- La ressource affectée permet-elle à un adversaire d'approfondir son accès ou d'étendre ses capacités pour mener à bien d'autres activités malveillantes (par exemple, un compte d'administrateur système compromis) ?
- La ressource est-elle stratégique (par exemple, un système d'entreprise clé compromis pourrait avoir un impact important sur les revenus) ?

Utilisez les directives suivantes :

- Une ressource alimentant des systèmes critiques ou contenant des données hautement sensibles peut être notée entre 75 et 100.
- Une ressource alimentant des systèmes importants (mais pas critiques) ou contenant des données modérément importantes peut être notée entre 25 et 74.
- Une ressource alimentant des systèmes sans importance ou contenant des données non sensibles doit être notée entre 0 et 24.

Exemple

```
"Criticality": 99
```

Détection

L'`Detection`objet fournit des informations sur la détection d'une séquence d'attaque à l'aide d'Amazon GuardDuty Extended Threat Detection. GuardDuty génère une détection de séquence d'attaque lorsque plusieurs événements correspondent à une activité potentiellement suspecte. Pour recevoir les résultats des séquences d' GuardDuty attaques dans AWS Security Hub CSPM,

vous devez l'avoir GuardDuty activé sur votre compte. Pour plus d'informations, consultez Amazon GuardDuty Extended Threat Detection dans le guide de GuardDuty l'utilisateur Amazon.

Exemple

```
"Detection": {
    "Sequence": {
     "Uid": "1111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
     "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
       "Uid": "1234567891",
       "MfAStatus": "DISABLED",
       "CreatedTime": "1716916944000",
       "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
       "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
       "Name": "ec2_instance_role_production",
       "Type": "AssumedRole",
       "Uid": "AROA987654321EXAMPLE:i-b188560f",
       "Account": {
        "Uid": "AccountId",
        "Name": "AccountName"
       }
      }
     }],
     "Endpoints": [{
      "Id": "EndpointId",
      "Ip": "203.0.113.1",
      "Domain": "example.com",
      "Port": 4040,
      "Location": {
       "City": "New York",
       "Country": "US",
       "Lat": 40.7123,
       "Lon": -74.0068
      },
      "AutonomousSystem": {
       "Name": "AnyCompany",
       "Number": 64496
      },
      "Connection": {
       "Direction": "INBOUND"
```

```
      }
     }],
     "Signals": [{
      "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
      "Title": "Someone ran a penetration test tool on your account.",
      "ActorIds": ["USER:AROA987654321EXAMPLE:i-b188560f:1234567891"],
      "Count": 19,
      "FirstSeenAt": 1716916943000,
      "SignalIndicators": [
       {
        "Key": "ATTACK_TACTIC",
        "Title": "Attack Tactic",
        "Values": [
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Data Destruction"
        ]
       },
      ],
      "LastSeenAt": 1716916944000,
      "Name": "Test:IAMUser/KaliLinux",
      "ResourceIds": [
       "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ],
      "Type": "FINDING"
     }],
     "SequenceIndicators": [
      {
       "Key": "ATTACK_TACTIC",
       "Title": "Attack Tactic",
       "Values": [
```

```
        "Discovery",
        "Exfiltration",
        "Impact"
       ]
      },
      {
       "Key": "HIGH_RISK_API",
       "Title": "High Risk Api",
       "Values": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBuckets"
        "s3:ListObjects"
       ]
      },
      {
       "Key": "ATTACK_TECHNIQUE",
       "Title": "Attack Technique",
       "Values": [
        "Cloud Service Discovery",
        "Data Destruction"
       ]
      }
     ]
    }
}
```

FindingProviderFields

`FindingProviderFields`inclut les attributs suivants :

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Les champs précédents sont imbriqués sous l'`FindingProviderFields`objet, mais ont des analogues du même nom que les champs ASFF de niveau supérieur. Lorsqu'un nouveau résultat est envoyé à Security Hub CSPM par un fournisseur de recherche, Security Hub CSPM renseigne

automatiquement l'`FindingProviderFields`objet s'il est vide en fonction des champs de niveau supérieur correspondants.

Les fournisseurs de recherche peuvent être mis à jour en `FindingProviderFields` utilisant l'`BatchImportFindings`API Security Hub CSPM. La recherche de fournisseurs ne peut pas mettre à jour cet objet avec `BatchUpdateFindings`.

Pour plus de détails sur la manière dont Security Hub CSPM gère les mises à jour depuis `FindingProviderFields` et `BatchImportFindings` vers les attributs de niveau supérieur correspondants, consultez. the section called "Mise à jour des résultats avec FindingProviderFields"

Les clients peuvent mettre à jour les champs de niveau supérieur à l'aide de cette `BatchUpdateFindings` opération. Les clients ne peuvent pas effectuer de mise à jour`FindingProviderFields`.

Exemple

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Indique quand le problème de sécurité potentiel ou l'événement détecté par une découverte a été observé pour la première fois.

Cet horodatage indique la date à laquelle l'événement ou la vulnérabilité a été observé pour la première fois. Par conséquent, il peut être différent de l'`CreatedAt`horodatage, qui reflète la date de création de cet enregistrement de recherche.

Pour les résultats de contrôle générés et mis à jour par Security Hub CSPM, cet horodatage peut également indiquer la dernière modification de l'état de conformité d'une ressource. Pour les autres types de résultats, cet horodatage doit être immuable entre les mises à jour de l'enregistrement de résultats, mais il peut être mis à jour si un horodatage plus précis est déterminé.

Exemple

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indique quand le problème de sécurité potentiel ou l'événement détecté par une découverte a été observé pour la dernière fois par le produit de résultats de sécurité.

Cet horodatage indique la date à laquelle l'événement ou la vulnérabilité a été observé pour la dernière fois ou pour la dernière fois. Par conséquent, il peut être différent de l'`UpdatedAt`horodatage, qui indique la dernière ou la dernière mise à jour de cet enregistrement de résultats.

Vous pouvez fournir cet horodatage, mais il n'est pas obligatoire lors de la première observation. Si vous remplissez ce champ lors de la première observation, l'horodatage doit être identique à l'horodatage. `FirstObservedAt` Vous devez mettre à jour ce champ pour refléter la dernière fois ou la fois la plus récente où l'horodatage a été observé chaque fois qu'une conclusion est observée.

Exemple

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

L'objet `Malware` fournit une liste de logiciels malveillants liés à un résultat.

Exemple

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
```

```
]
```

Réseau (retraité)

L'Networkobjet fournit des informations relatives au réseau concernant une découverte.

Cet objet est retiré. Pour fournir ces données, vous pouvez mapper les données à une ressource dans `Resources` ou utiliser l'`Action`objet.

Exemple

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

L'NetworkPathobjet fournit des informations sur un chemin réseau lié à une découverte. Chaque entrée `NetworkPath` représente une composante du chemin.

Exemple

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
```

```
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
    }
]
```

Remarque

L'Noteobjet spécifie une note définie par l'utilisateur que vous pouvez ajouter à une constatation.

Un fournisseur de conclusion peut fournir une note initiale pour une conclusion, mais ne peut pas ajouter de notes ensuite. Vous pouvez uniquement mettre à jour une note à l'aide de BatchUpdateFindings.

Exemple

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
```

```
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

L'PatchSummaryobjet fournit un résumé de l'état de conformité des correctifs pour une instance par rapport à une norme de conformité sélectionnée.

Exemple

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

Processus

L'Processobjet fournit des informations relatives au processus concernant une découverte.

Exemple :

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Indique quand Security Hub CSPM a reçu un résultat et a commencé à le traiter.

Cela diffère de `CreatedAt` et`UpdatedAt`, qui sont des horodatages obligatoires relatifs à l'interaction du fournisseur de recherche avec le problème de sécurité et la découverte. L'`ProcessedAt`horodatage indique à quel moment Security Hub CSPM commence à traiter une découverte. Un résultat apparaît dans le compte de l'utilisateur une fois le traitement terminé.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Type de données dans lequel les produits de résultats de sécurité peuvent inclure des informations supplémentaires spécifiques à la solution qui ne font pas partie du format d'identification de AWS sécurité défini.

Pour les résultats générés par les contrôles CSPM de Security Hub, `ProductFields` inclut des informations sur le contrôle. Consultez the section called "Génération et mise à jour des résultats de contrôle".

Ce champ ne doit pas contenir de données redondantes et ne doit pas contenir de données qui entrent en conflit avec les champs du AWS Security Finding Format.

Le préfixe `aws/` « » représente un espace de noms réservé aux AWS produits et services uniquement et ne doit pas être soumis avec les résultats d'intégrations tierces.

Bien que cela ne soit pas obligatoire, les produits doivent formater les noms de champs en tant que `company-id/product-id/field-name`, avec `company-id` et `product-id` qui correspondent à ceux fournis dans le `ProductArn` de la conclusion.

Les champs de référencement `Archival` sont utilisés lorsque Security Hub CSPM archive une découverte existante. Par exemple, Security Hub CSPM archive les résultats existants lorsque vous désactivez un contrôle ou une norme et lorsque vous activez ou désactivez les résultats de contrôle consolidés.

Ce champ peut également inclure des informations sur la norme qui inclut le contrôle qui a produit la découverte.

Exemple

```
"ProductFields": {
    "API", "DeleteTrail",
```

```
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Fournit le nom du produit qui a généré la découverte. Pour les résultats basés sur le contrôle, le nom du produit est Security Hub CSPM.

Security Hub CSPM renseigne cet attribut automatiquement pour chaque découverte. Vous ne pouvez pas le mettre à jour à l'aide de `BatchImportFindings` ou `BatchUpdateFindings`. L'exception à cette règle est lorsque vous utilisez une intégration personnalisée. Consultez the section called “Intégrations de produits personnalisées”.

Lorsque vous utilisez la console Security Hub CSPM pour filtrer les résultats par nom de produit, vous utilisez cet attribut.

Lorsque vous utilisez l'API CSPM de Security Hub pour filtrer les résultats par nom de produit, vous utilisez l'`aws/securityhub/ProductName`attribut ci-dessous. `ProductFields`

Security Hub CSPM ne synchronise pas ces deux attributs.

RecordState

Fournit l'état d'enregistrement d'une découverte.

Par défaut, les résultats qui ont été initialement générées par un service sont considérés comme `ACTIVE`.

L'état `ARCHIVED` indique qu'une conclusion doit être masquée. Les résultats archivés ne sont pas supprimés immédiatement. Vous pouvez les rechercher, les consulter et créer des rapports à leur sujet. Security Hub CSPM archive automatiquement les résultats basés sur les contrôles si la ressource associée est supprimée, si la ressource n'existe pas ou si le contrôle est désactivé.

`RecordState`est destiné à la recherche de fournisseurs et ne peut être mis à jour qu'à l'aide de `BatchImportFindings` cette opération. Vous ne pouvez pas le mettre à jour à l'aide de `BatchUpdateFindings` cette opération.

Pour suivre l'état d'avancement de votre enquête sur une découverte, utilisez `Workflow` au lieu de`RecordState`.

Si l'état de l'enregistrement passe de `ARCHIVED` à `ACTIVE` et que l'état du flux de travail de la découverte est `NOTIFIED` ou`RESOLVED`, Security Hub CSPM change automatiquement l'état du flux de travail en. `NEW`

Exemple

```
"RecordState": "ACTIVE"
```

Région

Spécifie la Région AWS source à partir de laquelle la découverte a été générée.

Security Hub CSPM renseigne cet attribut automatiquement pour chaque découverte. Vous ne pouvez pas le mettre à jour à l'aide de `BatchImportFindings` ou `BatchUpdateFindings`.

Exemple

```
"Region": "us-west-2"
```

RelatedFindings

Fournit une liste des résultats liés à la découverte actuelle.

`RelatedFindings`ne doit être mis à jour qu'avec l'opération `BatchUpdateFindings` d'API. Vous ne devez pas mettre à jour cet objet avec `BatchImportFindings`.

Pour les `BatchImportFindings` demandes, la recherche de fournisseurs doit utiliser l'`RelatedFindings`objet ci-dessous `FindingProviderFields`.

Pour consulter les descriptions des `RelatedFindings` attributs, consultez `RelatedFinding` la référence de AWS Security Hub l'API.

Exemple

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

Exemple

```
"RiskAssessment": {
    "Posture": {
        "FindingTotal": 4,
        "Indicators": [
            {
                "Type": "Reachability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/1234567890abcdef0",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/
abcdef01234567890",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            },
            {
                "Type": "Vulnerability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345abcdef6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
```

```
                    },
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            }
        ]
    }
}
```

Correction

L'objet `Remediation` fournit des informations sur les étapes de correction recommandées pour résoudre le résultat.

Exemple

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 CSPM documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Exemple

Spécifie s'il s'agit d'un résultat d'échantillon.

```
"Sample": true
```

SourceUrl

L'`SourceUrl`objet fournit une URL qui renvoie à une page concernant la découverte en cours dans le produit recherché.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

L'`ThreatIntelIndicator`objet fournit des informations sur les menaces liées à une découverte.

Exemple

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Menaces

L'`Threats`objet fournit des détails sur la menace détectée par une découverte.

Exemple

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Fournit une liste des paires de chaînes nom-valeur associées à la recherche. Ce sont des champs définis par l'utilisateur personnalisés qui sont ajoutés à une conclusion. Ces champs peuvent être générés automatiquement par le biais de votre configuration spécifique.

La recherche de fournisseurs ne doit pas utiliser ce champ pour les données générées par le produit. Les fournisseurs de recherche peuvent plutôt utiliser le `ProductFields` champ pour les données qui ne correspondent à aucun champ standard du format AWS de recherche de sécurité.

Ces champs peuvent uniquement être mis à jour à l'aide de `BatchUpdateFindings`.

Exemple

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Fournit la véracité d'une constatation. Les produits de résultats peuvent fournir une valeur de `UNKNOWN` pour ce champ. Un produit de résultats doit fournir une valeur pour ce champ s'il existe un analogue significatif dans le système du produit de résultats. Ce champ est généralement renseigné par une décision ou une action de l'utilisateur après avoir étudié un résultat.

Un fournisseur de conclusions peut fournir une valeur initiale pour cet attribut, mais ne peut plus le mettre à jour ensuite. Vous ne pouvez mettre à jour cet attribut qu'en utilisant `BatchUpdateFindings`.

```
"VerificationState": "Confirmed"
```

Vulnérabilités

L'Vulnerabilitiesobjet fournit une liste des vulnérabilités associées à une découverte.

Exemple

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
```

```
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
```

```
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Flux de travail

L'objet `Workflow` fournit des informations sur l'état de l'enquête dans un résultat.

Ce champ est destiné à être utilisé par les clients avec les outils de correction, d'orchestration et de gestion des tickets. Il n'est pas destiné à identifier les fournisseurs.

Vous ne pouvez mettre à jour le `Workflow` champ qu'avec `BatchUpdateFindings`. Les clients peuvent également le mettre à jour à partir de la console. Consultez the section called "Définition de l'état des résultats dans le flux de travail".

Exemple

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Retraité)

Cet objet est retiré et a été remplacé par le `Status` champ de l'`Workflow`objet.

Ce champ indique l'état du flux de travail d'une découverte. Les produits des conclusions peuvent fournir la valeur de `NEW` pour ce champ. Un produit de conclusion peut fournir une valeur pour ce champ s'il y a un produit similaire significatif dans les résultats du système du produit de conclusion.

Exemple

```
"WorkflowState": "NEW"
```

Ressources Objet ASFF

Dans le format ASFF (AWS Security Finding Format), l'`Resources`objet fournit des informations sur les ressources impliquées dans une découverte. Il contient un tableau contenant jusqu'à 32 objets de ressources. Pour déterminer comment les noms de ressources sont mis en forme, consultezAWS Format de recherche de sécurité (ASFF). Pour obtenir des exemples de chaque objet de ressource, sélectionnez une ressource dans la liste suivante.

Rubriques

- Attributs des ressources dans l'ASFF
- AwsAmazonMQ ressources en ASFF
- AwsApiGateway ressources en ASFF
- AwsAppSync ressources en ASFF
- AwsAthena ressources en ASFF
- AwsAutoScaling ressources en ASFF
- AwsBackup ressources en ASFF
- AwsCertificateManager ressources en ASFF
- AwsCloudFormation ressources en ASFF
- AwsCloudFront ressources en ASFF
- AwsCloudTrail ressources en ASFF
- AwsCloudWatch ressources en ASFF
- AwsCodeBuild ressources en ASFF
- AwsDms ressources en ASFF
- AwsDynamoDB ressources en ASFF
- AwsEc2 ressources en ASFF
- AwsEcr ressources en ASFF
- AwsEcs ressources en ASFF
- AwsEfs ressources en ASFF
- AwsEks ressources en ASFF
- AwsElasticBeanstalk ressources en ASFF
- AwsElasticSearch ressources en ASFF
- AwsElb ressources en ASFF

- AwsEventBridge ressources en ASFF
- AwsGuardDuty ressources en ASFF
- AwsIam ressources en ASFF
- AwsKinesis ressources en ASFF
- AwsKms ressources en ASFF
- AwsLambda
- AwsMsk ressources en ASFF
- AwsNetworkFirewall ressources en ASFF
- AwsOpenSearchService ressources en ASFF
- AwsRds ressources en ASFF
- AwsRedshift ressources en ASFF
- AwsRoute53 ressources en ASFF
- AWS S3 ressources en ASFF
- AwsSageMaker ressources en ASFF
- AwsSecretsManager ressources en ASFF
- AwsSns ressources en ASFF
- AwsSqs ressources en ASFF
- AwsSsm ressources en ASFF
- AwsStepFunctions ressources en ASFF
- AwsWaf ressources en ASFF
- AwsXray ressources en ASFF
- CodeRepository objet en ASFF
- Conteneur objet en ASFF
- Autre objet en ASFF

Attributs des ressources dans l'ASFF

Voici des descriptions et des exemples de l'`Resources`objet au format ASFF (AWS Security Finding Format). Pour plus d'informations sur ces champs, consultez Ressources.

ApplicationArn

Identifie l'Amazon Resource Name (ARN) de l'application impliquée dans la recherche.

Exemple

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Identifie le nom de l'application impliquée dans la découverte.

Exemple

```
"ApplicationName": "SampleApp"
```

DataClassification

Le DataClassification champ fournit des informations sur les données sensibles détectées sur la ressource.

Exemple

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
```

```
                    }
                ],
                "Pages": [],
                "Records": [],
                "Cells": []
            }
        },
        {
            "Count": 59,
            "Type": "EMAIL_ADDRESS",
            "Occurrences": {
                "Pages": [
                    {
                        "PageNumber": 1,
                        "OffsetRange": {
                            "Start": 1,
                            "End": 100,
                            "StartColumn": 10
                        },
                        "LineRange": {
                            "Start": 1,
                            "End": 100,
                            "StartColumn": 10
                        }
                    }
                ]
            }
        },
        {
            "Count": 2229,
            "Type": "URL",
            "Occurrences": {
               "LineRanges": [
                    {
                        "Start": 1,
                        "End": 13
                    }
               ]
            }
        },
        {
            "Count": 13826,
            "Type": "NameDetection",
            "Occurrences": {
```

```
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
                "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                "Name": "1712be25e7c7f53c731fe464f1c869b8",
                "Count": 2,
            }
        ],
        "TotalCount": 2
    }
  }
}
```

Détails

Le Details champ fournit des informations supplémentaires sur une seule ressource à l'aide des objets appropriés. Chaque ressource doit être fournie dans un objet de ressource distinct dans l'`Resources`objet.

Notez que si la taille de la recherche dépasse le maximum de 240 Ko, l'`Details`objet est supprimé de la recherche. Pour les résultats de contrôle utilisant AWS Config des règles, vous pouvez consulter les détails des ressources sur la AWS Config console.

Security Hub CSPM fournit un ensemble de détails sur les ressources disponibles pour les types de ressources pris en charge. Ces détails correspondent aux valeurs de l'`Type`objet. Utilisez les types fournis dans la mesure du possible.

Par exemple, si la ressource est un compartiment S3, définissez la ressource `Type` sur `AwsS3Bucket` et fournissez les détails de la ressource dans l'`AwsS3Bucket`objet.

L'`Other`objet vous permet de fournir des champs et des valeurs personnalisés. Vous utilisez l'`Other`objet dans les cas suivants :

- Le type de ressource (la valeur de la ressource`Type`) ne possède pas d'objet de détails correspondant. Pour fournir des informations sur la ressource, vous utilisez l'`Other`objet.
- L'objet correspondant au type de ressource n'inclut pas tous les champs que vous souhaitez renseigner. Dans ce cas, utilisez l'objet de détails du type de ressource pour renseigner les champs disponibles. Utilisez l'`Other`objet pour renseigner les champs qui ne figurent pas dans l'objet spécifique au type.
- Le type de ressource n'est pas l'un des types fournis. Dans ce cas, définissez `Resource.Type` sur `Other` et utilisez l'`Other`objet pour renseigner les détails.

Exemple

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
```

```
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

L'identifiant du type de ressource donné.

Pour les AWS ressources identifiées par Amazon Resource Names (ARN), il s'agit de l'ARN.

Pour les AWS ressources dépourvues d'ARN, il s'agit de l'identifiant tel que défini par le AWS service qui a créé la ressource.

Pour les AWS non-ressources, il s'agit d'un identifiant unique associé à la ressource.

Exemple

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partition

Partition dans laquelle se trouve la ressource. Une partition est un groupe de Régions AWS. Chacune Compte AWS est limitée à une partition.

Les partitions suivantes sont prises en charge :

- `aws` – Régions AWS
- `aws-cn` – Régions en Chine
- `aws-us-gov` – AWS GovCloud (US) Region

Exemple

```
"Partition": "aws"
```

Région

Code indiquant Région AWS où se trouve cette ressource. Pour une liste des codes de région, voir Points de terminaison https://docs.aws.amazon.com/general/latest/gr/rande.html#regional-endpoints régionaux.

Exemple

```
"Region": "us-west-2"
```

ResourceRole

Identifie le rôle de la ressource dans la découverte. Une ressource est soit la cible de l'activité de recherche, soit l'acteur qui a réalisé l'activité.

Exemple

```
"ResourceRole": "target"
```

Étiquettes

Ce champ fournit des informations sur la clé de balise et la valeur de la ressource impliquée dans une découverte. Vous pouvez baliser les ressources qui sont prises en charge par le `GetResources` fonctionnement de l'API de Groupes de ressources AWS balisage. Security Hub CSPM appelle cette opération via le rôle lié au service et récupère les balises de ressource si le `Resource.Id` champ AWS Security Finding Format (ASFF) est renseigné avec l'ARN de la ressource. AWS Les ID de ressources non valides sont ignorés.

Vous pouvez ajouter des balises de ressources aux résultats que Security Hub CSPM ingère, y compris les résultats provenant de produits intégrés Services AWS et tiers.

L'ajout de balises vous indique les balises qui étaient associées à une ressource au moment où la recherche a été traitée. Vous ne pouvez inclure l'`Tags`attribut que pour les ressources associées à une balise. Si une ressource n'a pas de balise associée, n'incluez pas d'attribut `Tags` dans le résultat.

L'inclusion de balises de ressources dans les résultats élimine le besoin de créer des pipelines d'enrichissement des données ou d'enrichir manuellement les métadonnées des résultats de sécurité. Vous pouvez également utiliser des balises pour rechercher ou filtrer les résultats et les informations et créer des règles d'automatisation.

Pour plus d'informations sur les restrictions qui s'appliquent aux balises, consultez la section Limites et exigences relatives à la dénomination des balises.

Dans ce champ, vous ne pouvez fournir que les balises qui existent sur une AWS ressource. Pour fournir des données qui ne sont pas définies dans le format AWS Security Finding, utilisez le sous-champ `Other` details.

Exemple

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Type

Type de ressource pour lequel vous fournissez des informations.

Dans la mesure du possible, utilisez l'un des types de ressources fournis, tel que `AwsEc2Instance` ou `AwsS3Bucket`.

Si le type de ressource ne correspond à aucun des types de ressources fournis, définissez la ressource `Type` sur et utilisez le sous-champ `Other` Détails pour renseigner les détails. `Other`

Les valeurs prises en charge sont répertoriées sous Ressources.

Exemple

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsAmazonMQ` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsAmazonMQBroker

`AwsAmazonMQBroker`fournit des informations sur un courtier Amazon MQ, qui est un environnement de courtier de messages exécuté sur Amazon MQ.

L'exemple suivant montre l'ASFF de l'`AwsAmazonMQBroker`objet. Pour consulter les descriptions des `AwsAmazonMQBroker` attributs, consultez AwsAmazonMQBroker la référence de AWS Security Hub l'API.

Exemple

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
```

```
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsApiGateway` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsApiGatewayRestApi

L'`AwsApiGatewayRestApi`objet contient des informations concernant une API REST dans la version 1 d'Amazon API Gateway.

Voici un exemple de `AwsApiGatewayRestApi` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayRestApi` attributs, consultez AwsApiGatewayRestApiDetails la référence de AWS Security Hub l'API.

Exemple

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

L'`AwsApiGatewayStage`objet fournit des informations sur un stage Amazon API Gateway version 1.

Voici un exemple de `AwsApiGatewayStage` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayStage` attributs, consultez AwsApiGatewayStageDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
```

```
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

L'`AwsApiGatewayV2Api`objet contient des informations concernant une API version 2 dans Amazon API Gateway.

Voici un exemple de `AwsApiGatewayV2Api` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayV2Api` attributs, consultez AwsApiGatewayV2ApiDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
```

```
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

`AwsApiGatewayV2Stage`contient des informations sur une étape de version 2 pour Amazon API Gateway.

Voici un exemple de `AwsApiGatewayV2Stage` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayV2Stage` attributs, consultez AwsApiGatewayV2StageDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
```

```
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```


AwsAppSync ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsAppSync` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`fournit des informations sur une API AWS AppSync GraphQL, qui est une construction de niveau supérieur pour votre application.

L'exemple suivant montre l'ASFF de l'`AwsAppSyncGraphQLApi`objet. Pour consulter les descriptions des `AwsAppSyncGraphQLApi` attributs, consultez AwsAppSyncGraphQLApi la référence de AWS Security Hub l'API.

Exemple

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsAthena` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsAthenaWorkGroup

`AwsAthenaWorkGroup`fournit des informations sur un groupe de travail Amazon Athena. Un groupe de travail vous permet de séparer les utilisateurs, les équipes, les applications ou les charges de travail. Il vous aide également à fixer des limites au traitement des données et à suivre les coûts.

L'exemple suivant montre l'ASFF de l'`AwsAthenaWorkGroup`objet. Pour consulter les descriptions des `AwsAthenaWorkGroup` attributs, consultez AwsAthenaWorkGroup la référence de AWS Security Hub l'API.

Exemple

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsAutoScaling` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsAutoScalingAutoScalingGroup

L'`AwsAutoScalingAutoScalingGroup`objet fournit des informations sur un groupe de mise à l'échelle automatique.

Voici un exemple de `AwsAutoScalingAutoScalingGroup` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsAutoScalingAutoScalingGroup` attributs, consultez AwsAutoScalingAutoScalingGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
```

```
}
```

AwsAutoScalingLaunchConfiguration

L'`AwsAutoScalingLaunchConfiguration`objet fournit des détails sur une configuration de lancement.

Voici un exemple de `AwsAutoScalingLaunchConfiguration` recherche dans le format ASFF (AWS Security Finding Format).

Pour consulter les descriptions des `AwsAutoScalingLaunchConfiguration` attributs, consultez AwsAutoScalingLaunchConfigurationDetails la référence de AWS Security Hub l'API.

Exemple

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
```

```
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsBackup` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsBackupBackupPlan

L'`AwsBackupBackupPlan`objet fournit des informations sur un plan AWS Backup de sauvegarde. Un plan de AWS Backup sauvegarde est une expression de politique qui définit quand et comment vous souhaitez sauvegarder vos AWS ressources.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsBackupBackupPlan`objet. Pour consulter les descriptions des `AwsBackupBackupPlan` attributs, consultez AwsBackupBackupPlan la référence de AWS Security Hub l'API.

Exemple

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
```

```
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

L'`AwsBackupBackupVault`objet fournit des informations sur un coffre-fort AWS Backup de sauvegarde. Un coffre-fort AWS Backup de sauvegarde est un conteneur qui stocke et organise vos sauvegardes.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsBackupBackupVault`objet. Pour consulter les descriptions des `AwsBackupBackupVault` attributs, consultez AwsBackupBackupVault la référence de AWS Security Hub l'API.

Exemple

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
```

```
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

L'`AwsBackupRecoveryPoint`objet fournit des informations sur une AWS Backup sauvegarde, également appelée point de restauration. Un point AWS Backup de restauration représente le contenu d'une ressource à un moment donné.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsBackupRecoveryPoint`objet. Pour consulter les descriptions des `AwsBackupBackupVault` attributs, consultez AwsBackupRecoveryPoint la référence de AWS Security Hub l'API.

Exemple

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
```

```
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```


AwsCertificateManager ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsCertificateManager` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsCertificateManagerCertificate

L'`AwsCertificateManagerCertificate`objet fournit des informations sur un certificat AWS Certificate Manager (ACM).

Voici un exemple de `AwsCertificateManagerCertificate` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsCertificateManagerCertificate` attributs, consultez AwsCertificateManagerCertificateDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
```

```
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsCloudFormation` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsCloudFormationStack

L'`AwsCloudFormationStack`objet fournit des détails sur une AWS CloudFormation pile imbriquée en tant que ressource dans un modèle de niveau supérieur.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsCloudFormationStack`objet. Pour consulter les descriptions des `AwsCloudFormationStack` attributs, consultez AwsCloudFormationStackDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
```

```
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsCloudFront` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsCloudFrontDistribution

L'`AwsCloudFrontDistribution`objet fournit des informations sur la configuration d'une CloudFront distribution Amazon.

Voici un exemple de `AwsCloudFrontDistribution` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsCloudFrontDistribution` attributs, consultez AwsCloudFrontDistributionDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
```

```
        "Bucket": "myawslogbucket.s3.amazonaws.com",
        "Enabled": false,
        "IncludeCookies": false,
        "Prefix": "myawslog/"
    },
    "OriginGroups": {
         "Items": [
            {
               "FailoverCriteria": {
                   "StatusCodes": {
                        "Items": [
                            200,
                            301,
                            404
                        ]
                        "Quantity": 3
                    }
               }
            }
          ]
    },
    "Origins": {
          "Items": [
              {
                 "CustomOriginConfig": {
                     "HttpPort": 80,
                     "HttpsPort": 443,
                     "OriginKeepaliveTimeout": 60,
                     "OriginProtocolPolicy": "match-viewer",
                     "OriginReadTimeout": 30,
                     "OriginSslProtocols": {
                       "Items": ["SSLv3", "TLSv1"],
                       "Quantity": 2
                     }
                 }
              },
          ]
    },
                 "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                 "Id": "my-origin",
                 "OriginPath": "/production",
                 "S3OriginConfig": {
                     "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
```

```
                }
            ]
        },
        "Status": "Deployed",
        "ViewerCertificate": {
               "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
               "Certificate": "ASCAJRRE5XYF52TKRY5M4",
               "CertificateSource": "iam",
               "CloudFrontDefaultCertificate": true,
               "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
               "MinimumProtocolVersion": "TLSv1.2_2021",
               "SslSupportMethod": "sni-only"
         },
         "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsCloudTrail` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsCloudTrailTrail

L'`AwsCloudTrailTrail`objet fournit des informations sur un AWS CloudTrail sentier.

Voici un exemple de `AwsCloudTrailTrail` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsCloudTrailTrail` attributs, consultez AwsCloudTrailTrailDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
```

```
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsCloudWatch` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsCloudWatchAlarm

L'`AwsCloudWatchAlarm`objet fournit des détails sur les CloudWatch alarmes Amazon qui surveillent une métrique ou exécutent une action lorsqu'une alarme change d'état.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsCloudWatchAlarm`objet. Pour consulter les descriptions des `AwsCloudWatchAlarm` attributs, consultez AwsCloudWatchAlarmDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsCloudWatchAlarm": {
 "ActionsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
```

```
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsCodeBuild` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsCodeBuildProject

L'objet `AwsCodeBuildProject` fournit des informations sur un projet AWS CodeBuild .

Voici un exemple de `AwsCodeBuildProject` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsCodeBuildProject` attributs, consultez AwsCodeBuildProjectDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
```

```
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "EncryptionKey": "string",
   "Certificate": "string",
   "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [
           {
                "Name": "string",
                "Type": "string",
                "Value": "string"
           }
      ],
   "ImagePullCredentialsType": "string",
   "PrivilegedMode": boolean,
   "RegistryCredential": {
       "Credential": "string",
       "CredentialProvider": "string"
   },
   "Type": "string"
   },
   "LogsConfig": {
        "CloudWatchLogs": {
             "GroupName": "string",
```

```
            "Status": "string",
            "StreamName": "string"
        },
        "S3Logs": {
            "EncryptionDisabled": boolean,
            "Location": "string",
            "Status": "string"
        }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
    },
    "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
}
```

AwsDms ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsDms` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsDmsEndpoint

L'`AwsDmsEndpoint`objet fournit des informations sur un point de terminaison AWS Database Migration Service (AWS DMS). Un point de terminaison fournit des informations de connexion, de type de banque de données et de localisation concernant votre banque de données.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsDmsEndpoint`objet. Pour consulter les descriptions des `AwsDmsEndpoint` attributs, consultez AwsDmsEndpointDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsDmsEndpoint": {
```

```
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

L'`AwsDmsReplicationInstance`objet fournit des informations sur une instance de réplication AWS Database Migration Service (AWS DMS). DMS utilise une instance de réplication pour se connecter à votre magasin de données source, lire les données source et formater les données en vue de leur consommation par le magasin de données cible.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsDmsReplicationInstance`objet. Pour consulter les descriptions des `AwsDmsReplicationInstance` attributs, consultez AwsDmsReplicationInstanceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
```

```
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

L'`AwsDmsReplicationTask`objet fournit des informations sur une tâche de réplication AWS Database Migration Service (AWS DMS). Une tâche de réplication déplace un ensemble de données du point de terminaison source vers le point de terminaison cible.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsDmsReplicationInstance`objet. Pour consulter les descriptions des `AwsDmsReplicationInstance` attributs, consultez AwsDmsReplicationInstance la référence de AWS Security Hub l'API.

Exemple

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
```

{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",

```
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsDynamoDB` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsDynamoDbTable

L'`AwsDynamoDbTable`objet fournit des informations sur une table Amazon DynamoDB.

Voici un exemple de `AwsDynamoDbTable` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsDynamoDbTable` attributs, consultez AwsDynamoDbTableDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
```

```
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
   ],
   "GlobalTableVersion": "V1",
   "ItemCount": 2705,
   "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
    ],
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
```

```
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
```

```
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2 ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsEc2` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsEc2ClientVpnEndpoint

L'`AwsEc2ClientVpnEndpoint`objet fournit des informations sur un AWS Client VPN point de terminaison. Un point de terminaison VPN client est la ressource que vous créez et configurez pour activer et gérer les sessions VPN client. C'est le point de terminaison pour toutes les sessions VPN client.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2ClientVpnEndpoint`objet. Pour consulter les descriptions des `AwsEc2ClientVpnEndpoint` attributs, consultez AwsEc2ClientVpnEndpointDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

L'`AwsEc2Eip`objet fournit des informations sur une adresse IP Elastic.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2Eip`objet. Pour consulter les descriptions des `AwsEc2Eip` attributs, consultez AwsEc2EipDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

L'`AwsEc2Instance`objet fournit des informations sur une instance Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2Instance`objet. Pour consulter les descriptions des `AwsEc2Instance` attributs, consultez AwsEc2InstanceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
```

```
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

L'`AwsEc2LaunchTemplate`objet contient des informations sur un modèle de lancement Amazon Elastic Compute Cloud qui spécifie les informations de configuration de l'instance.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2LaunchTemplate`objet. Pour consulter les descriptions des `AwsEc2LaunchTemplate` attributs, consultez AwsEc2LaunchTemplateDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
```

```
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

L'`AwsEc2NetworkAcl`objet contient des informations sur une liste de contrôle d'accès au réseau (ACL) Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2NetworkAcl`objet. Pour consulter les descriptions des `AwsEc2NetworkAcl` attributs, consultez AwsEc2NetworkAclDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
```

```
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

L'`AwsEc2NetworkInterface`objet fournit des informations sur une interface réseau Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2NetworkInterface`objet. Pour consulter les descriptions des `AwsEc2NetworkInterface` attributs, consultez AwsEc2NetworkInterfaceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

L'`AwsEc2RouteTable`objet fournit des informations sur une table de routage Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2RouteTable`objet. Pour consulter les descriptions des `AwsEc2RouteTable` attributs, consultez AwsEc2RouteTableDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

L'`AwsEc2SecurityGroup`objet décrit un groupe de sécurité Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2SecurityGroup`objet. Pour consulter les descriptions des `AwsEc2SecurityGroup` attributs, consultez AwsEc2SecurityGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

L'`AwsEc2Subnet`objet fournit des informations sur un sous-réseau dans Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2Subnet`objet. Pour consulter les descriptions des `AwsEc2Subnet` attributs, consultez AwsEc2SubnetDetails la référence de AWS Security Hub l'API.

Exemple

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

L'`AwsEc2TransitGateway`objet fournit des informations sur une passerelle de transit Amazon EC2 qui interconnecte vos clouds privés virtuels (VPC) et vos réseaux locaux.

Voici un exemple de `AwsEc2TransitGateway` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsEc2TransitGateway` attributs, consultez AwsEc2TransitGatewayDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
```

```
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

L'`AwsEc2Volume`objet fournit des informations sur un volume Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2Volume`objet. Pour consulter les descriptions des `AwsEc2Volume` attributs, consultez AwsEc2VolumeDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

L'`AwsEc2Vpc`objet fournit des informations sur un VPC Amazon EC2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2Vpc`objet. Pour consulter les descriptions des `AwsEc2Vpc` attributs, consultez AwsEc2VpcDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

L'`AwsEc2VpcEndpointService`objet contient des détails sur la configuration du service pour un service de point de terminaison VPC.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2VpcEndpointService`objet. Pour consulter les descriptions des `AwsEc2VpcEndpointService` attributs, consultez AwsEc2VpcEndpointServiceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
```

```
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

L'`AwsEc2VpcPeeringConnection`objet fournit des détails sur la connexion réseau entre deux VPC.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEc2VpcPeeringConnection`objet. Pour consulter les descriptions des `AwsEc2VpcPeeringConnection` attributs, consultez AwsEc2VpcPeeringConnectionDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
```

```
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```


AwsEcr ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsEcr` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsEcrContainerImage

L'`AwsEcrContainerImage`objet fournit des informations sur une image Amazon ECR.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcrContainerImage`objet. Pour consulter les descriptions des `AwsEcrContainerImage` attributs, consultez AwsEcrContainerImageDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

L'`AwsEcrRepository`objet fournit des informations sur un référentiel Amazon Elastic Container Registry.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcrRepository`objet. Pour consulter les descriptions des `AwsEcrRepository` attributs, consultez AwsEcrRepositoryDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsEcs` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsEcsCluster

L'`AwsEcsCluster`objet fournit des informations sur un cluster Amazon Elastic Container Service.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcsCluster`objet. Pour consulter les descriptions des `AwsEcsCluster` attributs, consultez AwsEcsClusterDetails la référence de AWS Security Hub l'API.

Exemple

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

L'`AwsEcsContainer`objet contient des informations sur un conteneur Amazon ECS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcsContainer`objet. Pour consulter les descriptions des `AwsEcsContainer` attributs, consultez AwsEcsContainerDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

L'`AwsEcsService`objet fournit des informations sur un service au sein d'un cluster Amazon ECS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcsService`objet. Pour consulter les descriptions des `AwsEcsService` attributs, consultez AwsEcsServiceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
```

```
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
```

```
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

L'`AwsEcsTask`objet fournit des informations sur une tâche Amazon ECS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcsTask`objet. Pour consulter les descriptions des `AwsEcsTask` attributs, consultez AwsEcsTask la référence de AWS Security Hub l'API.

Exemple

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
```

```
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

L'`AwsEcsTaskDefinition`objet contient des informations sur la définition d'une tâche. Une définition de tâche décrit les définitions de conteneur et de volume d'une tâche Amazon Elastic Container Service.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEcsTaskDefinition`objet. Pour consulter les descriptions des `AwsEcsTaskDefinition` attributs, consultez AwsEcsTaskDefinitionDetails la référence de AWS Security Hub l'API.

Exemple

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
```

```
                "LogDriver": "awslogs",
                "Options": {
                    "awslogs-group": "/ecs/sinatra-hi",
                    "awslogs-region": "ap-southeast-1",
                    "awslogs-stream-prefix": "ecs"
                },
                "SecretOptions": []

            },
            "MemoryReservation": 128,
            "Name": "web",
            "PortMappings": [
                {
                    "ContainerPort": 4567,
                    "HostPort":4567,
                    "Protocol": "tcp"
                }
            ],
            "Privileged": true,
            "StartTimeout": 10,
            "StopTimeout": 100,
        }
    ],
    "Family": "sinatra-hi",
    "NetworkMode": "host",
    "RequiresCompatibilities": ["EC2"],
    "Status": "ACTIVE",
    "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}
```

AwsEfs ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsEfs` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsEfsAccessPoint

L'`AwsEfsAccessPoint`objet fournit des informations sur les fichiers stockés dans Amazon Elastic File System.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEfsAccessPoint`objet. Pour consulter les descriptions des `AwsEfsAccessPoint` attributs, consultez AwsEfsAccessPointDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsEks` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsEksCluster

L'`AwsEksCluster`objet fournit des informations sur un cluster Amazon EKS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEksCluster`objet. Pour consulter les descriptions des `AwsEksCluster` attributs, consultez AwsEksClusterDetails la référence de AWS Security Hub l'API.

Exemple

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsElasticBeanstalk` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsElasticBeanstalkEnvironment

L'`AwsElasticBeanstalkEnvironment`objet contient des informations sur un AWS Elastic Beanstalk environnement.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsElasticBeanstalkEnvironment`objet. Pour consulter les descriptions des `AwsElasticBeanstalkEnvironment` attributs, consultez AwsElasticBeanstalkEnvironmentDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
```

```
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsElasticSearch` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsElasticSearchDomain

L'`AwsElasticSearchDomain`objet fournit des informations sur un domaine Amazon OpenSearch Service.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsElasticSearchDomain`objet. Pour consulter les descriptions des `AwsElasticSearchDomain` attributs, consultez AwsElasticSearchDomainDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
           "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "IndexSlowLogs": {
```

```
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
            },
            "SearchSlowLogs": {
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
            }
    },
    "NodeToNodeEncryptionOptions": {
            "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
            "AutomatedUpdateDate": "string",
            "Cancellable": boolean,
            "CurrentVersion": "string",
            "Description": "string",
            "NewVersion": "string",
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
    },
    "VPCOptions": {
            "AvailabilityZones": [
                "string"
            ],
            "SecurityGroupIds": [
                "string"
            ],
            "SubnetIds": [
                "string"
            ],
           "VPCId": "string"
    }
}
```

AwsElb ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsElb` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsElbLoadBalancer

L'`AwsElbLoadBalancer`objet contient des informations sur un équilibreur de charge classique.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsElbLoadBalancer`objet. Pour consulter les descriptions des `AwsElbLoadBalancer` attributs, consultez AwsElbLoadBalancerDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
```

```
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "amzn-s3-demo-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
```

```
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

L'objet `AwsElbv2LoadBalancer` fournit des informations sur un équilibreur de charge.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsElbv2LoadBalancer`objet. Pour consulter les descriptions des `AwsElbv2LoadBalancer` attributs, consultez AwsElbv2LoadBalancerDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
                            "Code": "string",
                            "Reason": "string"
                        },
```

```
                    "Type": "string",
                    "VpcId": "string"
                }
```

AwsEventBridge ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsEventBridge` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsEventSchemasRegistry

L'`AwsEventSchemasRegistry`objet fournit des informations sur un registre de EventBridge schémas Amazon. Un schéma définit la structure des événements qui sont envoyés à EventBridge. Les registres de schémas sont des conteneurs qui collectent et regroupent logiquement vos schémas.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEventSchemasRegistry`objet. Pour consulter les descriptions des `AwsEventSchemasRegistry` attributs, consultez AwsEventSchemasRegistry la référence de AWS Security Hub l'API.

Exemple

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

L'`AwsEventsEndpoint`objet fournit des informations sur un point de terminaison EventBridge mondial Amazon. Le terminal peut améliorer la disponibilité de votre application en la rendant Regional-fault tolérante.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEventsEndpoint`objet. Pour consulter les descriptions des `AwsEventsEndpoint` attributs, consultez AwsEventsEndpointDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

L'`AwsEventsEventbus`objet fournit des informations sur un point de terminaison EventBridge mondial Amazon. Le terminal peut améliorer la disponibilité de votre application en la rendant Regional-fault tolérante.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsEventsEventbus`objet. Pour consulter les descriptions des `AwsEventsEventbus` attributs, consultez AwsEventsEventbusDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid
\":\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule\",
\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsGuardDuty` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsGuardDutyDetector

L'`AwsGuardDutyDetector`objet fournit des informations sur un GuardDuty détecteur Amazon. Un détecteur est un objet qui représente le GuardDuty service. Un détecteur est nécessaire GuardDuty pour être opérationnel.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsGuardDutyDetector`objet. Pour consulter les descriptions des `AwsGuardDutyDetector` attributs, consultez AwsGuardDutyDetector la référence de AWS Security Hub l'API.

Exemple

```
"AwsGuardDutyDetector": {
```

```
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsIam` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsIamAccessKey

L'`AwsIamAccessKey`objet contient des informations sur une clé d'accès IAM liée à une découverte.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsIamAccessKey`objet. Pour consulter les descriptions des `AwsIamAccessKey` attributs, consultez AwsIamAccessKeyDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

L'`AwsIamGroup`objet contient des informations sur un groupe IAM.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsIamGroup`objet. Pour consulter les descriptions des `AwsIamGroup` attributs, consultez AwsIamGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
```

```
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

L'`AwsIamPolicy`objet représente une politique d'autorisations IAM.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsIamPolicy`objet. Pour consulter les descriptions des `AwsIamPolicy` attributs, consultez AwsIamPolicyDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

L'`AwsIamRole`objet contient des informations sur un rôle IAM, y compris toutes les politiques du rôle.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsIamRole`objet. Pour consulter les descriptions des `AwsIamRole` attributs, consultez AwsIamRoleDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17',       'Statement':
 [{'Effect': 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
```

```
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

L'`AwsIamUser`objet fournit des informations sur un utilisateur.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsIamUser`objet. Pour consulter les descriptions des `AwsIamUser` attributs, consultez AwsIamUserDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
```

```
        }
    ]
}
```

AwsKinesis ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsKinesis` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsKinesisStream

L'`AwsKinesisStream`objet fournit des informations sur Amazon Kinesis Data Streams.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsKinesisStream`objet. Pour consulter les descriptions des `AwsKinesisStream` attributs, consultez AwsKinesisStreamDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsKms` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsKmsKey

L'`AwsKmsKey`objet fournit des informations sur un AWS KMS key.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsKmsKey`objet. Pour consulter les descriptions des `AwsKmsKey` attributs, consultez AwsKmsKeyDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsLambda` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsLambdaFunction

L'`AwsLambdaFunction`objet fournit des détails sur la configuration d'une fonction Lambda.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsLambdaFunction`objet. Pour consulter les descriptions des `AwsLambdaFunction` attributs, consultez AwsLambdaFunctionDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
```

```
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

L'`AwsLambdaLayerVersion`objet fournit des détails sur la version d'une couche Lambda.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsLambdaLayerVersion`objet. Pour consulter les descriptions des `AwsLambdaLayerVersion` attributs, consultez AwsLambdaLayerVersionDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsMsk` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsMskCluster

L'`AwsMskCluster`objet fournit des informations sur un cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK).

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsMskCluster`objet. Pour consulter les descriptions des `AwsMskCluster` attributs, consultez AwsMskClusterDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
```

```
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsNetworkFirewall` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsNetworkFirewallFirewall

L'`AwsNetworkFirewallFirewall`objet contient des informations sur un AWS Network Firewall pare-feu.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsNetworkFirewallFirewall`objet. Pour consulter les descriptions des `AwsNetworkFirewallFirewall` attributs, consultez AwsNetworkFirewallFirewallDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

L'`AwsNetworkFirewallFirewallPolicy`objet fournit des informations sur une politique de pare-feu. Une politique de pare-feu définit le comportement d'un pare-feu réseau.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsNetworkFirewallFirewallPolicy`objet. Pour consulter les descriptions des `AwsNetworkFirewallFirewallPolicy` attributs, consultez AwsNetworkFirewallFirewallPolicyDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
```

```
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

L'`AwsNetworkFirewallRuleGroup`objet fournit des informations sur un groupe de AWS Network Firewall règles. Les groupes de règles sont utilisés pour inspecter et contrôler le trafic réseau. Les groupes de règles sans état s'appliquent à des paquets individuels. Les groupes de règles dynamiques s'appliquent aux paquets dans le contexte de leur flux de trafic.

Les groupes de règles sont référencés dans les politiques de pare-feu.

Les exemples suivants montrent le format ASFF (AWS Security Finding Format) de l'`AwsNetworkFirewallRuleGroup`objet. Pour consulter les descriptions des `AwsNetworkFirewallRuleGroup` attributs, consultez AwsNetworkFirewallRuleGroupDetails la référence de AWS Security Hub l'API.

Exemple : groupe de règles apatrides

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
```

```
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                           6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Exemple : groupe de règles avec état

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
                 {
                     "Action": "PASS",
                     "Header": {
                         "Destination": "Any",
                         "DestinationPort": "443",
                         "Direction": "ANY",
                         "Protocol": "TCP",
                         "Source": "Any",
                         "SourcePort": "Any"
                     },
                     "RuleOptions": [
                         {
                            "Keyword": "sid:1"
                         }
                     ]
                 }
             ]
         }
    }
}
```

Voici une liste d'exemples de valeurs valides pour les `AwsNetworkFirewallRuleGroup` attributs :

- `Action`

  Valeurs valides : `PASS` | `DROP` | `ALERT`

- `Protocol`

Valeurs valides : IP | TCP UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

  Valeurs valides : FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

  Valeurs valides : FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les AwsOpenSearchService ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsOpenSearchServiceDomain

L'AwsOpenSearchServiceDomainobjet contient des informations sur un domaine Amazon OpenSearch Service.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'AwsOpenSearchServiceDomainobjet. Pour consulter les descriptions des AwsOpenSearchServiceDomain attributs, consultez AwsOpenSearchServiceDomainDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
```

```
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
```

```
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsRds` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsRdsDbCluster

L'`AwsRdsDbCluster`objet fournit des informations sur un cluster de bases de données Amazon RDS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRdsDbCluster`objet. Pour consulter les descriptions des `AwsRdsDbCluster` attributs, consultez AwsRdsDbClusterDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
```

```
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

L'`AwsRdsDbClusterSnapshot`objet contient des informations sur un instantané de cluster de bases de données Amazon RDS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRdsDbClusterSnapshot`objet. Pour consulter les descriptions des `AwsRdsDbClusterSnapshot` attributs, consultez AwsRdsDbClusterSnapshotDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRdsDbClusterSnapshot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

L'`AwsRdsDbInstance`objet fournit des informations sur une instance de base de données Amazon RDS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRdsDbInstance`objet. Pour consulter les descriptions des `AwsRdsDbInstance` attributs, consultez AwsRdsDbInstanceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
```

```
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
```

```
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
```

```
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

L'`AwsRdsDbSecurityGroup`objet contient des informations sur un service de base de données relationnelle Amazon.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRdsDbSecurityGroup`objet. Pour consulter les descriptions des `AwsRdsDbSecurityGroup` attributs, consultez AwsRdsDbSecurityGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
```

```
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

L'`AwsRdsDbSnapshot`objet contient des informations sur un instantané de cluster de bases de données Amazon RDS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRdsDbSnapshot`objet. Pour consulter les descriptions des `AwsRdsDbSnapshot` attributs, consultez AwsRdsDbSnapshotDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
```

```
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription`Il contient des informations sur un abonnement aux notifications d'événements RDS. L'abonnement permet à RDS de publier des événements sur une rubrique SNS.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRdsEventSubscription`objet. Pour consulter les descriptions des `AwsRdsEventSubscription` attributs, consultez AwsRdsEventSubscriptionDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
```

```
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsRedshift` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsRedshiftCluster

L'`AwsRedshiftCluster`objet contient des informations sur un cluster Amazon Redshift.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRedshiftCluster`objet. Pour consulter les descriptions des `AwsRedshiftCluster` attributs, consultez AwsRedshiftClusterDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
```

```
            "PrivateIPAddress": "192.0.2.224",
            "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
```

```
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
```

```
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "amzn-s3-demo-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
```

```
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53 ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsRoute53` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsRoute53HostedZone

L'`AwsRoute53HostedZone`objet fournit des informations sur une zone hébergée Amazon Route 53, y compris les quatre serveurs de noms attribués à la zone hébergée. Une zone hébergée représente un ensemble d'enregistrements qui peuvent être gérés ensemble et qui appartiennent à un seul nom de domaine parent.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsRoute53HostedZone`objet. Pour consulter les descriptions des `AwsRoute53HostedZone` attributs, consultez AwsRoute53HostedZoneDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
```

```
        }
    ]
}
```

AWS S3 ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsS3` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsS3AccessPoint

`AwsS3AccessPoint`fournit des informations sur un point d'accès Amazon S3. Les points d'accès S3 sont des points de terminaison réseau nommés attachés à des compartiments S3 que vous pouvez utiliser pour effectuer des opérations sur les objets S3.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsS3AccessPoint`objet. Pour consulter les descriptions des `AwsS3AccessPoint` attributs, consultez AwsS3AccessPointDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "amzn-s3-demo-bucket",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock`fournit des informations sur la configuration du bloc d'accès public Amazon S3 pour les comptes.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsS3AccountPublicAccessBlock`objet. Pour consulter les descriptions des `AwsS3AccountPublicAccessBlock` attributs, consultez AwsS3AccountPublicAccessBlockDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

L'`AwsS3Bucket`objet fournit des informations sur un compartiment Amazon S3.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsS3Bucket`objet. Pour consulter les descriptions des `AwsS3Bucket` attributs, consultez AwsS3BucketDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
```

```
            "Filter": {
                "Predicate": {
                    "Operands": [
                        {
                            "Prefix": "tmp/",
                            "Type": "LifecyclePrefixPredicate"
                        },
                        {
                            "Tag": {
                                "Key": "ArchiveAge",
                                "Value": "9m"
                            },
                            "Type": "LifecycleTagPredicate"
                        }
                    ],
                    "Type": "LifecycleAndOperator"
                }
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-123456789012",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"BucketNotificationConfiguration": {
```

```
      "Configurations": [{
       "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
       "Events": [
        "s3:ObjectCreated:Put"
       ],
       "Filter": {
        "S3KeyFilter": {
         "FilterRules": [
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
          "Value": "pre"
         },
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
          "Value": "suf"
         },
         ]
        }
       },
       "Type": "LambdaConfiguration"
      }]
     },
     "BucketVersioningConfiguration": {
      "IsMfaDeleteEnabled": true,
      "Status": "Off"
     },
     "BucketWebsiteConfiguration": {
      "ErrorDocument": "error.html",
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
```

```
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

Objet AWS S3

L'`AwsS3Object`objet fournit des informations sur un objet Amazon S3.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsS3Object`objet. Pour consulter les descriptions des `AwsS3Object` attributs, consultez AwsS3ObjectDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsSageMaker` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsSageMakerNotebookInstance

L'`AwsSageMakerNotebookInstance`objet fournit des informations sur une instance de bloc-notes Amazon SageMaker AI, qui est une instance de calcul d'apprentissage automatique exécutant l'application Jupyter Notebook.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsSageMakerNotebookInstance`objet. Pour consulter les descriptions des `AwsSageMakerNotebookInstance` attributs, consultez AwsSageMakerNotebookInstanceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
```

```
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsSecretsManager` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsSecretsManagerSecret

L'`AwsSecretsManagerSecret`objet fournit des informations sur un secret du Secrets Manager.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsSecretsManagerSecret`objet. Pour consulter les descriptions des `AwsSecretsManagerSecret` attributs, consultez AwsSecretsManagerSecretDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
```

```
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsSns` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsSnsTopic

L'`AwsSnsTopic`objet contient des informations sur une rubrique d'Amazon Simple Notification Service.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsSnsTopic`objet. Pour consulter les descriptions des `AwsSnsTopic` attributs, consultez AwsSnsTopicDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
```

```
        "Endpoint": "http://sampleendpoint.com",
        "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsSqs` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsSqsQueue

L'`AwsSqsQueue`objet contient des informations concernant une file d'attente Amazon Simple Queue Service.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsSqsQueue`objet. Pour consulter les descriptions des `AwsSqsQueue` attributs, consultez AwsSqsQueueDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsSsm` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsSsmPatchCompliance

L'`AwsSsmPatchCompliance`objet fournit des informations sur l'état d'un correctif sur une instance en fonction de la référence de correctif qui a été utilisée pour appliquer le correctif à l'instance.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsSsmPatchCompliance`objet. Pour consulter les descriptions des `AwsSsmPatchCompliance` attributs, consultez AwsSsmPatchComplianceDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsStepFunctions` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsStepFunctionStateMachine

L'`AwsStepFunctionStateMachine`objet fournit des informations sur une machine à AWS Step Functions états, qui est un flux de travail composé d'une série d'étapes pilotées par des événements.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsStepFunctionStateMachine`objet. Pour consulter les descriptions des `AwsStepFunctionStateMachine` attributs, consultez AwsStepFunctionStateMachine la référence de AWS Security Hub l'API.

Exemple

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsWaf` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsWafRateBasedRule

L'`AwsWafRateBasedRule`objet contient des informations sur une règle AWS WAF basée sur le taux pour les ressources globales. Une règle AWS WAF basée sur le taux fournit des paramètres pour indiquer quand autoriser, bloquer ou comptabiliser une demande. Rate-based les règles incluent le nombre de demandes qui arrivent au cours d'une période spécifiée.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafRateBasedRule`objet. Pour consulter les descriptions des `AwsWafRateBasedRule` attributs, consultez AwsWafRateBasedRuleDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

L'`AwsWafRegionalRateBasedRule`objet contient des informations sur une règle basée sur les taux pour les ressources régionales. Une règle basée sur le taux fournit des paramètres pour indiquer quand autoriser, bloquer ou comptabiliser une demande. Rate-based les règles incluent le nombre de demandes qui arrivent au cours d'une période spécifiée.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafRegionalRateBasedRule`objet. Pour consulter les descriptions des `AwsWafRegionalRateBasedRule` attributs, consultez AwsWafRegionalRateBasedRuleDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

L'`AwsWafRegionalRule`objet fournit des informations sur une règle AWS WAF régionale. Cette règle identifie les requêtes Web que vous souhaitez autoriser, bloquer ou comptabiliser.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafRegionalRule`objet. Pour consulter les descriptions des `AwsWafRegionalRule` attributs, consultez AwsWafRegionalRuleDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

L'`AwsWafRegionalRuleGroup`objet fournit des informations sur un groupe de règles AWS WAF régional. Un groupe de règles est un ensemble de règles prédéfinies que vous ajoutez à une liste de contrôle d'accès Web (ACL Web).

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafRegionalRuleGroup`objet. Pour consulter les descriptions des `AwsWafRegionalRuleGroup` attributs, consultez AwsWafRegionalRuleGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
```

```
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`fournit des détails sur une liste de contrôle d'accès Web AWS WAF régionale (ACL Web). Une ACL Web contient les règles qui identifient les demandes que vous souhaitez autoriser, bloquer ou compter.

Voici un exemple de `AwsWafRegionalWebAcl` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayV2Stage` attributs, consultez AwsWafRegionalWebAclDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
```

```
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`fournit des informations sur une AWS WAF règle. Une AWS WAF règle identifie les requêtes Web que vous souhaitez autoriser, bloquer ou comptabiliser.

Voici un exemple de `AwsWafRule` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayV2Stage` attributs, consultez AwsWafRuleDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`fournit des informations sur un groupe de AWS WAF règles. Un groupe de AWS WAF règles est un ensemble de règles prédéfinies que vous ajoutez à une liste de contrôle d'accès Web (ACL Web).

Voici un exemple de `AwsWafRuleGroup` recherche dans le format ASFF (AWS Security Finding Format). Pour consulter les descriptions des `AwsApiGatewayV2Stage` attributs, consultez AwsWafRuleGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
```

```
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

L'`AwsWafv2RuleGroup`objet fournit des détails sur un groupe de règles AWS WAF V2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafv2RuleGroup`objet. Pour consulter les descriptions des `AwsWafv2RuleGroup` attributs, consultez AwsWafv2RuleGroupDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
```

```
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

L'`AwsWafWebAcl`objet fournit des détails sur une ACL AWS WAF Web.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafWebAcl`objet. Pour consulter les descriptions des `AwsWafWebAcl` attributs, consultez AwsWafWebAclDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
```

```
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

L'`AwsWafv2WebAcl`objet fournit des détails sur une ACL Web AWS WAF V2.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsWafv2WebAcl`objet. Pour consulter les descriptions des `AwsWafv2WebAcl` attributs, consultez AwsWafv2WebAclDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
```

```
      }
     }],
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "TestingJsonBodyMetric"
     }
}
```

AwsXray ressources en ASFF

Voici des exemples de syntaxe ASFF (AWS Security Finding Format) pour les `AwsXray` ressources.

AWS Security Hub CSPM normalise les résultats provenant de diverses sources dans l'ASFF. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

AwsXrayEncryptionConfig

L'`AwsXrayEncryptionConfig`objet contient des informations sur la configuration de chiffrement pour AWS X-Ray.

L'exemple suivant montre le format ASFF (AWS Security Finding Format) pour l'`AwsXrayEncryptionConfig`objet. Pour consulter les descriptions des `AwsXrayEncryptionConfig` attributs, consultez AwsXrayEncryptionConfigDetails la référence de AWS Security Hub l'API.

Exemple

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository objet en ASFF

L'`CodeRepository`objet fournit des informations sur un référentiel de code externe que vous avez connecté à AWS des ressources et que vous avez configuré Amazon Inspector pour détecter les vulnérabilités.

L'exemple suivant montre la syntaxe ASFF (AWS Security Finding Format) de l'`CodeRepository`objet. Pour consulter les descriptions des `CodeRepository` attributs, consultez

CodeRepositoryDetails la référence de AWS Security Hub l'API. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

Exemple

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Conteneur objet en ASFF

L'exemple suivant montre la syntaxe ASFF (AWS Security Finding Format) de l'`Container`objet. Pour consulter les descriptions des `Container` attributs, consultez ContainerDetails la référence de AWS Security Hub l'API. Pour des informations générales sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

Exemple

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Autre objet en ASFF

Dans le format ASFF (AWS Security Finding Format), l'`Other`objet spécifie des champs et des valeurs personnalisés. Pour plus d'informations sur l'ASFF, consultezAWS Format de recherche de sécurité (ASFF).

À l'aide de l'`Other`objet, vous pouvez spécifier des champs et des valeurs personnalisés pour une ressource. Vous pouvez utiliser l'`Other`objet dans les cas suivants :

- Le type de ressource n'a pas d'`Details`objet correspondant. Pour spécifier les détails d'une ressource, utilisez l'`Other`objet.
- L'`Details`objet du type de ressource n'inclut pas tous les attributs que vous souhaitez spécifier. Dans ce cas, utilisez l'`Details`objet correspondant au type de ressource pour spécifier les attributs disponibles. Utilisez l'`Other`objet pour spécifier des attributs qui ne figurent pas dans l'`Details`objet spécifique au type.
- Le type de ressource n'est pas l'un des types fournis. Dans ce cas, définissez `Resource.Type` `Other` et utilisez l'`Other`objet pour spécifier les détails.

Type : carte contenant jusqu'à 50 paires clé-valeur

Chaque paire clé-valeur doit répondre aux exigences suivantes.

- La clé doit contenir moins de 128 caractères.
- La valeur doit contenir moins de 1 024 caractères.

Afficher des informations dans Security Hub CSPM

Dans AWS Security Hub CSPM, un aperçu est un ensemble de résultats connexes. Un aperçu peut identifier une zone de sécurité spécifique qui nécessite une attention et une intervention. Par exemple, un aperçu peut signaler les instances EC2 pour lesquelles des pratiques de sécurité inappropriées ont été détectées. Un aperçu rassemble les résultats de l'ensemble des fournisseurs de résultats.

Chaque aperçu est défini par une instruction Group by (Regrouper par) et par des filtres facultatifs. L'instruction Group by (Regrouper par) indique comment regrouper les résultats qui coïncident et identifie le type d'élément auquel l'aperçu s'applique. Par exemple, si un aperçu est regroupé par identificateur de ressource, l'aperçu génère une liste d'identificateurs de ressource. Les filtres facultatifs identifient les résultats correspondants à l'aperçu. Par exemple, vous souhaiterez peut-être consulter uniquement les résultats provenant de fournisseurs spécifiques ou les résultats associés à des types de ressources spécifiques.

Security Hub CSPM propose plusieurs informations gérées intégrées. Vous ne pouvez pas modifier ou supprimer les informations gérées. Pour suivre les problèmes de sécurité propres à votre AWS environnement et à votre utilisation, vous pouvez créer des informations personnalisées.

La page Insights de la console AWS Security Hub CSPM affiche la liste des informations disponibles.

Par défaut, la liste affiche à la fois des informations gérées et personnalisées. Pour filtrer la liste d'informations en fonction du type d'aperçu, choisissez le type d'aperçu dans le menu déroulant situé à côté du champ de filtre.

- Pour afficher toutes les informations disponibles, sélectionnez Toutes les informations. Il s'agit de l'option par défaut.
- Pour afficher uniquement les informations gérées, choisissez Security Hub CSPM managed insights.
- Pour afficher uniquement les informations personnalisées, sélectionnez Informations personnalisées.

Vous pouvez également filtrer la liste des aperçus en fonction du nom de l'aperçu. Pour ce faire, dans le champ de filtre, saisissez le texte à utiliser pour filtrer la liste. Le filtre ne fait pas la distinction majuscules/minuscules. Le filtre recherche les aperçus dont le texte se trouve n'importe où dans le nom de l'aperçu.

Un aperçu ne renvoie de résultats que si vous avez activé des intégrations ou des normes qui produisent des résultats correspondants. Par exemple, l'information gérée 29. Les meilleures ressources en fonction du nombre d'échecs des contrôles CIS ne donnent de résultats que si vous activez une version de la norme de référence du Center for Internet Security (CIS) AWS Foundations.

Examiner les informations contenues dans Security Hub CSPM et agir en conséquence

Pour chaque information, AWS Security Hub CSPM détermine d'abord les résultats qui correspondent aux critères du filtre, puis utilise l'attribut de regroupement pour regrouper les résultats correspondants.

Sur la page Insights de la console, vous pouvez consulter les résultats et prendre des mesures en conséquence.

Si vous activez l'agrégation interrégionale, les résultats des informations gérées (lorsque vous êtes connecté à la région d'agrégation) incluent les résultats de la région d'agrégation et des régions liées.

Les résultats des informations personnalisées, si les informations ne sont pas filtrées par région, incluent également les résultats de la région d'agrégation et des régions liées (lorsque vous êtes connecté à la région d'agrégation). Dans les autres régions, les résultats d'Insight ne concernent que cette région.

Pour plus d'informations sur la configuration de l'agrégation entre régions, consultezthe section called "Agrégation des données entre les régions".

Afficher les résultats des analyses et prendre des mesures en conséquence

Les résultats de l'aperçu consistent en une liste regroupée des résultats de l'aperçu. Par exemple, si l'aperçu est groupé par identifiant de ressource, les résultats de l'analyse sont la liste des identificateurs de ressources. Chaque élément de la liste des résultats indique le nombre de résultats correspondants pour cet élément.

Si les résultats sont regroupés par identifiant de ressource ou type de ressource, les résultats incluent toutes les ressources dans les résultats correspondants. Cela inclut les ressources dont le type est différent de celui spécifié dans les critères de filtre. Par exemple, un aperçu identifie les résultats associés aux compartiments S3. Si un résultat correspondant contient à la fois une ressource de compartiment S3 et une ressource clé d'accès IAM, les résultats d'analyse incluent les deux ressources.

Sur la console Security Hub CSPM, la liste des résultats est triée du plus grand au moins élevé. Security Hub CSPM ne peut afficher que 100 résultats. S'il existe plus de 100 valeurs de regroupement, seules les 100 premières s'affichent.

En plus de la liste des résultats, les résultats d'analyse affichent un ensemble de graphiques résumant le nombre de résultats correspondants pour les attributs suivants.

- Étiquette de gravité — Nombre de résultats pour chaque étiquette de gravité
- Compte AWS ID — Les cinq principaux identifiants de compte pour les résultats correspondants
- Type de ressource — Les cinq principaux types de ressources pour les résultats correspondants
- ID de ressource — Les cinq principaux identifiants de ressources pour les résultats correspondants
- Nom du produit - Les cinq principaux fournisseurs de résultats correspondants

Si vous avez configuré des actions personnalisées, vous pouvez envoyer les résultats sélectionnés à une action personnalisée. L'action doit être associée à une CloudWatch règle Amazon pour le

type `Security Hub Insight Results` d'événement. Pour de plus amples informations, veuillez consulter the section called "Réponse et remédiation automatisées". Si vous n'avez pas configuré d'actions personnalisées, le menu Actions est désactivé.

Security Hub CSPM console

Pour consulter les résultats d'Insight et prendre des mesures en conséquence (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le panneau de navigation, choisissez Insights.
3. Pour afficher la liste des résultats de l'aperçu, choisissez le nom de l'aperçu.
4. Activez la case à cocher pour chaque résultat à envoyer à l'action personnalisée.
5. Dans le menu Actions choisissez l'action personnalisée.

Security Hub CSPM API, AWS CLI

Pour consulter les résultats des analyses et prendre des mesures en conséquence (API, AWS CLI)

Pour afficher les résultats d'analyse, utilisez le >GetInsightResults fonctionnement de l'API CSPM Security Hub. Si vous utilisez le AWS CLI, exécutez la get-insight-results commande.

Pour identifier l'information pour laquelle les résultats doivent être renvoyés, vous avez besoin de l'ARN insight. Pour obtenir les ARN d'aperçu pour des informations personnalisées, utilisez l'opération `GetInsights` d'API ou la get-insight-results commande.

L'exemple suivant extrait les résultats pour l'aperçu spécifié. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Pour plus d'informations sur la création d'actions personnalisées par programmation, consultez. Utiliser des actions personnalisées pour envoyer des résultats et des informations à EventBridge

Afficher les résultats d'Insight et prendre des mesures en conséquence (console)

À partir d'une liste de résultats d'analyse sur la console Security Hub CSPM, vous pouvez afficher la liste des résultats pour chaque résultat.

Pour afficher les résultats des analyses et prendre des mesures en conséquence (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le panneau de navigation, choisissez Insights.
3. Pour afficher la liste des résultats de l'aperçu, choisissez le nom de l'aperçu.
4. Pour afficher la liste des résultats d'une analyse, choisissez l'élément dans la liste des résultats. La liste des conclusions montre les conclusions actives du résultat d'analyse sélectionné dont l'état de flux de travail est `NEW` ou `NOTIFIED`.

À partir de la liste des résultats, vous pouvez effectuer les actions suivantes :

- Filtrage des résultats dans Security Hub CSPM
- Révision des détails et de l'historique des découvertes
- Configuration de l'état du flux de travail des résultats dans Security Hub CSPM
- Envoi des résultats à une action CSPM personnalisée de Security Hub

Informations gérées dans Security Hub CSPM

AWSSecurity Hub CSPM fournit plusieurs informations gérées.

Vous ne pouvez pas modifier ou supprimer les informations gérées par Security Hub CSPM. Vous pouvez consulter les résultats de l'aperçu. Vous pouvez également utiliser un aperçu géré comme base pour un nouvel aperçu personnalisé.

Comme pour tous les résultats, un aperçu ne renvoie des résultats que si vous avez activé les intégrations de produits ou les normes de sécurité qui génèrent des résultats correspondants.

Pour les informations regroupées par identifiant de ressource, les résultats incluent les identifiants de toutes les ressources dans les résultats correspondants. Cela inclut les ressources dont le type est différent de celui indiqué dans les critères de filtre. Par exemple, l'aperçu 2 de la liste suivante identifie les résultats associés aux compartiments Amazon S3. Si un résultat correspondant contient

à la fois une ressource de compartiment S3 et une ressource de clé d'accès IAM, les résultats d'analyse incluent les deux ressources.

Security Hub CSPM propose actuellement les informations gérées suivantes :

1. AWSressources contenant le plus de résultats

   ARN : `arn:aws:securityhub:::insight/securityhub/default/1`

   Regroupés par : identifiant de ressource

   Recherche de filtres :

   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`
2. Compartiments S3 avec des autorisations de lecture et d'écriture publique

   ARN : `arn:aws:securityhub:::insight/securityhub/default/10`

   Regroupés par : identifiant de ressource

   Recherche de filtres :

   - Le type commence par `Effects/Data Exposure`
   - Le type de ressource est `AwsS3Bucket`
   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`
3. AMI qui génèrent le plus de conclusions

   ARN : `arn:aws:securityhub:::insight/securityhub/default/3`

   Regroupé par : ID de l'image de l'instance EC2

   Recherche de filtres :

   - Le type de ressource est `AwsEc2Instance`
   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`
4. Instances EC2 impliquées dans Tactiques, Techniques et Procédures (TTP) connues

   ARN : `arn:aws:securityhub:::insight/securityhub/default/14`

Regroupés par : ID de ressource

Recherche de filtres :

- Le type commence par `TTPs`
- Le type de ressource est `AwsEc2Instance`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

5. AWSdirecteurs dont l'activité liée aux clés d'accès est suspecte

   ARN : `arn:aws:securityhub:::insight/securityhub/default/9`

   Regroupés par : nom principal de la clé d'accès IAM

   Recherche de filtres :

   - Le type de ressource est `AwsIamAccessKey`
   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`

6. AWSinstances de ressources qui ne répondent pas aux normes de sécurité/meilleures pratiques

   ARN : `arn:aws:securityhub:::insight/securityhub/default/6`

   Regroupés par : ID de ressource

   Recherche de filtres :

   - Le type est `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`

7. AWSressources associées à une éventuelle exfiltration de données

   ARN : `arn:aws:securityhub:::insight/securityhub/default/7`

   Regroupés par : ID de ressource

   Recherche de filtres :

   - Le type commence par Effects/Data Exfiltration/

- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

8. AWSressources associées à une consommation non autorisée de ressources

   ARN : `arn:aws:securityhub:::insight/securityhub/default/8`

   Regroupés par : ID de ressource

   Recherche de filtres :

   - Le type commence par `Effects/Resource Consumption`
   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`

9. Compartiments S3 qui ne respectent pas les normes de sécurité ou les bonnes pratiques

   ARN : `arn:aws:securityhub:::insight/securityhub/default/11`

   Regroupés par : ID de ressource

   Recherche de filtres :

   - Le type de ressource est `AwsS3Bucket`
   - Le type est `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - L'état de l'enregistrement est `ACTIVE`
   - L'état du flux de travail est `NEW` ou `NOTIFIED`

10. Compartiments S3 avec des données sensibles

    ARN : `arn:aws:securityhub:::insight/securityhub/default/12`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type de ressource est `AwsS3Bucket`
    - Le type commence par `Sensitive Data Identifications/`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

11. Informations d'identification susceptibles d'avoir fui

    ARN : `arn:aws:securityhub:::insight/securityhub/default/13`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type commence par `Sensitive Data Identifications/Passwords/`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`
12. Instances EC2 avec des correctifs de sécurité manquants pour des vulnérabilités importantes

    ARN : `arn:aws:securityhub:::insight/securityhub/default/16`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type commence par `Software and Configuration Checks/Vulnerabilities/CVE`
    - Le type de ressource est `AwsEc2Instance`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`
13. Instances EC2 avec un comportement inhabituel général

    ARN : `arn:aws:securityhub:::insight/securityhub/default/17`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type commence par `Unusual Behaviors`
    - Le type de ressource est `AwsEc2Instance`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`
14. Instances EC2 avec des ports accessibles à partir d'Internet

    ARN : `arn:aws:securityhub:::insight/securityhub/default/18`

    Regroupés par : ID de ressource

Recherche de filtres :

- Le type commence par `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- Le type de ressource est `AwsEc2Instance`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

15. Instances EC2 qui ne respectent pas les normes de sécurité ou les bonnes pratiques

    ARN : `arn:aws:securityhub:::insight/securityhub/default/19`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type commence par l'un des éléments suivants :
      - `Software and Configuration Checks/Industry and Regulatory Standards/`
      - `Software and Configuration Checks/AWSSecurity Best Practices`
    - Le type de ressource est `AwsEc2Instance`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

16. Instances EC2 ouvertes à Internet

    ARN : `arn:aws:securityhub:::insight/securityhub/default/21`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type commence par `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Le type de ressource est `AwsEc2Instance`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

17. Instances EC2 associées à la reconnaissance d'adversaire

    ARN : `arn:aws:securityhub:::insight/securityhub/default/22`

Regroupés par : ID de ressource

Recherche de filtres :

- Le type commence par TTPs/Discovery/Recon
- Le type de ressource est `AwsEc2Instance`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

18. AWSressources associées à des logiciels malveillants

ARN : `arn:aws:securityhub:::insight/securityhub/default/23`

Regroupés par : ID de ressource

Recherche de filtres :

- Le type commence par l'un des éléments suivants :
  - `Effects/Data Exfiltration/Trojan`
  - `TTPs/Initial Access/Trojan`
  - `TTPs/Command and Control/Backdoor`
  - `TTPs/Command and Control/Trojan`
  - `Software and Configuration Checks/Backdoor`
  - `Unusual Behaviors/VM/Backdoor`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

19. AWSressources associées aux problèmes de cryptomonnaie

ARN : `arn:aws:securityhub:::insight/securityhub/default/24`

Regroupés par : ID de ressource

Recherche de filtres :

- Le type commence par l'un des éléments suivants :
  - `Effects/Resource Consumption/Cryptocurrency`
  - `TTPs/Command and Control/CryptoCurrency`
- L'état de l'enregistrement est `ACTIVE`

- L'état du flux de travail est `NEW` ou `NOTIFIED`

20. AWSressources ayant fait l'objet de tentatives d'accès non autorisées

    ARN : `arn:aws:securityhub:::insight/securityhub/default/25`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type commence par l'un des éléments suivants :
      - `TTPs/Command and Control/UnauthorizedAccess`
      - `TTPs/Initial Access/UnauthorizedAccess`
      - `Effects/Data Exfiltration/UnauthorizedAccess`
      - `Unusual Behaviors/User/UnauthorizedAccess`
      - `Effects/Resource Consumption/UnauthorizedAccess`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

21. Indicateurs intel de menace avec le plus d'occurrences au cours de la dernière semaine

    ARN : `arn:aws:securityhub:::insight/securityhub/default/26`

    Recherche de filtres :

    - Créé au cours des 7 derniers jours

22. Principaux comptes par nombre de conclusions

    ARN : `arn:aws:securityhub:::insight/securityhub/default/27`

    Regroupés par : Compte AWS ID

    Recherche de filtres :

    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

23. Principaux produits par nombre de conclusions

    ARN : `arn:aws:securityhub:::insight/securityhub/default/28`

    Regroupés par : Nom du produit

Recherche de filtres :

- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

24. Gravité par nombre de conclusions

    ARN : `arn:aws:securityhub:::insight/securityhub/default/29`

    Regroupés par : étiquette de gravité

    Recherche de filtres :

    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

25. Principaux compartiments S3 par nombre de conclusions

    ARN : `arn:aws:securityhub:::insight/securityhub/default/30`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type de ressource est `AwsS3Bucket`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

26. Principales instances EC2 par nombre de conclusions

    ARN : `arn:aws:securityhub:::insight/securityhub/default/31`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Le type de ressource est `AwsEc2Instance`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

27. Principales AMI par nombre de conclusions

    ARN : `arn:aws:securityhub:::insight/securityhub/default/32`

Regroupé par : ID de l'image de l'instance EC2

Recherche de filtres :

- Le type de ressource est `AwsEc2Instance`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

28. Principaux utilisateurs IAM par nombre de conclusions

ARN : `arn:aws:securityhub:::insight/securityhub/default/33`

Regroupés par : ID de clé d'accès IAM

Recherche de filtres :

- Le type de ressource est `AwsIamAccessKey`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

29. Principales ressources par nombre de vérifications CIS ayant échoué

ARN : `arn:aws:securityhub:::insight/securityhub/default/34`

Regroupés par : ID de ressource

Recherche de filtres :

- L'ID du générateur commence par `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- Mise à jour le dernier jour
- Le statut de conformité est `FAILED`
- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

30. Principales intégrations par nombre de conclusions

ARN : `arn:aws:securityhub:::insight/securityhub/default/35`

Regroupés par : ARN du produit

Recherche de filtres :

- L'état de l'enregistrement est `ACTIVE`
- L'état du flux de travail est `NEW` ou `NOTIFIED`

31. Ressources avec les contrôles de sécurité ayant le plus échoué

    ARN : `arn:aws:securityhub:::insight/securityhub/default/36`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - Mise à jour le dernier jour
    - Le statut de conformité est `FAILED`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

32. Utilisateurs IAM présentant une activité suspecte

    ARN : `arn:aws:securityhub:::insight/securityhub/default/37`

    Regroupés par : utilisateur IAM

    Recherche de filtres :

    - Le type de ressource est `AwsIamUser`
    - L'état de l'enregistrement est `ACTIVE`
    - L'état du flux de travail est `NEW` ou `NOTIFIED`

33. Ressources contenant le plus de AWS Health résultats

    ARN : `arn:aws:securityhub:::insight/securityhub/default/38`

    Regroupés par : ID de ressource

    Recherche de filtres :

    - `ProductName`est égal `Health`

34. Ressources contenant le plus de AWS Config résultats

    ARN : `arn:aws:securityhub:::insight/securityhub/default/39`

    Regroupés par : ID de ressource

Recherche de filtres :

- `ProductName`est égal `Config`

35. Applications ayant obtenu le plus de résultats

ARN : `arn:aws:securityhub:::insight/securityhub/default/40`

Regroupés par : ResourceApplicationArn

Recherche de filtres :

- `RecordState`est égal `ACTIVE`
- `Workflow.Status`est égal à `NEW` ou `NOTIFIED`

Comprendre les informations personnalisées dans Security Hub CSPM

Outre les informations gérées par AWS Security Hub CSPM, vous pouvez créer des informations personnalisées dans Security Hub CSPM pour suivre les problèmes spécifiques à votre environnement. Les informations personnalisées vous aident à suivre un sous-ensemble de problèmes sélectionnés.

Voici quelques exemples d'informations personnalisées qu'il peut être utile de configurer :

- Si vous possédez un compte administrateur, vous pouvez configurer un aperçu personnalisé pour suivre les résultats critiques et de gravité élevée qui affectent les comptes des membres.
- Si vous comptez sur un AWS service intégré spécifique, vous pouvez configurer un aperçu personnalisé pour suivre les résultats critiques et de gravité élevés de ce service.
- Si vous comptez sur une intégration tierce, vous pouvez configurer un aperçu personnalisé pour suivre les résultats critiques et de gravité élevés de ce produit intégré.

Vous pouvez créer des aperçus personnalisés à partir de zéro ou modifier des aperçus personnalisés ou gérés existants.

Chaque aperçu peut être configuré avec les options suivantes :

- Attribut de regroupement : l'attribut de regroupement détermine quels éléments sont affichés dans la liste des résultats d'analyse. Par exemple, si l'attribut de regroupement est Nom du produit, les résultats d'analyse affichent le nombre de résultats associés à chaque fournisseur de résultats.

- Filtres facultatifs : les filtres permettent d'affiner les résultats correspondants pour obtenir un aperçu.

  Un résultat n'est inclus dans les résultats d'analyse que s'il correspond à tous les filtres fournis. Par exemple, si les filtres sont « Le nom du produit est GuardDuty » et `AwsS3Bucket` « Le type de ressource est », les résultats correspondants doivent correspondre à ces deux critères.

  Cependant, Security Hub CSPM applique une logique BOOLÉENNE OU aux filtres qui utilisent le même attribut mais des valeurs différentes. Par exemple, si les filtres sont « Le nom du produit est GuardDuty » et « Le nom du produit est Amazon Inspector », un résultat correspond s'il a été généré par Amazon GuardDuty ou Amazon Inspector.

Si vous utilisez l'identifiant de ressource ou le type de ressource comme attribut de regroupement, les résultats d'analyse incluent toutes les ressources figurant dans les résultats correspondants. La liste n'est pas limitée aux ressources qui correspondent à un filtre de type de ressource. Par exemple, un aperçu identifie les résultats associés aux compartiments S3 et regroupe ces résultats par identifiant de ressource. Un résultat correspondant contient à la fois une ressource de compartiment S3 et une ressource de clé d'accès IAM. Les résultats d'analyse incluent les deux ressources.

Si vous activez l'agrégation entre régions, puis créez un aperçu personnalisé, celui-ci s'applique aux résultats correspondants dans la région d'agrégation et les régions liées. L'exception est si votre aperçu inclut un filtre par région.

Création d'un aperçu personnalisé

Dans AWS Security Hub CSPM, des informations personnalisées peuvent être utilisées pour collecter un ensemble spécifique de résultats et suivre les problèmes propres à votre environnement. Pour obtenir des informations générales sur les informations personnalisées, consultezComprendre les informations personnalisées dans Security Hub CSPM.

Choisissez votre méthode préférée et suivez les étapes pour créer un aperçu personnalisé dans Security Hub CSPM

Security Hub CSPM console

Pour créer un aperçu personnalisé (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

2. Dans le panneau de navigation, choisissez Insights.
3. Choisissez Create insight (Créer une information).
4. Pour sélectionner l'attribut de regroupement pour l'aperçu :
    a. Choisissez le champ de recherche pour afficher les options de filtre.
    b. Choisissez Group by (Regrouper par).
    c. Sélectionnez l'attribut à utiliser pour regrouper les résultats associés à cette analyse.
    d. Cliquez sur Appliquer.
5. Vous pouvez éventuellement sélectionner les filtres supplémentaires à utiliser pour obtenir ces informations. Pour chaque filtre, définissez les critères de filtre, puis choisissez Appliquer.
6. Choisissez Create insight (Créer une information).
7. Entrez un nom Insight, puis choisissez Create Insight.

Security Hub CSPM API

Pour créer un aperçu personnalisé (API)

1. Pour créer un aperçu personnalisé, utilisez le CreateInsight fonctionnement de l'API CSPM Security Hub. Si vous utilisez le AWS CLI, exécutez la create-insight commande.
2. Renseignez le `Name` paramètre avec un nom pour votre aperçu personnalisé.
3. Renseignez le `Filters` paramètre pour spécifier les résultats à inclure dans l'aperçu.
4. Renseignez le `GroupByAttribute` paramètre pour spécifier quel attribut est utilisé pour regrouper les résultats inclus dans l'aperçu.
5. Vous pouvez éventuellement renseigner le `SortCriteria` paramètre pour trier les résultats selon un champ spécifique.

L'exemple suivant crée un aperçu personnalisé qui inclut des résultats critiques avec le type de `AwsIamRole` ressource. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Pour créer un aperçu personnalisé (PowerShell)

1. Utilisez l'applet de commande `New-SHUBInsight`.
2. Renseignez le `Name` paramètre avec un nom pour votre aperçu personnalisé.
3. Renseignez le `Filter` paramètre pour spécifier les résultats à inclure dans l'aperçu.
4. Renseignez le `GroupByAttribute` paramètre pour spécifier quel attribut est utilisé pour regrouper les résultats inclus dans l'aperçu.

Si vous avez activé l'agrégation entre régions et que vous utilisez cette applet de commande depuis la région d'agrégation, les informations s'appliquent à la mise en correspondance des résultats issus de l'agrégation et des régions liées.

Exemple

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Création d'un aperçu personnalisé à partir d'un aperçu géré (console uniquement)

Vous ne pouvez pas enregistrer les modifications apportées à un aperçu géré ni le supprimer. Vous pouvez toutefois utiliser un aperçu géré comme base pour un aperçu personnalisé. Il s'agit d'une option disponible uniquement sur la console Security Hub CSPM.

Pour créer un aperçu personnalisé à partir d'un aperçu géré (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le panneau de navigation, choisissez Insights.

3. Choisissez l'aperçu géré à partir duquel vous souhaitez travailler.
4. Modifiez la configuration d'Insight selon vos besoins.
   - Pour modifier l'attribut utilisé pour regrouper les résultats dans l'aperçu :
     a. Pour supprimer le regroupement existant, choisissez le X à côté du paramètre Grouper par.
     b. Cliquez sur la barre de recherche.
     c. Sélectionnez l'attribut à utiliser pour le regroupement.
     d. Cliquez sur Appliquer.
   - Pour supprimer un filtre de l'aperçu, choisissez le X encerclé à côté du filtre.
   - Pour ajouter un filtre à l'aperçu :
     a. Cliquez sur la barre de recherche.
     b. Sélectionnez l'attribut et la valeur à utiliser comme filtre.
     c. Cliquez sur Appliquer.
5. Lorsque vos mises à jour sont terminées, choisissez Create insight (Créer un aperçu).
6. Lorsque vous y êtes invité, entrez un nom Insight, puis choisissez Create Insight.

Modifier un aperçu personnalisé

Vous pouvez modifier un aperçu personnalisé existant pour modifier la valeur de regroupement et les filtres. Après avoir apporté les modifications, vous pouvez enregistrer les mises à jour de l'aperçu d'origine ou enregistrer la version mise à jour en tant que nouvel aperçu.

Dans AWS Security Hub CSPM, des informations personnalisées peuvent être utilisées pour collecter un ensemble spécifique de résultats et suivre les problèmes propres à votre environnement. Pour obtenir des informations générales sur les informations personnalisées, consultezComprendre les informations personnalisées dans Security Hub CSPM.

Pour modifier un aperçu personnalisé, choisissez votre méthode préférée et suivez les instructions.

Security Hub CSPM console

Pour modifier un aperçu personnalisé (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/

2. Dans le panneau de navigation, choisissez Insights.
3. Choisissez l'aperçu personnalisé à modifier.
4. Modifiez la configuration d'Insight selon vos besoins.
   - Pour modifier l'attribut utilisé pour regrouper les résultats dans l'aperçu :
     a. Pour supprimer le regroupement existant, choisissez le X à côté du paramètre Grouper par.
     b. Cliquez sur la barre de recherche.
     c. Sélectionnez l'attribut à utiliser pour le regroupement.
     d. Cliquez sur Appliquer.
   - Pour supprimer un filtre de l'aperçu, choisissez le X encerclé à côté du filtre.
   - Pour ajouter un filtre à l'aperçu :
     a. Cliquez sur la barre de recherche.
     b. Sélectionnez l'attribut et la valeur à utiliser comme filtre.
     c. Cliquez sur Appliquer.
5. Lorsque vous avez terminé les mises à jour, choisissez Save insight (Enregistrer l'aperçu).
6. Lorsque vous y êtes invité, effectuez l'une des opérations suivantes :
   - Pour mettre à jour les informations existantes afin de refléter vos modifications, choisissez Mettre à jour, ***<Insight_Name>*** puis cliquez sur Enregistrer les informations.
   - Pour créer un aperçu avec les mises à jour, choisissez Save new insight (Enregistrer un nouvel aperçu). Renseignez le champ Insight name (Nom de l'aperçu), puis choisissez Save insight (Enregistrer l'aperçu).

Security Hub CSPM API

Pour modifier un aperçu personnalisé (API)

1. Utilisez le `UpdateInsight` fonctionnement de l'API Security Hub CSPM. Si vous utilisez la update-insight commande AWS CLI run the.
2. Pour identifier l'aperçu personnalisé que vous souhaitez mettre à jour, indiquez le nom de ressource Amazon (ARN) de l'aperçu. Pour obtenir l'ARN d'un aperçu personnalisé, utilisez l'`GetInsights`opération ou la get-insights commande.
3. Mettez à jour les `GroupByAttribute` paramètres `NameFilters`, et si nécessaire.

L'exemple suivant met à jour l'aperçu spécifié. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

Pour modifier un aperçu personnalisé (PowerShell)

1. Utilisez l'applet de commande `Update-SHUBInsight`.
2. Pour identifier l'aperçu personnalisé, indiquez le nom de ressource Amazon (ARN) de l'aperçu. Pour obtenir l'ARN d'un aperçu personnalisé, utilisez l'`Get-SHUBInsight`applet de commande.
3. Mettez à jour les `GroupByAttribute` paramètres `NameFilter`, et si nécessaire.

Exemple

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Supprimer un aperçu personnalisé

Dans AWS Security Hub CSPM, des informations personnalisées peuvent être utilisées pour collecter un ensemble spécifique de résultats et suivre les problèmes propres à votre environnement. Pour obtenir des informations générales sur les informations personnalisées, consultezComprendre les informations personnalisées dans Security Hub CSPM.

Pour supprimer un aperçu personnalisé, choisissez votre méthode préférée et suivez les instructions. Vous ne pouvez pas supprimer un aperçu géré.

Security Hub CSPM console

Pour supprimer un aperçu personnalisé (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le panneau de navigation, choisissez Insights.
3. Recherchez l'aperçu personnalisé à supprimer.
4. Pour en savoir plus, choisissez l'icône Plus d'options (les trois points situés dans le coin supérieur droit de la carte).
5. Sélectionnez Delete (Supprimer).

Security Hub CSPM API

Pour supprimer un aperçu personnalisé (API)

1. Utilisez le `DeleteInsight` fonctionnement de l'API Security Hub CSPM. Si vous utilisez la delete-insight commande AWS CLI run the.
2. Pour identifier l'aperçu personnalisé à supprimer, indiquez l'ARN de l'aperçu. Pour obtenir l'ARN d'un aperçu personnalisé, utilisez l'`GetInsights`opération ou la get-insights commande.

L'exemple suivant supprime l'aperçu spécifié. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

Pour supprimer un aperçu personnalisé (PowerShell)

1. Utilisez l'applet de commande `Remove-SHUBInsight`.
2. Pour identifier l'aperçu personnalisé, indiquez l'ARN de l'aperçu. Pour obtenir l'ARN d'un aperçu personnalisé, utilisez l'`Get-SHUBInsight`applet de commande.

Exemple

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Modification automatique des résultats et prise en compte des résultats dans Security Hub CSPM

AWSSecurity Hub CSPM possède des fonctionnalités qui modifient automatiquement les résultats et prennent des mesures en fonction de vos spécifications.

Security Hub CSPM prend actuellement en charge deux types d'automatisations :

- Règles d'automatisation : mettez à jour et supprimez automatiquement les résultats en temps quasi réel en fonction de critères que vous définissez.
- Réponse et correction automatisées : créez des EventBridge règles Amazon personnalisées qui définissent les actions automatiques à entreprendre en fonction de résultats et d'informations spécifiques.

Les règles d'automatisation sont utiles lorsque vous souhaitez mettre à jour automatiquement les champs de recherche au format ASFF (AWSSecurity Finding Format). Par exemple, vous pouvez utiliser une règle d'automatisation pour mettre à jour le niveau de gravité ou l'état du flux de travail des résultats issus d'intégrations tierces spécifiques. L'utilisation de la règle d'automatisation élimine

le besoin de mettre à jour manuellement le niveau de gravité ou l'état du flux de travail de chaque découverte provenant de ce produit tiers.

EventBridge les règles sont utiles lorsque vous souhaitez prendre des mesures en dehors de Security Hub CSPM en ce qui concerne des résultats spécifiques ou envoyer des résultats spécifiques à des outils tiers à des fins de correction ou d'investigation supplémentaire. Les règles peuvent être utilisées pour déclencher des actions prises en charge, telles que l'appel d'une AWS Lambda fonction ou la notification d'un résultat spécifique à une rubrique Amazon Simple Notification Service (Amazon SNS).

Les règles d'automatisation entrent en vigueur avant EventBridge leur application. C'est-à-dire que les règles d'automatisation sont déclenchées et mettent à jour un résultat avant de le EventBridge recevoir. EventBridge les règles s'appliquent ensuite au résultat mis à jour.

Lorsque vous configurez des automatisations pour les contrôles de sécurité, nous vous recommandons de filtrer en fonction de l'ID du contrôle plutôt que du titre ou de la description. Alors que Security Hub CSPM met occasionnellement à jour les titres et les descriptions des contrôles, les identifiants de contrôle restent les mêmes.

Rubriques

- Comprendre les règles d'automatisation dans Security Hub CSPM
- Utilisation à EventBridge des fins de réponse et de correction automatisées

Comprendre les règles d'automatisation dans Security Hub CSPM

Vous pouvez utiliser des règles d'automatisation pour mettre à jour automatiquement les résultats dans AWS Security Hub CSPM. Au fur et à mesure qu'il ingère les résultats, le Security Hub CSPM peut appliquer diverses règles, telles que la suppression des résultats, la modification de leur gravité et l'ajout de notes. Ces actions de règle modifient les résultats qui correspondent aux critères que vous avez spécifiés.

Voici des exemples de cas d'utilisation des règles d'automatisation :

- Augmenter la gravité d'une constatation jusqu'à ce `CRITICAL` que son identifiant de ressource fasse référence à une ressource critique pour l'entreprise.
- Augmenter la gravité d'une constatation de `HIGH` à `CRITICAL` si la constatation affecte les ressources dans des comptes de production spécifiques.

- Attribuer des résultats spécifiques présentant un statut de `SUPPRESSED` flux de `INFORMATIONAL` travail grave.

Vous pouvez créer et gérer des règles d'automatisation à partir d'un compte administrateur Security Hub CSPM uniquement.

Les règles s'appliquent à la fois aux nouvelles découvertes et aux découvertes mises à jour. Vous pouvez créer une règle personnalisée à partir de zéro ou utiliser un modèle de règle fourni par Security Hub CSPM. Vous pouvez également commencer par un modèle et le modifier selon vos besoins.

Définition des critères et des actions des règles

À partir d'un compte administrateur Security Hub CSPM, vous pouvez créer une règle d'automatisation en définissant un ou plusieurs critères de règle et une ou plusieurs actions de règle. Lorsqu'un résultat correspond aux critères définis, Security Hub CSPM lui applique les actions de règle. Pour plus d'informations sur les critères et actions disponibles, consultezCritères de règle et actions de règle disponibles.

Security Hub CSPM prend actuellement en charge un maximum de 100 règles d'automatisation pour chaque compte administrateur.

Le compte administrateur Security Hub CSPM peut également modifier, afficher et supprimer les règles d'automatisation. Une règle s'applique à la correspondance des résultats dans le compte administrateur et dans tous ses comptes membres. En fournissant des identifiants de compte de membre comme critère de règle, les administrateurs de Security Hub CSPM peuvent également utiliser des règles d'automatisation pour mettre à jour ou supprimer les résultats de comptes de membres spécifiques.

Une règle d'automatisation s'applique uniquement dans le Région AWS pays dans lequel elle a été créée. Pour appliquer une règle dans plusieurs régions, l'administrateur doit créer la règle dans chaque région. Cela peut être effectué via la console Security Hub CSPM, l'API Security Hub CSPM ou. AWS CloudFormation Vous pouvez également utiliser un script de déploiement multirégional.

Critères de règle et actions de règle disponibles

Les champs ASFF (AWSSecurity Finding Format) suivants sont actuellement pris en charge en tant que critères pour les règles d'automatisation :

Critère de règle	Opérateurs de filtre	Type de champ
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	Sélectionnez : [FAILED,NOT_AVAILABLE ,PASSED,WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
CreatedAt	Start, End, DateRange	Date (formatée au format : T21:47:39.269Z 01/12/02)

Critère de règle	Opérateurs de filtre	Type de champ
`Criticality`	`Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)`	Number
`Description`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`FirstObservedAt`	`Start, End, DateRange`	Date (formatée au format : T21:47:39.269Z 01/12/02)
`GeneratorId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`Id`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`LastObservedAt`	`Start, End, DateRange`	Date (formatée au format : T21:47:39.269Z 01/12/02)
`NoteText`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`NoteUpdatedAt`	`Start, End, DateRange`	Date (formatée au format : T21:47:39.269Z 01/12/02)

Critère de règle	Opérateurs de filtre	Type de champ
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne

Critère de règle	Opérateurs de filtre	Type de champ
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceType	Is, Is Not	Sélectionnez (voir Ressources prises en charge par ASFF)
SeverityLabel	Is, Is Not	Sélectionnez : [CRITICAL,HIGH,MEDIUM,LOW,INFORMATIONAL]

Critère de règle	Opérateurs de filtre	Type de champ
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Chaîne
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	Date (formatée au format : T21:47:39.269Z 01/12/02)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	Sélectionnez : [NEW,NOTIFIED,RESOLVED,SUPPRESSED]

Pour les critères étiquetés sous forme de champs de chaîne, l'utilisation de différents opérateurs de filtre sur le même champ affecte la logique d'évaluation. Pour plus d'informations, consultez le document StringFilterde référence AWSde l'API Security Hub CSPM.

Chaque critère prend en charge un nombre maximum de valeurs pouvant être utilisées pour filtrer les résultats correspondants. Pour connaître les limites de chaque critère, consultez le document de AutomationRulesFindingFiltersréférence AWSde l'API Security Hub CSPM.

Les champs ASFF suivants sont actuellement pris en charge en tant qu'actions pour les règles d'automatisation :

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Pour plus d'informations sur des champs ASFF spécifiques, consultez AWSla section Syntaxe ASFF (Security Finding Format).

> **Tip**
>
> Si vous souhaitez que Security Hub CSPM cesse de générer des résultats pour un contrôle spécifique, nous vous recommandons de désactiver le contrôle plutôt que d'utiliser une règle d'automatisation. Lorsque vous désactivez un contrôle, Security Hub CSPM arrête d'effectuer des contrôles de sécurité sur celui-ci et de générer des résultats pour celui-ci. Vous n'avez donc pas à payer de frais pour ce contrôle. Nous recommandons d'utiliser des règles d'automatisation pour modifier les valeurs de champs ASFF spécifiques pour les résultats correspondant à des critères définis. Pour plus d'informations sur la désactivation des contrôles, consultezDésactivation des contrôles dans Security Hub CSPM.

Résultats évalués par les règles d'automatisation

Une règle d'automatisation évalue les résultats nouveaux et mis à jour que Security Hub CSPM génère ou ingère dans le cadre de l'BatchImportFindingsopération une fois que vous avez créé

la règle. Security Hub CSPM met à jour les résultats des contrôles toutes les 12 à 24 heures ou lorsque l'état de la ressource associée change. Pour de plus amples informations, veuillez consulter Planification de l'exécution des vérifications de sécurité.

Les règles d'automatisation évaluent les résultats originaux fournis par le fournisseur. Les fournisseurs peuvent fournir de nouveaux résultats et mettre à jour les résultats existants en `BatchImportFindings` utilisant l'API Security Hub CSPM. Si les champs suivants n'existent pas dans le résultat initial, Security Hub CSPM les renseigne automatiquement, puis utilise les valeurs renseignées dans l'évaluation par la règle d'automatisation :

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

Une fois que vous avez créé une ou plusieurs règles d'automatisation, celles-ci ne sont pas déclenchées si vous mettez à jour les champs de recherche à l'aide de l'BatchUpdateFindingsopération. Si vous créez une règle d'automatisation et effectuez une `BatchUpdateFindings` mise à jour qui affectent le même champ de recherche, la dernière mise à jour définit la valeur de ce champ. Prenons l'exemple suivant :

1. Vous utilisez cette `BatchUpdateFindings` opération pour modifier la valeur du `Workflow.Status` champ d'une recherche de `NEW` à`NOTIFIED`.
2. Si vous appelez`GetFindings`, le `Workflow.Status` champ a désormais une valeur de`NOTIFIED`.
3. Vous créez une règle d'automatisation qui fait passer le `Workflow.Status` champ du résultat de `NEW` à`SUPPRESSED`. (Rappelez-vous que les règles ignorent les mises à jour effectuées à l'aide de cette `BatchUpdateFindings` opération.)
4. Le fournisseur de résultats utilise l'`BatchImportFindings`opération pour mettre à jour le résultat et modifie la valeur du `Workflow.Status` champ du résultat en`NEW`.
5. Si vous appelez`GetFindings`, le `Workflow.Status` champ a désormais une valeur de`SUPPRESSED`. C'est le cas parce que la règle d'automatisation a été appliquée et qu'il s'agit de la dernière action entreprise sur la base du résultat.

Lorsque vous créez ou modifiez une règle sur la console Security Hub CSPM, celle-ci affiche une version bêta des résultats correspondant aux critères de la règle. Alors que les règles d'automatisation évaluent les résultats originaux envoyés par le fournisseur de recherche, la version bêta de la console reflète les résultats dans leur état final tel qu'ils seraient affichés en réponse à l'GetFindingsopération (c'est-à-dire une fois que des actions de règles ou d'autres mises à jour ont été appliquées au résultat).

Comment fonctionne l'ordre des règles

Lorsque vous créez des règles d'automatisation, vous attribuez un ordre à chaque règle. Cela détermine l'ordre dans lequel Security Hub CSPM applique vos règles d'automatisation, et cela devient important lorsque plusieurs règles concernent le même résultat ou champ de recherche.

Lorsque plusieurs actions de règle concernent le même résultat ou le même champ de recherche, la règle ayant la valeur numérique la plus élevée pour l'ordre des règles s'applique en dernier lieu et produit l'effet final.

Lorsque vous créez une règle dans la console Security Hub CSPM, Security Hub CSPM attribue automatiquement l'ordre des règles en fonction de l'ordre de création des règles. La dernière règle créée possède la valeur numérique la plus faible pour l'ordre des règles et s'applique donc en premier. Security Hub CSPM applique les règles suivantes par ordre croissant.

Lorsque vous créez une règle via l'API Security Hub CSPM ouAWS CLI, Security Hub CSPM applique la règle dont la valeur numérique la plus faible est la première. `RuleOrder` Il applique ensuite les règles suivantes par ordre croissant. Si plusieurs résultats sont identiques`RuleOrder`, Security Hub CSPM applique une règle avec une valeur antérieure pour le `UpdatedAt` champ en premier (c'est-à-dire que la règle la plus récemment modifiée s'applique en dernier lieu).

Vous pouvez modifier l'ordre des règles à tout moment.

Exemple d'ordre des règles :

Règle A (l'ordre des règles est**1**) :

- Critères de la règle A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` est `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` est `NEW`

  - `Workflow.Status` = `ACTIVE`
- Actions en vertu de la règle A
  - Mettre à jour `Confidence` vers `95`
  - Mettre à jour `Severity` vers `CRITICAL`

Règle B (l'ordre des règles est**2**) :

- Critères de la règle B
  - `AwsAccountId` = `123456789012`
- Actions relevant de la règle B
  - Mettre à jour `Severity` vers `INFORMATIONAL`

Les actions de la règle A s'appliquent d'abord aux résultats du Security Hub CSPM qui répondent aux critères de la règle A. Ensuite, les actions de la règle B s'appliquent aux résultats du Security Hub CSPM avec l'ID de compte spécifié. Dans cet exemple, étant donné que la règle B s'applique `Severity` en dernier, la valeur finale des résultats provenant de l'ID de compte spécifié est`INFORMATIONAL`. Sur la base de l'action de la règle A, la valeur `Confidence` finale des résultats correspondants est`95`.

Création de règles d'automatisation

Une règle d'automatisation peut être utilisée pour mettre à jour automatiquement les résultats dans AWS Security Hub CSPM. Vous pouvez créer une règle d'automatisation personnalisée à partir de zéro ou, sur la console Security Hub CSPM, utiliser un modèle de règle prérempli. Pour obtenir des informations générales sur le fonctionnement des règles d'automatisation, consultezComprendre les règles d'automatisation dans Security Hub CSPM.

Vous ne pouvez créer qu'une seule règle d'automatisation à la fois. Pour créer plusieurs règles d'automatisation, suivez les procédures de la console à plusieurs reprises ou appelez l'API ou la commande à plusieurs reprises avec les paramètres souhaités.

Vous devez créer une règle d'automatisation dans chaque région et chaque compte dans lesquels vous souhaitez que la règle s'applique aux résultats.

Lorsque vous créez une règle d'automatisation dans la console Security Hub CSPM, Security Hub CSPM affiche une version bêta des résultats auxquels s'applique votre règle. La version bêta

n'est actuellement pas prise en charge si vos critères de règle incluent un filtre CONTAINS ou NOT_CONTAINS. Vous pouvez choisir ces filtres pour les types de champs de type carte et chaîne.

> **Important**
>
> AWSvous recommande de ne pas inclure d'informations d'identification personnelle, confidentielles ou sensibles dans le nom, la description ou d'autres champs de votre règle.

Création d'une règle d'automatisation personnalisée

Choisissez votre méthode préférée et suivez les étapes ci-dessous pour créer une règle d'automatisation personnalisée.

Console

Pour créer une règle d'automatisation personnalisée (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Automations.
3. Choisissez Créer une règle. Pour Type de règle, choisissez Créer une règle personnalisée.
4. Dans la section Règle, saisissez un nom de règle unique et une description de votre règle.
5. Pour les critères, utilisez les menus déroulants Clé, Opérateur et Valeur pour définir vos critères de règle. Vous devez spécifier au moins un critère de règle.

   Si les critères que vous avez sélectionnés sont pris en charge, la console affiche une version bêta des résultats correspondant à vos critères.
6. Pour l'action automatisée, utilisez les menus déroulants pour spécifier les champs de recherche à mettre à jour lorsque les résultats correspondent aux critères de votre règle. Vous devez spécifier au moins une action de règle.
7. Pour le statut de la règle, choisissez si vous souhaitez que la règle soit activée ou désactivée après sa création.
8. (Facultatif) Développez la section Paramètres supplémentaires. Sélectionnez Ignorer les règles suivantes pour les résultats correspondant à ces critères si vous souhaitez que cette règle soit la dernière à être appliquée aux résultats correspondant aux critères des règles.

9. (Facultatif) Pour les balises, ajoutez des balises sous forme de paires clé-valeur pour identifier facilement la règle.
10. Choisissez Créer une règle.

API

Pour créer une règle d'automatisation personnalisée (API)

1. Exécutez `CreateAutomationRule`depuis le compte administrateur du Security Hub CSPM. Cette API crée une règle avec un Amazon Resource Name (ARN) spécifique.
2. Donnez un nom et une description à la règle.
3. Définissez le `IsTerminal` paramètre sur `true` si vous souhaitez que cette règle soit la dernière à être appliquée aux résultats correspondant aux critères de la règle.
4. Pour le `RuleOrder` paramètre, indiquez l'ordre de la règle. Security Hub CSPM applique d'abord les règles avec une valeur numérique inférieure pour ce paramètre.
5. Pour le `RuleStatus` paramètre, spécifiez si vous souhaitez que Security Hub CSPM active et commence à appliquer la règle aux résultats après sa création. La valeur par défaut est `ENABLED` si aucune valeur n'est spécifiée. La valeur de `DISABLED` signifie que la règle est suspendue après sa création.
6. Pour le `Criteria` paramètre, indiquez les critères que Security Hub CSPM doit utiliser pour filtrer vos résultats. L'action de la règle s'appliquera aux résultats correspondant aux critères. Pour obtenir la liste des critères pris en charge, consultezCritères de règle et actions de règle disponibles.
7. Pour le `Actions` paramètre, indiquez les actions que vous souhaitez que Security Hub CSPM entreprenne en cas de correspondance entre un résultat et les critères que vous avez définis. Pour obtenir la liste des actions prises en charge, consultezCritères de règle et actions de règle disponibles.

L'exemple de AWS CLI commande suivant crée une règle d'automatisation qui met à jour l'état du flux de travail et note les résultats correspondants. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub create-automation-rule \
--actions '[{
```

```
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Création d'une règle d'automatisation à partir d'un modèle (console uniquement)

Les modèles de règles reflètent les cas d'utilisation courants des règles d'automatisation. Actuellement, seule la console Security Hub CSPM prend en charge les modèles de règles. Procédez comme suit pour créer une règle d'automatisation à partir d'un modèle dans la console.

Pour créer une règle d'automatisation à partir d'un modèle (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Automations.
3. Choisissez Créer une règle. Pour Type de règle, choisissez Créer une règle à partir d'un modèle.
4. Sélectionnez un modèle de règle dans le menu déroulant.
5. (Facultatif) Si cela est nécessaire pour votre cas d'utilisation, modifiez les sections Règle, Critères et Actions automatisées. Vous devez spécifier au moins un critère de règle et une action de règle.

Si les critères que vous avez sélectionnés sont pris en charge, la console affiche une version bêta des résultats correspondant à vos critères.

6. Pour le statut de la règle, choisissez si vous souhaitez que la règle soit activée ou désactivée après sa création.
7. (Facultatif) Développez la section Paramètres supplémentaires. Sélectionnez Ignorer les règles suivantes pour les résultats correspondant à ces critères si vous souhaitez que cette règle soit la dernière à être appliquée aux résultats correspondant aux critères des règles.
8. (Facultatif) Pour les balises, ajoutez des balises sous forme de paires clé-valeur pour identifier facilement la règle.
9. Choisissez Créer une règle.

Afficher les règles d'automatisation

Une règle d'automatisation peut être utilisée pour mettre à jour automatiquement les résultats dans AWS Security Hub CSPM. Pour obtenir des informations générales sur le fonctionnement des règles d'automatisation, consultezComprendre les règles d'automatisation dans Security Hub CSPM.

Choisissez votre méthode préférée et suivez les étapes pour afficher vos règles d'automatisation existantes et les détails de chaque règle.

Pour consulter un historique de la façon dont les règles d'automatisation ont modifié vos résultats, voirRévision des détails et de l'historique des recherches dans Security Hub CSPM.

Console

Pour consulter les règles d'automatisation (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Automations.
3. Choisissez un nom de règle. Vous pouvez également sélectionner une règle.
4. Choisissez Actions et Afficher.

API

Pour consulter les règles d'automatisation (API)

1. Pour consulter les règles d'automatisation de votre compte, lancez-le `ListAutomationRules`depuis le compte administrateur du Security Hub CSPM. Cette API renvoie les ARN des règles et les autres métadonnées associées à vos règles. Aucun paramètre d'entrée n'est requis pour cette API, mais vous pouvez éventuellement le fournir `MaxResults` pour limiter le nombre de résultats et `NextToken` en tant que paramètre de pagination. La valeur initiale de `NextToken` doit êtreNULL.
2. Pour plus de détails sur les règles, y compris les critères et les actions d'une règle, exécutez `BatchGetAutomationRules`depuis le compte administrateur Security Hub CSPM. Fournissez les ARN des règles d'automatisation pour lesquelles vous souhaitez obtenir des détails.

   L'exemple suivant permet de récupérer les détails des règles d'automatisation spécifiées. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

   ```
   $ aws securityhub batch-get-automation-rules \
   --automation-rules-arns '["arn:aws:securityhub:us-
   east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
   cdef-EXAMPLE22222"]' \
   --region us-east-1
   ```

Modification des règles d'automatisation

Une règle d'automatisation peut être utilisée pour mettre à jour automatiquement les résultats dans AWS Security Hub CSPM. Pour obtenir des informations générales sur le fonctionnement des règles d'automatisation, consultezComprendre les règles d'automatisation dans Security Hub CSPM.

Après avoir créé une règle d'automatisation, l'administrateur délégué du Security Hub CSPM peut modifier la règle. Lorsque vous modifiez une règle d'automatisation, les modifications s'appliquent aux résultats nouveaux et mis à jour que Security Hub CSPM génère ou ingère après la modification de la règle.

Choisissez votre méthode préférée et suivez les étapes pour modifier le contenu d'une règle d'automatisation. Vous pouvez modifier une ou plusieurs règles à l'aide d'une seule demande. Pour

obtenir des instructions sur la modification de l'ordre des règles, voirModification de l'ordre des règles d'automatisation.

Console

Pour modifier les règles d'automatisation (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Automations.
3. Sélectionnez la règle que vous souhaitez modifier. Choisissez Action et Modifier.
4. Modifiez la règle comme vous le souhaitez, puis choisissez Enregistrer les modifications.

API

Pour modifier les règles d'automatisation (API)

1. Exécutez `BatchUpdateAutomationRules`depuis le compte administrateur du Security Hub CSPM.
2. Pour le `RuleArn` paramètre, indiquez l'ARN de la ou des règles que vous souhaitez modifier.
3. Fournissez les nouvelles valeurs pour les paramètres que vous souhaitez modifier. Vous pouvez modifier n'importe quel paramètre saufRuleArn.

L'exemple suivant met à jour la règle d'automatisation spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
```

```
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

Modification de l'ordre des règles d'automatisation

Une règle d'automatisation peut être utilisée pour mettre à jour automatiquement les résultats dans AWS Security Hub CSPM. Pour obtenir des informations générales sur le fonctionnement des règles d'automatisation, consultezComprendre les règles d'automatisation dans Security Hub CSPM.

Après avoir créé une règle d'automatisation, l'administrateur délégué du Security Hub CSPM peut modifier la règle.

Si vous souhaitez conserver les mêmes critères et actions, mais modifier l'ordre dans lequel Security Hub CSPM applique une règle d'automatisation, vous pouvez modifier uniquement l'ordre des règles. Choisissez votre méthode préférée et suivez les étapes pour modifier l'ordre des règles.

Pour obtenir des instructions sur la modification des critères ou des actions d'une règle d'automatisation, consultezModification des règles d'automatisation.

Console

Pour modifier l'ordre des règles d'automatisation (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Automations.

3. Sélectionnez la règle dont vous souhaitez modifier l'ordre. Choisissez Modifier la priorité.
4. Choisissez Déplacer vers le haut pour augmenter la priorité de la règle d'une unité. Choisissez Déplacer vers le bas pour diminuer la priorité des règles d'une unité. Choisissez Déplacer vers le haut pour attribuer à la règle un ordre de 1 (cela lui donne la priorité sur les autres règles existantes).

> **Note**
>
> Lorsque vous créez une règle dans la console Security Hub CSPM, Security Hub CSPM attribue automatiquement l'ordre des règles en fonction de l'ordre de création des règles. La dernière règle créée possède la valeur numérique la plus faible pour l'ordre des règles et s'applique donc en premier.

API

Pour modifier l'ordre des règles d'automatisation (API)

1. Utilisez l'`BatchUpdateAutomationRules`opération depuis le compte administrateur du Security Hub CSPM.
2. Pour le `RuleArn` paramètre, indiquez l'ARN de la ou des règles dont vous souhaitez modifier l'ordre.
3. Modifiez la valeur du `RuleOrder` champ.

> **Note**
>
> Si plusieurs règles sont identiques`RuleOrder`, Security Hub CSPM applique une règle avec une valeur antérieure pour le `UpdatedAt` champ en premier (c'est-à-dire que la règle la plus récemment modifiée s'applique en dernier lieu).

Supprimer ou désactiver les règles d'automatisation

Une règle d'automatisation peut être utilisée pour mettre à jour automatiquement les résultats dans AWS Security Hub CSPM. Pour obtenir des informations générales sur le fonctionnement des règles d'automatisation, consultezComprendre les règles d'automatisation dans Security Hub CSPM.

Lorsque vous supprimez une règle d'automatisation, Security Hub CSPM la supprime de votre compte et ne l'applique plus aux résultats. Au lieu de supprimer une règle, vous pouvez désactiver une règle. Cela permet de conserver la règle pour une utilisation future, mais Security Hub CSPM ne l'appliquera pas aux résultats correspondants tant que vous ne l'aurez pas activée.

Choisissez votre méthode préférée et suivez les étapes pour supprimer une règle d'automatisation. Vous pouvez supprimer une ou plusieurs règles en une seule demande.

Console

Pour supprimer ou désactiver les règles d'automatisation (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sélectionnez Automations.
3. Sélectionnez la ou les règles que vous souhaitez supprimer. Choisissez Action et Supprimer (pour conserver une règle, mais la désactiver temporairement, choisissez Désactiver).
4. Confirmez votre choix et choisissez Delete (Supprimer).

API

Pour supprimer ou désactiver les règles d'automatisation (API)

1. Utilisez l'`BatchDeleteAutomationRules`opération depuis le compte administrateur du Security Hub CSPM.
2. Pour le `AutomationRulesArns` paramètre, indiquez l'ARN de la ou des règles que vous souhaitez supprimer (pour conserver une règle, mais la désactiver temporairement, fournissez `DISABLED` le `RuleStatus` paramètre).

L'exemple suivant supprime la règle d'automatisation spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Exemples de règles d'automatisation

Cette section fournit des exemples de règles d'automatisation pour les cas d'utilisation courants de Security Hub CSPM. Ces exemples correspondent à des modèles de règles disponibles sur la console Security Hub CSPM.

Atteignez le niveau de gravité à Critique lorsqu'une ressource spécifique, telle qu'un compartiment S3, est menacée

Dans cet exemple, les critères des règles sont mis `ResourceId` en correspondance lorsque le résultat correspond à un compartiment Amazon Simple Storage Service (Amazon S3) spécifique. L'action de la règle consiste à modifier la gravité des résultats correspondants en`CRITICAL`. Vous pouvez modifier ce modèle pour l'appliquer à d'autres ressources.

Exemple de demande d'API :

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
            "Comparison": "EQUALS"
```

```
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Exemple de commande CLI :

```
$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
```

```
}],
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Accroître la sévérité des constatations relatives aux ressources dans les comptes de production

Dans cet exemple, les critères des règles sont mis en correspondance lorsqu'une constatation de `HIGH` gravité est générée dans des comptes de production spécifiques. L'action de la règle consiste à modifier la gravité des résultats correspondants en`CRITICAL`.

Exemple de demande d'API :

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
```

```
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Exemple de commande CLI :

```
aws securityhub create-automation-rule \
--no-is-terminal \
```

```
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
```

```
}]' \
--region us-east-1
```

Supprimer les résultats informationnels

Dans cet exemple, les critères des règles sont mis en correspondance pour les résultats de `INFORMATIONAL` gravité envoyés à Security Hub CSPM par Amazon. GuardDuty L'action de la règle consiste à modifier le statut du flux de travail des résultats correspondants sur`SUPPRESSED`.

Exemple de demande d'API :

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
```

```
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Exemple de commande CLI :

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
```

```
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Utilisation à EventBridge des fins de réponse et de correction automatisées

En créant des règles dans Amazon EventBridge, vous pouvez répondre automatiquement aux résultats du AWS Security Hub CSPM. Security Hub CSPM envoie les résultats sous forme d'événements EventBridge en temps quasi réel. Vous pouvez rédiger des règles simples pour indiquer les événements qui vous intéressent et les actions automatisées à effectuer lorsqu'un événement correspond à une règle. Les actions pouvant être déclenchées automatiquement sont les suivantes :

- Invocation d'une fonction AWS Lambda
- Invocation de la commande d'exécution d'Amazon EC2
- Relais de l'événement à Amazon Kinesis Data Streams
- Activation d'une machine à AWS Step Functions états
- Notification d'une rubrique Amazon SNS ou d'une file d'attente Amazon SQS
- Envoi d'un résultat à un service de billetterie tiers, de conversation instantané, de gestion des informations et des événements de sécurité (SIEM) ou à un outil de réponse aux incidents et de gestion des incidents

Security Hub CSPM envoie automatiquement toutes les nouvelles découvertes et toutes les mises à jour des découvertes existantes EventBridge sous forme EventBridge d'événements. Vous pouvez également créer des actions personnalisées qui vous permettent d'envoyer des résultats et des résultats d'analyse sélectionnés à EventBridge.

Vous configurez ensuite EventBridge des règles pour répondre à chaque type d'événement.

Pour plus d'informations sur l'utilisation EventBridge, consultez le guide de EventBridge l'utilisateur Amazon .

> **Note**
>
> Il est recommandé de s'assurer que les autorisations d'accès accordées à vos utilisateurs EventBridge utilisent des politiques de moindre privilège Gestion des identités et des accès AWS (IAM) qui n'accordent que les autorisations requises.
> Pour plus d'informations, consultez la section Gestion des identités et des accès sur Amazon EventBridge.

Un ensemble de modèles de réponse et de correction automatisées entre comptes est également disponible dans AWS Solutions. Les modèles exploitent les règles EventBridge d'événements et les fonctions Lambda. Vous déployez la solution à l'aide CloudFormation de et AWS Systems Manager. La solution peut créer des actions de réponse et de correction entièrement automatisées. Il peut également utiliser les actions personnalisées CSPM de Security Hub pour créer des actions de réponse et de correction déclenchées par l'utilisateur. Pour plus de détails sur la configuration et l'utilisation de la solution, consultez la page Réponse de sécurité automatisée sur la AWS solution.

Rubriques

- Types d'événements CSPM de Security Hub dans EventBridge
- EventBridge formats d'événements pour Security Hub CSPM
- Configuration d'une EventBridge règle pour les résultats CSPM de Security Hub
- Utiliser des actions personnalisées pour envoyer des résultats et des informations à EventBridge

Types d'événements CSPM de Security Hub dans EventBridge

Security Hub CSPM utilise les types d' EventBridge événements Amazon suivants pour s'intégrer. EventBridge

Sur le EventBridge tableau de bord de Security Hub CSPM, All Events inclut tous ces types d'événements.

Tous les résultats (Résultats du Security Hub - Importés)

Security Hub CSPM envoie automatiquement toutes les nouvelles découvertes et toutes les mises à jour des découvertes existantes EventBridge sous forme Security Hub Findings - Imported d'événements. Chaque Security Hub Findings - Imported événement contient une seule découverte.

Chaque `BatchUpdateFindings` demande `BatchImportFindings` et déclenche un Security Hub Findings - Imported événement.

Pour les comptes administrateurs, le flux d'événements EventBridge inclut des événements contenant des résultats provenant à la fois de leur compte et de leurs comptes membres.

Dans une région d'agrégation, le flux d'événements inclut des événements pour les résultats de la région d'agrégation et des régions liées. Cross-Region les résultats sont inclus dans le flux d'événements en temps quasi réel. Pour plus d'informations sur la configuration de l'agrégation de recherche, consultezthe section called “Agrégation des données entre les régions”.

Vous pouvez définir des règles EventBridge qui acheminent automatiquement les résultats vers un flux de travail de correction, un outil tiers ou une autre EventBridge cible prise en charge. Les règles peuvent inclure des filtres qui n'appliquent la règle que si la découverte comporte des valeurs d'attribut spécifiques.

Vous utilisez cette méthode pour envoyer automatiquement tous les résultats, ou tous les résultats présentant des caractéristiques spécifiques, à un flux de travail de réponse ou de correction.

Consultez the section called “Configuration d'une EventBridge règle”.

Résultats relatifs aux actions personnalisées (Résultats du Security Hub : action personnalisée)

Security Hub CSPM envoie également les résultats associés à des actions personnalisées EventBridge sous forme Security Hub Findings - Custom Action d'événements.

Cela est utile pour les analystes travaillant avec la console Security Hub CSPM qui souhaitent envoyer un résultat spécifique, ou un petit ensemble de résultats, à un flux de travail de réponse ou de correction. Vous pouvez sélectionner une action personnalisée pour un maximum de 20 résultats à la fois. Chaque découverte est envoyée en EventBridge tant qu' EventBridge événement distinct.

Lorsque vous créez une action personnalisée, vous lui attribuez un ID d'action personnalisé. Vous pouvez utiliser cet ID pour créer une EventBridge règle qui exécute une action spécifique après avoir reçu un résultat associé à cet ID d'action personnalisé.

Consultez the section called “Configuration et utilisation d'actions personnalisées”.

Par exemple, vous pouvez créer une action personnalisée dans Security Hub CSPM appelée. `send_to_ticketing` Ensuite EventBridge, vous créez une règle qui est déclenchée lorsque vous EventBridge recevez un résultat qui inclut l'ID d'action `send_to_ticketing` personnalisé. La règle inclut la logique qui permet d'envoyer le résultat à votre système de tickets. Vous pouvez ensuite

sélectionner les résultats dans Security Hub CSPM et utiliser l'action personnalisée dans Security Hub CSPM pour envoyer manuellement les résultats à votre système de billetterie.

Pour des exemples montrant comment envoyer les résultats du Security Hub CSPM à des EventBridge fins de traitement ultérieur, consultez Comment intégrer les actions personnalisées AWS Security Hub CSPM PagerDuty et Comment activer les actions personnalisées dans AWS Security Hub CSPM sur le blog AWS Partner Network (APN).

Résultats d'analyse pour les actions personnalisées (Résultats de Security Hub Insight)

Vous pouvez également utiliser des actions personnalisées pour envoyer des ensembles de résultats d'analyse EventBridge sous forme d'Security Hub Insight Resultsévénements. Les résultats d'analyse sont les ressources qui correspondent à une idée. Notez que lorsque vous envoyez des résultats d'analyse à EventBridge, vous n'envoyez pas les résultats à EventBridge. Vous envoyez uniquement les identificateurs de ressources associés aux résultats d'analyse. Vous pouvez envoyer jusqu'à 100 identifiants de ressource à la fois.

Comme pour les actions personnalisées pour les résultats, vous devez d'abord créer l'action personnalisée dans Security Hub CSPM, puis créer une règle dans. EventBridge

Consultez the section called “Configuration et utilisation d'actions personnalisées”.

Supposons, par exemple, que vous voyiez un résultat d'intérêt particulier que vous souhaitez partager avec un collègue. Dans ce cas, vous pouvez utiliser une action personnalisée pour envoyer ce résultat d'analyse au collègue via un système de chat ou de billetterie.

EventBridge formats d'événements pour Security Hub CSPM

Les types d'Security Hub Insight Resultsévénements Security Hub Findings - Imported Security Findings - Custom Action, et utilisent les formats d'événements suivants.

Le format d'événement est le format utilisé lorsque Security Hub CSPM envoie un événement à. EventBridge

Résultats du Security Hub - Importés

Security Hub Findings - Importedévénements envoyés depuis Security Hub CSPM au EventBridge format suivant.

```
{
   "version":"0",
```

```
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

*<finding content>*est le contenu, au format JSON, du résultat envoyé par l'événement. Chaque événement envoie un résultat unique.

Pour une liste complète des attributs de recherche, consultezAWS Format de recherche de sécurité (ASFF).

Pour plus d'informations sur la configuration EventBridge des règles déclenchées par ces événements, consultezthe section called "Configuration d'une EventBridge règle".

Résultats du Security Hub : action personnalisée

Security Hub Findings - Custom Actionévénements envoyés depuis Security Hub CSPM au EventBridge format suivant. Chaque résultat est envoyé lors d'un événement distinct.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
```

```
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*est le contenu, au format JSON, du résultat envoyé par l'événement. Chaque événement envoie un résultat unique.

Pour une liste complète des attributs de recherche, consultezAWS Format de recherche de sécurité (ASFF).

Pour plus d'informations sur la configuration EventBridge des règles déclenchées par ces événements, consultezthe section called "Configuration et utilisation d'actions personnalisées".

Résultats de Security Hub Insight

Security Hub Insight Resultsévénements envoyés depuis Security Hub CSPM au EventBridge format suivant.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
```

```
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Pour plus d'informations sur la création d'une EventBridge règle déclenchée par ces événements, consultezthe section called "Configuration et utilisation d'actions personnalisées".

Configuration d'une EventBridge règle pour les résultats CSPM de Security Hub

Vous pouvez créer une règle dans Amazon EventBridge qui définit une action à effectuer lorsqu'un Security Hub Findings - Imported événement est reçu. Security Hub Findings - Importedles événements sont déclenchés par des mises à jour provenant à la fois `BatchUpdateFindings` des opérations `BatchImportFindings` et.

Chaque règle contient un modèle d'événement qui identifie les événements qui déclenchent la règle. Le modèle d'événement contient toujours la source de l'événement (`aws.securityhub`) et le type d'événement (Résultats de Security Hub - Importés). Le modèle d'événement peut également spécifier des filtres pour identifier les résultats auxquels la règle s'applique.

La règle d'événement identifie ensuite les cibles de la règle. Les cibles sont les actions à effectuer lorsque EventBridge reçoit un événement Security Hub Findings - Imported et que le résultat correspond aux filtres.

Les instructions fournies ici utilisent la EventBridge console. Lorsque vous utilisez la console, crée EventBridge automatiquement la politique basée sur les ressources requise qui permet d' EventBridge écrire dans Amazon CloudWatch Logs.

Vous pouvez également utiliser le `PutRule` fonctionnement de l' EventBridge API. Toutefois, si vous utilisez l' EventBridge API, vous devez créer la politique basée sur les ressources. Pour plus d'informations sur la politique requise, consultez la section CloudWatch Consigne les autorisations dans le guide de EventBridge l'utilisateur Amazon.

Format du modèle d'événement

Le format du modèle d'événement pour Security Hub Findings - Imported events est le suivant :

```
{
```

```
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`identifie Security Hub CSPM comme étant le service qui génère l'événement.
- `detail-type`identifie le type d'événement.
- `detail`est facultatif et fournit les valeurs de filtre pour le modèle d'événement. Si le modèle d'événement ne contient aucun `detail` champ, tous les résultats déclenchent la règle.

Vous pouvez filtrer les résultats en fonction de n'importe quel attribut de recherche. Pour chaque attribut, vous fournissez un tableau d'une ou de plusieurs valeurs séparées par des virgules.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Si vous fournissez plusieurs valeurs pour un attribut, ces valeurs sont jointes par`OR`. Un résultat correspond au filtre d'un attribut individuel si le résultat possède l'une des valeurs répertoriées. Par exemple, si vous fournissez les deux valeurs `INFORMATIONAL` et `LOW` comme valeurs pour`Severity.Label`, le résultat correspond s'il possède une étiquette de gravité égale à `INFORMATIONAL` ou`LOW`.

Les attributs sont joints par`AND`. Un résultat correspond s'il correspond aux critères de filtre pour tous les attributs fournis.

Lorsque vous fournissez une valeur d'attribut, elle doit refléter l'emplacement de cet attribut dans la structure ASFF (AWS Security Finding Format).

> **Tip**
>
> Lorsque vous filtrez les résultats des contrôles, nous vous recommandons d'utiliser les champs `SecurityControlId` ou `SecurityControlArn` ASFF comme filtres, plutôt que

`Title` ou`Description`. Ces derniers champs peuvent changer occasionnellement, tandis que l'ID de contrôle et l'ARN sont des identifiants statiques.

Dans l'exemple suivant, le modèle d'événement fournit des valeurs de filtre pour `ProductArn` et. Ainsi`Severity.Label`, une recherche correspond si elle est générée par Amazon Inspector et si elle possède une étiquette de gravité égale à `INFORMATIONAL` ou`LOW`.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Création d'une règle d'événement

Vous pouvez utiliser un modèle d'événement prédéfini ou un modèle d'événement personnalisé pour créer une règle dans EventBridge. Si vous sélectionnez un motif prédéfini, renseignez EventBridge automatiquement `source` et`detail-type`. EventBridge fournit également des champs permettant de spécifier des valeurs de filtre pour les attributs de recherche suivants :

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`

- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Pour créer une EventBridge règle (console)

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. À l'aide des valeurs suivantes, créez une EventBridge règle qui surveille la recherche d'événements :
   - Pour Type de règle, choisissez Règle avec un modèle d'événement.
   - Choisissez comment créer le modèle d'événement.

Pour créer le modèle d'événement avec...	Faites ceci...
Un modèle	Dans la section Modèle d'événement, choisissez les options suivantes : • Pour Source d'événement, choisissez Services AWS . • Pour le AWS service, choisissez Security Hub. • Pour Type d'événement, choisissez Résultats de Security Hub - Importés. • (Facultatif) Pour rendre la règle plus précise, ajoutez des valeurs de filtre. Par exemple, pour limiter la règle aux résultats dont les états d'enregistrement sont actifs, pour

Pour créer le modèle d'événement avec...	Faites ceci...	
	les états d'enregistrement spécifiques, choisissez Actif.	

Pour créer le modèle d'événement avec...	Faites ceci...
Un modèle d'événement personnalisé (Utilisez un modèle personnalisé si vous souhaitez filtrer les résultats en fonction d'attributs qui n'apparaissent pas dans la EventBridge console.)	• Dans la section Modèle d'événement, choisissez Modèles personnalisés (éditeur JSON), puis collez le modèle d'événement suivant dans la zone de texte : `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>"] } } }` • Mettez à jour le modèle d'événement pour inclure l'attribut et les valeurs d'attribut que vous souhaitez utiliser comme filtre. Par exemple, pour appliquer la règle aux

Pour créer le modèle d'événement avec...	Faites ceci...	
	résultats dont l'état de vérification est deTRUE_POSITIVE , utilisez l'exemple de modèle suivant : `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Pour Types de cibles, choisissez un AWS service, et pour Sélectionner une cible, choisissez une cible telle qu'une rubrique ou une AWS Lambda fonction Amazon SNS. La cible est déclenchée lorsqu'un événement correspond au modèle d'événement défini dans la règle est reçu.

Pour plus d'informations sur la création de règles, consultez la section Création de EventBridge règles Amazon qui réagissent à des événements dans le Guide de EventBridge l'utilisateur Amazon.

Utiliser des actions personnalisées pour envoyer des résultats et des informations à EventBridge

Pour utiliser les actions personnalisées de AWS Security Hub CSPM afin d'envoyer des résultats ou des informations à Amazon EventBridge, vous devez d'abord créer l'action personnalisée dans Security Hub CSPM. Vous pouvez ensuite définir des règles EventBridge qui s'appliquent à vos actions personnalisées.

Vous pouvez créer jusqu'à 50 actions personnalisées.

Si vous activez l'agrégation entre régions et gérez les résultats provenant de la région d'agrégation, créez des actions personnalisées dans la région d'agrégation.

La règle EventBridge utilisée utilise le nom de ressource Amazon (ARN) issu de l'action personnalisée.

Création d'une action personnalisée

Lorsque vous créez une action personnalisée dans AWS Security Hub CSPM, vous spécifiez son nom, sa description et un identifiant unique.

Une action personnalisée spécifie les actions à effectuer lorsqu'un EventBridge événement correspond à une EventBridge règle. Security Hub CSPM envoie chaque résultat EventBridge sous forme d'événement.

Choisissez votre méthode préférée et suivez les étapes pour créer une action personnalisée.

Console

Pour créer une action personnalisée dans Security Hub CSPM (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Settings (Paramètres), puis Custom actions (Actions personnalisées).
3. Choisissez Create custom action (Créer une action personnalisée).
4. Renseignez les champs Name (Nom), Description et Custom action ID (ID d'action personnalisé) pour l'action.

   La valeur du champ Name (Nom) doit comporter moins de 20 caractères.

L'ID d'action personnalisé doit être unique pour chaque AWS compte.

5. Choisissez Create custom action (Créer une action personnalisée).
6. Notez la valeur de Custom action ARN (ARN de l'action personnalisé). Vous devez utiliser l'ARN lorsque vous créez une règle à associer à cette action dans EventBridge.

API

Pour créer une action personnalisée (API)

Utilisez l'CreateActionTargetopération. Si vous utilisez le AWS CLI, exécutez la commande https://docs.aws.amazon.com/cli/latest/reference/securityhub/create-action-target.html create-action-target.

L'exemple suivant crée une action personnalisée pour envoyer les résultats à un outil de correction. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Définition d'une règle dans EventBridge

Pour déclencher une action personnalisée dans Amazon EventBridge, vous devez créer une règle correspondante dans EventBridge. La définition de la règle inclut le nom de ressource Amazon (ARN) de l'action personnalisée.

Le modèle d'événement d'un événement Security Hub Findings - Custom Action a le format suivant :

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Le modèle d'événement d'un événement Security Hub Insight Results a le format suivant :

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Dans les deux modèles, *<custom action ARN>* se trouve l'ARN d'une action personnalisée. Vous pouvez configurer une règle qui s'applique à plusieurs actions personnalisées.

Les instructions fournies ici concernent la EventBridge console. Lorsque vous utilisez la console, crée EventBridge automatiquement la politique basée sur les ressources requise qui permet d'écrire dans EventBridge les CloudWatch journaux.

Vous pouvez également utiliser le `PutRule` fonctionnement de l' EventBridge API. Toutefois, si vous utilisez l' EventBridge API, vous devez créer la politique basée sur les ressources. Pour plus de détails sur la politique requise, consultez la section CloudWatch Consigne les autorisations dans le guide de EventBridge l'utilisateur Amazon.

Pour définir une règle dans EventBridge (EventBridge console)

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le panneau de navigation, choisissez Rules.
3. Choisissez Créer une règle.
4. Saisissez un nom et une description pour la règle.
5. Pour Event bus (Bus d'événement), sélectionnez le bus d'événement que vous souhaitez associer à cette règle. Si vous souhaitez que cette règle mette en correspondance les événements en provenance de votre compte, sélectionnez Par défaut. Lorsqu'un service AWS de votre compte émet un événement, il accède toujours au bus d'événement par défaut de votre compte.
6. Pour Type de règle, choisissez Règle avec un modèle d'événement.
7. Choisissez Suivant.
8. Pour Event source (Source de l'événement), choisissez AWS events (Événements).
9. Pour Modèle d'événement, choisissez Formulaire de modèle d'événement.

10. Pour Source d'événement, choisissez Services AWS .
11. Pour le AWS service, choisissez Security Hub.
12. Pour Event type (Type d'événement), effectuez l'une des actions suivantes :

    - Pour créer une règle à appliquer lorsque vous envoyez des résultats à une action personnalisée, choisissez Security Hub Findings - Custom Action.
    - Pour créer une règle à appliquer lorsque vous envoyez des résultats d'analyse à une action personnalisée, choisissez Security Hub Insight Results.
13. Choisissez des ARN d'action personnalisés spécifiques, ajoutez un ARN d'action personnalisé.

    Si la règle s'applique à plusieurs actions personnalisées, choisissez Ajouter pour ajouter d'autres ARN d'action personnalisés.
14. Choisissez Suivant.
15. Sous Sélectionner les cibles, choisissez et configurez la cible à invoquer lorsque cette règle correspond.
16. Choisissez Suivant.
17. (Facultatif) Saisissez une ou plusieurs balises pour la règle. Pour plus d'informations, consultez les EventBridge balises Amazon dans le guide de EventBridge l'utilisateur Amazon.
18. Choisissez Suivant.
19. Consultez les détails de la règle et choisissez Create rule (Créer une règle).

    Lorsque vous effectuez une action personnalisée sur des résultats ou des informations dans votre compte, des événements sont générés dans EventBridge.

Sélection d'une action personnalisée pour les résultats et les informations

Une fois que vous avez créé des actions personnalisées et des EventBridge règles Amazon EventBridge pour AWS Security Hub CSPM, vous pouvez envoyer des résultats et des informations à des fins de gestion et de traitement automatiques.

Les événements ne sont envoyés EventBridge que dans le compte sur lequel ils ont été consultés. Si vous visualisez un résultat à l'aide d'un compte administrateur, l'événement est envoyé EventBridge dans le compte administrateur.

Pour que les appels d' AWS API soient efficaces, les implémentations du code cible doivent transférer les rôles aux comptes membres. Cela signifie également que le rôle dans lequel vous passez doit être déployé auprès de chaque membre lorsqu'une action est nécessaire.

Pour envoyer les résultats à EventBridge (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Afficher la liste des résultats :
   - Dans Résultats, vous pouvez consulter les résultats de toutes les intégrations de produits et de tous les contrôles activés.
   - Dans Normes de sécurité, vous pouvez accéder à la liste des résultats générés par un contrôle spécifique. Pour de plus amples informations, veuillez consulter Examiner les détails des contrôles dans Security Hub CSPM.
   - Dans Intégrations, vous pouvez accéder à la liste des résultats générés par une intégration activée. Pour de plus amples informations, veuillez consulter Affichage des résultats d'une intégration de Security Hub CSPM.
   - Dans Insights, vous pouvez accéder à une liste de résultats pour obtenir un résultat d'analyse. Pour de plus amples informations, veuillez consulter Examiner les informations contenues dans Security Hub CSPM et agir en conséquence.
3. Sélectionnez les résultats à envoyer EventBridge. Vous pouvez sélectionner jusqu'à 20 résultats à la fois.
4. Dans Actions, choisissez l'action personnalisée qui correspond à la EventBridge règle à appliquer.

   Security Hub CSPM envoie un événement Security Hub Findings - Custom Action distinct pour chaque découverte.

Pour envoyer les résultats d'Insight à EventBridge (console)

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le panneau de navigation, choisissez Insights.
3. Sur la page Insights, choisissez l'aperçu qui inclut les résultats à envoyer EventBridge.
4. Sélectionnez les résultats d'analyse à envoyer EventBridge. Vous pouvez sélectionner jusqu'à 20 résultats à la fois.
5. Dans Actions, choisissez l'action personnalisée qui correspond à la EventBridge règle à appliquer.

Utilisation du tableau de bord dans Security Hub CSPM

Sur la console Security Hub CSPM, le tableau de bord récapitulatif affiche un résumé de vos risques, de vos séquences d'attaques et de votre couverture de sécurité. Ce tableau de bord vous aide à identifier les risques et les séquences d'attaques en fonction de la gravité et de la couverture du compte pour différentes fonctionnalités de sécurité. Chaque fois que vous ouvrez le tableau de bord, celui-ci s'actualise automatiquement. Notez toutefois que les scores de sécurité et les états de contrôle sont actualisés toutes les 24 heures.

Vous pouvez personnaliser le tableau de bord récapitulatif en y ajoutant et en supprimant différents widgets de sécurité. Vous pouvez également spécifier des critères de filtre pour récupérer et afficher certains types de données. Si vous personnalisez le tableau de bord, Security Hub enregistre vos paramètres de personnalisation. Si d'autres utilisateurs de votre compte personnalisent le tableau de bord, leurs modifications sont enregistrées indépendamment de vos paramètres de personnalisation.

Si vous avez configuré l'agrégation interrégionale dans Security Hub CSPM, le tableau de bord récapitulatif affiche vos données agrégées. Si votre compte est le compte d'administrateur délégué d'une organisation, les données incluent les résultats relatifs à votre compte et à vos comptes de membres. Si votre compte est un compte de membre ou un compte autonome, les données incluent les résultats uniquement pour votre compte.

Rubriques

- Widgets disponibles pour le tableau de bord Summary
- Filtrer le tableau de bord récapitulatif dans Security Hub CSPM
- Personnalisation du tableau de bord récapitulatif dans Security Hub CSPM

Widgets disponibles pour le tableau de bord Summary

Le tableau de bord récapitulatif comprend des widgets qui reflètent le paysage moderne des menaces de sécurité du cloud, guidés par les opérations de sécurité et les expériences des AWS clients. Certains widgets sont affichés par défaut alors que d'autres ne le sont pas. Vous pouvez personnaliser votre affichage du tableau de bord en ajoutant ou en supprimant des widgets.

Pour ajouter un widget, choisissez Ajouter un widget en haut du tableau de bord. Vous pouvez ensuite parcourir la liste des widgets disponibles ou saisir le titre d'un widget dans la barre de recherche. Lorsque vous trouvez le widget à ajouter, faites-le glisser vers l'emplacement où vous

souhaitez qu'il apparaisse sur le tableau de bord. Pour de plus amples informations, veuillez consulter Personnalisation du tableau de bord.

Widgets affichés par défaut

Par défaut, le tableau de bord Résumé inclut les widgets suivants.

Principales séquences de menaces

Affiche les séquences de menaces les plus graves. Les résultats des séquences de menaces, connus sous le nom de résultats de séquences d'attaques sur Amazon GuardDuty, mettent en corrélation plusieurs événements afin d'identifier les menaces potentielles pour votre AWS environnement. Les séquences de menaces peuvent inclure des comportements d'attaque en cours ou récents (dans un délai de 24 heures) dans votre environnement, ce qui peut à son tour entraîner de nouvelles compromissions. La protection GuardDuty S3 doit GuardDuty être activée pour recevoir les résultats des séquences de menaces dans Security Hub CSPM.

Principaux risques

Affiche un résumé des principaux risques de votre environnement. Le haut du widget affiche le nombre de risques pour chaque niveau de gravité. Vous pouvez choisir un niveau de gravité pour accéder à la page Risques où les risques sont filtrés selon le niveau de gravité sélectionné. Les risques les plus fréquents dans votre environnement apparaissent en premier. Ce widget vous permet de hiérarchiser les risques à atténuer.

Couverture de sécurité

Résume l'étendue de votre couverture de sécurité, sur la base des résultats du contrôle de couverture. Les contrôles de couverture vérifient si un Service AWS élément spécifique et ses fonctionnalités sont activés (par exemple,[Macie.1] Amazon Macie devrait être activé). Ce widget vous permet de vous assurer que vous disposez de `PASSED` résultats pour les contrôles de couverture. La console Security Hub CSPM fournit des liens depuis ce widget pour vous aider à activer les fonctionnalités de sécurité manquantes. Nous vous recommandons d'utiliser une configuration centralisée pour activer les fonctionnalités de sécurité manquantes sur plusieurs Comptes AWS réseaux et Régions AWS. Pour de plus amples informations, veuillez consulter Comprendre la configuration centrale dans Security Hub CSPM.

Normes de sécurité

Affiche votre score de sécurité récapitulatif le plus récent et le score de sécurité pour chaque norme Security Hub CSPM. Les scores de sécurité, compris entre 0 et 100 %, représentent la proportion de contrôles réussis par rapport à tous vos contrôles activés. Pour plus d'informations

sur ces scores, consultezMéthode de calcul des scores de sécurité. Ce widget vous aide à comprendre votre position globale en matière de sécurité.

Les actifs ayant obtenu le plus de résultats

Fournit une vue d'ensemble des ressources, des comptes et des applications qui présentent le plus de résultats. La liste est triée par ordre décroissant selon le nombre de résultats. Dans le widget, chaque onglet affiche les six principaux éléments de cette catégorie, regroupés par niveau de gravité et par type de ressource. Si vous choisissez un chiffre dans la colonne Total des résultats, Security Hub CSPM ouvre une page qui affiche les résultats de l'actif. Ce widget vous permet d'identifier rapidement quels actifs principaux présentent des menaces de sécurité potentielles.

Résultats par région

Indique le nombre total de résultats, regroupés par niveau de gravité, pour chacun des Région AWS cas dans lesquels Security Hub CSPM est activé. Ce widget vous permet d'identifier les problèmes de sécurité susceptibles d'affecter certaines régions. Si vous ouvrez le tableau de bord dans votre région d'agrégation, ce widget vous permet de surveiller les problèmes de sécurité potentiels dans chaque région liée.

Types de menaces les plus courants

Fournit une ventilation des 10 types de menaces les plus courants dans votre AWS environnement. Cela inclut des menaces telles que l'augmentation des privilèges, l'utilisation d'informations d'identification exposées ou la communication avec des adresses IP malveillantes.

Pour consulter ces données, Amazon GuardDuty doit être activé. Si c'est le cas, choisissez un type de menace dans ce widget pour ouvrir la GuardDuty console et consulter les résultats relatifs à cette menace. Ce widget vous permet d'évaluer les menaces potentielles dans le contexte d'autres problèmes de sécurité.

Vulnérabilités logicielles avec exploits

Fournit un résumé des vulnérabilités logicielles présentes dans votre AWS environnement et dont les exploits sont connus. Vous pouvez également consulter une liste des vulnérabilités pour lesquelles des correctifs sont disponibles et pour lesquels des correctifs sont disponibles.

Pour afficher ces données, Amazon Inspector doit être activé. Si c'est le cas, choisissez une statistique dans ce widget pour ouvrir la console Amazon Inspector et consulter plus de détails sur la vulnérabilité. Ce widget vous permet d'évaluer les vulnérabilités logicielles dans le contexte d'autres problèmes de sécurité.

De nouvelles découvertes au fil du temps

Montre les tendances du nombre de nouvelles découvertes quotidiennes au cours des 90 derniers jours. Vous pouvez ventiler les données par niveau de gravité ou par fournisseur pour plus de contexte. Ce widget vous permet de savoir si le volume de recherche a augmenté ou diminué à des moments précis au cours des 90 derniers jours.

Ressources contenant le plus de résultats

Fournit un résumé des ressources qui ont généré le plus de résultats, ventilées selon les types de ressources suivants : compartiments Amazon Simple Storage Service (Amazon S3), instances Amazon Elastic Compute Cloud (Amazon EC2) et AWS Lambda fonctions.

Dans le widget, chaque onglet se concentre sur l'un des types de ressources précédents et répertorie les 10 instances de ressources qui ont généré le plus de résultats. Pour passer en revue les résultats d'une ressource spécifique, choisissez l'instance de ressource. Ce widget vous permet de trier les résultats de sécurité associés à des AWS ressources communes.

Widgets masqués par défaut

Les widgets suivants sont également disponibles pour le tableau de bord Résumé, mais ils sont masqués par défaut.

AMI présentant le plus grand nombre de résultats

Fournit une liste des 10 Amazon Machine Images (AMI) qui ont généré le plus de résultats. Ces données ne sont disponibles que si Amazon EC2 est activé pour votre compte. Il vous aide à identifier les AMI qui présentent des risques de sécurité potentiels.

Directeurs IAM ayant obtenu le plus de résultats

Fournit une liste des 10 utilisateurs Gestion des identités et des accès AWS (IAM) qui ont généré le plus de résultats. Ce widget vous permet d'effectuer des tâches administratives et de facturation. Il vous indique quels utilisateurs contribuent le plus à l'utilisation de Security Hub CSPM.

Comptes présentant le plus grand nombre de résultats (par gravité)

Affiche un graphique des 10 comptes qui ont généré le plus de résultats, regroupés par niveau de gravité. Ce widget vous permet de déterminer les comptes sur lesquels concentrer les efforts d'analyse et de correction.

Comptes présentant le plus de résultats (par type de ressource)

Affiche un graphique des 10 comptes qui ont généré le plus de résultats, regroupés par type de ressource. Ce widget vous permet de déterminer les comptes et les types de ressources à prioriser pour l'analyse et la correction.

Perspectives

Répertorie cinq informations gérées par Security Hub CSPM et le nombre de résultats qu'elles ont générés. Les informations identifient un domaine de sécurité spécifique qui nécessite une attention particulière.

Les derniers résultats des AWS intégrations

Indique le nombre de résultats que vous avez reçus d'Integrated dans Security Hub CSPM. Services AWS Il indique également la date à laquelle vous avez reçu les derniers résultats de chaque service intégré. Ce widget fournit des données de résultats consolidées provenant de plusieurs Services AWS. Pour en savoir plus, choisissez un service intégré. Security Hub CSPM ouvre ensuite la console pour ce service.

Filtrer le tableau de bord récapitulatif dans Security Hub CSPM

Vous pouvez organiser le tableau de bord récapitulatif sur la console Security Hub CSPM afin qu'il n'inclue que les données de sécurité les plus pertinentes pour vous. Par exemple, si vous faites partie d'une équipe d'application, vous pouvez créer une vue dédiée pour une application critique dans votre environnement de production. Si vous faites partie d'une équipe de sécurité, vous pouvez créer une vue dédiée qui vous permet de vous concentrer sur les résultats présentant un niveau de gravité élevé.

Pour créer ces vues sélectionnées, entrez des critères de filtre dans la zone de filtre située au-dessus du tableau de bord. Si vous appliquez des critères de filtre, ceux-ci s'appliquent à toutes les données et à tous les widgets du tableau de bord, à l'exception des données des widgets Insights et Security Standards. Pour obtenir la liste des widgets disponibles sur le tableau de bord, consultezWidgets disponibles pour le tableau de bord Summary.

Vous pouvez filtrer les données à l'aide des champs suivants :

- Nom du compte
- ID de compte

- ARN de l'application
- Application name (Nom de l'application)
- Nom du produit (pour un produit Service AWS ou un produit tiers qui envoie des résultats à Security Hub CSPM)
- Enregistrer l'état
- Région
- Balise de ressource
- Sévérité
- État du flux de travail

Par défaut, les données du tableau de bord sont filtrées selon les critères suivants : `Workflow.Status` est `NOTIFIED` ou`NEW`, et `RecordState` est`ACTIVE`. Ces critères apparaissent au-dessus du tableau de bord, en dessous de la zone de filtre. Pour supprimer ces critères, choisissez X dans le jeton de filtre correspondant aux critères que vous souhaitez supprimer.

Si vous appliquez des critères de filtre que vous souhaitez réutiliser, vous pouvez les enregistrer en tant que jeu de filtres. Un ensemble de filtres est un ensemble de critères de filtre que vous créez et enregistrez pour les appliquer à nouveau lorsque vous consultez les données sur le tableau de bord Résumé. Vous pouvez créer et enregistrer un ensemble de filtres qui utilise tous les champs disponibles, à l'exception des champs suivants : ARN de l'application, nom de l'application et balise de ressource.

Création et enregistrement de jeux de filtres

Suivez ces étapes pour créer et enregistrer un ensemble de filtres.

Pour créer et enregistrer un ensemble de filtres

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Résumé.
3. Dans la zone de filtre située au-dessus du tableau de bord Résumé, entrez les critères de filtre pour le jeu de filtres.
4. Dans le menu Effacer les filtres, choisissez Enregistrer le nouveau jeu de filtres.
5. Dans la boîte de dialogue Enregistrer le jeu de filtres, entrez un nom pour le jeu de filtres.

6. (Facultatif) Pour utiliser le filtre défini par défaut chaque fois que vous ouvrez la page Résumé, sélectionnez l'option permettant de la définir comme affichage par défaut.
7. Choisissez Enregistrer.

Pour basculer entre les ensembles de filtres que vous avez créés et enregistrés, utilisez le menu Choisir un ensemble de filtres situé au-dessus du tableau de bord Résumé. Lorsque vous sélectionnez un ensemble de filtres, Security Hub CSPM applique les critères du jeu de filtres aux données du tableau de bord.

Mettre à jour ou supprimer des ensembles de filtres

Suivez ces étapes pour mettre à jour ou supprimer un ensemble de filtres existant. Si vous supprimez un ensemble de filtres qui est actuellement défini comme affichage par défaut du tableau de bord Résumé, votre affichage par défaut est réinitialisé à l'affichage CSPM par défaut de Security Hub.

Pour mettre à jour ou supprimer un ensemble de filtres

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Résumé.
3. Dans le menu Choisir un ensemble de filtres situé au-dessus de la page Résumé, choisissez le jeu de filtres.
4. Dans le menu Effacer les filtres, effectuez l'une des opérations suivantes :
   - Pour mettre à jour le jeu de filtres, choisissez Mettre à jour le jeu de filtres actuel. Entrez ensuite vos modifications dans la boîte de dialogue qui apparaît.
   - Pour supprimer le jeu de filtres, choisissez Supprimer le jeu de filtres actuel. Choisissez ensuite Supprimer dans la boîte de dialogue qui s'affiche.

Personnalisation du tableau de bord récapitulatif dans Security Hub CSPM

Vous pouvez personnaliser le tableau de bord récapitulatif de la console Security Hub CSPM de plusieurs manières. Par exemple, vous pouvez ajouter et supprimer des widgets dans le tableau de bord. Vous pouvez également réorganiser et redimensionner les widgets sur le tableau de bord. Pour obtenir la liste des widgets disponibles et une description de chacun d'entre eux, consultezWidgets disponibles pour le tableau de bord Summary.

Si vous personnalisez le tableau de bord, Security Hub CSPM applique immédiatement vos modifications et enregistre les nouveaux paramètres de votre tableau de bord. Vos modifications s'appliquent à votre affichage du tableau de bord dans tous Régions AWS les navigateurs.

Pour personnaliser le Résumé tableau de bord

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, choisissez Résumé.
3. Effectuez l'une des actions suivantes :

   - Pour ajouter un widget, choisissez Ajouter des widgets dans le coin supérieur droit de la page. Dans la barre de recherche, saisissez le titre du widget à ajouter. Faites ensuite glisser le widget vers l'emplacement de votre choix.
   - Pour supprimer un widget, choisissez les trois points dans le coin supérieur droit du widget.
   - Pour déplacer un widget, choisissez la poignée située dans le coin supérieur gauche du widget, puis faites glisser le widget vers l'emplacement de votre choix.
   - Pour modifier la taille d'un widget, choisissez la poignée de redimensionnement dans le coin inférieur droit du widget. Faites glisser le bord du widget jusqu'à ce que le widget atteigne la taille de votre choix.

Pour rétablir ultérieurement les paramètres d'origine, choisissez Rétablir la mise en page par défaut en haut de la page.

Limites régionales pour Security Hub CSPM

Certaines fonctionnalités du AWS Security Hub CSPM ne sont disponibles que dans certains cas. Régions AWS Les sections suivantes précisent ces limites régionales. Pour une liste complète de toutes les régions dans lesquelles Security Hub CSPM est actuellement disponible, consultez la section Points de terminaison et quotas du AWS Security Hub dans le. Références générales AWS

Cross-Region restrictions d'agrégation

DansAWS GovCloud (US) Regions, l'agrégation entre régions est disponible pour les résultats, la recherche de mises à jour et les informations AWS GovCloud (US) Regions uniquement. Plus précisément, vous pouvez agréger les résultats, rechercher des mises à jour et des informations uniquement entre les régions AWS GovCloud AWS GovCloud (US-EastUS-West) et ().

Dans les régions de Chine, l'agrégation entre régions est disponible uniquement pour les résultats, les mises à jour et les informations concernant les régions de Chine. Plus précisément, vous pouvez agréger les résultats, trouver des mises à jour et des informations uniquement entre les régions de Chine (Pékin) et de Chine (Ningxia).

Vous ne pouvez pas utiliser une région désactivée par défaut comme région d'agrégation. Pour obtenir la liste des régions désactivées par défaut, consultez la section Activer ou désactiver Régions AWS dans votre compte dans le Guide de Gestion de compte AWS référence.

Disponibilité des intégrations par région

Certaines intégrations ne sont pas toutes Régions AWS disponibles. Sur la console Security Hub CSPM, aucune intégration n'apparaît sur la page Intégrations si elle n'est pas disponible dans la région à laquelle vous êtes actuellement connecté.

Intégrations prises en charge dans les régions de Chine (Pékin) et de Chine (Ningxia)

Dans les régions de Chine (Pékin) et de Chine (Ningxia), Security Hub CSPM prend uniquement en charge les intégrations suivantes avec : Services AWS

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems ManagerOpsCenter
- AWS Systems ManagerGestionnaire de correctifs

Dans les régions de Chine (Pékin) et de Chine (Ningxia), Security Hub CSPM prend uniquement en charge les intégrations tierces suivantes :

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar

- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Intégrations prises en charge dans leAWS GovCloud (US-East)andAWS GovCloud (US-West)Régions

Dans les AWS GovCloud (US-West) régions AWS GovCloud (US-East) et, Security Hub CSPM prend uniquement en charge les intégrations suivantes avec : Services AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- Analyseur d'accès IAM
- Amazon Inspector
- AWS IoT Device Defender

Dans les AWS GovCloud (US-West) régions AWS GovCloud (US-East) et, Security Hub CSPM prend uniquement en charge les intégrations tierces suivantes :

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian

- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(disponible uniquement en AWS GovCloud (US-West))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Disponibilité des normes par région

La norme de AWS Control Tower gestion des services n'est disponible que pour les supports concernésRégions AWS. AWS Control Tower Pour obtenir la liste des régions AWS Control Tower actuellement prises en charge, consultez la section How Régions AWS Work AWS Control Tower With du guide de AWS Control Tower l'utilisateur.

La norme de balisage des AWS ressources n'est pas disponible dans la région Asie-Pacifique (Taipei).

D'autres normes de sécurité sont disponibles dans toutes les régions où Security Hub CSPM est actuellement disponible.

Disponibilité des contrôles par région

Certains contrôles CSPM du Security Hub ne sont pas tous disponibles. Régions AWS Pour obtenir la liste des contrôles qui ne sont pas disponibles dans chaque région, consultezLimites régionales des contrôles CSPM du Security Hub.

Sur la console Security Hub CSPM, aucun contrôle n'apparaît dans la liste des contrôles s'il n'est pas disponible dans la région à laquelle vous êtes actuellement connecté. L'exception est une région d'agrégation. Si vous définissez une région d'agrégation et que vous vous connectez à cette région, la console affiche les commandes disponibles dans la région d'agrégation ou dans une ou plusieurs régions liées.

Limites régionales des contrôles CSPM du Security Hub

Certains contrôles CSPM de AWS Security Hub ne sont pas disponibles dans tous. Régions AWS Cette page indique quels contrôles ne sont pas disponibles dans certaines régions.

Sur la console Security Hub CSPM, aucun contrôle n'apparaît dans la liste des contrôles s'il n'est pas disponible dans la région à laquelle vous êtes actuellement connecté. L'exception est une région d'agrégation. Si vous définissez une région d'agrégation et que vous vous connectez à cette région, la console affiche les commandes disponibles dans la région d'agrégation ou dans une ou plusieurs régions liées.

Régions AWS

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Malaisie)

- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Nouvelle Zélande)
- Asie-Pacifique (Osaka)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Taipei)
- Asie-Pacifique (Thaïlande)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Canada-Ouest (Calgary)
- Chine (Pékin)
- Chine (Ningxia)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Milan)
- Europe (Paris)
- Europe (Espagne)
- Europe (Stockholm)
- Europe (Zurich)
- Israël (Tel Aviv)
- Mexique (Centre)
- Middle East (Bahrain)
- Moyen-Orient (EAU)
- Amérique du Sud (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

USA Est (Virginie du Nord)

Les contrôles suivants ne sont pas pris en charge dans la région de l'Est des États-Unis (Virginie du Nord).

- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

USA Est (Ohio)

Les commandes suivantes ne sont pas prises en charge dans la région de l'Est des États-Unis (Ohio).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

USA Ouest (Californie du Nord)

Les commandes suivantes ne sont pas prises en charge dans la région de l'Ouest des États-Unis (Californie du Nord).

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré

- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée

- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données

- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

USA Ouest (Oregon)

Les commandes suivantes ne sont pas prises en charge dans la région Ouest des États-Unis (Oregon).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés

- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Afrique (Le Cap)

Les contrôles suivants ne sont pas pris en charge dans la région Afrique (Le Cap).

- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée

- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager

- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées

- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [RDS.1] L'instantané RDS doit être privé
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie

- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Asie-Pacifique (Hong Kong)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Hong Kong).

- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes

- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées

- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées

- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos

- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Hyderabad)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Hyderabad).

- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock

- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées

- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau

- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé

- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services

- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées

- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité

- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch

- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés

- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Jakarta)

Les commandes suivantes ne sont pas prises en charge dans la région Asie-Pacifique (Jakarta).

- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée

- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager

- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée

- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics

- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée

- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Malaisie)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Malaisie).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée

- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Athena.4] La journalisation des groupes de travail Athena doit être activée
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.2]AWS Backuples points de récupération doivent être étiquetés
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés

- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste

- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.1] la journalisation des DataSync tâches doit être activée
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry

- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine

- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées

- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [ES.9] Les domaines Elasticsearch doivent être balisés
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés

- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.1]AWS Glueles emplois doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM

- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés

- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité

- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée

- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit
- [RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut

- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet

- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux

- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles

- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Melbourne)

Les commandes suivantes ne sont pas prises en charge dans la région Asie-Pacifique (Melbourne).

- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC

- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda

- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés

- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés

- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins

- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés

- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines

- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [RDS.1] L'instantané RDS doit être privé
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS

- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés

- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Mumbai)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Mumbai).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré

- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés

- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Asie-Pacifique (Nouvelle Zélande)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Nouvelle-Zélande).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.1] API Gateway REST et la journalisation de l'exécution des WebSocket API doivent être activés
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.3] Les étapes de l'API REST API Gateway doivent avoir AWS X-Ray traçage activé
- [APIGateway.4] API Gateway doit être associée à une ACL Web WAF

- [APIGateway.5] Les données du cache de l'API REST API Gateway doivent être chiffrées au repos
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Athena.2] Les catalogues de données Athena doivent être balisés
- [Athena.3] Les groupes de travail Athena doivent être étiquetés
- [Athena.4] La journalisation des groupes de travail Athena doit être activée
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2

- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.2]AWS Backuples points de récupération doivent être étiquetés
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées

- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard

- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste
- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.1] la journalisation des DataSync tâches doit être activée
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos

- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR

- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry
- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.172] Les paramètres d'accès public EC2 VPC Block devraient bloquer le trafic de passerelle Internet
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys

- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [ECS.18] Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS
- [ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée
- [ECS.20] Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux
- [ECS.21] Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge

- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.16] Les équilibreurs de charge des applications doivent être associés à un AWS WAF ACL web
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés
- [ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé

- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [ES.9] Les domaines Elasticsearch doivent être balisés
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ

- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.1]AWS Glueles emplois doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.1] GuardDuty doit être activé
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [GuardDuty.3] Les GuardDuty IPsets doivent être balisés
- [GuardDuty.4] les GuardDuty détecteurs doivent être étiquetés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées

- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées

- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé

- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles

- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde

- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit
- [RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge

- [Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public
- [Redshift.3] Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift
- [Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift
- [Redshift.6] Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures
- [Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.11] Les clusters Redshift doivent être balisés
- [Redshift.13] Les instantanés du cluster Redshift doivent être balisés
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions

- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet
- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager
- [SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
- [SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT

- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.1]AWS Transfer Familyles flux de travail doivent être balisés
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.11]AWS WAFla journalisation des ACL Web doit être activée
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Osaka)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Osaka).

- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées

- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée

- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry
- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés

- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public

- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
- [SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Séoul)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Séoul).

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos

- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs

- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Asie-Pacifique (Singapour)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Singapour).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda

- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Asie-Pacifique (Sydney)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Sydney).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut

- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Asie-Pacifique (Taipei)

Les commandes suivantes ne sont pas prises en charge dans la région Asie-Pacifique (Taipei).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [ACM.3] Les certificats ACM doivent être balisés
- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.1] API Gateway REST et la journalisation de l'exécution des WebSocket API doivent être activés
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.3] Les étapes de l'API REST API Gateway doivent avoir AWS X-Ray traçage activé
- [APIGateway.4] API Gateway doit être associée à une ACL Web WAF
- [APIGateway.5] Les données du cache de l'API REST API Gateway doivent être chiffrées au repos
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées

- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Athena.2] Les catalogues de données Athena doivent être balisés
- [Athena.3] Les groupes de travail Athena doivent être étiquetés
- [Athena.4] La journalisation des groupes de travail Athena doit être activée
- [AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser les contrôles de santé ELB
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [AutoScaling.10] Les groupes EC2 Auto Scaling doivent être balisés
- [Autoscaling.5] Les instances Amazon EC2 lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresses IP publiques
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.2]AWS Backuples points de récupération doivent être étiquetés
- [Backup.3]AWS Backuples coffres-forts doivent être étiquetés
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés

- [Backup.5]AWS Backuples plans de sauvegarde doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.2] les CloudFormation piles doivent être étiquetées
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées

- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CloudTrail.9] les CloudTrail sentiers doivent être balisés
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard

- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste
- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.1] la journalisation des DataSync tâches doit être activée
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.1] Les instances de réplication du Database Migration Service ne doivent pas être publiques
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité

- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.5] Les tables DynamoDB doivent être balisées
- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.10] Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2
- [EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.33] Les pièces jointes de la passerelle de transit EC2 doivent être étiquetées
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.35] Les interfaces réseau EC2 doivent être étiquetées

- [EC2.36] Les passerelles client EC2 doivent être étiquetées
- [EC2.37] Les adresses IP Elastic EC2 doivent être balisées
- [EC2.38] Les instances EC2 doivent être étiquetées
- [EC2.39] Les passerelles Internet EC2 doivent être étiquetées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.41] Les ACL du réseau EC2 doivent être balisées
- [EC2.42] Les tables de routage EC2 doivent être étiquetées
- [EC2.43] Les groupes de sécurité EC2 doivent être balisés
- [EC2.44] Les sous-réseaux EC2 doivent être balisés
- [EC2.45] Les volumes EC2 doivent être balisés
- [EC2.46] Les Amazon VPC doivent être balisés
- [EC2.47] Les services de point de terminaison Amazon VPC doivent être balisés
- [EC2.48] Les journaux de flux Amazon VPC doivent être balisés
- [EC2.49] Les connexions d'appairage Amazon VPC doivent être étiquetées
- [EC2.50] Les passerelles VPN EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.52] Les passerelles de transit EC2 doivent être étiquetées
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry
- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager

- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.172] Les paramètres d'accès public EC2 VPC Block devraient bloquer le trafic de passerelle Internet
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.2] Aucune adresse IP publique ne doit être attribuée automatiquement aux services ECS
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur

- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.13] Les services ECS doivent être balisés
- [ECS.14] Les clusters ECS doivent être balisés
- [ECS.15] Les définitions de tâches ECS doivent être étiquetées
- [ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [ECS.18] Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS
- [ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée
- [ECS.20] Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux
- [ECS.21] Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.5] Les points d'accès EFS doivent être balisés
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.1] Les points de terminaison du cluster EKS ne doivent pas être accessibles au public
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.6] Les clusters EKS doivent être balisés

- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.3] Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS
- [ELB.7] Le drainage des connexions doit être activé pour les équilibreurs de charge classiques
- [ELB.8] Les équilibreurs de charge classiques dotés d'écouteurs SSL doivent utiliser une politique de sécurité prédéfinie qui est solide AWS Config durée
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.16] Les équilibreurs de charge des applications doivent être associés à un AWS WAF ACL web
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés
- [ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication

- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.1] Le chiffrement au repos doit être activé pour les domaines Elasticsearch
- [ES.2] Les domaines Elasticsearch ne doivent pas être accessibles au public
- [ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [ES.5] La journalisation des audits doit être activée pour les domaines Elasticsearch
- [ES.6] Les domaines Elasticsearch doivent comporter au moins trois nœuds de données
- [ES.7] Les domaines Elasticsearch doivent être configurés avec au moins trois nœuds principaux dédiés
- [ES.8] Les connexions aux domaines Elasticsearch doivent être chiffrées conformément à la dernière politique de sécurité TLS
- [ES.9] Les domaines Elasticsearch doivent être balisés
- [EventBridge.2] les bus EventBridge d'événements doivent être étiquetés
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources

- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.1]AWS Glueles emplois doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.1] GuardDuty doit être activé
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [GuardDuty.3] Les GuardDuty IPsets doivent être balisés
- [GuardDuty.4] les GuardDuty détecteurs doivent être étiquetés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée

- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM

- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.23] Les analyseurs IAM Access Analyzer doivent être étiquetés
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés

- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.2] Les flux Kinesis doivent être balisés
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.3]AWS KMS keysne doit pas être supprimé par inadvertance
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.6] Les fonctions Lambda doivent être balisées
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée

- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.7] Les pare-feux Network Firewall doivent être étiquetés
- [NetworkFirewall.8] Les politiques de pare-feu de Network Firewall doivent être étiquetées
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall

- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.16] Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.17] Les instances de base de données RDS doivent être configurées pour copier les balises dans les instantanés
- [RDS.19] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements de cluster critiques
- [RDS.20] Les abonnements de notification d'événements RDS existants doivent être configurés pour les événements d'instance de base de données critiques
- [RDS.21] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements de groupe de paramètres de base de données critiques
- [RDS.22] Un abonnement aux notifications d'événements RDS doit être configuré pour les événements critiques du groupe de sécurité des bases de données
- [RDS.23] Les instances RDS ne doivent pas utiliser le port par défaut d'un moteur de base de données

- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.28] Les clusters de bases de données RDS doivent être balisés
- [RDS.29] Les instantanés du cluster de bases de données RDS doivent être balisés
- [RDS.30] Les instances de base de données RDS doivent être balisées
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.32] Les instantanés de base de données RDS doivent être balisés
- [RDS.33] Les groupes de sous-réseaux de base de données RDS doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit
- [RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit

- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public
- [Redshift.2] Les connexions aux clusters Amazon Redshift doivent être chiffrées pendant le transit
- [Redshift.3] Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift
- [Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift
- [Redshift.6] Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures
- [Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.11] Les clusters Redshift doivent être balisés
- [Redshift.12] Les abonnements aux notifications d'événements Redshift doivent être balisés
- [Redshift.13] Les instantanés du cluster Redshift doivent être balisés
- [Redshift.14] Les groupes de sous-réseaux du cluster Redshift doivent être balisés
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés

- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet
- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie

- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés

- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [SecretsManager.1] La rotation automatique des secrets des secrets de Secrets Manager doit être activée
- [SecretsManager.2] Les secrets de Secrets Manager configurés avec une rotation automatique devraient être correctement pivotés
- [SecretsManager.3] Supprimer les secrets inutilisés du Gestionnaire de Secrets
- [SecretsManager.4] Les secrets de Secrets Manager doivent être renouvelés dans un délai spécifié
- [SecretsManager.5] Les secrets de Secrets Manager doivent être balisés
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.3] Les sujets SNS doivent être balisés
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.1] Les instances Amazon EC2 doivent être gérées parAWS Systems Manager
- [SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
- [SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [StepFunctions.2] Les activités de Step Functions doivent être étiquetées

- [Transfer.1]AWS Transfer Familyles flux de travail doivent être balisés
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.11]AWS WAFla journalisation des ACL Web doit être activée
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Thaïlande)

Les contrôles suivants ne sont pas pris en charge dans la région Asie-Pacifique (Thaïlande).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS

- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Athena.2] Les catalogues de données Athena doivent être balisés
- [Athena.3] Les groupes de travail Athena doivent être étiquetés
- [Athena.4] La journalisation des groupes de travail Athena doit être activée
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.2]AWS Backuples points de récupération doivent être étiquetés
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés

- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste

- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.1] la journalisation des DataSync tâches doit être activée
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry

- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.172] Les paramètres d'accès public EC2 VPC Block devraient bloquer le trafic de passerelle Internet
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte

- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [ECS.18] Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS
- [ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée
- [ECS.20] Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux
- [ECS.21] Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées

- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques

- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [ES.9] Les domaines Elasticsearch doivent être balisés
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.1]AWS Glueles emplois doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.1] GuardDuty doit être activé
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée

- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe

- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés

- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié

- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds

- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit

- [RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public

- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet
- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1

- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public

- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.1]AWS Transfer Familyles flux de travail doivent être balisés
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos

- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Asie-Pacifique (Tokyo)

Les commandes suivantes ne sont pas prises en charge dans la région Asie-Pacifique (Tokyo).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés

- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Canada (Centre)

Les contrôles suivants ne sont pas pris en charge dans la région du Canada (Centre).

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé

- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés

- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Canada-Ouest (Calgary)

Les commandes suivantes ne sont pas prises en charge dans la région de l'Ouest du Canada (Calgary).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Athena.4] La journalisation des groupes de travail Athena doit être activée
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés

- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine

- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos

- [DataSync.1] la journalisation des DataSync tâches doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde

- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry
- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée

- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine

- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé

- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos

- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole

- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées

- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier

- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall

- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch

- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit
- [RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public

- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet
- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1

- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos

- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Chine (Pékin)

Les contrôles suivants ne sont pas pris en charge dans la région Chine (Pékin).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits

- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés

- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard

- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste
- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés

- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.36] Les passerelles client EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager

- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés
- [ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [GuardDuty.3] Les GuardDuty IPsets doivent être balisés
- [GuardDuty.4] les GuardDuty détecteurs doivent être étiquetés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée

- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.23] Les analyseurs IAM Access Analyzer doivent être étiquetés
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées

- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles

- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.7] La protection contre la suppression des clusters RDS doit être activée
- [RDS.12] L'authentification IAM doit être configurée pour les clusters RDS
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité
- [RDS.16] Les clusters de base de données Aurora doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé

- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.28] Les clusters de bases de données RDS doivent être balisés
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés

- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet
- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Chine (Ningxia)

Les contrôles suivants ne sont pas pris en charge dans la région Chine (Ningxia).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée

- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes

- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés

- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste
- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde

- [EC2.36] Les passerelles client EC2 doivent être étiquetées
- [EC2.50] Les passerelles VPN EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés
- [ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés

- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [GuardDuty.3] Les GuardDuty IPsets doivent être balisés
- [GuardDuty.4] les GuardDuty détecteurs doivent être étiquetés
- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée

- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.23] Les analyseurs IAM Access Analyzer doivent être étiquetés
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées

- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public
- [Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge
- [Lambda.3] Les fonctions Lambda doivent se trouver dans un VPC
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.6] Les fonctions Lambda doivent être balisées
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds

- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante

- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée

- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.2] Les activités de Step Functions doivent être étiquetées
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Europe (Francfort)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Francfort).

- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit

- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Europe (Irlande)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Irlande).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée

- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Europe (Londres)

Les commandes suivantes ne sont pas prises en charge dans la région Europe (Londres).

- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée

- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés

- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

Europe (Milan)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Milan).

- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée

- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés

- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos

- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [RDS.1] L'instantané RDS doit être privé
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SSM.2] Les instances Amazon EC2 gérées par Systems Manager doivent avoir un statut de conformité aux correctifs de COMPLIANT après l'installation d'un correctif
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Europe (Paris)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Paris).

- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés

- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés

- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie

- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Europe (Espagne)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Espagne).

- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes

- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés

- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics

- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.1] Les instantanés Amazon EBS ne doivent pas être configurés pour être restaurables publiquement
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2

- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées

- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés

- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Lambda.1] Les politiques relatives à la fonction Lambda devraient interdire l'accès public
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch

- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [RDS.1] L'instantané RDS doit être privé
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch

- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées

- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Europe (Stockholm)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Stockholm).

- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés

- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée

- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés

- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Europe (Zurich)

Les contrôles suivants ne sont pas pris en charge dans la région Europe (Zurich).

- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés

- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine

- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL

- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)

- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée

- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées

- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster

- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée

- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [RDS.1] L'instantané RDS doit être privé
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée

- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Israël (Tel Aviv)

Les contrôles suivants ne sont pas pris en charge dans la région d'Israël (Tel Aviv).

- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2

- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit

- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée

- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés

- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry
- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS

- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [ELB.2] Les équilibreurs de charge classiques avec SSL/HTTPS écouteurs doivent utiliser un certificat fourni par AWS Certificate Manager
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch

- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole

- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus
- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées

- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé

- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [RDS.1] L'instantané RDS doit être privé
- [RDS.4] Les instantanés du cluster RDS et les instantanés de base de données doivent être chiffrés au repos
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.29] Les instantanés du cluster de bases de données RDS doivent être balisés
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch

- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé

- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Mexique (Centre)

Les commandes suivantes ne sont pas prises en charge dans la région du Mexique (Centre).

- [ACM.1] Importé et ACM-issued les certificats doivent être renouvelés après une période spécifiée
- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits

- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Athena.4] La journalisation des groupes de travail Athena doit être activée
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.2]AWS Backuples points de récupération doivent être étiquetés
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés

- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes

- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CloudTrail.7] Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.1] Les URL du référentiel source CodeBuild Bitbucket ne doivent pas contenir d'informations d'identification sensibles
- [CodeBuild.2] les variables d'environnement CodeBuild du projet ne doivent pas contenir d'informations d'identification en texte clair
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste

- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos
- [DataSync.1] la journalisation des DataSync tâches doit être activée
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate

- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde
- [DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.34] Les tables de routage de la passerelle de transit EC2 doivent être balisées
- [EC2.40] Les passerelles NAT EC2 doivent être étiquetées
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants
- [EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'administration des serveurs distants
- [EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR
- [EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry

- [EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.171] La journalisation des connexions VPN EC2 doit être activée
- [EC2.172] Les paramètres d'accès public EC2 VPC Block devraient bloquer le trafic de passerelle Internet
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.182] Les paramètres de blocage de l'accès public doivent être activés pour les instantanés Amazon EBS
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte

- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [ECS.18] Les définitions de tâches ECS doivent utiliser le chiffrement en transit pour les volumes EFS
- [ECS.19] Les fournisseurs de capacité ECS devraient avoir activé la protection des terminaisons gérée
- [ECS.20] Les définitions de tâches ECS doivent configurer les utilisateurs non root dans les définitions de conteneurs Linux
- [ECS.21] Les définitions de tâches ECS doivent configurer les utilisateurs non administrateurs dans les définitions de conteneurs Windows
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement
- [EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS
- [EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés
- [EKS.7] Les configurations du fournisseur d'identité EKS doivent être balisées

- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques

- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.3] Les domaines Elasticsearch doivent crypter les données envoyées entre les nœuds
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [ES.9] Les domaines Elasticsearch doivent être balisés
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.1]AWS Glueles emplois doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.1] GuardDuty doit être activé
- [GuardDuty.2] GuardDuty les filtres doivent être balisés

- [GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée
- [GuardDuty.6] La protection GuardDuty Lambda doit être activée
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.10] La protection GuardDuty S3 doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.7] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.10] Les politiques de mot de passe pour les utilisateurs IAM doivent avoir des configurations strictes
- [IAM.11] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre majuscule
- [IAM.12] Assurez-vous que la politique de mot de passe IAM nécessite au moins une lettre minuscule
- [IAM.13] Assurez-vous que la politique de mot de passe IAM nécessite au moins un symbole
- [IAM.14] Assurez-vous que la politique de mot de passe IAM nécessite au moins un chiffre
- [IAM.15] Assurez-vous que la politique de mot de passe IAM exige une longueur de mot de passe minimale de 14 ou plus

- [IAM.16] Assurez-vous que la politique de mot de passe IAM empêche la réutilisation des mots de passe
- [IAM.17] Assurez-vous que la politique de mot de passe IAM expire les mots de passe dans un délai de 90 jours ou moins
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoT.4]AWS IoT Coreles autorisateurs doivent être étiquetés
- [IoT.5]AWS IoT Coreles alias de rôle doivent être balisés
- [IoT.6]AWS IoT Coreles politiques doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées

- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch
- [MQ.4] Les courtiers Amazon MQ doivent être étiquetés
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé

- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines

- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch
- [RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch

- [RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit
- [RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit
- [RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.1] Les clusters Amazon Redshift devraient interdire l'accès public
- [Redshift.2] Les connexions aux clusters Amazon Redshift doivent être chiffrées pendant le transit
- [Redshift.3] Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift
- [Redshift.4] La journalisation des audits doit être activée sur les clusters Amazon Redshift
- [Redshift.6] Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures
- [Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.11] Les clusters Redshift doivent être balisés

- [Redshift.13] Les instantanés du cluster Redshift doivent être balisés
- [Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes
- [Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.7] Les compartiments S3 à usage général doivent utiliser la réplication entre régions
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet

- [S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux

- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [ServiceCatalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.3] Les instances Amazon EC2 gérées par Systems Manager doivent avoir le statut de conformité des associations COMPLIANT
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée

- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Middle East (Bahrain)

Les contrôles suivants ne sont pas pris en charge dans la région Moyen-Orient (Bahreïn).

- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public

- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.10] Les magasins de données sur les événements CloudTrail du lac doivent être chiffrés et gérés par le clientAWS KMS keys
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos

- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DocumentDB.6] Les clusters Amazon DocumentDB doivent être chiffrés pendant le transport
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.20] Les deux tunnels VPN pour un AWS Site-to-Site La connexion VPN devrait être active
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys
- [ECS.17] Les définitions de tâches ECS ne doivent pas utiliser le mode réseau hôte
- [EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés

- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ
- [FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ
- [FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport

- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [NetworkFirewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.41] Les instances de base de données RDS pour SQL Server doivent être chiffrées en transit
- [RDS.42] Les instances de base de données RDS pour MariaDB doivent publier des journaux dans Logs CloudWatch
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.44] Les instances de base de données RDS pour MariaDB doivent être chiffrées en transit
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-réseaux publics comportant des itinéraires vers des passerelles Internet
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.4] Les espaces de noms Redshift Serverless doivent être chiffrés et gérés par le clientAWS KMS keys
- [RedshiftServerless.5] Les espaces de noms Redshift Serverless ne doivent pas utiliser le nom d'utilisateur administrateur par défaut
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.8] les instances de SageMaker bloc-notes doivent fonctionner sur les plates-formes prises en charge
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [Transfer.3] La journalisation des connecteurs Transfer Family doit être activée
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Moyen-Orient (EAU)

Les contrôles suivants ne sont pas pris en charge dans la région du Moyen-Orient (Émirats arabes unis).

- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées

- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFormation.3] la protection contre les terminaisons doit être activée pour les CloudFormation piles
- [CloudFormation.4] les CloudFormation piles doivent avoir des rôles de service associés
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés

- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudTrail.6] Assurez-vous que le compartiment S3 utilisé pour stocker les CloudTrail journaux n'est pas accessible au public
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [Detective.1] Les graphes de comportement des détectives doivent être balisés
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.3] Les abonnements aux événements DMS doivent être étiquetés
- [DMS.4] Les instances de réplication DMS doivent être étiquetées
- [DMS.5] Les groupes de sous-réseaux de réplication DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée

- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune
- [DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé
- [DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS
- [DMS.13] Les instances de réplication DMS doivent être configurées pour utiliser plusieurs zones de disponibilité
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.4] Les instances EC2 arrêtées doivent être supprimées après une période spécifiée
- [EC2.14] Les groupes de sécurité ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 ou : :/0 vers le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés

- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [EC2.180] La source/destination vérification doit être activée sur les interfaces réseau EC2
- [EC2.181] Les modèles de lancement EC2 doivent activer le chiffrement pour les volumes EBS attachés
- [EC2.183] Les connexions VPN EC2 doivent utiliser le protocole IKEv2
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [EFS.1] Elastic File System doit être configuré pour crypter les données des fichiers au repos à l'aide de AWS KMS
- [EFS.2] Les volumes Amazon EFS doivent figurer dans les plans de sauvegarde
- [EKS.9] Les groupes de nœuds EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées
- [ELB.18] Les auditeurs de l'application et de l'équilibreur de charge réseau doivent utiliser des protocoles sécurisés pour crypter les données en transit
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés

- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.1] Les nœuds principaux du cluster Amazon EMR ne doivent pas avoir d'adresses IP publiques
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.4]AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue
- [GuardDuty.2] GuardDuty les filtres doivent être balisés
- [IAM.1] Les politiques IAM ne doivent pas autoriser des privilèges administratifs « * » complets
- [IAM.2] Les utilisateurs IAM ne doivent pas être associés à des politiques IAM
- [IAM.3] Les clés d'accès des utilisateurs IAM doivent être renouvelées tous les 90 jours ou moins
- [IAM.4] La clé d'accès de l'utilisateur root IAM ne doit pas exister
- [IAM.5] La MFA doit être activée pour tous les utilisateurs IAM disposant d'un mot de passe de console
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.8] Les informations d'identification utilisateur IAM non utilisées doivent être supprimées
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.18] Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avecAWS Support
- [IAM.19] Le MFA doit être activé pour tous les utilisateurs IAM
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.22] Les informations d'identification utilisateur IAM non utilisées pendant 45 jours doivent être supprimées
- [IAM.24] Les rôles IAM doivent être balisés

- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.27] La AWSCloudShellFullAccess politique ne doit pas être attachée aux identités IAM
- [Inspector.1] La numérisation Amazon Inspector EC2 doit être activée
- [Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [KMS.1] Les politiques gérées par le client IAM ne doivent pas autoriser les actions de déchiffrement sur toutes les clés KMS
- [KMS.2] Les principaux IAM ne devraient pas avoir de politiques IAM en ligne autorisant les actions de déchiffrement sur toutes les clés KMS
- [Lambda.7] Les fonctions Lambda doivent avoir AWS X-Ray traçage actif activé
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée

- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.4] L'accès public aux clusters MSK doit être désactivé
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [MSK.6] Les clusters MSK doivent désactiver l'accès non authentifié
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [Opensearch.9] OpenSearch les domaines doivent être balisés
- [Opensearch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logicielle installée
- [Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.18] Les déploiements doivent être activés pour les clusters Redshift Multi-AZ
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés

- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails

- [SQS.1] Les files d'attente Amazon SQS doivent être chiffrées au repos
- [SQS.2] Les files d'attente SQS doivent être étiquetées
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [SSM.7] Le paramètre de blocage du partage public doit être activé pour les documents SSM
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

Amérique du Sud (São Paulo)

Les contrôles suivants ne sont pas pris en charge dans la région Amérique du Sud (São Paulo).

- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public

- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés

- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoT.1]AWS IoT Device Defenderles profils de sécurité doivent être balisés
- [IoT.2]AWS IoT Coreles mesures d'atténuation doivent être étiquetées
- [IoT.3]AWS IoT Coreles dimensions doivent être étiquetées
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS

- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles

AWS GovCloud (US-East)

Les commandes suivantes ne sont pas prises en charge dans la AWS GovCloud (US-East) Région.

- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées

- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2
- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public

- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées
- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard

- [Cognito.2] Les pools d'identités Cognito ne doivent pas autoriser les identités non authentifiées
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste
- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [Connect.2] La CloudWatch journalisation des instances Connect Customer doit être activée
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL
- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés

- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.47] Les services de point de terminaison Amazon VPC doivent être balisés
- [EC2.52] Les passerelles de transit EC2 doivent être étiquetées
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées
- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur

- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés
- [ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés
- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés

- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes
- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [Glue.3]AWS Glueles transformations de machine learning doivent être cryptées au repos
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.9] La MFA doit être activée pour l'utilisateur root

- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées
- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby

- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall

- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos
- [RDS.31] Les groupes de sécurité RDS DB doivent être balisés
- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données

- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS
- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.1] Les instances Amazon SageMaker Notebook ne doivent pas disposer d'un accès direct à Internet

- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.16] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les conteneurs principaux
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés
- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SageMaker.19] SageMaker les modèles doivent utiliser un registre privé dans VPC pour les pipelines d'inférence multi-conteneurs
- [SES.1] Les listes de contacts SES doivent être étiquetées
- [SES.2] Les ensembles de configuration SES doivent être étiquetés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails

- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [SSM.6] La CloudWatch journalisation devrait être activée dans SSM Automation
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [StepFunctions.2] Les activités de Step Functions doivent être étiquetées
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles
- [WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos
- [WorkSpaces.2] les volumes WorkSpaces racine doivent être chiffrés au repos

AWS GovCloud (US-West)

Les commandes suivantes ne sont pas prises en charge dans la AWS GovCloud (US-West) Région.

- [ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits

- [Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS
- [Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization
- [APIGateway.2] Les étapes de l'API REST API Gateway doivent être configurées pour utiliser des certificats SSL pour l'authentification du backend
- [APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [APIGateway.10] Les intégrations d'API Gateway V2 doivent utiliser le protocole HTTPS pour les connexions privées
- [APIGateway.11] Les noms de domaine API Gateway doivent utiliser les politiques de sécurité recommandées
- [Amplify.1] Les applications Amplify doivent être étiquetées
- [Amplify.2] Les branches Amplify doivent être étiquetées
- [AppConfig.1]AWS AppConfigles applications doivent être étiquetées
- [AppConfig.2]AWS AppConfigles profils de configuration doivent être balisés
- [AppConfig.3]AWS AppConfigles environnements doivent être balisés
- [AppConfig.4]AWS AppConfigles associations d'extensions doivent être étiquetées
- [AppFlow.1] AppFlow Les flux Amazon doivent être balisés
- [AppRunner.1] Les services App Runner doivent être balisés
- [AppRunner.2] Les connecteurs VPC App Runner doivent être étiquetés
- [AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos
- [AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée
- [AppSync.4]AWS AppSyncLes API GraphQL doivent être balisées
- [AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API
- [AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport
- [AutoScaling.2] Le groupe Amazon EC2 Auto Scaling doit couvrir plusieurs zones de disponibilité
- [AutoScaling.3] Les configurations de lancement du groupe Auto Scaling doivent configurer les instances EC2 pour qu'elles nécessitent le service de métadonnées d'instance version 2 (IMDSv2)
- [AutoScaling.6] Les groupes Auto Scaling doivent utiliser plusieurs types d'instances dans plusieurs zones de disponibilité
- [AutoScaling.9] Les groupes Amazon EC2 Auto Scaling doivent utiliser les modèles de lancement Amazon EC2

- [Backup.4]AWS Backuples plans de rapport doivent être étiquetés
- [Batch.1] Les files d'attente de tâches par lots doivent être étiquetées
- [Batch.2] Les politiques de planification par lots doivent être étiquetées
- [Batch.3] Les environnements de calcul par lots doivent être balisés
- [Batch.4] Les propriétés des ressources de calcul dans les environnements de calcul Batch gérés doivent être balisées
- [BedrockAgentCore.1] Les environnements d' AgentCore exécution de Bedrock doivent être configurés en mode réseau VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways devrait exiger une autorisation pour les demandes entrantes
- [BedrockAgentCore.3] La AgentCore mémoire Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.4] La AgentCore passerelle Bedrock doit être cryptée et gérée par le clientAWS KMSclés
- [BedrockAgentCore.5] Les navigateurs AgentCore personnalisés de Bedrock ne doivent pas utiliser le mode réseau public
- [BedrockAgentCore.6] L'enregistrement de session devrait être activé dans les navigateurs AgentCore personnalisés Bedrock
- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine configuré par défaut
- [CloudFront.3] CloudFront les distributions devraient nécessiter un cryptage en transit
- [CloudFront.4] CloudFront les distributions doivent avoir le basculement d'origine configuré
- [CloudFront.5] CloudFront les distributions doivent avoir la journalisation activée
- [CloudFront.6] CloudFront les distributions doivent avoir le WAF activé
- [CloudFront.7] CloudFront les distributions doivent utiliser des SSL/TLS certificats personnalisés
- [CloudFront.8] CloudFront les distributions doivent utiliser le SNI pour traiter les requêtes HTTPS
- [CloudFront.9] CloudFront les distributions doivent crypter le trafic vers des origines personnalisées
- [CloudFront.10] CloudFront les distributions ne doivent pas utiliser de protocoles SSL obsolètes entre les emplacements périphériques et les origines personnalisées
- [CloudFront.12] CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes
- [CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine
- [CloudFront.14] les CloudFront distributions doivent être étiquetées

- [CloudFront.15] CloudFront les distributions doivent utiliser la politique de sécurité TLS recommandée
- [CloudFront.16] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine pour les origines des URL des fonctions Lambda
- [CloudFront.17] CloudFront les distributions doivent utiliser des groupes de clés fiables pour les URL signées et les cookies
- [CloudWatch.17] les actions CloudWatch d'alarme doivent être activées
- [CodeArtifact.1] les CodeArtifact référentiels doivent être balisés
- [CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés
- [CodeBuild.4] les environnements de CodeBuild projet doivent avoir une journalisationAWS Configdurée
- [CodeGuruProfiler.1] Les groupes de CodeGuru profilage de profileurs doivent être balisés
- [CodeGuruReviewer.1] Les associations de référentiels des CodeGuru réviseurs doivent être étiquetées
- [Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard
- [Cognito.3] Les politiques de mots de passe pour les groupes d'utilisateurs Cognito doivent être configurées de manière robuste
- [Cognito.4] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour une authentification personnalisée
- [Cognito.5] Le MFA doit être activé pour les groupes d'utilisateurs Cognito
- [Cognito.6] La protection contre la suppression des groupes d'utilisateurs Cognito doit être activée
- [Connect.1] Les types d'objets des profils clients Amazon Connect doivent être balisés
- [DataSync.2] DataSync les tâches doivent être étiquetées
- [DMS.2] Les certificats DMS doivent être balisés
- [DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée
- [DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée
- [DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée
- [DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL

- [DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos
- [DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate
- [DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- [DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch
- [DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée
- [DynamoDB.3] Les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- [DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit
- [EC2.21] Les ACL réseau ne doivent pas autoriser l'entrée à partir de la version 0.0.0. 0/0 vers le port 22 ou le port 3389
- [EC2.22] Les groupes de sécurité Amazon EC2 non utilisés doivent être supprimés
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [EC2.24] Les types d'instances paravirtuelles Amazon EC2 ne doivent pas être utilisés
- [EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde
- [EC2.38] Les instances EC2 doivent être étiquetées
- [EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager
- [EC2.60] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager
- [EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)
- [EC2.173] Les demandes EC2 Spot Fleet avec paramètres de lancement doivent permettre le chiffrement des volumes EBS attachés
- [EC2.174] Les ensembles d'options DHCP EC2 doivent être balisés
- [EC2.175] Les modèles de lancement EC2 doivent être balisés
- [EC2.176] Les listes de préfixes EC2 doivent être étiquetées

- [EC2.177] Les sessions EC2 Traffic Mirror doivent être étiquetées
- [EC2.178] Les filtres de rétroviseurs EC2 doivent être étiquetés
- [EC2.179] Les cibles du miroir de trafic EC2 doivent être étiquetées
- [ECR.1] Les référentiels privés ECR doivent avoir la numérisation d'images configurée
- [ECR.2] Les référentiels privés ECR doivent avoir l'immuabilité des balises configurée
- [ECR.3] Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée
- [ECR.4] Les référentiels publics ECR doivent être étiquetés
- [ECS.3] Les définitions de tâches ECS ne doivent pas partager l'espace de noms de processus de l'hôte
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ECS.5] Les définitions de tâches ECS doivent configurer les conteneurs de manière à ce qu'ils soient limités à l'accès en lecture seule aux systèmes de fichiers racine
- [ECS.8] Les secrets ne doivent pas être transmis en tant que variables d'environnement de conteneur
- [ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation
- [ECS.10] Les services ECS Fargate doivent fonctionner sur la dernière version de la plateforme Fargate
- [ECS.12] Les clusters ECS doivent utiliser Container Insights
- [EFS.3] Les points d'accès EFS devraient appliquer un répertoire racine
- [EFS.4] Les points d'accès EFS devraient renforcer l'identité de l'utilisateur
- [EKS.2] Les clusters EKS doivent fonctionner sur une version de Kubernetes prise en charge
- [EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée
- [ELB.10] L'équilibreur de charge classique doit couvrir plusieurs zones de disponibilité
- [ELB.12] L'équilibreur de charge d'application doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.13] Les équilibreurs de charge des applications, des réseaux et des passerelles doivent couvrir plusieurs zones de disponibilité
- [ELB.14] L'équilibreur de charge classique doit être configuré avec le mode défensif ou le mode d'atténuation de désynchronisation le plus strict
- [ELB.21] Les groupes cibles de l'équilibreur de charge des applications et du Network Load Balancer doivent utiliser des protocoles de contrôle de santé chiffrés
- [ELB.22] Les groupes cibles ELB doivent utiliser des protocoles de transport cryptés

- [ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées
- [ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters
- [ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- [ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos
- [ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport
- [ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions antérieures doivent avoir Redis OSS AUTH activé
- [ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut
- [ElasticBeanstalk.1] Les environnements Elastic Beanstalk devraient avoir activé les rapports de santé améliorés
- [ElasticBeanstalk.2] Les mises à jour de la plateforme gérée par Elastic Beanstalk doivent être activées
- [ElasticBeanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch
- [EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
- [EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos
- [EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport
- [ES.4] La journalisation des erreurs du domaine Elasticsearch dans les CloudWatch journaux doit être activée
- [EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- [EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux
- [FraudDetector.1] Les types d'entités Amazon Fraud Detector doivent être balisés
- [FraudDetector.2] Les étiquettes Amazon Fraud Detector doivent être étiquetées
- [FraudDetector.3] Les résultats d'Amazon Fraud Detector doivent être étiquetés
- [FraudDetector.4] Les variables Amazon Fraud Detector doivent être étiquetées
- [FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes

- [FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes
- [GlobalAccelerator.1] Les accélérateurs Global Accelerator doivent être étiquetés
- [GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée
- [GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée
- [GuardDuty.9] GuardDuty La protection RDS doit être activée
- [GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée
- [GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée
- [GuardDuty.13] GuardDuty La surveillance du temps d'exécution EC2 doit être activée
- [IAM.6] Le MFA matériel doit être activé pour l'utilisateur root
- [IAM.9] La MFA doit être activée pour l'utilisateur root
- [IAM.21] Les politiques gérées par le client IAM que vous créez ne doivent pas autoriser les actions génériques pour les services
- [IAM.24] Les rôles IAM doivent être balisés
- [IAM.25] Les utilisateurs IAM doivent être tagués
- [IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé
- [Inspector.3] La numérisation du code Lambda par Amazon Inspector doit être activée
- [IoTSiteWise.1]AWSLes modèles SiteWise d'actifs IoT devraient être étiquetés
- [IoTSiteWise.2]AWS SiteWise Les tableaux de bord de l'IoT doivent être balisés
- [IoTSiteWise.3]AWS SiteWise Les passerelles IoT doivent être étiquetées
- [IoTSiteWise.4]AWS SiteWise Les portails IoT doivent être étiquetés
- [IoTSiteWise.5]AWS SiteWise Les projets IoT doivent être étiquetés
- [IoTTwinMaker.1]AWSLes tâches de TwinMaker synchronisation de l'IoT doivent être étiquetées
- [IoTTwinMaker.2]AWSLes TwinMaker espaces de travail IoT doivent être étiquetés
- [IoTTwinMaker.3]AWSLes TwinMaker scènes IoT doivent être étiquetées
- [IoTTwinMaker.4]AWS TwinMaker Les entités IoT doivent être étiquetées
- [IoTWireless.1]AWSLes groupes de multidiffusion IoT Wireless doivent être étiquetés
- [IoTWireless.2]AWSLes profils de service IoT Wireless doivent être balisés
- [IoTWireless.3]AWSLes tâches IoT FUOTA doivent être étiquetées
- [IVS.1] Les paires de clés de lecture IVS doivent être étiquetées

- [IVS.2] Les configurations d'enregistrement IVS doivent être étiquetées
- [IVS.3] Les canaux IVS doivent être balisés
- [Keyspaces.1] Les espaces de touches Amazon Keyspaces doivent être balisés
- [Kinesis.1] Les flux Kinesis doivent être chiffrés au repos
- [KMS.5] Les clés KMS ne doivent pas être accessibles au public
- [Lambda.5] Les fonctions Lambda du VPC doivent fonctionner dans plusieurs zones de disponibilité
- [Macie.1] Amazon Macie devrait être activé
- [Macie.2] La découverte automatique des données sensibles par Macie doit être activée
- [MQ.5] Les courtiers ActiveMQ doivent utiliser le mode déploiement active/standby
- [MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- [MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier
- [MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée
- [MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport
- [MSK.5] La journalisation des connecteurs MSK doit être activée
- [Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune
- [Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [Neptune.9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité
- [NetworkFirewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité

- [NetworkFirewall.2] La journalisation du Network Firewall doit être activée
- [NetworkFirewall.3] Les politiques de Network Firewall doivent être associées à au moins un groupe de règles
- [NetworkFirewall.4] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets complets.
- [NetworkFirewall.5] L'action apatride par défaut pour les politiques de Network Firewall doit être « drop » ou « forward » pour les paquets fragmentés.
- [NetworkFirewall.6] Le groupe de règles Stateless Network Firewall ne doit pas être vide
- [NetworkFirewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall
- [Opensearch.1] le chiffrement au repos doit être activé dans les OpenSearch domaines
- [Opensearch.2] OpenSearch les domaines ne doivent pas être accessibles au public
- [Opensearch.3] OpenSearch les domaines doivent crypter les données envoyées entre les nœuds
- [Opensearch.4] la journalisation des erreurs de OpenSearch domaine dans CloudWatch Logs doit être activée
- [Opensearch.5] la journalisation des audits doit être activée dans les OpenSearch domaines
- [Opensearch.6] OpenSearch les domaines doivent avoir au moins trois nœuds de données
- [Opensearch.7] le contrôle d'accès détaillé des OpenSearch domaines doit être activé
- [Opensearch.8] Les connexions aux OpenSearch domaines doivent être cryptées selon la dernière politique de sécurité TLS
- [PCA.1]CA privée AWSl'autorité de certification racine doit être désactivée
- [PCA.2]AWSLes autorités de certification privées de l'autorité de certification doivent être étiquetées
- [RDS.14] Le retour en arrière doit être activé sur les clusters Amazon Aurora
- [RDS.15] Les clusters de bases de données RDS doivent être configurés pour plusieurs zones de disponibilité
- [RDS.24] Les clusters de bases de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.25] Les instances de base de données RDS doivent utiliser un nom d'utilisateur d'administrateur personnalisé
- [RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos

- [RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs
- [RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée
- [RDS.43] Les proxys de base de données RDS doivent nécessiter un cryptage TLS pour les connexions
- [RDS.45] La journalisation des audits doit être activée pour les clusters de bases de données Aurora MySQL
- [RDS.47] Les clusters de bases de données RDS pour PostgreSQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.48] Les clusters de bases de données RDS pour MySQL doivent être configurés pour copier les balises dans les instantanés de base de données
- [RDS.50] Les clusters de bases de données RDS doivent avoir une période de rétention des sauvegardes suffisante
- [RDS.51] Les clusters globaux RDS doivent fonctionner sur une version d'Aurora MySQL prise en charge
- [Redshift.7] Les clusters Redshift doivent utiliser un routage VPC amélioré
- [Redshift.8] Les clusters Amazon Redshift ne doivent pas utiliser le nom d'utilisateur d'administrateur par défaut
- [Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [Redshift.11] Les clusters Redshift doivent être balisés
- [Redshift.13] Les instantanés du cluster Redshift doivent être balisés
- [Redshift.17] Les groupes de paramètres du cluster Redshift doivent être balisés
- [RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré
- [RedshiftServerless.2] Les connexions aux groupes de travail Redshift Serverless doivent être requises pour utiliser le protocole SSL
- [RedshiftServerless.3] Les groupes de travail Redshift Serverless devraient interdire l'accès public
- [RedshiftServerless.6] Les espaces de noms Redshift Serverless doivent exporter les journaux vers Logs CloudWatch
- [Route53.1] Les bilans de santé de la Route 53 doivent être étiquetés
- [Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS

- [S3.10] Les compartiments S3 à usage général dont la gestion des versions est activée doivent avoir des configurations de cycle de vie
- [S3.11] Les notifications d'événements doivent être activées dans les compartiments S3 à usage général
- [S3.12] Les ACL ne doivent pas être utilisées pour gérer l'accès des utilisateurs aux compartiments à usage général S3
- [S3.13] Les compartiments S3 à usage général doivent avoir des configurations de cycle de vie
- [S3.20] La suppression MFA doit être activée pour les buckets S3 à usage général
- [S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés
- [S3.25] Les compartiments de répertoires S3 doivent avoir des configurations de cycle de vie
- [SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée
- [SageMaker.6] les configurations d'image de l' SageMaker application doivent être balisées
- [SageMaker.7] les SageMaker images doivent être étiquetées
- [SageMaker.9] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir le chiffrement du trafic inter-conteneurs activé
- [SageMaker.10] les définitions de tâches d'explicabilité du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.11] SageMaker les définitions de tâches relatives à la qualité des données doivent avoir l'isolation réseau activée
- [SageMaker.12] les définitions de tâches liées au biais du SageMaker modèle doivent avoir l'isolation réseau activée
- [SageMaker.13] les définitions de tâches de qualité des SageMaker modèles doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.14] les calendriers SageMaker de surveillance doivent avoir l'isolation réseau activée
- [SageMaker.15] les définitions de tâches liées au biais du SageMaker modèle doivent avoir le cryptage du trafic inter-conteneurs activé
- [SageMaker.17] les boutiques hors ligne des groupes de SageMaker fonctionnalités doivent être cryptées avec AWS KMS clés

- [SageMaker.18] les boutiques en ligne de groupes de SageMaker fonctionnalités avec stockage standard doivent être cryptées avec AWS KMS clés
- [SES.3] Les ensembles de configuration SES doivent avoir le protocole TLS activé pour l'envoi d'e-mails
- [SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public
- [SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public
- [SSM.4] Les documents SSM ne doivent pas être publics
- [SSM.5] Les documents SSM doivent être balisés
- [StepFunctions.1] La journalisation des machines à états Step Functions doit être activée
- [StepFunctions.2] Les activités de Step Functions doivent être étiquetées
- [Transfer.4] Les accords Transfer Family doivent être étiquetés
- [Transfer.5] Les certificats Transfer Family doivent être étiquetés
- [Transfer.6] Les connecteurs Transfer Family doivent être étiquetés
- [Transfer.7] Les profils Transfer Family doivent être balisés
- [WAF.1]AWS WAFLa journalisation classique de l'ACL Web globale doit être activée
- [WAF.2]AWS WAFLes règles régionales classiques doivent comporter au moins une condition
- [WAF.3]AWS WAFLes groupes de règles régionaux classiques doivent avoir au moins une règle
- [WAF.4]AWS WAFLes ACL Web régionales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.6]AWS WAFLes règles globales classiques doivent comporter au moins une condition
- [WAF.7]AWS WAFLes groupes de règles globaux classiques doivent comporter au moins une règle
- [WAF.8]AWS WAFLes ACL Web globales classiques doivent comporter au moins une règle ou un groupe de règles
- [WAF.10]AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles
- [WAF.12]AWS WAFles CloudWatch métriques doivent être activées pour les règles

Création de ressources Security Hub CSPM avec CloudFormation

AWSSecurity Hub CSPM s'intègre AWS CloudFormation à un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que

vous souhaitez (telles que les règles d'automatisation), et CloudFormation qui fournit et configure ces ressources pour vous.

Lorsque vous l'utilisezCloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Security Hub CSPM de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis distribuez les mêmes ressources encore et encore dans plusieurs Comptes AWS régions.

Security Hub (CSPM) etCloudFormationmodèles

Pour fournir et configurer des ressources pour Security Hub CSPM et les services associés, vous devez comprendre le fonctionnement des CloudFormationmodèles. Les modèles sont des fichiers texte au format JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos CloudFormation piles.

Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser CloudFormation Designer pour vous aider à démarrer avec les CloudFormation modèles. Pour plus d'informations, voir Qu'est-ce que CloudFormation Designer ? dans le guide de AWS CloudFormation l'utilisateur.

Vous pouvez créer des CloudFormation modèles pour les types de ressources CSPM du Security Hub suivants :

- Activation du Security Hub CSPM
- Désignation de l'administrateur Security Hub CSPM délégué pour une organisation
- Spécifiez la façon dont votre organisation est configurée dans Security Hub CSPM
- Mise en place d'une norme de sécurité
- Activation de l'agrégation entre régions
- Création d'une politique de configuration centrale et association de celle-ci à des comptes, à une unité organisationnelle (UO) ou à la racine
- Création d'un aperçu personnalisé
- Création d'une règle d'automatisation
- Personnalisation des paramètres de contrôle
- Souscription à l'intégration d'un produit tiers

Pour plus d'informations, notamment des exemples de modèles JSON et YAML pour les ressources, consultez la référence au type de ressource AWS Security Hub CSPM dans le guide de l'AWS CloudFormationutilisateur.

En savoir plus surCloudFormation

Pour en savoir plusCloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormationGuide de l'utilisateur
- CloudFormationAPI Reference
- AWS CloudFormationGuide de l'utilisateur de l'interface de ligne de commande

Abonnement aux annonces CSPM de Security Hub avec Amazon SNS

Cette section fournit des informations sur l'abonnement aux annonces AWS Security Hub CSPM auprès d'Amazon Simple Notification Service (Amazon SNS) afin de recevoir des notifications concernant le Security Hub CSPM.

Après votre inscription, vous recevrez des notifications concernant les événements suivants (notez les informations correspondantes `AnnouncementType` pour chaque événement) :

- `NEW_STANDARDS_CONTROLS`— De nouveaux contrôles ou normes CSPM du Security Hub ont été ajoutés.
- `RETIRED_STANDARDS_CONTROLS`— Les contrôles ou normes CSPM existants du Security Hub ont été retirés.

Les notifications sont proposées dans tous les formats pris en charge par Amazon SNS. Vous pouvez vous abonner aux annonces de Security Hub CSPM dans tous les sites où Régions AWSSecurity Hub CSPM est disponible.

Un utilisateur doit être `Subscribe` autorisé à s'abonner à une rubrique Amazon SNS. Vous pouvez y parvenir avec les politiques Amazon SNS, les politiques IAM ou les deux. Pour plus d'informations, consultez les politiques IAM et Amazon SNS réunies dans le guide du développeur Amazon Simple Notification Service.

> **Note**
>
> Security Hub CSPM envoie à tous les abonnés des annonces Amazon SNS concernant les mises à jour du service Security Hub CSPM. Compte AWS Pour recevoir des notifications

concernant les résultats du Security Hub CSPM, consultez. Révision des détails et de l'historique des recherches dans Security Hub CSPM

Vous pouvez vous abonner à une file d'attente Amazon Simple Queue Service (Amazon SQS) pour un sujet Amazon SNS, mais vous devez utiliser le nom de ressource Amazon (ARN) d'un sujet Amazon SNS situé dans la même région. Pour plus d'informations, consultez la section Abonnement d'une file d'attente à une rubrique Amazon SNS dans le manuel Amazon Simple Queue Service Developer Guide.

Vous pouvez également utiliser une AWS Lambda fonction pour invoquer des événements lorsque vous recevez des notifications. Pour plus d'informations, y compris un exemple de code de fonction, consultez Tutoriel : Utilisation AWS Lambda avec Amazon Simple Notification Service dans le manuel du AWS Lambda développeur.

Les ARN des rubriques Amazon SNS pour chaque région sont les suivants.

Région AWS	ARN de rubrique Amazon SNS
USA Est (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
USA Est (Virginie du Nord)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
USA Ouest (Californie du Nord)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
USA Ouest (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
Afrique (Le Cap)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`

Région AWS	ARN de rubrique Amazon SNS
Asie-Pacifique (Hong Kong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asie-Pacifique (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`
Asie-Pacifique (Jakarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asie-Pacifique (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Asie-Pacifique (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asia Pacific (Seoul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asie-Pacifique (Singapour)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Asie-Pacifique (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`
Asie-Pacifique (Tokyo)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`

Région AWS	ARN de rubrique Amazon SNS
Canada (Centre)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
Chine (Pékin)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`
China (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Europe (Francfort)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Europe (Irlande)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Europe (Londres)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Europe (Milan)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Europe (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
Europe (Espagne)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`

Région AWS	ARN de rubrique Amazon SNS
Europe (Stockholm)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Europe (Zurich)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
Israël (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Middle East (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Moyen-Orient (EAU)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
Amérique du Sud (São Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (US-East)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (US-West)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Les messages sont généralement les mêmes d'une région à l'autre au sein d'une partition. Vous pouvez donc vous abonner à une région de chaque partition pour recevoir des annonces qui concernent toutes les régions de cette partition. Les annonces associées aux comptes des membres ne sont pas répliquées dans le compte administrateur. Par conséquent, chaque compte, y compris

le compte administrateur, ne disposera que d'une copie de chaque annonce. Vous pouvez choisir le compte que vous souhaitez utiliser pour vous abonner aux annonces du Security Hub CSPM.

Pour plus d'informations sur le coût de l'abonnement aux annonces CSPM de Security Hub, consultez la tarification d'Amazon SNS.

Abonnement aux annonces CSPM de Security Hub (console)

1. Ouvrez la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans la liste des régions, choisissez la région dans laquelle vous souhaitez vous abonner aux annonces du Security Hub CSPM. L'exemple utilise la région `us-west-2`.
3. Dans le panneau de navigation, choisissez Abonnements, puis Créer un abonnement.
4. Entrez l'ARN du sujet dans le champ ARN du sujet. Par exemple, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Dans Protocol, choisissez la manière dont vous souhaitez recevoir les annonces du Security Hub CSPM. Si vous choisissez E-mail, pour Endpoint, entrez l'adresse e-mail que vous souhaitez utiliser pour recevoir les annonces.
6. Choisissez Créer un abonnement.
7. Confirmez votre abonnement. Par exemple, si vous avez choisi le protocole e-mail, Amazon SNS enverra un message de confirmation d'abonnement à l'adresse e-mail que vous avez fournie.

Abonnement aux annonces CSPM de Security Hub (AWS CLI)

1. Exécutez la commande suivante :

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Confirmez votre abonnement. Par exemple, si vous avez choisi le protocole e-mail, Amazon SNS enverra un message de confirmation d'abonnement à l'adresse e-mail que vous avez fournie.

Format du message Amazon SNS

Les exemples suivants montrent les annonces du Security Hub CSPM d'Amazon SNS concernant l'introduction de nouveaux contrôles de sécurité. Le contenu des messages varie en fonction du type

d'annonce, mais le format est le même pour tous les types d'annonce. Facultativement, un `Link` champ fournissant des détails sur l'annonce peut être inclus.

Exemple : annonce du Security Hub CSPM concernant de nouveaux contrôles (protocole de courrier électronique)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to theAWSFoundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront
 (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27),
 Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic
 Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon
 Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service
 (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1),AWS Network Firewall(NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. "
}
```

Exemple : annonce CSPM du Security Hub concernant de nouveaux contrôles (protocole Email-JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":
\"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard\",\"Description\":\"We have added 36 new
 controls to theAWSFoundational Security Best Practices standard. These
 include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4,
 AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront (CloudFront.10),
 Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic
```

```
 Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service
 (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System
 (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2),
 Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1),AWS
 Network Firewall(NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon
 OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Désactivation du Security Hub CSPM

Vous pouvez désactiver AWS Security Hub CSPM à l'aide de la console Security Hub CSPM ou de l'API Security Hub. Si vous désactivez Security Hub CSPM, vous pourrez le réactiver ultérieurement.

Si votre organisation utilise une configuration centralisée, l'administrateur délégué du Security Hub CSPM peut créer des politiques de configuration qui désactivent le Security Hub CSPM pour des comptes et des unités organisationnelles (UO) spécifiques et permettent de maintenir le Security Hub CSPM activé pour les autres. Les politiques de configuration affectent la région d'origine et toutes les régions associées. Pour de plus amples informations, veuillez consulter Comprendre la configuration centrale dans Security Hub CSPM.

Si vous désactivez Security Hub CSPM pour un compte, voici ce qui se produit :

- Toutes les normes et contrôles CSPM du Security Hub sont désactivés pour le compte.

- Security Hub CSPM arrête de générer, de mettre à jour et d'ingérer les résultats du compte.
- Après 30 jours, Security Hub CSPM supprime définitivement tous les résultats archivés existants pour le compte. Les résultats ne peuvent pas être récupérés à l'aide de Security Hub CSPM.
- Après 90 jours, Security Hub CSPM supprime définitivement tous les résultats actifs existants pour le compte. Les résultats ne peuvent pas être récupérés à l'aide de Security Hub CSPM.
- Au bout de 90 jours, Security Hub CSPM supprime définitivement toutes les informations existantes et les paramètres de configuration du Security Hub CSPM pour le compte. Les données et les paramètres ne peuvent pas être récupérés.

Pour conserver les résultats existants, vous pouvez les exporter vers un compartiment S3 avant de désactiver Security Hub CSPM. Vous pouvez le faire en utilisant une action personnalisée avec une EventBridge règle Amazon. Pour de plus amples informations, veuillez consulter Utilisation à EventBridge des fins de réponse et de correction automatisées.

Si vous réactivez Security Hub CSPM dans les 90 jours suivant sa désactivation pour un compte, vous retrouvez l'accès aux résultats actifs existants, ainsi qu'aux informations et aux paramètres de configuration du Security Hub CSPM pour le compte. Si vous réactivez Security Hub CSPM dans les 30 jours, vous retrouverez également l'accès aux résultats archivés existants pour le compte. Cependant, les résultats existants peuvent être inexacts car ils refléteront l'état de votre AWS environnement lorsque vous avez désactivé Security Hub CSPM. En outre, lorsque vous réactivez des normes et des contrôles individuels, Security Hub CSPM peut initialement générer des résultats dupliqués pour des AWS ressources spécifiques, en fonction des normes et des contrôles que vous activez. Pour ces raisons, nous vous recommandons d'effectuer l'une des opérations suivantes :

- Modifiez le statut du flux de travail de tous les résultats existants sur « `RESOLVED` Avant de désactiver Security Hub CSPM ». Pour de plus amples informations, veuillez consulter Définition de l'état des résultats dans le flux de travail.
- Désactivez toutes les normes au moins six jours avant de désactiver Security Hub CSPM. Security Hub CSPM archive ensuite tous les résultats existants dans la mesure du possible, généralement dans un délai de trois à cinq jours. Pour de plus amples informations, veuillez consulter Désactivation d'une norme.

Vous ne pouvez pas désactiver Security Hub CSPM dans les cas suivants :

- Votre compte est le compte administrateur délégué du Security Hub CSPM d'une organisation. Si vous utilisez la configuration centralisée, vous ne pouvez pas associer de politique de configuration

qui désactive Security Hub CSPM pour le compte d'administrateur délégué. L'association peut réussir pour d'autres comptes, mais Security Hub CSPM n'applique pas la politique au compte d'administrateur délégué.

- Votre compte est un compte administrateur Security Hub CSPM sur invitation, et vous avez des comptes de membre. Avant de désactiver Security Hub CSPM, vous devez dissocier tous les comptes de vos membres. Pour savoir comment procéder, consultez the section called "Dissociation des comptes membres".

Avant que le propriétaire d'un compte membre puisse désactiver Security Hub CSPM, le compte doit se dissocier de son compte administrateur. Pour un compte d'organisation, seul le compte administrateur peut dissocier un compte de membre. Pour de plus amples informations, veuillez consulter the section called "Dissociation des comptes des membres de l'organisation". Pour un compte invité manuellement, le compte administrateur ou le compte membre peut dissocier le compte. Pour plus d'informations, consultez the section called "Dissociation des comptes membres" ou the section called "Dissociation d'un compte administrateur". La dissociation n'est pas requise si vous utilisez la configuration centralisée, car l'administrateur du Security Hub CSPM peut créer une politique qui désactive le Security Hub CSPM pour des comptes de membres spécifiques.

Lorsque vous désactivez Security Hub CSPM pour un compte, celui-ci est désactivé uniquement pour le moment. Région AWS Toutefois, si vous utilisez la configuration centrale pour désactiver Security Hub CSPM pour des comptes spécifiques, il est désactivé dans la région d'origine et dans toutes les régions associées.

Pour désactiver Security Hub CSPM, choisissez votre méthode préférée et suivez les étapes.

Security Hub CSPM console

Procédez comme suit pour désactiver Security Hub CSPM à l'aide de la console.

Pour désactiver Security Hub CSPM

1. Ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Dans la section Disable Security Hub CSPM, choisissez Disable Security Hub CSPM.
4. Lorsque vous êtes invité à confirmer, choisissez Disable Security Hub CSPM.

Security Hub API

Pour désactiver Security Hub CSPM par programmation, utilisez l'API DisableSecurityHubSecurity HubAWS. Ou, si vous utilisez leAWS CLI, exécutez la commande disable-security-hub. Par exemple, la commande suivante désactive Security Hub CSPM dans le système actuel : Région AWS

```
$ aws securityhub disable-security-hub
```

Sécurité dans AWS Security Hub CSPM

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : elle AWS est responsable de la protection de l'infrastructure qui exécute AWS les services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-partyles auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Security Hub CSPM, veuillez consulter AWS Services in Scope by Compliance Program (français non garanti).
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Security Hub CSPM. Les rubriques suivantes vous montrent comment configurer Security Hub CSPM pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources CSPM de votre Security Hub.

Rubriques

- Protection des données dans AWS Security Hub CSPM

- AWS Gestion des identités et des accès pour Security Hub CSPM
- Validation de conformité pour AWS Security Hub CSPM
- Résilience dans AWS Hub de sécurité
- Sécurité de l'infrastructure dans AWS Security Hub CSPM
- AWS Security Hub CSPM et les points de terminaison VPC d'interface (AWS PrivateLink)

Protection des données dans AWS Security Hub CSPM

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Security Hub CSPM. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble des AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les conditions légales de la région . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour enregistrer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le Guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Security Hub CSPM ou autre à Services AWS l'aide de la console, de l'API ou AWS des kits de AWS CLI développement logiciel. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Security Hub CSPM est une offre de services multi-locataires. Pour garantir la protection des données, Security Hub CSPM chiffre les données au repos et les données en transit entre les services des composants.

AWS Gestion des identités et des accès pour Security Hub CSPM

Gestion des identités et des accès AWS (IAM) permet à un Service AWS administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (possède des autorisations) à utiliser les ressources de Security Hub. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment Security Hub fonctionne avec IAM
- Identity-based exemples de politiques pour AWS Security Hub CSPM
- Service-linked rôles pour AWS Security Hub CSPM
- AWS politiques gérées pour Security Hub
- Résolution des problèmes AWS Security Hub CSPM identité et accès

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Security Hub CSPM identité et accès)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Security Hub fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based exemples de politiques pour AWS Security Hub CSPM)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identité. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), de l'authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une interface de ligne de commande pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à l' Services AWS aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de votre annuaire d'entreprise, de votre fournisseur d'identité Web ou Directory Service qui accède à l' Services AWS aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le Guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous associez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques en ligne (intégrées directement dans une identité unique) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Security Hub fonctionne avec IAM

Avant d'utiliser Gestion des identités et des accès AWS (IAM) pour gérer l'accès à AWS Security Hub CSPM, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Security Hub CSPM.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Security Hub CSPM

Fonctionnalité IAM	Prise en charge de Security Hub CSPM
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui

Fonctionnalité IAM	Prise en charge de Security Hub CSPM
Ressources de politique	Non
Clés de condition de politique	Oui
Listes de contrôle d'accès (ACL)	Non
Attribute-based contrôle d'accès (ABAC) — balises dans les politiques	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Rôles du service	Non
Service-linked rôles	Oui

Pour une vue d'ensemble de la façon dont Security Hub CSPM et d'autres Services AWS fonctionnent avec la plupart des fonctionnalités IAM, consultez Services AWS le Guide de l'utilisateur IAM consacré à l'utilisation d'IAM.

Identity-based politiques pour Security Hub CSPM

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous pouvez joindre à une identité, telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Security Hub CSPM prend en charge les politiques basées sur l'identité. Pour de plus amples informations, veuillez consulter Identity-based exemples de politiques pour AWS Security Hub CSPM.

Resource-based politiques pour Security Hub CSPM

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Security Hub CSPM ne prend pas en charge les politiques basées sur les ressources. Vous ne pouvez pas associer une politique IAM directement à une ressource CSPM Security Hub.

Actions politiques pour Security Hub CSPM

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de stratégie dans Security Hub CSPM utilisent le préfixe suivant avant l'action :

```
securityhub:
```

Par exemple, pour accorder à un utilisateur l'autorisation d'activer Security Hub CSPM, qui est une action correspondant au `EnableSecurityHub` fonctionnement de l'API Security Hub CSPM, incluez l'`securityhub:EnableSecurityHub`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Security Hub CSPM définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

```
"Action": "securityhub:EnableSecurityHub"
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple :

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Vous pouvez également spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Get`, incluez l'action suivante :

```
"Action": "securityhub:Get*"
```

Cependant, une bonne pratique consiste à créer des stratégies qui suivent le principe du moindre privilège. En d'autres termes, vous devez créer des stratégies qui incluent uniquement les autorisations requises pour effectuer une tâche spécifique.

L'utilisateur doit avoir accès à l'`DescribeStandardsControl`opération pour avoir accès à `BatchGetSecurityControlsBatchGetStandardsControlAssociations`, et`ListStandardsControlAssociations`.

L'utilisateur doit avoir accès à l'`UpdateStandardsControls`opération pour avoir accès à`BatchUpdateStandardsControlAssociations`, et`UpdateSecurityControl`.

Pour obtenir la liste des actions CSPM de Security Hub, consultez la section Actions définies par AWS Security Hub CSPM dans la référence d'autorisation de service. Pour des exemples de politiques qui spécifient les actions CSPM de Security Hub, consultez. Identity-based exemples de politiques pour AWS Security Hub CSPM

Ressources politiques pour Security Hub CSPM

Prend en charge les ressources de politique : non

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Security Hub CSPM définit les types de ressources suivants :

- Hub
- Produit (langue française non garantie)
- Agrégateur de recherche, également appelé agrégateur interrégional
- Règle d'automatisation
- Politique de configuration

Vous pouvez spécifier ces types de ressources dans les politiques à l'aide des ARN.

Pour obtenir la liste des types de ressources CSPM de Security Hub et la syntaxe ARN de chacun d'entre eux, consultez la section Types de ressources définis par AWS Security Hub CSPM dans la référence d'autorisation de service. Pour savoir quelles actions vous pouvez spécifier pour chaque type de ressource, consultez la section Actions définies par AWS Security Hub CSPM dans la référence d'autorisation de service. Pour des exemples de politiques qui spécifient des ressources, consultezIdentity-based exemples de politiques pour AWS Security Hub CSPM.

Clés de condition de politique pour Security Hub CSPM

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition,

tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, consultez les clés contextuelles de conditions AWS globales dans le guide de l'utilisateur IAM.

Pour obtenir la liste des clés de condition CSPM de Security Hub, consultez la section Clés de condition pour AWS Security Hub CSPM dans la référence d'autorisation de service. Pour savoir avec quelles actions et quelles ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Security Hub CSPM. Pour des exemples de politiques utilisant des clés de condition, consultezIdentity-based exemples de politiques pour AWS Security Hub CSPM.

Listes de contrôle d'accès (ACL) dans Security Hub CSPM

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Security Hub CSPM ne prend pas en charge les ACL, ce qui signifie que vous ne pouvez pas associer une ACL à une ressource Security Hub CSPM.

Attribute-based contrôle d'accès (ABAC) avec Security Hub CSPM

Prise en charge d'ABAC (balises dans les politiques) : Oui

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à celle de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration

de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Vous pouvez associer des balises aux ressources CSPM de Security Hub. Vous pouvez également contrôler l'accès aux ressources en fournissant des informations de balise dans l'`Condition`élément d'une politique.

Pour plus d'informations sur le balisage des ressources CSPM de Security Hub, consultez. Balisage des ressources du Security Hub Pour un exemple de politique basée sur l'identité qui contrôle l'accès à une ressource en fonction de balises, consultez. Identity-based exemples de politiques pour AWS Security Hub CSPM

Utilisation d'informations d'identification temporaires avec Security Hub CSPM

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès de courte durée aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous pouvez obtenir des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRole ou GetFederationToken.

Security Hub CSPM prend en charge l'utilisation d'informations d'identification temporaires.

Sessions d'accès direct pour Security Hub CSPM

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Par exemple, Security Hub CSPM envoie des requêtes FAS en aval Services AWS lorsque vous intégrez Security Hub CSPM à AWS Organizations et lorsque vous désignez le compte administrateur CSPM Security Hub délégué pour une organisation dans Organisations.

Pour les autres tâches, Security Hub CSPM utilise un rôle lié à un service pour effectuer des actions en votre nom. Pour plus de détails sur ce rôle, consultezService-linked rôles pour AWS Security Hub CSPM.

Rôles de service pour Security Hub CSPM

Security Hub CSPM n'assume ni n'utilise de rôles de service. Pour effectuer des actions en votre nom, Security Hub CSPM utilise un rôle lié à un service. Pour plus de détails sur ce rôle, consultezService-linked rôles pour AWS Security Hub CSPM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut entraîner des problèmes opérationnels liés à votre utilisation de Security Hub CSPM. Modifiez les rôles de service uniquement lorsque Security Hub CSPM fournit des instructions à cet effet.

Service-linked rôles pour Security Hub CSPM

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre compte Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Security Hub CSPM utilise un rôle lié à un service pour effectuer des actions en votre nom. Pour plus de détails sur ce rôle, consultezService-linked rôles pour AWS Security Hub CSPM.

Identity-based exemples de politiques pour AWS Security Hub CSPM

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources CSPM de Security Hub. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API Console de gestion AWS AWS CLI, ou. Un administrateur doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes ayant besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Security Hub CSPM
- Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations
- Exemple : autoriser les utilisateurs à créer et à gérer une politique de configuration
- Exemple : autoriser les utilisateurs à consulter les résultats
- Exemple : autoriser les utilisateurs à créer et à gérer des règles d'automatisation

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer des ressources Security Hub sur votre compte, y accéder ou les supprimer. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations avec le moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par le AWS client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un outil spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger une authentification multifacteur (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root Compte AWS, activez l'authentification multifacteur pour renforcer la sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Security Hub CSPM

Pour accéder à la AWS Security Hub CSPM console, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des détails sur les ressources CSPM de Security Hub dans votre. Compte AWS Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour vous assurer que ces utilisateurs et rôles peuvent utiliser la console Security Hub CSPM, associez également la politique AWS gérée suivante à l'entité. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

JSON

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

```
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut des autorisations pour effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : autoriser les utilisateurs à créer et à gérer une politique de configuration

Cet exemple montre comment créer une politique IAM qui permet à un utilisateur de créer, d'afficher, de mettre à jour et de supprimer des politiques de configuration. Cet exemple de politique permet également à l'utilisateur de démarrer, d'arrêter et de visualiser les associations de politiques. Pour que cette politique IAM fonctionne, l'utilisateur doit être l'administrateur CSPM délégué de Security Hub pour une organisation.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
```

```
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : autoriser les utilisateurs à consulter les résultats

Cet exemple montre comment créer une politique IAM permettant à un utilisateur de consulter les résultats du Security Hub CSPM.

JSON

```
{
```

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

Exemple : autoriser les utilisateurs à créer et à gérer des règles d'automatisation

Cet exemple montre comment créer une politique IAM permettant à un utilisateur de créer, d'afficher, de mettre à jour et de supprimer des règles d'automatisation CSPM de Security Hub. Pour que cette politique IAM fonctionne, l'utilisateur doit être un administrateur CSPM de Security Hub. Pour limiter les autorisations, par exemple pour permettre à un utilisateur de consulter uniquement les règles d'automatisation, vous pouvez supprimer les autorisations de création, de mise à jour et de suppression.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
```

```
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked rôles pour AWS Security Hub CSPM

AWS Security Hub CSPM utilise un rôle lié à un service Gestion des identités et des accès AWS (IAM) nommé. `AWSServiceRoleForSecurityHub` Ce rôle lié à un service est un rôle IAM directement lié à Security Hub CSPM. Il est prédéfini par Security Hub CSPM et inclut toutes les autorisations dont Security Hub CSPM a besoin pour appeler d'autres AWS ressources Services AWS et les surveiller en votre nom. Security Hub CSPM utilise ce rôle lié à un service partout Régions AWS où Security Hub CSPM est disponible.

Un rôle lié à un service facilite la configuration de Security Hub CSPM car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Security Hub CSPM définit les autorisations de son rôle lié à un service et, sauf indication contraire, seul Security Hub CSPM peut assumer ce rôle. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et vous ne pouvez associer cette politique d'autorisations à aucune autre entité IAM.

Pour consulter les détails du rôle lié à un service, vous pouvez utiliser la console Security Hub CSPM. Dans le volet de navigation, choisissez Général sous Paramètres. Ensuite, dans la section Autorisations de service, choisissez Afficher les autorisations de service.

Vous ne pouvez supprimer le rôle lié au service Security Hub CSPM qu'après avoir désactivé Security Hub CSPM dans toutes les régions où il est activé. Cela protège les ressources CSPM de votre Security Hub car vous ne pouvez pas supprimer par inadvertance les autorisations d'accès à celles-ci.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM et recherchez les services dont la valeur est Oui dans la colonne des rôles. Service-linked Choisissez Oui avec un lien pour consulter la documentation sur les rôles liés à un service pour ce service.

Rubriques

- Service-linked autorisations de rôle pour Security Hub CSPM
- Création d'un rôle lié à un service pour Security Hub CSPM
- Modification d'un rôle lié à un service pour Security Hub CSPM
- Supprimer un rôle lié à un service pour Security Hub CSPM

Service-linked autorisations de rôle pour Security Hub CSPM

Security Hub CSPM utilise le rôle lié à un service nommé. `AWSServiceRoleForSecurityHub` Il s'agit d'un rôle lié à un service requis pour accéder AWS Security Hub CSPM à vos ressources. Ce rôle lié à un service permet à Security Hub CSPM d'effectuer des tâches telles que la réception des résultats d'autres utilisateurs Services AWS et la configuration de l' AWS Config infrastructure requise pour effectuer des contrôles de sécurité. Le rôle lié à un service `AWSServiceRoleForSecurityHub` fait confiance au service `securityhub.amazonaws.com` pour endosser le rôle.

Le rôle lié à un service `AWSServiceRoleForSecurityHub` utilise la stratégie gérée par `AWSSecurityHubServiceRolePolicy`.

Vous devez accorder des autorisations pour permettre à une identité IAM (telle qu'un rôle, un groupe ou un utilisateur) de créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForSecurityHub` lié à un service soit créé avec succès, l'identité IAM que vous utilisez pour accéder à Security Hub CSPM doit disposer des autorisations requises. Pour accorder les autorisations requises, associez la stratégie suivante à l'identité IAM.

JSON

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

```
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Création d'un rôle lié à un service pour Security Hub CSPM

Le rôle `AWSServiceRoleForSecurityHub` lié à un service est créé automatiquement lorsque vous activez Security Hub CSPM pour la première fois ou que vous activez Security Hub CSPM dans une région où vous ne l'aviez pas activé auparavant. Vous pouvez également créer le rôle `AWSServiceRoleForSecurityHub` lié à un service manuellement à l'aide de la console IAM, de l'interface de ligne de commande IAM ou de l'API IAM. Pour de plus amples informations sur la création manuelle d'un rôle, veuillez consulter Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

> **Important**
>
> Le rôle lié à un service créé pour un compte administrateur Security Hub CSPM ne s'applique pas aux comptes membres CSPM Security Hub associés.

Modification d'un rôle lié à un service pour Security Hub CSPM

Security Hub CSPM ne vous permet pas de modifier le rôle lié au `AWSServiceRoleForSecurityHub` service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Security Hub CSPM

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

Lorsque vous désactivez Security Hub CSPM, Security Hub CSPM ne supprime pas automatiquement le rôle lié au `AWSServiceRoleForSecurityHub` service pour vous. Si vous réactivez Security Hub CSPM, le service peut alors recommencer à utiliser le rôle lié au service existant. Si vous n'avez plus besoin d'utiliser Security Hub CSPM, vous pouvez supprimer manuellement le rôle lié au service.

> **Important**
>
> Avant de supprimer le rôle `AWSServiceRoleForSecurityHub` lié à un service, vous devez d'abord désactiver Security Hub CSPM dans toutes les régions où il est activé. Pour de plus amples informations, veuillez consulter Désactivation du Security Hub CSPM. Si Security Hub CSPM n'est pas désactivé lorsque vous tentez de supprimer le rôle lié à un service, la suppression échoue.

Pour supprimer le rôle `AWSServiceRoleForSecurityHub` lié à un service, vous pouvez utiliser la console IAM, l'interface de ligne de commande IAM ou l'API IAM. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour Security Hub

Une politique AWS gérée est une politique autonome qui est créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte

toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou que de nouvelles opérations d'API deviennent disponibles pour des services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS stratégie gérée : AWSSecurityHubFullAccess

Vous pouvez associer la politique `AWSSecurityHubFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent à un principal d'accéder pleinement à toutes les actions CSPM de Security Hub. Cette politique doit être associée à un mandant avant qu'il n'active Security Hub CSPM manuellement pour son compte. Par exemple, les responsables disposant de ces autorisations peuvent à la fois consulter et mettre à jour l'état des résultats. Ils peuvent également configurer des informations personnalisées, activer des intégrations et activer et désactiver les normes et les contrôles. Les responsables d'un compte administrateur peuvent également gérer les comptes des membres.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `securityhub`— Permet aux administrateurs d'accéder pleinement à toutes les actions CSPM de Security Hub.
- `guardduty`— Permet aux directeurs d'effectuer la gestion du cycle de vie complet d'un détecteur, la gestion administrative de l'organisation, la gestion des comptes des membres et la configuration à l'échelle de l'organisation dans Amazon. GuardDuty Cela inclut les actions d'API : GetDetector ListDetector, CreateDetector, UpdateDetector, DeleteDetector, EnableOrganizationAdminAccount, ListOrganizationAdminAccounts, CreateMembers, UpdateOrganizationConfiguration, DescribeOrganizationConfiguration.
- `iam`— Permet aux directeurs de créer un rôle lié à un service pour Security Hub CSPM et Security Hub et d'obtenir les rôles, les politiques et les versions des politiques.
- `inspector`— Permet aux administrateurs d'obtenir des informations sur l'état du compte, de l'activer ou de le désactiver, de déléguer la gestion administrative et de gérer la configuration de l'organisation dans Amazon Inspector. Cela inclut les actions d'API : BatchGetAccountStatus, Activer, Désactiver EnableDelegatedAdminAccount,

DisableDelegatedAdminAccount, ListDelegatedAdminAccounts, UpdateOrganizationConfiguration, DescribeOrganizationConfiguration.

- `pricing`— Permet aux directeurs d'obtenir une liste de prix Services AWS et des produits.
- `account`— Permet aux administrateurs d'obtenir des informations sur les régions du compte afin de faciliter la gestion des régions dans Security Hub.

Pour passer en revue les autorisations relatives à cette politique, consultez AWSSecurityHubFullAccess le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSSecurityHubReadOnlyAccess

Vous pouvez associer la politique `AWSSecurityHubReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations dans Security Hub CSPM. Les responsables auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour dans Security Hub CSPM. Par exemple, les directeurs disposant de ces autorisations peuvent consulter la liste des résultats associés à leur compte, mais ne peuvent pas modifier le statut d'un résultat. Ils peuvent consulter les résultats des informations, mais ne peuvent pas créer ni configurer d'informations personnalisées. Ils ne peuvent pas configurer de contrôles ou d'intégrations de produits.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `securityhub`— Permet aux utilisateurs d'effectuer des actions qui renvoient une liste d'éléments ou des détails sur un élément. Cela inclut les opérations d'API qui commencent par `GetList`, ou`Describe`.

Pour passer en revue les autorisations relatives à cette politique, consultez AWSSecurityHubReadOnlyAccess le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSSecurityHubOrganizationsAccess

Vous pouvez associer la politique `AWSSecurityHubOrganizationsAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives pour activer et gérer Security Hub, Security Hub CSPM, Amazon GuardDuty et Amazon Inspector pour une organisation en. AWS Organizations Les autorisations associées à cette politique permettent au compte de gestion de l'organisation

de désigner le compte administrateur délégué pour Security Hub, Security Hub CSPM, Amazon GuardDuty et Amazon Inspector. Ils permettent également au compte administrateur délégué d'activer les comptes d'organisation en tant que comptes de membres.

Cette politique fournit uniquement des autorisations pour AWS Organizations. Le compte de gestion de l'organisation et le compte d'administrateur délégué nécessitent également des autorisations pour les actions associées. Ces autorisations peuvent être accordées à l'aide de la politique `AWSSecurityHubFullAccess` gérée.

La création ou la mise à jour d'une politique d'administrateur délégué dans un compte de gestion nécessite des autorisations supplémentaires qui ne sont pas fournies dans cette politique. Pour effectuer ces actions, il est recommandé d'ajouter des autorisations pour la AWSOrganizationsFullAccess politique `organizations:PutResourcePolicy` ou de la joindre.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `organizations:ListAccounts`— Permet aux directeurs de récupérer la liste des comptes qui font partie d'une organisation.
- `organizations:DescribeOrganization`— Permet aux directeurs de récupérer des informations sur l'organisation.
- `organizations:ListRoots`— Permet aux directeurs de répertorier la racine d'une organisation.
- `organizations:ListDelegatedAdministrators`— Permet aux directeurs de répertorier l'administrateur délégué d'une organisation.
- `organizations:ListAWSServiceAccessForOrganization`— Permet aux directeurs de répertorier les informations Services AWS utilisées par une organisation.
- `organizations:ListOrganizationalUnitsForParent`— Permet aux directeurs d'école de répertorier les unités organisationnelles (UO) enfants d'une UO parent.
- `organizations:ListAccountsForParent`— Permet aux directeurs d'école de répertorier les comptes enfants d'une unité d'organisation parentale.
- `organizations:ListParents`— Répertorie la racine ou les unités organisationnelles (UO) qui font office de parent immédiat de l'unité d'organisation ou du compte enfant spécifié.
- `organizations:DescribeAccount` : autorise les principaux à extraire des informations sur un compte dans l'organisation.
- `organizations:DescribeOrganizationalUnit`— Permet aux directeurs de récupérer des informations sur une unité d'organisation.

- `organizations:ListPolicies`— Récupère la liste de toutes les politiques d'une organisation d'un type donné.
- `organizations:ListPoliciesForTarget`— Répertorie les politiques qui sont directement associées à la racine, à l'unité organisationnelle (OU) ou au compte cible spécifié.
- `organizations:ListTargetsForPolicy`— Répertorie toutes les racines, les unités organisationnelles (UO) et les comptes auxquels la politique spécifiée est attachée.
- `organizations:EnableAWSServiceAccess`— Permet aux directeurs d'activer l'intégration avec les organisations.
- `organizations:RegisterDelegatedAdministrator`— Permet aux administrateurs principaux de désigner le compte administrateur délégué.
- `organizations:DeregisterDelegatedAdministrator`— Permet aux administrateurs principaux de supprimer le compte administrateur délégué.
- `organizations:DescribePolicy`— Récupère les informations relatives à une politique.
- `organizations:DescribeEffectivePolicy`— Renvoie le contenu de la politique effective pour le type de politique et le compte spécifiés.
- `organizations:CreatePolicy`— Crée une politique d'un type spécifique que vous pouvez associer à un compte root, à une unité organisationnelle (OU) ou à un AWS compte individuel.
- `organizations:UpdatePolicy`— Met à jour une politique existante avec un nouveau nom, une nouvelle description ou un nouveau contenu.
- `organizations:DeletePolicy`— Supprime la politique spécifiée de votre organisation.
- `organizations:AttachPolicy`— Associe une politique à un compte root, à une unité organisationnelle (OU) ou à un compte individuel.
- `organizations:DetachPolicy`— Détache une politique d'une racine cible, d'une unité organisationnelle (OU) ou d'un compte.
- `organizations:EnablePolicyType`— Active un type de politique dans une racine.
- `organizations:DisablePolicyType`— Désactive un type de politique d'organisation dans une racine.
- `organizations:TagResource`— Ajoute une ou plusieurs balises à une ressource spécifiée.
- `organizations:UntagResource`— Supprime toutes les balises contenant les clés spécifiées d'une ressource spécifiée.
- `organizations:ListTagsForResource`— Répertorie les balises associées à une ressource spécifiée.

- `organizations:DescribeResourcePolicy`— Récupère les informations relatives à une politique de ressources.

Pour passer en revue les autorisations relatives à cette politique, consultez AWSSecurityHubOrganizationsAccess le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSSecurityHubServiceRolePolicy

Vous ne pouvez pas joindre de `AWSSecurityHubServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Security Hub CSPM d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter the section called "Service-linked rôles".

Cette politique accorde des autorisations administratives qui permettent au rôle lié au service d'effectuer des tâches telles que l'exécution de contrôles de sécurité pour les contrôles CSPM de Security Hub.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `cloudtrail`— Récupérez des informations sur les CloudTrail sentiers.
- `cloudwatch`— Récupérez les CloudWatch alarmes actuelles et les indicateurs de santé du connecteur.
- `logs`— Récupérez les filtres métriques pour CloudWatch les journaux.
- `sns`— Récupère la liste des abonnements à une rubrique SNS.
- `config`— Récupérez des informations sur les enregistreurs de configuration, les ressources et AWS Config les règles. Gérez les enregistreurs de configuration liés aux services Security Hub CSPM et les enregistreurs de configuration liés aux services tiers. Créez et supprimez AWS Config des règles et exécutez des évaluations en fonction de ces règles. Répertoriez les enregistreurs de configuration et obtenez des informations sur les connecteurs pour prendre en charge les intégrations cloud tierces.
- `iam`— Récupérez et générez des rapports d'identification pour les comptes, et créez le rôle lié au service pour. AWS Config
- `organizations`— Récupérez les informations relatives au compte et à l'unité organisationnelle (OU) d'une organisation.

- `securityhub`— Récupérez des informations sur la manière dont le service, les normes et les contrôles Security Hub CSPM sont configurés.
- `tag`— Récupérez des informations sur les balises de ressources.

Pour passer en revue les autorisations relatives à cette politique, consultez AWSSecurityHubServiceRolePolicy le AWS Managed Policy Reference Guide.

Mises à jour de Security Hub pour AWS stratégies gérées

Le tableau suivant fournit des informations sur les mises à jour des politiques AWS gérées pour AWS Security Hub et Security Hub CSPM depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les mises à jour des politiques, abonnez-vous au flux RSS sur la page d'historique des documents de Security Hub.

Modifier	Description	Date
AWSSecurityHubServiceRolePolicy— Politique mise à jour	Security Hub CSPM a mis à jour la politique pour prendre en charge l'intégration de tiers. La mise à jour ajoute les autorisations suivantes : gérer les enregistreurs de configuration tiers, répertorier les enregistreurs de configuration, obtenir des informations sur le connecteur et récupérer les mesures de santé du connecteur.	30 juin 2026
AWSSecurityHubServiceRolePolicy— Politique mise à jour	Security Hub CSPM a mis à jour la politique pour ajouter des autorisations permettant de gérer les enregistreurs de configuration liés aux services Security Hub CSPM et de	29 avril 2026

Modifier	Description	Date
	créer le rôle lié aux services. AWS Config	
AWSSecurityHubOrganizationsAccess— Politique mise à jour	Security Hub a mis à jour la politique pour ajouter des autorisations permettant de décrire les politiques relatives aux ressources afin de prendre en charge les fonctionnalités de Security Hub. Security Hub est en version préliminaire et est susceptible d'être modifiée.	12 novembre 2025
AWSSecurityHubFullAccess— Politique mise à jour	Security Hub a mis à jour la politique pour ajouter des fonctionnalités relatives à la gestion GuardDuty, à Amazon Inspector et à la gestion des comptes afin de prendre en charge les fonctionnalités de Security Hub. Security Hub est en version préliminaire et est susceptible d'être modifiée.	17 novembre 2025
AWSSecurityHubOrganizationsAccess : mise à jour d'une politique existante	Security Hub a ajouté de nouvelles autorisations à la politique. Les autorisations permettent à la direction de l'organisation d'activer et de gérer Security Hub et Security Hub CSPM pour une organisation.	17 juin 2025

Modifier	Description	Date
AWSSecurityHubFullAccess : mise à jour d'une politique existante	Security Hub CSPM a ajouté de nouvelles autorisations qui permettent aux directeurs de créer un rôle lié à un service pour Security Hub.	17 juin 2025
AWSSecurityHubFullAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour la politique pour obtenir le détail des prix Services AWS et des produits.	24 avril 2024
AWSSecurityHubReadOnlyAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour cette politique gérée en ajoutant un `Sid` champ.	22 février 2024
AWSSecurityHubFullAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour la politique afin de déterminer si Amazon GuardDuty et Amazon Inspector sont activés dans un compte. Cela permet aux clients de rassembler des informations relatives à la sécurité provenant de plusieurs sources. Services AWS	16 novembre 2023

Modifier	Description	Date
AWSSecurityHubOrganizationsAccess— Mise à jour d'une politique existante	Security Hub CSPM a mis à jour la politique pour accorder des autorisations supplémentaires afin de permettre un accès en lecture seule aux AWS Organizations fonctionnalités d'administrateur délégué. Cela inclut des détails tels que la racine, les unités organisationnelles (UO), les comptes, la structure organisationnelle et l'accès aux services.	16 novembre 2023
AWSSecurityHubServiceRolePolicy : mise à jour d'une politique existante	Security Hub CSPM a ajouté les `UpdateSecurityControl` autorisations `BatchGetSecurityControls` `DisassociateFromAdministratorAccount`, et pour lire et mettre à jour les propriétés de contrôle de sécurité personnalisables.	26 novembre 2023
AWSSecurityHubServiceRolePolicy – Mise à jour d'une politique existante	Security Hub CSPM a ajouté l'`tag:GetResources` autorisation de lire les balises de ressources liées aux résultats.	7 novembre 2023

Modifier	Description	Date
AWSSecurityHubServiceRolePolicy : mise à jour d'une politique existante	Security Hub CSPM a ajouté l'`BatchGetStandardsControlAssociations` autorisation d'obtenir des informations sur l'état d'activation d'un contrôle dans une norme.	27 septembre 2023
AWSSecurityHubServiceRolePolicy : mise à jour d'une politique existante	Security Hub CSPM a ajouté de nouvelles autorisations pour obtenir des AWS Organizations données et lire et mettre à jour les configurations de Security Hub CSPM, y compris les normes et les contrôles.	20 septembre 2023
AWSSecurityHubServiceRolePolicy : mise à jour d'une politique existante	Security Hub CSPM a déplacé l'`config:DescribeConfigRuleEvaluationStatus` autorisation existante vers une autre déclaration de la politique. L'`config:DescribeConfigRuleEvaluationStatus` autorisation est désormais appliquée à toutes les ressources.	17 mars 2023

Modifier	Description	Date
AWSSecurityHubServiceRolePolicy : mise à jour d'une politique existante	Security Hub CSPM a déplacé l'`config:PutEvaluations` autorisation existante vers une autre déclaration de la politique. L'`config:PutEvaluations` autorisation est désormais appliquée à toutes les ressources.	14 juillet 2021
AWSSecurityHubServiceRolePolicy : mise à jour d'une politique existante	Security Hub CSPM a ajouté une nouvelle autorisation pour permettre au rôle lié au service de fournir des résultats d'évaluation à. AWS Config	29 juin 2021
AWSSecurityHubServiceRolePolicy— Ajouté à la liste des politiques gérées	Ajout d'informations sur la politique gérée AWSSecurityHubServiceRolePolicy, qui est utilisée par le rôle lié au service Security Hub CSPM.	11 juin 2021
AWSSecurityHubOrganizationsAccess— Nouvelle politique	Security Hub CSPM a ajouté une nouvelle politique qui accorde les autorisations nécessaires à l'intégration de Security Hub CSPM aux organisations.	15 mars 2021
Security Hub CSPM a commencé à suivre les modifications	Security Hub CSPM a commencé à suivre les modifications apportées à ses politiques AWS gérées.	15 mars 2021

Résolution des problèmes AWS Security Hub CSPM identité et accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation AWS Security Hub CSPM d'un IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Security Hub CSPM
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite accéder par programmation à Security Hub CSPM
- Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à Security Hub CSPM
- Je veux autoriser des personnes extérieures à mon Compte AWS pour accéder aux ressources CSPM de mon Security Hub

Je ne suis pas autorisé à effectuer une action dans Security Hub CSPM

Si cela vous Console de gestion AWS indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` essaie d'utiliser la console pour afficher les détails d'un *`widget`* mais n'y est pas `securityhub:`*`GetWidget`* autorisé.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `securityhub:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Security Hub.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Security Hub. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite accéder par programmation à Security Hub CSPM

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la section Connexion pour le

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
		développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, reportez-vous AWS CLI à la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à Security Hub CSPM

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Je veux autoriser des personnes extérieures à mon Compte AWS pour accéder aux ressources CSPM de mon Security Hub

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Security Hub prend en charge ces fonctionnalités, consultezComment Security Hub fonctionne avec IAM.
- Pour savoir comment donner accès à vos ressources par l'intermédiaire de celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS qui vous appartient dans le Guide de l'utilisateur IAM.
- Pour savoir comment donner accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Validation de conformité pour AWS Security Hub CSPM

Notre nouvelle expérience AWS d'inscription n'est pas conçue pour les charges de travail réglementées. Si vous utilisez notre nouvelle interface d' AWS inscription, mais que vous souhaitez l'utiliser AWS pour des charges de travail réglementées, vous pouvez vous inscrire à des fonctionnalités AWS (avancées) ou activer des fonctionnalités avancées pour votre AWS environnement.

Pour savoir si un s' Service AWS inscrit dans le cadre de programmes de conformité spécifiques, consultez Services AWS la section Étendue par programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Résilience dans AWS Hub de sécurité

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur Régions AWS les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans AWS Security Hub CSPM

En tant que service géré, AWS Security Hub CSPM il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et la manière de AWS protéger l'infrastructure, consultez AWS Cloud Security. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans Security Pillar AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder à Security Hub CSPM via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Suites de chiffrement avec une confidentialité directe parfaite (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

AWS Security Hub CSPM et les points de terminaison VPC d'interface (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre VPC et AWS Security Hub CSPM en créant un point de terminaison VPC d'interface. Les points de terminaison de l'interface sont alimentés par AWS PrivateLink une technologie qui vous permet d'accéder en privé aux API CSPM de Security Hub sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API CSPM de Security Hub. Le trafic entre votre VPC et Security Hub CSPM ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux. Pour plus d'informations, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC avec interface dans le guide Amazon Virtual Private Cloud.

Considérations relatives aux terminaux VPC Security Hub CSPM

Avant de configurer un point de terminaison VPC d'interface pour Security Hub CSPM, assurez-vous de consulter les prérequis et les autres informations figurant dans le guide Amazon Virtual Private Cloud.

Security Hub CSPM prend en charge les appels vers toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison VPC d'interface pour Security Hub CSPM

Vous pouvez créer un point de terminaison VPC pour le service Security Hub CSPM à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez la section Créer un point de terminaison VPC dans le guide Amazon Virtual Private Cloud.

Créez un point de terminaison VPC pour Security Hub CSPM en utilisant le nom de service suivant :

`com.amazonaws.region.securityhub`

Où se *region* trouve le code de région applicable Région AWS.

Si vous activez le DNS privé pour le terminal, vous pouvez envoyer des demandes d'API à Security Hub CSPM en utilisant son nom DNS par défaut pour la région, par exemple `securityhub.us-east-1.amazonaws.com` pour la région USA Est (Virginie du Nord).

Création d'une politique de point de terminaison VPC pour Security Hub CSPM

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à Security Hub CSPM. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez la section Contrôler l'accès aux terminaux VPC à l'aide de politiques relatives aux terminaux dans le guide Amazon Virtual Private Cloud.

Exemple : politique de point de terminaison VPC pour les actions CSPM de Security Hub

Voici un exemple de politique de point de terminaison pour Security Hub CSPM. Lorsqu'elle est attachée à un terminal, cette politique donne accès aux actions CSPM de Security Hub répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
```

```
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Sous-réseaux partagés

Vous ne pouvez pas créer, décrire, modifier ou supprimer des points de terminaison d'un VPC dans des sous-réseaux qui sont partagés avec vous. Toutefois, vous pouvez utiliser les points de terminaison d'un VPC dans les sous-réseaux qui sont partagés avec vous. Pour plus d'informations sur le partage de VPC, consultez la section Partager vos sous-réseaux VPC avec d'autres comptes dans le guide Amazon Virtual Private Cloud.

Journalisation des appels de l'API Security Hub avec CloudTrail

AWSSecurity Hub CSPM est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Security Hub CSPM. CloudTrail capture les appels d'API pour Security Hub CSPM sous forme d'événements. Les appels capturés incluent des appels provenant de la console Security Hub CSPM et des appels de code vers les opérations de l'API Security Hub CSPM. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Security Hub CSPM. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents sur la CloudTrail console dans Historique des événements. À l'aide des informations CloudTrail collectées, vous pouvez déterminer la demande envoyée à Security Hub CSPM, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, notamment comment le configurer et l'activer, consultez le guide de AWS CloudTrail l'utilisateur.

Informations CSPM du Security Hub dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité événementielle prise en charge se produit dans Security Hub CSPM, cette activité est

enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte . Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre compte, y compris ceux liés au Security Hub CSPM, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Security Hub CSPM prend en charge l'enregistrement de toutes les actions de l'API Security Hub CSPM sous forme d'événements dans des journaux. CloudTrail Pour consulter la liste des opérations CSPM du Security Hub, consultez le document de référence de l'API CSPM du Security Hub.

Lorsque l'activité associée aux actions suivantes est enregistrée CloudTrail, la valeur de `responseElements` est définie sur`null`. Cela garantit que les informations sensibles ne sont pas incluses dans CloudTrail les journaux.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou Gestion des identités et des accès AWS (IAM)
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Exemple : entrées du fichier journal CSPM du Security Hub

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateInsight`action. Dans cet exemple, une information appelée `Test Insight` est créée. L'attribut `ResourceId` est spécifié en tant qu'agrégateur Group by (Regrouper par), et aucun filtre facultatif n'est spécifié pour ces informations. Pour en savoir plus sur les informations, consultez Afficher des informations dans Security Hub CSPM.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
```

```
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Balisage des ressources du Security Hub

Une balise est une étiquette facultative que vous pouvez définir et attribuer aux AWS ressources, notamment à certains types de ressources AWS Security Hub CSPM. Les balises peuvent vous aider à identifier, classer et gérer ces types de ressources de différentes façons, notamment par objectif, par propriétaire, par environnement ou selon d’autres critères. Par exemple, vous pouvez utiliser des balises pour distinguer les ressources, identifier les ressources qui répondent à certaines exigences de conformité ou à certains flux de travail, ou répartir les coûts.

Vous pouvez ajouter des balises aux types de ressources CSPM du Security Hub suivants :

- Règles d’automatisation
- Politiques de configuration
- Hub ressource

Principes fondamentaux du balisage

Une ressource peut avoir jusqu'à 50 balises. Chaque balise est constituée d'une clé de balise obligatoire et d'une valeur de balise facultative que vous définissez. Une clé de balise est une étiquette générale qui fait office de catégorie pour une valeur de balise plus spécifique. Une valeur de balise tient lieu de descripteur pour une clé de balise.

Par exemple, si vous créez différentes règles d'automatisation pour différents environnements (un ensemble de règles d'automatisation pour les comptes de test et un autre pour les comptes de production), vous pouvez attribuer une clé de `Environment` balise à ces règles. La valeur de balise associée peut `Test` correspondre aux règles associées aux comptes de test et `Prod` aux règles associées aux comptes de production et aux unités d'organisation.

Lorsque vous définissez et attribuez des balises aux ressources AWS Security Hub CSPM, gardez à l'esprit les points suivants :

- Chaque ressource peut avoir un maximum de 50 balises.
- Pour chaque ressource, chaque clé de balise doit être unique et ne peut avoir qu'une seule valeur de balise.
- Les clés et les valeurs des balises distinguent les majuscules et minuscules. À titre de bonne pratique, nous vous recommandons de définir une stratégie de capitalisation des balises et de mettre en œuvre cette stratégie de manière cohérente dans l'ensemble de vos ressources.

- Une clé de balise peut comporter un maximum de 128 UTF-8 caractères. La valeur d'une balise peut comporter un maximum de 256 UTF-8 caractères. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @
- Le `aws:` préfixe est réservé à l'usage deAWS. Vous ne pouvez pas l'utiliser dans les clés ou les valeurs de balise que vous définissez. En outre, vous ne pouvez pas modifier ou supprimer les clés de balise ou les valeurs qui utilisent ce préfixe. Les balises qui utilisent ce préfixe ne sont pas comptabilisées dans le quota de 50 balises par ressource.
- Tous les tags que vous attribuez ne sont disponibles que pour vous Compte AWS et uniquement dans le pays Région AWS dans lequel vous les attribuez.
- Si vous attribuez des balises à une ressource à l'aide de Security Hub CSPM, les balises ne sont appliquées qu'à la ressource stockée directement dans Security Hub CSPM dans le cas applicable. Région AWS Ils ne s'appliquent à aucune ressource de support associée que Security Hub CSPM crée, utilise ou gère pour vous dans d'autres domaines. Services AWS Par exemple, si vous attribuez des balises à une règle d'automatisation qui met à jour les résultats relatifs à Amazon Simple Storage Service (Amazon S3), les balises sont appliquées uniquement à votre règle d'automatisation dans Security Hub CSPM pour la région spécifiée. Ils ne sont pas appliqués à vos compartiments S3. Pour attribuer également des balises à une ressource associée, vous pouvez utiliser Groupes de ressources AWS ou Service AWS celle qui stocke la ressource, par exemple Amazon S3 pour un compartiment S3. L'attribution de balises aux ressources associées peut vous aider à identifier les ressources de support pour vos ressources Security Hub CSPM.
- Si vous supprimez une ressource, toutes les balises qui lui sont attribuées sont également supprimées.

> **Important**
>
> Ne stockez pas de données confidentielles ou d'autres types de données sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnesServices AWS, notammentAWS Billing and Cost Management. Ils ne sont pas destinés à être utilisés pour des données sensibles.

Pour ajouter et gérer des balises pour les ressources Security Hub CSPM, vous pouvez utiliser la console Security Hub CSPM, l'API Security Hub CSPM ou l'API de balisage. Groupes de ressources AWS Avec Security Hub CSPM, vous pouvez ajouter des balises à une ressource lorsque vous la créez. Vous pouvez également ajouter et gérer des balises pour des ressources existantes

individuelles. Avec Resource Groups, vous pouvez ajouter et gérer des balises en bloc pour plusieurs ressources existantes réparties sur plusieursServices AWS, y compris Security Hub CSPM.

Pour obtenir des conseils supplémentaires sur le balisage et les meilleures pratiques, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur des AWSressources de balisage.

Utilisation de balises dans les politiques IAM

Une fois que vous avez commencé à baliser les ressources, vous pouvez définir des autorisations basées sur des balises au niveau des ressources dans les politiques Gestion des identités et des accès AWS (IAM). En utilisant les balises de cette manière, vous pouvez mettre en œuvre un contrôle granulaire des utilisateurs et des rôles autorisés à créer et à étiqueter des ressources, et des utilisateurs et rôles autorisés à ajouter, modifier et supprimer des balises de manière plus générale. Compte AWS Pour contrôler l'accès en fonction des balises, vous pouvez utiliser les clés de condition associées aux balises dans l'élément Condition des politiques IAM.

Par exemple, vous pouvez créer une politique IAM qui permet à un utilisateur d'avoir un accès complet à toutes les ressources CSPM du AWS Security Hub, si le `Owner` tag de la ressource indique son nom d'utilisateur :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Si vous définissez des autorisations au niveau des ressources basées sur des balises, les autorisations prennent effet immédiatement. Vos ressources sont ainsi plus sécurisées dès leur création et vous pouvez rapidement commencer à appliquer l'utilisation des balises pour les nouvelles ressources. Vous pouvez également utiliser des autorisations au niveau des ressources afin de contrôler les clés et les valeurs de balise qui peuvent être associés à des ressources nouvelles et existantes. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises dans le guide de l'utilisateur IAM.

Ajouter des balises aux ressources CSPM du Security Hub

Une balise est une étiquette que vous pouvez définir et attribuer à AWS des ressources, notamment à certains types de ressources AWS Security Hub CSPM. À l'aide de balises, vous pouvez identifier, classer et gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Par exemple, vous pouvez utiliser des balises pour : appliquer des politiques, répartir les coûts, distinguer les versions des ressources ou identifier les ressources qui répondent à certaines exigences de conformité ou à certains flux de travail.

Vous pouvez ajouter des balises aux types de ressources CSPM du Security Hub suivants :

- Règles d'automatisation
- Politiques de configuration
- Hub ressource

Une ressource peut avoir jusqu'à 50 balises. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Une clé de balise est une étiquette générale qui fait office de catégorie pour une valeur de balise plus spécifique. Une valeur de balise tient lieu de descripteur pour une clé de balise. Pour plus d'informations sur les options et les exigences en matière de balisage, consultezPrincipes fondamentaux du balisage.

Pour ajouter des balises à une ressource Security Hub CSPM, vous pouvez utiliser la console Security Hub CSPM ou l'API Security Hub CSPM. Cependant, la console ne prend pas en charge l'ajout de balises à la Hub ressource.

Après avoir ajouté des balises, vous pouvez modifier la balise et modifier la clé ou la valeur de la balise.

Pour ajouter ou modifier des balises pour plusieurs ressources CSPM du Security Hub en même temps, utilisez les opérations de balisage de l'API de balisage. Groupes de ressources AWS

> **Important**
>
> L'ajout de balises à une ressource peut affecter l'accès à cette ressource. Avant d'ajouter une balise à une ressource, passez en revue les politiques Gestion des identités et des accès AWS (IAM) susceptibles d'utiliser des balises pour contrôler l'accès aux ressources.

Console

Pour ajouter des balises à une ressource Security Hub CSPM (console)

Lorsque vous créez une règle d'automatisation ou une politique de configuration, la console Security Hub CSPM propose des options permettant d'y ajouter des balises. Vous pouvez fournir la clé et la valeur de la balise dans la section Tags.

Security Hub CSPM API

Pour ajouter des balises à une ressource CSPM (API) du Security Hub

Pour créer une ressource et y ajouter une ou plusieurs balises par programmation, utilisez l'opération appropriée au type de ressource que vous souhaitez créer :

- Pour créer une politique de configuration et y ajouter une ou plusieurs balises, appelez l'CreateConfigurationPolicyAPI ou, si vous l'utilisezAWS CLI, exécutez la commande create-configuration-policy.
- Pour créer une règle d'automatisation et y ajouter une ou plusieurs balises, appelez l'CreateAutomationRuleAPI ou, si vous l'utilisezAWS CLI, exécutez la commande create-automation-rule.
- Pour activer Security Hub CSPM et ajouter une ou plusieurs balises à votre Hub ressource, appelez l'EnableSecurityHubAPI ou, si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande enable-security-hub.

Dans votre demande, utilisez le `tags` paramètre pour spécifier la clé de balise et la valeur de balise facultative pour chaque balise à ajouter à la ressource. Le `tags` paramètre spécifie un tableau d'objets. Chaque objet spécifie une clé de balise et la valeur de balise associée.

Pour ajouter une ou plusieurs balises à une ressource existante, utilisez l'TagResourceAPI Security Hub CSPM ou, si vous utilisez laAWS CLI, exécutez la commande tag-resource. Dans votre demande, spécifiez le Amazon Resource Name (ARN) de la ressource à laquelle vous souhaitez ajouter une balise. Utilisez le `tags` paramètre pour spécifier la clé de balise (`key`) et la valeur de balise facultative (`value`) pour chaque balise à ajouter. Le `tags` paramètre spécifie un tableau d'objets, un objet pour chaque clé de balise et la valeur de balise associée.

Par exemple, la AWS CLI commande suivante ajoute une clé de `Environment` balise avec une valeur de `Prod` balise à la politique de configuration spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

Exemple de commande CLI :

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

Où :

- `resource-arn`spécifie l'ARN de la politique de configuration à laquelle ajouter une balise.
- *`Environment`*est la clé de balise de la balise à ajouter à la règle.
- *`Prod`*est la valeur de balise pour la clé de balise spécifiée (*`Environment`*).

Dans l'exemple suivant, la commande ajoute plusieurs balises à la politique de configuration.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Pour chaque objet d'un `tags` tableau, les `value` arguments `key` et sont obligatoires. Toutefois, la valeur de l'`value`argument peut être une chaîne vide. Si vous ne souhaitez pas associer une valeur de balise à une clé de balise, ne spécifiez pas de valeur pour l'`value`argument. Par exemple, la commande suivante ajoute une clé de `Owner` balise sans valeur de balise associée :

```
$ aws securityhub tag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Si une opération de balisage réussit, Security Hub CSPM renvoie une réponse HTTP 200 vide. Sinon, Security Hub CSPM renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Modification des balises pour les ressources CSPM du Security Hub

À mesure que votre environnement ou vos exigences évoluent au fil du temps, vous pouvez évaluer les balises existantes pour vos ressources AWS Security Hub CSPM et modifier les balises si nécessaire. Une étiquette est une étiquette que vous définissez et attribuez à une ou plusieurs AWS ressources, y compris certains types de ressources Macie. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Une clé de balise est une étiquette générale qui fait office de catégorie pour une valeur de balise plus spécifique. Une valeur de balise tient lieu de descripteur pour une clé de balise.

Les balises peuvent vous aider à identifier, classer et gérer ces types de ressources de différentes façons, notamment par objectif, par propriétaire, par environnement ou selon d'autres critères. Par exemple, vous pouvez utiliser des balises pour : appliquer des politiques, répartir les coûts, distinguer les versions des ressources ou identifier les ressources qui répondent à certaines exigences de conformité ou à certains flux de travail.

Vous pouvez ajouter des balises aux types de ressources CSPM du Security Hub suivants :

- Règles d'automatisation
- Politiques de configuration
- Hub ressource

Pour modifier les clés ou les valeurs de balise d'une ressource Security Hub CSPM, vous pouvez utiliser l'API Security Hub CSPM. La console Security Hub CSPM ne prend actuellement pas en charge la modification des balises.

> **Important**
>
> La modification des balises d'une ressource peut affecter l'accès à cette ressource. Avant de modifier une balise pour une ressource, passez en revue les politiques Gestion des identités et des accès AWS (IAM) susceptibles d'utiliser des balises pour contrôler l'accès aux ressources.

Security Hub CSPM API

Pour modifier les balises d'une ressource CSPM (API) du Security Hub

Lorsque vous modifiez une balise pour une ressource par programmation, vous remplacez la balise existante par de nouvelles valeurs. Par conséquent, la meilleure façon de modifier une balise dépend de la modification d'une clé de balise, d'une valeur de balise ou des deux. Pour modifier une clé de balise, supprimez la balise actuelle et ajoutez-en une nouvelle.

Pour modifier ou supprimer uniquement la valeur de balise associée à une clé de balise, remplacez la valeur existante à l'aide de l'TagResourceAPI Security Hub CSPM. Si vous utilisez leAWS CLI, exécutez la commande tag-resource. Dans votre demande, spécifiez le Amazon Resource Name (ARN) de la ressource dont vous souhaitez modifier ou supprimer la valeur de balise.

Pour modifier la valeur d'une balise, utilisez le `tags` paramètre pour spécifier la clé de balise dont vous souhaitez modifier la valeur de balise. Vous devez également spécifier la nouvelle valeur de balise pour la clé. Par exemple, la AWS CLI commande suivante modifie la valeur de balise de `Prod` à `Test` pour la clé de `Environment` balise affectée à la règle d'automatisation spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Où :

- `resource-arn`spécifie l'ARN de la politique de configuration.
- *`Environment`*est la clé de balise associée à la valeur de balise à modifier.

- *Test*est la nouvelle valeur de balise pour la clé de balise spécifiée (*Environment*).

Pour supprimer une valeur de balise d'une clé de balise, ne spécifiez pas de valeur pour l'`value`argument de la clé dans le `tags` paramètre. Par exemple :

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Si l'opération réussit, Security Hub CSPM renvoie une réponse HTTP 200 vide. Sinon, Security Hub CSPM renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Révision des balises pour les ressources CSPM du Security Hub

Après avoir ajouté ou modifié des balises pour les ressources AWS Security Hub CSPM, vous pouvez voir les clés de balise et les valeurs de balise que possède actuellement une ressource. Une étiquette est une étiquette que vous définissez et attribuez à une ou plusieurs AWS ressources, y compris certains types de ressources Macie. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Une clé de balise est une étiquette générale qui fait office de catégorie pour une valeur de balise plus spécifique. Une valeur de balise tient lieu de descripteur pour une clé de balise.

Les balises peuvent vous aider à identifier, classer et gérer ces types de ressources de différentes façons, notamment par objectif, par propriétaire, par environnement ou selon d'autres critères. Par exemple, vous pouvez utiliser des balises pour : appliquer des politiques, répartir les coûts, distinguer les versions des ressources ou identifier les ressources qui répondent à certaines exigences de conformité ou à certains flux de travail.

Vous pouvez ajouter des balises aux types de ressources CSPM du Security Hub suivants :

- Règles d'automatisation
- Politiques de configuration
- Hub ressource

Vous pouvez consulter les balises d'une règle d'automatisation ou d'une politique de configuration Security Hub CSPM à l'aide de la console Security Hub CSPM ou de l'API Security Hub CSPM. La

console ne prend pas en charge la révision des balises de la Hub ressource. Par programmation, vous pouvez consulter les balises de n'importe quelle ressource.

Pour consulter les balises de plusieurs ressources CSPM du Security Hub en même temps, utilisez les opérations de balisage de l'API de balisage. Groupes de ressources AWS

Console

Pour consulter les balises d'une ressource Security Hub CSPM (console)

1. À l'aide des informations d'identification de l'administrateur Security Hub CSPM, ouvrez la console AWS Security Hub CSPM à l'adresse. https://console.aws.amazon.com/securityhub/
2. Selon le type de ressource auquel vous souhaitez ajouter une balise, effectuez l'une des opérations suivantes :
   - Pour consulter les balises d'une règle d'automatisation, choisissez Automations dans le volet de navigation. Choisissez ensuite une règle d'automatisation.
   - Pour consulter les balises d'une politique de configuration, choisissez Configuration dans le volet de navigation. Ensuite, dans l'onglet Stratégies, sélectionnez l'option à côté d'une politique de configuration. Un panneau latéral s'ouvre et indique le nombre de balises attribuées à la politique. Vous pouvez développer l'en-tête Tags pour afficher les clés et les valeurs des balises.

La section Balises répertorie toutes les balises actuellement attribuées à la ressource.

Security Hub CSPM API

Pour consulter les balises d'une ressource CSPM (API) du Security Hub

Pour récupérer et consulter les balises d'une ressource existante, appelez l'ListTagsForResourceAPI. Dans votre demande, utilisez le `resourceArn` paramètre pour spécifier le nom de ressource Amazon (ARN) de la ressource.

Si vous utilisez leAWS CLI, exécutez la commande list-tags-for-resource et utilisez le paramètre `resource-arn` pour spécifier l'ARN de la ressource. Par exemple :

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Si l'opération aboutit, Security Hub CSPM renvoie un tableau. `tags` Chaque objet du tableau spécifie une balise (clé de balise et valeur de balise) actuellement attribuée à la ressource. Par exemple :

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Où `Environment``CostCenter`, et `Owner` sont les clés de balise attribuées à la ressource. `Prod`est la valeur de balise associée à la clé de `Environment` balise. `12345`est la valeur de balise associée à la clé de `CostCenter` balise. Aucune valeur de `Owner` balise n'est associée à la clé de balise.

Pour récupérer la liste de toutes les ressources Security Hub CSPM dotées de balises et de toutes les balises attribuées à chacune de ces ressources, utilisez le GetResourcesfonctionnement de l'API de Groupes de ressources AWS balisage. Dans votre demande, définissez la valeur du `ResourceTypeFilters` paramètre sur`securityhub`. Pour ce faireAWS CLI, exécutez la commande get-resources et définissez la valeur du `resource-type-filters` paramètre sur. `securityhub` Par exemple :

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Si l'opération aboutit, Resource Groups renvoie un `ResourceTagMappingList` tableau. Le tableau contient un objet pour chaque ressource Security Hub CSPM dotée de balises. Chaque objet spécifie l'ARN d'une ressource Security Hub CSPM, ainsi que les clés de balise et les valeurs attribuées à la ressource.

Supprimer les balises des ressources CSPM du Security Hub

Si vous ajoutez des balises à une ressource AWS Security Hub CSPM, vous pouvez ensuite en supprimer une ou plusieurs. Une balise est une étiquette que vous définissez et attribuez aux AWS ressources, notamment à certains types de ressources Security Hub CSPM. Vous pouvez ajouter, modifier et supprimer des balises dans les types suivants de ressources Security Hub CSPM : règles d'automatisation, politiques de configuration et ressource. Hub

Pour supprimer des balises d'une ressource AWS Security Hub CSPM individuelle, vous pouvez utiliser l'API Security Hub CSPM. La console Security Hub CSPM ne prend actuellement pas en charge la suppression des balises.

Pour supprimer des balises de plusieurs ressources CSPM du Security Hub en même temps, utilisez les opérations de balisage de l'API de balisage. Groupes de ressources AWS

> **Important**
>
> La suppression de balises d'une ressource peut affecter l'accès à cette ressource. Avant de supprimer un tag, passez en revue les politiques Gestion des identités et des accès AWS (IAM) susceptibles d'utiliser le tag pour contrôler l'accès aux ressources.

Security Hub CSPM API

Pour supprimer des balises d'une ressource CSPM (API) du Security Hub

Pour supprimer une ou plusieurs balises d'une ressource par programmation, utilisez l'API UntagResourceSecurity Hub CSPM. Dans votre demande, utilisez le `resourceArn` paramètre pour spécifier le nom de ressource Amazon (ARN) de la ressource dont vous souhaitez supprimer une balise. Utilisez le `tagKeys` paramètre pour spécifier la clé de balise de la balise à supprimer. Pour supprimer plusieurs balises, ajoutez le `tagKeys` paramètre et l'argument de chaque balise à supprimer, séparés par une esperluette (&), par exemple,. `tagKeys=key1&tagKeys=key2` Pour supprimer uniquement une valeur de balise spécifique (et non une clé de balise) d'une ressource, modifiez la balise au lieu de la supprimer.

Si vous utilisez leAWS CLI, exécutez la commande untag-resource pour supprimer une ou plusieurs balises d'une ressource. Pour le `resource-arn` paramètre, spécifiez l'ARN de la ressource dont vous souhaitez supprimer une balise. Utilisez le `tag-keys` paramètre pour spécifier la clé de balise de la balise à supprimer. Par exemple, la commande suivante supprime

la `Environment` balise (à la fois la clé et la valeur de la balise) de la politique de configuration spécifiée :

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Where `resource-arn` indique l'ARN de la politique de configuration dont il faut supprimer une balise et *`Environment`* indique la clé de balise de la balise à supprimer.

Pour supprimer plusieurs balises d'une ressource, ajoutez chaque clé de balise supplémentaire en tant qu'argument pour le `tag-keys` paramètre. Par exemple :

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Si l'opération réussit, Security Hub CSPM renvoie une réponse HTTP 200 vide. Sinon, Security Hub CSPM renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Quotas pour Security Hub

Vous Compte AWS disposez de certains quotas par défaut, anciennement appelés limites, pour chacun d'entre euxService AWS. Ces quotas correspondent au nombre maximum de ressources de service ou d'opérations pour votre compte. Cette rubrique contient des liens vers les quotas qui s'appliquent aux ressources et aux opérations du AWS Security Hub pour votre compte. Sauf indication contraire, chaque quota s'applique à votre compte dans chacune d'entre ellesRégion AWS.

Certains quotas peuvent être augmentés, mais pas tous. Pour demander l'augmentation d'un quota, utilisez la console Service Quotas. Pour savoir comment demander une augmentation, consultez la section Demander une augmentation de quota dans le Guide de l'utilisateur du Service Quotas. Si aucun quota n'est disponible sur la console Service Quotas, utilisez le formulaire d'augmentation des limites de service sur le AWS Support Center Console pour demander une augmentation du quota.

Quotas maximaux

Pour obtenir la liste des quotas qui s'appliquent aux ressources du AWS Security Hub, consultez AWSla section Points de terminaison et quotas du Security Hub dans le Références générales AWS.

Quotas tarifaires

Pour obtenir la liste des quotas qui s'appliquent aux opérations de l'API AWS Security Hub, consultez le AWSSecurity Hub API Reference.

Si vous configurez l'agrégation entre régions dans Security Hub CSPM, un appel vers les régions liées `BatchImportFindings` et la région d'agrégation aura un `BatchUpdateFindings` impact sur celles-ci. L'`GetFindings`opération extrait les résultats des régions liées et de la région d'agrégation. Cependant, les `UpdateStandardsControl` opérations `BatchEnableStandards` et le sont Region-specific.

Historique des documents pour AWS Security Hub Guide de l'utilisateur

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version de AWS Security Hub et Security Hub CSPM. Pour les versions des nouveaux contrôles CSPM Security Hub, la date indique à quel moment les contrôles commencent à être disponibles dans les versions prises en charge. Régions AWS La disponibilité des contrôles peut prendre 1 à 2 semaines dans toutes les régions prises en charge. Pour plus de détails sur les modifications importantes apportées aux contrôles existants, consultezJournal des modifications pour les contrôles CSPM de Security Hub.

Pour recevoir des notifications concernant les mises à jour du guide de l'utilisateur de AWS Security Hub, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Informations détaillées mises à jour sur les résultats de l'analyse réseau	Ajout d'informations sur les résultats d'information générés par l'analyse réseau.	3 septembre 2026
Liste des ports d'analyse réseau mise à jour	Ajout de la liste des ports actuellement pris en charge par la numérisation réseau.	18 août 2026
Contrôles de sécurité mis à jour	Security Hub CSPM a supprimé le EFS.6 contrôle de la norme FSBP (AWS Foundational Security Best Practices). Ce contrôle reste disponible dans les normes NIST SP 800-53 Rev. 5, NIST SP 800-171 Revision 2 et PCI DSS v4.0.1.	3 août 2026
Documentation d'activation améliorée de Security Hub	Amélioration des instructi ons de la page Gestion de la configuration des comptes	7 juillet 2026

	membres dans une AWS organisation.	
Documentation sur la fonctionnalité de numérisation réseau ajoutée	Ajout de la documentation pour la fonctionnalité d'analyse réseau de Security Hub	7 juillet 2026
Inventaire de l'IA	Ajout de l'inventaire de l'IA, qui fournit une vue unifiée des ressources d'intelligence artificielle (IA) et d'apprent issage automatique (ML) gérées et auto-hébergées dans votre AWS environne ment. Pour plus d'informations, consultez l'inventaire de l'IA dans AWS Security Hub.	7 juillet 2026
Mises à jour d'une politique gérée — `AWSSecuri tyHubV2ServiceRole Policy`	Security Hub a mis à jour la politique AWS gérée nomméeAWSSecuri tyHubV2ServiceRole Policy . Les mises à jour ont ajouté des autorisations pour prendre en charge les intégrati ons tierces, notamment la gestion d'enregistreurs de configuration tiers, la création et la gestion de connecteurs et l'obtention de jetons d'identité Web pour la fédération.	30 juin 2026

Mises à jour d'une politique gérée — `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM a mis à jour la politique AWS gérée nommée. `AWSSecurityHubServiceRolePolicy` Les mises à jour ont ajouté des autorisations pour prendre en charge les intégrations tierces. Il s'agit notamment de gérer des enregistreurs de configuration tiers et de récupérer les mesures de santé du connecteur.	30 juin 2026
Nouvelle norme de sécurité	Security Hub CSPM a publié la norme AI Security Best Practices. Cette norme fournit un ensemble de contrôles sélectionnés qui détectent lorsque les ressources d'IA déployées ne sont pas conformes aux meilleures pratiques de sécurité.	30 juin 2026
Nouveaux contrôles de sécurité	Security Hub CSPM a publié huit nouveaux contrôles pour la norme AI Security Best Practices. Les nouvelles commandes sont les suivantes : Bedrock.1 BedrockAgentCore.7 SageMaker.20 SageMaker.21, SageMaker.22, SageMaker.23, SageMaker.24, et SageMaker.25.	30 juin 2026

Mises à jour du type de caractère d'impact et de la gravité pour les résultats d'exposition	Ajout du type de trait d'impact aux résultats d'exposition. L'impact décrit le rayon d'explosion potentiel en cas de compromission d'une ressource, sur la base des autorisations effectives des Gestion des identités et des accès AWS principaux acteurs associés. Mise à jour du calcul de la gravité pour utiliser une matrice des risques de probabilité et d'impact conforme aux directives du NIST. Ajout de conseils de remédiation par ressource pour les caractéristiques du chemin d'accès aux impacts.	23 juin 2026
Mises à jour des normes et contrôles de sécurité	Nous avons retiré les RDS.18 commandes ECS.1 et les avons retirées de toutes les normes applicables. Depuis le retrait du EC2-Classic réseau Amazon, les instances Amazon Relational Database Service (Amazon RDS) ne peuvent plus être déployées en dehors d'un VPC.	5 juin 2026

Mises à jour pour l'enregistreur lié au service CSPM	Ajout d'informations relatives au nouvel enregistreur de configuration lié aux services qui permet à Security Hub CSPM d'effectuer des contrôles de sécurité en fonction des informations de configuration des ressources.	27 mai 2026
Résultats d'accès non utilisés	Security Hub a ajouté une fonctionnalité permettant de générer et d'afficher les résultats d'accès non utilisés à partir d'IAM Access Analyzer Comprendre les résultats d'accès inutilisés dans Security Hub	19 mai 2026

Nouveaux contrôles de sécurité	Security Hub CSPM a publié cinq nouveaux contrôles . Certains contrôles sont conformes à la norme FSBP (AWS Foundational Security Best Practices). La plupart des commandes sont conformes aux exigences de la norme NIST SP 800-53 Rev. 5. • Pour la norme AWS FSBP, les identifiants des contrôles applicables sont les suivants : BedrockAgentCore.5 et BedrockAgentCore.6. • Pour le NIST SP 800-53 Rev. 5, les identifiants des contrôles applicables sont les suivants : BedrockAgentCore.3, et BedrockAgentCore.4. SageMaker.18	15 mai 2026
Mises à jour d'une politique gérée — `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM a mis à jour la politique AWS gérée nommée. `AWSSecurityHubServiceRolePolicy` Les mises à jour ont ajouté des autorisations pour gérer les enregistreurs de configuration liés aux services Security Hub CSPM et créer le rôle lié aux services. AWS Config	29 avril 2026

Nouveaux contrôles de sécurité	Security Hub CSPM a publié quatre nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices). Les nouvelles commandes sont les suivantes : BedrockAgentCore.1 BedrockAgentCore.2, RDS.51, et SageMaker.19.	22 avril 2026
Nouveaux contrôles de sécurité	Security Hub CSPM a publié cinq nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices). Les nouvelles commandes sont les suivantes : APIGateway.11 EC2.183 EKS.9, SageMaker.16, et SageMaker.17.	7 avril 2026
Mises à jour des normes et contrôles de sécurité	Nous avons retiré les AppSync.6 contrôles AppSync.1 et les avons retirés de la norme FSBP (AWS Foundational Security Best Practices). AWS AppSync fournit désormais un cryptage par défaut sur tous les caches d'API actuels et futurs.	9 mars 2026
Mises à jour des normes et contrôles de sécurité	Nous avons retiré le ECS.1 contrôle et l'avons retiré de la norme FSBP (AWS Foundational Security Best Practices) et de la norme NIST SP 800-53 Rev. 5.	4 mars 2026

Nouveaux contrôles de sécurité	Security Hub CSPM a publié onze nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices). Les nouvelles commandes sont les suivantes : APIGateway.10 ELB.21 ELB.22, RDS.50, SageMaker.9 SageMaker.10 SageMaker.11 SageMaker .12 SageMaker.13 SageMaker.14, et SageMaker .15.	16 février 2026
Mises à jour des normes et contrôles de sécurité	Nous avons retiré le MQ.3 contrôle et l'avons retiré de toutes les normes applicables. Nous avons retiré le contrôle en raison des exigences d'Amazon MQ relatives aux mises à niveau automatiques des versions mineures. Auparavant, ce contrôle s'appliquait à la norme FSBP (AWS Foundational Security Best Practices), à la norme NIST SP 800-53 Rev. 5 et à la norme PCI DSS v4.0.1.	12 janvier 2026

Mises à jour de la documentation relative à l'estimateur de coûts	Ajout de détails à la documentation de l'estimateur de coûts de Security Hub sur la manière d'accorder un accès croisé pour effectuer des estimations dans des comptes autres que le compte de gestion.	12 janvier 2026
Nouveaux contrôles de sécurité	Security Hub CSPM a publié cinq nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices). Les nouvelles commandes sont les suivantes : CloudFormation.4 CloudFront.17 ECS.19, ECS.20, et ECS.21.	6 janvier 2026
Mises à jour des normes et contrôles de sécurité	En raison des exigences d'Amazon MQ relatives aux mises à niveau automatiques des versions mineures, nous prévoyons de retirer MQ.3 et de supprimer le contrôle de toutes les normes applicables le 12 janvier 2026. Actuellement, le contrôle s'applique à la norme FSBP (AWS Foundational Security Best Practices), à la norme NIST SP 800-53 Rev. 5 et à la norme PCI DSS v4.0.1.	12 décembre 2025

Contenu mis à jour pour Service-Managed Standard : AWS Control Tower	Contenu mis à jour pour la version Service-Managed Standard : AWS Control Tower afin de fournir de meilleure s instructions concernant la création, l'affichage et la désactivation des contrôles dans le formulaire standard. AWS Control Tower	8 décembre 2025
Nouveaux contrôles de sécurité	Security Hub CSPM a publié sept nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices). Les nouvelles commandes sont les suivantes : Cognito.4 Cognito.5 Cognito.6, EC2.182, CloudFormation.3, ECS.18, et SES.3.	8 décembre 2025
Contenu mis à jour pour la disponibilité générale de Security Hub	Contenu ajouté pour prendre en charge la version de disponibilité générale de AWS Security Hub	2 décembre 2025
Contenu mis à jour pour Security Hub	Ajout de contenu pour les tendances et l'agrégation des régions. Ces modificat ions sont compatibles avec la version préliminaire de Security Hub.	21 novembre 2025

Mises à jour d'une politique gérée — AWSSecurityHubV2ServiceRolePolicy	Security Hub a mis à jour la politique AWS gérée nomméeAWSSecurityHubV2ServiceRolePolicy . Les mises à jour ont ajouté des fonctionnalités de mesure pour Amazon Elastic Container Registry et Amazon AWS Lambda CloudWatch, ainsi que Gestion des identités et des accès AWS pour prendre en charge les fonctionnalités de Security Hub. Les mises à jour ont également ajouté la prise en charge des AWS Config en registreurs mondiaux. Ces modifications sont compatibles avec la version préliminaire de Security Hub.	17 novembre 2025
Mises à jour d'une politique gérée — AWSSecurityHubOrganizationsAccess	Security Hub a mis à jour la politique AWS gérée nomméeAWSSecurityHubOrganizationsAccess . Les mises à jour ont ajouté des autorisations pour décrire les politiques de ressources qui prennent en charge les fonctionnalités de Security Hub. Ces modifications sont compatibles avec la version préliminaire de Security Hub.	17 novembre 2025

Mises à jour d'une politique gérée — AWSSecurityHubFullAccess	Security Hub a mis à jour la politique AWS gérée nomméeAWSSecurityHubFullAccess . Les mises à jour ont ajouté des fonctionnalités relatives à la gestion GuardDuty, à Amazon Inspector et à la gestion des comptes afin de prendre en charge les fonctionnalités de Security Hub. Ces modifications sont compatibles avec la version préliminaire de Security Hub.	17 novembre 2025
Mises à jour des contrôles de sécurité	Nous avons modifié la sévérité de 10 contrôles CSPM de Security Hub : CloudFront.7 CloudTrail.5 ELB.7, GuardDuty.7, MQ.3, Opensearch.10, RDS.7 ServiceCatalog.1 SNS.4, et. SQS.3 Pour une description détaillée des modifications, consultez le journal des modifications pour les contrôles CSPM de Security Hub.	13 novembre 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié six nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices). Les nouvelles commandes sont les suivantes : Cognito.3 DMS.13 EC2.181, RDS.43, RDS.47, et RDS.48.	28 octobre 2025
Nouvelle norme de sécurité	Security Hub CSPM fournit désormais une norme de sécurité conforme à la norme CIS AWS Foundations Benchmark v5.0.0. Cette nouvelle norme inclut 40 contrôles de sécurité existants . Les contrôles effectuent des contrôles automatisés qui évaluent la conformité de certaines ressources à un sous-ensemble des exigences définies par le cadre.	16 octobre 2025
Nouvelle intégration tierce	Elasticest une nouvelle intégration tierce qui peut recevoir les résultats de Security Hub CSPM.	3 octobre 2025

Mises à jour des normes et contrôles de sécurité	Nous avons retiré les RedshiftServerless.7 commandes Redshift.9 et les avons retirées de toutes les normes applicables. Nous avons retiré ces contrôles en raison des limites inhérente s à Amazon Redshift qui empêchaient de corriger efficacement `FAILED` les résultats des contrôles. Auparavant, ces contrôles s'appliquaient à la norme FSBP (AWS Foundational Security Best Practices) et à la norme NIST SP 800-53 Rev. 5. Le Redshift.9 contrôle s'appliquait également à la norme de AWS Control Tower gestion des services.	24 septembre 2025
Disponibilité par région	Security Hub CSPM est désormais disponible dans la région Asie-Pacifique (Nouvelle-Zélande). Pour une liste complète des Régions AWS endroits où Security Hub CSPM est actuellem ent disponible, consultez la section Points de terminaison et quotas AWS Security Hub dans le. Références générales AWS	19 septembre 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié deux nouveaux contrôles pour la norme FSBP (AWS Foundational Security Best Practices) : et. CloudFront.16 RDS.46	3 septembre 2025
Disponibilité par région	La norme AWS Resource Tagging est désormais disponible dans les régions Asie-Pacifique (Thaïlande) et Mexique (Centre).	29 août 2025
Mises à jour des normes et contrôles de sécurité	En raison des limites d'Amazon Redshift, nous prévoyons de retirer les RedshiftServerless.7 commandes Redshift.9 et de les supprimer de toutes les normes applicables le 15 septembre 2025. Actuellement, ces contrôles s'appliquent à la norme FSBP (AWS Foundational Security Best Practices) et à la norme NIST SP 800-53 Rev. 5. Le Redshift.9 contrôle s'applique également à la norme de AWS Control Tower gestion des services.	15 août 2025

Nouvel objet contenant les détails des ressources dans l'ASFF	Le format ASFF (AWS Security Finding Format) inclut désormais un objet `CodeRepository` ressource. Cet objet fournit des informations sur un référentiel de code externe que vous avez connecté à AWS des ressources et que vous avez configuré Amazon Inspector pour détecter les vulnérabilités.	1er août 2025
Disponibilité par région	Security Hub CSPM est désormais disponible dans la région Asie-Pacifique (Taipei). Pour une liste complète des Régions AWS endroits où Security Hub CSPM est actuellement disponible, consultez la section Points de terminaison et quotas AWS Security Hub dans le. Références générales AWS	23 juillet 2025
Nouvelle intégration tierce	Dynatraceest une nouvelle intégration tierce qui peut recevoir les résultats de Security Hub CSPM.	18 juillet 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié 13 nouveaux contrôles. La plupart des contrôles sont conformes à la norme FSBP (AWS Foundational Security Best Practices). Certaines commandes sont conformes aux exigences de la norme NIST SP 800-53 Rev. 5. • Pour la norme AWS FSBP, les identifiants des contrôles applicables sont les suivants : CloudFront.15 Cognito.2 EC2.180 ELB.18 MSK.4, MSK.5, MSK.6, RDS.45, Redshift.18, S3.25 SSM.6, et SSM.7. • Pour le NIST SP 800-53 Rev. 5, les identifiants des contrôles applicables sont les suivants : et. Lambda.7 RDS.45	15 juillet 2025

Mises à jour de la génération des résultats de contrôle	Pour vous aider à suivre les changements de conformité, Security Hub CSPM met désormais à jour les résultats de contrôle existants, au lieu d'en générer de nouveaux, lorsque l'état de conformité de certaines ressources change. Cela signifie que vous pouvez utiliser les données fournies par les résultats individuels pour suivre les changements de conformité de certaines ressources par rapport à des contrôles particuliers.	3 juillet 2025
Mises à jour des normes et contrôles de sécurité	Nous avons supprimé le IAM.13 contrôle de la norme PCI DSS v4.0.1. Nous avons également supprimé le IAM.17 contrôle de la norme NIST SP 800-171 Revision 2. Les normes n'exigent pas explicitement les contrôles fournis par ces contrôles. Nous avons également mis à jour les informations relatives aux exigences associées à ces normes pour certains contrôles qui vérifient les politiques de mot de passe IAM : IAM.7 et IAM.10 via IAM.17.	30 juin 2025

Mises à jour de la recherche de rétention	Security Hub CSPM stocke désormais les résultats archivés pendant 30 jours au lieu de 90 jours, ce qui permet de réduire le bruit de recherche. Pour une conservation à long terme, vous pouvez exporter les résultats vers un compartiment S3 en utilisant une action personnalisée associée à une règle Amazon EventBridge .	20 juin 2025
Mises à jour des politiques gérées existantes	Security Hub CSPM a ajouté une nouvelle autorisation à la politique AWS gérée nommée. `AWSSecurityHubOrganizationsAccess` L'autorisation permet à la direction de l'organisation d'activer et de gérer Security Hub et Security Hub CSPM au sein d'une organisation. Security Hub CSPM a également ajouté une nouvelle autorisation à la politique AWS gérée nommée. `AWSSecurityHubFullAccess` L'autorisation permet aux administrateurs de créer un rôle lié à un service pour Security Hub.	18 juin 2025

Version préliminaire publique et nouvelle politique gérée pour Security Hub	Version préliminaire publique de AWS Security Hub et du guide de l'utilisateur AWS de Security Hub . Cette version inclut une nouvelle politique AWS gérée,`AWSSecurityHubV2ServiceRolePolicy` . La politique permet à Security Hub de gérer AWS Config les règles et les ressources Security Hub dans l'organisation du client et pour le compte de celui-ci. Security Hub est en version préliminaire et est susceptible d'être modifiée.	17 juin 2025
Mises à jour des normes et contrôles de sécurité	Nous avons supprimé le IAM.10 contrôle de la norme PCI DSS v4.0.1. Ce contrôle vérifie si les politiques relatives aux mots de passe des comptes pour les utilisateurs IAM répondent aux exigences minimales, notamment une longueur de mot de passe minimale de 7 caractères. La norme PCI DSS v4.0.1 exige désormais que les mots de passe comportent au moins 8 caractères. Le IAM.10 contrôle continue de s'appliquer à la norme PCI DSS v3.2.1, qui impose des exigences de mot de passe différentes.	30 mai 2025

Nouvelle norme de sécurité	Security Hub CSPM fournit désormais une norme de sécurité qui s'aligne sur le cadre de cybersécurité et de conformité du NIST SP 800-171 Revision 2. Cette nouvelle norme inclut plus de 60 contrôles de sécurité existants. Les contrôles effectuent des contrôles automatisés qui évaluent la conformité de certaines Services AWS ressource s à un sous-ensemble des exigences définies par le cadre.	29 mai 2025
Mises à jour des contrôles de sécurité	Security Hub CSPM a annulé la publication du contrôle suivant dans tous les cas Régions AWS : [RDS.46] Les instances de base de données RDS ne doivent pas être déployées dans des sous-rése aux publics dotés de routes vers des passerelles Internet. Auparavant, ce contrôle était compatible avec la norme FSBP (AWS Foundational Security Best Practices).	8 mai 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié 9 nouveaux contrôles. La plupart des contrôles sont conformes à la norme FSBP (AWS Foundational Security Best Practices). Certaines commandes sont conformes aux exigences de la norme NIST SP 800-53 Rev. 5. • Pour la norme AWS FSBP, les identifiants des contrôles applicables sont les suivants : DocumentDB.6 RDS.44 RedshiftServerless.2, RedshiftServerless.3, RedshiftServerless.5, RedshiftServerless.6, et RedshiftServerless.7 (retiré ultérieurement). • Pour le NIST SP 800-53 Rev. 5, les identifiants des contrôles applicables sont les suivants : CloudTrail.10 RedshiftServerless.4, et RedshiftServerless.7 (retiré ultérieurement).	7 mai 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié 24 nouveaux contrôles. La plupart des contrôles sont conformes aux meilleure s pratiques de sécurité AWS fondamentales (FSBP) ou à la norme AWS Resource Tagging. Certaines commandes sont conformes aux exigences de la norme NIST SP 800-53 Rev. 5. • Pour la norme AWS FSBP, les identifiants des contrôles applicables sont les suivants : EC2.173, RDS.41 RDS.42, et SageMaker.8. • Pour la norme de balisage des AWS ressources, les ID des contrôles applicables sont les suivants : Amplify.1 Amplify.2 Batch.4 DataSync.2 EC2.174 EC2.175 EC2.176, EC2.177, EC2.178, EC2.179, Redshift.17, SageMaker.6, SageMaker .7 SSM.5, Transfer.4 Transfer.5, Transfer.6, et Transfer.7. • Pour le NIST SP 800-53 Rev. 5, les identifiants des contrôles applicables sont les suivants : et. ECS.17 RDS.42	16 avril 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié quatre nouveaux contrôles pour la norme des meilleures AWS pratiques de sécurité fondamentales. Les commandes sont les suivantes : • the section called "[FSx.3] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour le déploiement Multi-AZ" • the section called "[FSx.4] Les systèmes de fichiers FSx pour NetApp ONTAP doivent être configurés pour le déploiement Multi-AZ" • the section called "[FSx.5] Les systèmes de fichiers FSx for Windows File Server doivent être configurés pour Multi-AZ le déploiement" • the section called "[RedshiftServerless.1] Les groupes de travail Amazon Redshift Serverless doivent utiliser un routage VPC amélioré"	18 mars 2025

Mises à jour des normes et contrôles de sécurité	Nous avons supprimé le contrôle RDS.18 de sécurité (retiré ultérieurement) de la norme AWS Foundational Security Best Practices et avons automatisé les vérifications conformément aux exigences de la norme NIST SP 800-53 Rev. 5. Depuis le retrait du EC2-Classic réseau Amazon, les instances Amazon Relational Database Service (Amazon RDS) ne peuvent plus être déployées en dehors d'un VPC.	07 mars 2025
Mises à jour des résultats des contrôles	Security Hub CSPM génère désormais des `WARNING` résultats pour un contrôle activé si l'enregistrement des ressources n'est pas activé AWS Config pour le type de ressource vérifié par le contrôle. Cela peut vous aider à identifier et à corriger les éventuelles lacunes de configuration lors de vos contrôles de sécurité.	25 février 2025

Nouveaux contrôles de sécurité	Security Hub CSPM a publié 11 nouveaux contrôles. Les commandes sont les suivantes : • the section called "[Connect .2] La CloudWatch journalisation des instances Connect Customer doit être activée" • the section called "[ECR.5] Les référentiels ECR doivent être chiffrés et gérés par le client AWS KMS keys" • the section called "[ELB.17] Les équilibreurs de charge des applications et du réseau dotés d'écouteurs doivent utiliser les politiques de sécurité recommandées" • the section called "[Glue.4] AWS GlueLes tâches Spark doivent s'exécuter sur les versions prises en charge deAWS Glue" • the section called "[GuardDuty.11] La surveillance du temps GuardDuty d'exécution doit être activée" • the section called "[GuardDuty.12] La surveillance du temps d'exécution GuardDuty ECS doit être activée" • the section called "[GuardDuty.13] GuardDuty La	24 février 2025

surveillance du temps d'exécution EC2 doit être activée"

- the section called "[Network Firewall.10] La protection contre les modifications de sous-réseau doit être activée sur les pare-feux Network Firewall"
- the section called "[RDS.40] Les instances de base de données RDS pour SQL Server doivent publier des CloudWatch journaux dans Logs"
- the section called "[SQS.3] Les politiques d'accès aux files d'attente SQS ne doivent pas autoriser l'accès public"
- the section called "[Transfer.3] La journalisation des connecteurs Transfer Family doit être activée"

Nouveaux contrôles de sécurité	Security Hub CSPM a publié 37 nouveaux contrôles pour la norme de balisage des AWS ressources. Security Hub CSPM a également publié les nouveaux contrôles suivants : • the section called "[EMR.3] Les configurations de sécurité Amazon EMR doivent être chiffrées au repos" • the section called "[EMR.4] Les configurations de sécurité Amazon EMR doivent être cryptées pendant le transport" • the section called "[SageMaker.5] SageMaker les modèles doivent avoir l'isolation réseau activée"	22 janvier 2025
Nouveau contrôle de sécurité	Security Hub CSPM a publié les paramètres EC2.172 EC2 VPC Block Public Access qui devraient bloquer le trafic de la passerelle Internet.	15 janvier 2025

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM Security Hub suivants sont disponibles. • the section called "[Cognito.1] La protection contre les menaces des groupes d'utilisateurs Cognito doit être activée avec un mode d'application complète des fonctions pour l'authentification standard" • the section called "[RDS.38] Les instances de base de données RDS pour PostgreSQL doivent être chiffrées en transit" • the section called "[RDS.39] Les instances de base de données RDS pour MySQL doivent être chiffrées en transit" • the section called "[Redshift.16] Les groupes de sous-réseaux du cluster Redshift doivent avoir des sous-réseaux provenant de plusieurs zones de disponibilité"	17 décembre 2024

Security Hub CSPM prend en charge la norme PCI DSS v4.0.1	Security Hub CSPM prend désormais en charge la version 4.0.1 de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Pour plus d'informations sur la norme et les contrôles qui s'y appliquent, consultez la section PCI DSS dans Security Hub CSPM.	11 décembre 2024
Security Hub CSPM reçoit les résultats de la séquence GuardDuty d'attaques	Security Hub CSPM reçoit désormais les résultats des séquences d'attaque s d'Amazon GuardDuty Extended Threat Detection . Les détails relatifs à la détection des séquences d'attaques sont disponibl es dans l'objet Detection du AWS Security Finding Format (ASFF).	1er décembre 2024
Security Hub CSPM est pris en charge dans la nouvelle version Région AWS	Security Hub CSPM est désormais disponible dans la région Asie-Pacifique (Malaisie). Certains contrôles de sécurité ont des limites régionales. Pour obtenir la liste des contrôles qui ne sont pas disponibles dans cette région, consultez la section Limites régionales des contrôles CSPM de Security Hub.	22 novembre 2024

Modifications apportées à Config.1	Security Hub CSPM a augmenté la sévérité du Config.1 contrôle de `MEDIUM` à `CRITICAL` et a ajouté de nouveaux codes d'état et des raisons d'état pour les erreurs de détection. Config.1 Pour plus d'informations sur les modifications, consultez l'entrée du 20 novembre 2024 dans le journal des modifications pour les contrôles CSPM de Security Hub.	20 novembre 2024

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM Security Hub suivants sont disponibles. Ces contrôles font partie des meilleures pratiques de sécurité AWS fondamentales et de la norme NIST SP 800-53 Rev. 5, et ils évaluent si un cloud privé virtuel (VPC) que vous gérez possède une interface, un point de terminaison VPC pour une ressource OR. Service AWS AWS • the section called "[EC2.55] Les VPC doivent être configurés avec un point de terminaison d'interface pour l'API ECR" • the section called "[EC2.56] Les VPC doivent être configurés avec un point de terminaison d'interface pour Docker Registry" • the section called "[EC2.57] Les VPC doivent être configurés avec un point de terminaison d'interface pour Systems Manager" • the section called "[EC2.58] Les VPC doivent être configurés avec un point de terminaison d'interface pour les contacts de Systems Manager Incident Manager" • the section called "[EC2.60] Les VPC doivent être	15 novembre 2024

configurés avec un point de terminaison d'interface pour Systems Manager Incident Manager”

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM Security Hub suivants sont disponibles. • the section called "[AppSync.1]AWS AppSyncLes caches d'API doivent être chiffrés au repos" • the section called "[AppSync.6]AWS AppSyncLes caches d'API doivent être chiffrés pendant le transport" • the section called "[EC2.170] Les modèles de lancement EC2 doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)" • the section called "[EC2.171] La journalisation des connexions VPN EC2 doit être activée" • the section called "[EFS.8] Les systèmes de fichiers EFS doivent être chiffrés au repos" • the section called "[KMS.5] Les clés KMS ne doivent pas être accessibles au public" • the section called "[SNS.4] Les politiques d'accès aux rubriques du SNS ne devraient pas autoriser l'accès public"	18 octobre 2024

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM Security Hub suivants sont disponibles. • the section called "[ECS.16] Les ensembles de tâches ECS ne doivent pas attribuer automatiquement d'adresses IP publiques" • the section called "[GuardDuty.7] La surveillance du temps d'exécution GuardDuty EKS doit être activée" • the section called "[Kinesis.3] Les flux Kinesis doivent avoir une période de conservation des données adéquate" • the section called "[MSK.3] Les connecteurs MSK Connect doivent être chiffrés pendant le transport" • the section called "[RDS.36] Les instances de base de données RDS pour PostgreSQL doivent publier des journaux dans Logs CloudWatch" • the section called "[RDS.37] Les clusters de bases de données Aurora PostgreSQL doivent publier des journaux dans Logs CloudWatch"	3 octobre 2024

- the section called "[S3.24] Les paramètres de blocage de Multi-Region l'accès public aux points d'accès S3 doivent être activés"

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM Security Hub suivants sont disponibles. • the section called "[Athena.4] La journalisation des groupes de travail Athena doit être activée" • the section called "[CodeBuild.7] les exportations de groupes de CodeBuild rapports doivent être cryptées au repos" • the section called "[DataSync.1] la journalisation des DataSync tâches doit être activée" • the section called "[EFS.7] Les sauvegardes automatiques doivent être activées sur les systèmes de fichiers EFS" • Glue.2 (retraité) • the section called "[Glue.3] AWS Glueles transformations de machine learning doivent être cryptées au repos" • the section called "[WorkSpaces.1] les volumes WorkSpaces d'utilisateurs doivent être chiffrés au repos" • the section called "[WorkSpaces.2] les volumes	30 août 2024

	WorkSpaces racine doivent être chiffrés au repos"	
Nouveau panneau de recherche	Le nouveau panneau de recherche de la console Security Hub CSPM vous permet de prendre rapidement des mesures en fonction des résultats, de consulter les détails des ressources et l'historique des recherches, et de rechercher d'autres informations pertinentes concernant une découverte.	16 août 2024
Mettre à jour pour Config.1 contrôler	Le Config.1 contrôle vérifie s'il AWS Config est activé, utilise le rôle lié au service et enregistre les ressources pour les contrôles activés. Security Hub CSPM a ajouté un paramètre de contrôle personnalisé nommé. `includeConfigServiceLinkedRoleCheck` En définissant ce paramètre sur`false`, vous pouvez choisir de ne pas vérifier s'il AWS Config utilise le rôle lié à un service.	15 août 2024

Désigner une région d'origine sans régions liées	Vous pouvez désormais créer un agrégateur de recherches et établir une région d'origine sans lier aucune région Régions AWS à la région d'origine. Cela vous permet d'activer la configuration centralisée sans spécifier de régions liées.	25 juillet 2024

Sélectionnez les commandes disponibles dans d'autres régions	Les contrôles suivants sont désormais disponibles en option Régions AWS, notamment USA Est (Virginie du Nord) et USA Est (Ohio). • the section called "[DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos" • the section called "[DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune" • the section called "[DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé" • the section called "[DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS" • the section called "[DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit" • the section called "[EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des	15 juillet 2024

adresses IP publiques au lancement"

- the section called "[EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés"
- the section called "[FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes"
- the section called "[MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch"
- [MQ.3] Les courtiers Amazon MQ devraient activer la mise à niveau automatique des versions mineures
- the section called "[Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés"
- the section called "[Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes"
- the section called "[SageMaker.4] les variantes de production

de SageMaker terminaux doivent avoir un nombre d'instances initial supérieur à 1"

- the section called "[Service Catalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement"
- the section called "[Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux"

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[GuardDuty.5] La surveillance du journal d'audit GuardDuty EKS doit être activée" • the section called "[GuardDuty.6] La protection GuardDuty Lambda doit être activée" • the section called "[GuardDuty.8] La protection contre les GuardDuty programmes malveillants pour EC2 doit être activée" • the section called "[GuardDuty.9] GuardDuty La protection RDS doit être activée" • the section called "[GuardDuty.10] La protection GuardDuty S3 doit être activée" • the section called "[Inspector.1] La numérisation Amazon Inspector EC2 doit être activée" • the section called "[Inspector.2] La numérisation ECR d'Amazon Inspector doit être activée" • the section called "[Inspector.3] La numérisation du	11 juillet 2024

code Lambda par Amazon Inspector doit être activée"

- the section called "[Inspector.4] Le scan standard Amazon Inspector Lambda doit être activé"

Publication de CIS AWS Foundations Benchmark v3.0.0	Security Hub CSPM a publié la version 3.0.0 du Center for Internet Security (CIS) AWS Foundations Benchmark. La version inclut les nouveaux contrôles suivants, ainsi que des mappages avec plusieurs contrôles existants. • the section called "[EC2.53] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis la version 0.0.0. 0/0 vers les ports d'administration de serveurs distants" • the section called "[EC2.54] Les groupes de sécurité EC2 ne doivent pas autoriser l'entrée depuis : :/0 vers les ports d'adminis tration des serveurs distants" • the section called "[IAM.26] SSL/TLS Les certificats expirés gérés dans IAM doivent être supprimés" • the section called "[IAM.27] La AWSCloudShellFullA ccess politique ne doit pas être attachée aux identités IAM" • the section called "[IAM.28] L'analyseur d'accès externe IAM Access Analyzer doit être activé"	13 mai 2024

- the section called "[S3.22] Les compartiments S3 à usage général doivent enregistrer les événements d'écriture au niveau de l'objet"
- the section called "[S3.23] Les compartiments S3 à usage général doivent enregistrer les événements de lecture au niveau de l'objet"

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[DataFirehose.1] Les flux de diffusion de Firehose doivent être chiffrés au repos" • the section called "[DMS.10] L'autorisation IAM doit être activée sur les points de terminaison DMS pour les bases de données Neptune" • the section called "[DMS.11] Les points de terminaison DMS pour MongoDB doivent avoir un mécanisme d'authentification activé" • the section called "[DMS.12] TLS doit être activé sur les points de terminaison DMS pour Redis OSS" • the section called "[DynamoDB.7] Les clusters DynamoDB Accelerator doivent être chiffrés en transit" • the section called "[EFS.6] Les cibles de montage EFS ne doivent pas être associées à des sous-réseaux qui attribuent des adresses IP publiques au lancement"	3 mai 2024

- the section called "[EKS.3] Les clusters EKS doivent utiliser des secrets Kubernetes chiffrés"
- the section called "[FSx.2] Les systèmes de fichiers FSx for Lustre doivent être configurés pour copier les balises dans les sauvegardes"
- the section called "[MQ.2] Les courtiers ActiveMQ doivent diffuser les journaux d'audit à CloudWatch"
- [MQ.3] Les courtiers Amazon MQ devraient activer la mise à niveau automatique des versions mineures
- the section called "[Opensearch.11] OpenSearch les domaines doivent avoir au moins trois nœuds principaux dédiés"
- the section called "[Redshift.15] Les groupes de sécurité Redshift doivent autoriser l'entrée sur le port du cluster uniquement à partir d'origines restreintes"
- the section called "[SageMaker.4] les variantes de production de SageMaker terminaux doivent avoir un nombre

	d'instances initial supérieur à 1” • the section called “[Service Catalog.1] Les portefeuilles de Service Catalog doivent être partagés au sein d'unAWSorganisation uniquement” • the section called “[Transfer.2] Les serveurs Transfer Family ne doivent pas utiliser le protocole FTP pour la connexion des terminaux”	
AWS Norme de balisage des ressources	La norme de balisage AWS des ressources de Security Hub CSPM est désormais disponible pour tous, ainsi que les nouveaux contrôles qui s'appliquent à la norme.	30 avril 2024
Mise à jour de la politique gérée existante	Security Hub CSPM a mis à jour la politique AWS gérée nommée `AmazonSecurityHubFullAccess` pour obtenir des informations sur les prix Services AWS et les produits.	24 avril 2024

In-context configuration des paramètres de contrôle	Si vous utilisez la configuration centralisée, vous pouvez désormais configurer les paramètres de contrôle dans leur contexte, à partir de la page de détails d'un contrôle sur la console Security Hub CSPM.	29 mars 2024
Mise à jour de la politique gérée existante	Security Hub CSPM a mis à jour la politique AWS gérée nommée `AWSSecurityHubReadOnlyAccess` en ajoutant un `Sid` champ.	22 février 2024
Nouveau contrôle de sécurité	Le contrôle [Macie.2] La découverte automatique des données sensibles par Macie devrait être activée est désormais disponible. Pour les limites régionales de ce contrôle, voir Disponibilité des contrôles par région.	19 février 2024
Security Hub CSPM disponible dans l'ouest du Canada (Calgary)	Security Hub CSPM est désormais disponible dans l'ouest du Canada (Calgary) . Toutes les fonctionnalités de Security Hub CSPM sont désormais disponibles dans cette région, à l'exception de certains contrôles de sécurité. Pour plus d'informations, consultez la section Disponibilité des contrôles par région.	20 décembre 2023

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[Backup.1]AWS Backuples points de récupération doivent être chiffrés au repos" • the section called "[DynamoDB.6] La protection contre la suppression des tables DynamoDB doit être activée" • the section called "[EC2.51] La journalisation des connexions client doit être activée sur les points de terminaison VPN EC2" • the section called "[EKS.8] Les clusters EKS doivent avoir la journalisation des audits activée" • the section called "[EMR.2] Le paramètre de blocage de l'accès public à Amazon EMR doit être activé" • the section called "[FSx.1] Les systèmes de fichiers FSx pour OpenZFS doivent être configurés pour copier les balises vers les sauvegardes et les volumes" • the section called "[Macie.1] Amazon Macie devrait être activé"	14 décembre 2023

- the section called "[MSK.2] Les clusters MSK doivent avoir une surveillance améliorée configurée"
- the section called "[Neptune .9] Les clusters de base de données Neptune doivent être déployés dans plusieurs zones de disponibilité"
- the section called "[Network Firewall.1] Les pare-feux Network Firewall doivent être déployés dans plusieurs zones de disponibilité"
- the section called "[Network Firewall.2] La journalisation du Network Firewall doit être activée"
- the section called "[Opensea rch.10] OpenSearch les domaines doivent avoir la dernière mise à jour logiciell e installée"
- the section called "[PCA.1]C A privée AWSl'autorité de certification racine doit être désactivée"
- the section called "[S3.19] Les paramètres de blocage de l'accès public aux points d'accès S3 doivent être activés"
- the section called "[S3.20] La suppression MFA doit

	être activée pour les buckets S3 à usage général"	
Trouver un enrichissement	Security Hub CSPM a ajouté les nouveaux champs de recherche `AwsAccountName` `ApplicationArn` , et `ApplicationName` au AWS Security Finding Format (ASFF).	27 novembre 2023
Améliorations du tableau de bord récapitulatif	Vous pouvez désormais accéder à davantage de widgets de tableau de bord sur la page Résumé de la console Security Hub CSPM, enregistrer des ensembles de filtres de tableau de bord pour vous concentrer rapidement sur des problèmes de sécurité spécifiques et personnaliser la disposition du tableau de bord.	27 novembre 2023
Configuration centralisée	La configuration centralisée est désormais disponible. Grâce à la configuration centralisée, l'administrateur délégué Security Hub CSPM peut configurer le Security Hub CSPM, les normes et les contrôles sur plusieurs comptes d'organisation, unités organisationnelles (UO) et régions.	27 novembre 2023

Mises à jour de la politique gérée	Security Hub CSPM a ajouté de nouvelles autorisations à la politique `AWSSecurityHubServiceRolePolicy` gérée qui permettent à Security Hub CSPM de lire et de mettre à jour les propriétés de contrôle de sécurité personnalisables.	26 novembre 2023
Paramètres de contrôle personnalisés	Vous pouvez désormais personnaliser les valeurs des paramètres pour certains contrôles CSPM de Security Hub. Cela peut rendre les résultats d'un contrôle spécifique plus pertinents par rapport aux exigences de votre entreprise et à vos attentes en matière de sécurité.	26 novembre 2023
Mises à jour des politiques gérées	Security Hub CSPM a mis à jour `AWSSecurityHubFullAccess` et `AWSSecurityHubOrganizationsAccess` géré les politiques qui vous permettent d'utiliser, respectivement, les fonctionnalités de Security Hub CSPM et l'intégration avec. AWS Organizations	16 novembre 2023

Contrôles de sécurité existants ajoutés à la Service-Managed norme : AWS Control Tower	Les contrôles CSPM Security Hub existants suivants ont été ajoutés à Service-Managed Standard :. AWS Control Tower • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	14 novembre 2023

Mises à jour de la politique gérée	Security Hub CSPM a ajouté une nouvelle autorisation de balisage à la politique `AWSSecurityHubServiceRolePolicy` gérée qui permet à Security Hub CSPM de lire les balises de ressources liées aux résultats.	7 novembre 2023

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[AppSync.5]AWS AppSyncLes API GraphQL ne doivent pas être authentifiées avec des clés d'API" • the section called "[DMS.6] La mise à niveau automatique des versions mineures des instances de réplication DMS doit être activée" • the section called "[DMS.7] La journalisation des tâches de réplication DMS pour la base de données cible doit être activée" • the section called "[DMS.8] La journalisation des tâches de réplication DMS pour la base de données source doit être activée" • the section called "[DMS.9] Les points de terminaison DMS doivent utiliser le protocole SSL" • the section called "[DocumentDB.3] Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics"	10 octobre 2023

- the section called "[DocumentDB.4] Les clusters Amazon DocumentDB doivent publier les journaux d'audit dans Logs CloudWatch"
- the section called "[DocumentDB.5] La protection contre la suppression des clusters Amazon DocumentDB doit être activée"
- the section called "[ECS.9] Les définitions de tâches ECS doivent avoir une configuration de journalisation"
- the section called "[EventBridge.3] les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources"
- the section called "[EventBridge.4] la réplication des événements doit être activée sur les points de terminaison EventBridge globaux"
- the section called "[MSK.1] Les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier"
- the section called "[MQ.5] Les courtiers ActiveMQ

doivent utiliser le mode déploiement active/standby"

- the section called "[MQ.6] Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster"
- the section called "[Network Firewall.9] La protection contre les suppressions doit être activée sur les pare-feux Network Firewall"
- the section called "[RDS.34] Les clusters de bases de données Aurora MySQL doivent publier des journaux d'audit dans CloudWatch Logs"
- the section called "[RDS.35] La mise à niveau automatique des versions mineures des clusters de bases de données RDS doit être activée"
- the section called "[Route53.2] Les zones hébergées publiques de Route 53 doivent enregistrer les requêtes DNS"
- the section called "[WAF.12] AWS WAFles CloudWatch métriques doivent être activées pour les règles"

Mises à jour de la politique gérée	Security Hub CSPM a ajouté de nouvelles actions Organisations à la politique `AWSSecurityHubServiceRolePolicy` gérée qui permettent à Security Hub CSPM de récupérer les informations relatives aux comptes et aux unités organisationnelles (OU). Nous avons également ajouté de nouvelles actions Security Hub CSPM qui permettent à Security Hub CSPM de lire et de mettre à jour les configurations de service, y compris les normes et les contrôles.	27 septembre 2023

Contrôles de sécurité existants ajoutés à la Service-Managed norme : AWS Control Tower	Les contrôles CSPM Security Hub existants suivants ont été ajoutés à Service-Managed Standard :. AWS Control Tower • the section called "[Athena.1] Les groupes de travail Athena doivent être chiffrés au repos" • the section called "[DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos" • the section called "[DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate" • the section called "[Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos" • the section called "[Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch" • the section called "[Neptune.3] Les instantanés du cluster de base de données	26 septembre 2023

Neptune ne doivent pas être publics"

- the section called "[Neptune .4] La protection contre la suppression des clusters de base de données Neptune doit être activée"
- the section called "[Neptune .5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées"
- the section called "[Neptune .6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos"
- the section called "[Neptune .7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune"
- the section called "[Neptune .8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés"
- the section called "[RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos"

Vue des contrôles consolidés et résultats des contrôles consolidés disponibles dans AWS GovCloud (US)	La vue des contrôles consolidés et les résultats des contrôles consolidés sont désormais disponibles dans le AWS GovCloud (US) Region. La page Contrôles de la console Security Hub CSPM affiche toutes vos commandes, quelles que soient les normes. Chaque contrôle possède le même identifiant de contrôle pour toutes les normes. Lorsque vous activez les résultats des contrôles consolidés, vous recevez un seul résultat par contrôle de sécurité, même lorsqu'un contrôle s'applique à plusieurs normes activées.	6 septembre 2023

Affichage des contrôles consolidés et résultats des contrôles consolidés disponibles dans les régions de Chine	La vue des contrôles consolidés et les résultats des contrôles consolidés sont désormais disponibles dans les régions de Chine. La page Contrôles de la console Security Hub CSPM affiche toutes vos commandes, quelles que soient les normes. Chaque contrôle possède le même identifiant de contrôle pour toutes les normes. Lorsque vous activez les résultats des contrôles consolidés, vous recevez un seul résultat par contrôle de sécurité, même lorsqu'un contrôle s'applique à plusieurs normes activées.	28 août 2023
Security Hub CSPM disponible dans la région d'Israël (Tel Aviv)	Security Hub CSPM est désormais disponible en Israël (Tel Aviv). Toutes les fonctionnalités de Security Hub CSPM sont désormais disponibles dans cette région, à l'exception de certains contrôles de sécurité. Pour plus d'informations, consultez la section Disponibilité des contrôles par région.	08 août 2023

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[Athena.1] Les groupes de travail Athena doivent être chiffrés au repos" • the section called "[DocumentDB.1] Les clusters Amazon DocumentDB doivent être chiffrés au repos" • the section called "[DocumentDB.2] Les clusters Amazon DocumentDB doivent disposer d'une période de conservation des sauvegardes adéquate" • the section called "[Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos" • the section called "[Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch" • the section called "[Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics"	28 juillet 2023

- the section called "[Neptune .4] La protection contre la suppression des clusters de base de données Neptune doit être activée"
- the section called "[Neptune .5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées"
- the section called "[Neptune .6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos"
- the section called "[Neptune .7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune"
- the section called "[Neptune .8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés"
- the section called "[RDS.27] Les clusters de bases de données RDS doivent être chiffrés au repos"

Nouveaux opérateurs pour les critères des règles d'automatisation	Vous pouvez désormais utiliser les opérateurs de comparaison CONTAINS et NOT_CONTAINS pour la carte des règles d'automatisation et les critères de chaîne.	25 juillet 2023
Règles d'automatisation	Security Hub CSPM propose désormais des règles d'automatisation qui mettent automatiquement à jour les résultats en fonction des critères que vous spécifiez.	13 juin 2023
Nouvelle intégration tierce	Snykest une nouvelle intégration tierce qui envoie les résultats à Security Hub CSPM.	12 juin 2023

Contrôles de sécurité existants ajoutés à la Service-Managed norme : AWS Control Tower	Les contrôles CSPM Security Hub existants suivants ont été ajoutés à Service-Managed Standard :. AWS Control Tower • the section called "[Account.1] Les coordonnées de sécurité doivent être fournies pourCompte AWS" • the section called "[APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation" • the section called "[APIGateway.9] La journalisation des accès doit être configuré e pour les étapes API Gateway V2" • the section called "[CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés" • the section called "[EC2.25] Les modèles de lancement Amazon EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau" • the section called "[ELB.1] L'équilibreur de charge des applications doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS"	12 juin 2023

- the section called "[Redshift.10] Les clusters Redshift doivent être chiffrés au repos"
- the section called "[SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé"
- the section called "[SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes"
- the section called "[WAF.10] AWS WAFLes ACL Web doivent avoir au moins une règle ou un groupe de règles"

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[ACM.2] Les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits" • the section called "[AppSync.2]AWS AppSyncla journalisation au niveau du champ doit être activée" • the section called "[CloudFront.13] CloudFront les distributions doivent utiliser le contrôle d'accès à l'origine" • the section called "[Elastic Beanstalk.3] Elastic Beanstalk devrait diffuser les logs vers CloudWatch" • the section called "[S3.17] Les compartiments S3 à usage général doivent être chiffrés au repos avec AWS KMS keys" • the section called "[StepFunctions.1] La journalisation des machines à états Step Functions doit être activée"	6 juin 2023

Security Hub CSPM disponible en Asie-Pacifique (Melbourne)	Security Hub CSPM est désormais disponible en Asie-Pacifique (Melbourne). Toutes les fonctionnalités de Security Hub CSPM sont désormais disponibles dans cette région, à l'exception de certains contrôles de sécurité. Pour plus d'informations, consultez la section Disponibilité des contrôles par région.	25 mai 2023
Trouver l'histoire	Security Hub CSPM peut désormais suivre l'historique d'une découverte au cours des 90 derniers jours.	4 mai 2023

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM de Security Hub suivants sont disponibles : • the section called "[EKS.1] Les points de terminaison du cluster EKS ne doivent pas être accessibles au public" • the section called "[ELB.16] Les équilibreurs de charge des applications doivent être associés à un AWS WAF ACL web" • the section called "[Redshift.10] Les clusters Redshift doivent être chiffrés au repos" • the section called "[S3.15] Les compartiments S3 à usage général doivent avoir le verrouillage des objets activé"	29 mars 2023
Support étendu pour les résultats de contrôle consolidés	La réponse de sécurité automatisée sur la AWS version 2.0.0 prend désormais en charge les résultats des contrôles consolidés.	24 mars 2023

Security Hub CSPM disponible en version neuve Régions AWS	Security Hub CSPM est désormais disponible en Asie-Pacifique (Hyderabad), en Europe (Espagne) et en Europe (Zurich). Les contrôles disponibles dans ces régions sont limités.	21 mars 2023
Mise à jour de la politique gérée	Security Hub CSPM a mis à jour une autorisation existante dans la politique `AWSSecurityHubServiceRolePolicy` gérée.	17 mars 2023

Nouveaux contrôles de sécurité pour la norme NIST 800-53	Security Hub CSPM a ajouté les contrôles de sécurité suivants, applicables à la norme NIST 800-53 : • the section called "[Account.2]Comptes AWSdevrait faire partie d'unAWS Organizationsorganization" • the section called "[CloudWatch.15] CloudWatch les actions spécifiées doivent être configurées pour les alarmes" • the section called "[CloudWatch.16] les groupes de CloudWatch journaux doivent être conservés pendant une période spécifiée" • the section called "[CloudWatch.17] les actions CloudWatch d'alarme doivent être activées" • the section called "[DynamoDB.4] Les tables DynamoDB doivent être présentes dans un plan de sauvegarde" • the section called "[EC2.28] Les volumes EBS doivent être couverts par un plan de sauvegarde"	3 mars 2023

	• EC2.29 — Les instances EC2 doivent être lancées dans un VPC (retiré) • the section called "[RDS.26] Les instances de base de données RDS doivent être protégées par un plan de sauvegarde" • the section called "[S3.14] Les compartiments S3 à usage général doivent avoir le contrôle de version activé" • the section called "[WAF.11] AWS WAFla journalisation des ACL Web doit être activée"	
Institut national des normes et de la technologie (NIST) 800-53 Rev. 5	Security Hub CSPM prend désormais en charge la norme NIST 800-53 Rev. 5 avec plus de 200 contrôles de sécurité applicables.	28 février 2023

Vue consolidée des contrôles et résultats des contrôles	Avec la publication de la vue consolidée des contrôles, la page Contrôles de la console Security Hub CSPM affiche tous vos contrôles, quelles que soient les normes. Chaque contrôle possède le même identifiant de contrôle pour toutes les normes. Lorsque vous activez les résultats des contrôles consolidés, vous recevez un seul résultat par contrôle de sécurité, même lorsqu'un contrôle s'applique à plusieurs normes activées.	23 février 2023

Nouveaux contrôles de sécurité	Les nouveaux contrôles CSPM Security Hub suivants sont disponibles. Certains contrôles ont des limites régionales. • the section called "[ElastiCache.1] Les sauvegardes automatiques des clusters ElastiCache (Redis OSS) doivent être activées" • the section called "[ElastiCache.2] les mises à niveau automatiques des versions mineures devraient être activées sur les ElastiCache clusters" • the section called "[ElastiCache.3] le basculement automatique doit être activé pour les groupes de ElastiCache réplication" • the section called "[ElastiCache.4] les groupes de ElastiCache réplication doivent être chiffrés au repos" • the section called "[ElastiCache.5] les groupes ElastiCache de réplication doivent être chiffrés pendant le transport" • the section called "[ElastiCache.6] Les groupes de réplication ElastiCache (Redis OSS) des versions	16 février 2023

	antérieures doivent avoir Redis OSS AUTH activé" • the section called "[ElastiCache.7] les ElastiCache clusters ne doivent pas utiliser le groupe de sous-réseaux par défaut"	
Nouveaux champs ASFF	Security Hub CSPM a ajouté ProductFields.ArchivalReasons:0/Description et ProductFields.ArchivalReasons:0/ReasonCode au AWS Security Finding Format (ASFF).	8 février 2023
Nouveaux champs ASFF	Security Hub CSPM a ajouté Compliance.AssociatedStandards et Compliance.SecurityControlId au AWS Security Finding Format (ASFF).	31 janvier 2023
Les détails de la vulnérabilité sont désormais disponibles	Vous pouvez désormais consulter les détails des vulnérabilités dans la console Security Hub CSPM pour les résultats qu'Amazon Inspector envoie à Security Hub CSPM.	14 janvier 2023
Security Hub CSPM est disponible au Moyen-Orient (Émirats arabes unis)	Security Hub CSPM est désormais disponible au Moyen-Orient (Émirats arabes unis). Certains contrôles ont des limites régionales.	12 janvier 2023

Ajout d'une intégration tierce avec MetricStream	Security Hub CSPM prend désormais en charge une intégration tierce MetricStr eam dans toutes les régions, à l'exception de la Chine et. AWS GovCloud (US)	11 janvier 2023
Augmentation de la limite de comptes organisationnels	Security Hub CSPM prend désormais en charge jusqu'à 11 000 comptes membres pour chaque compte administr ateur Security Hub CSPM par région.	27 décembre 2022
ElasticBeanstalk.3 annulé	Security Hub CSPM a annulé le contrôle [ElasticB eanstalk.3] Elastic Beanstalk devrait diffuser les journaux CloudWatch depuis la norme FSBP dans toutes les régions.	21 décembre 2022
Security Hub CSPM ajoute de nouveaux contrôles de sécurité	Les nouveaux contrôles Security Hub CSPM sont disponibles pour les clients qui ont activé la norme FSBP. Certains contrôles ont des limites régionales.	15 décembre 2022

Conseils sur les fonctionnalités à venir	Security Hub CSPM prévoit de publier deux nouvelles fonctionnalités : la vue consolidée des contrôles et la consolidation des résultats des contrôles. Ces fonctionnalités à venir peuvent avoir un impact sur les flux de travail existants qui reposent sur la recherche de champs et de valeurs par le contrôle.	9 décembre 2022
L'intégration d'Amazon Security Lake est désormais disponible	Security Lake s'intègre désormais à Security Hub CSPM en recevant les résultats de Security Hub CSPM.	29 novembre 2022
Support pour Service-Managed Standard : AWS Control Tower	Security Hub CSPM prend en charge une nouvelle norme de sécurité appelée Service-Managed Standard :. AWS Control Tower AWS Control Tower gère cette norme.	28 novembre 2022
CIS AWS Foundations Benchmark v1.4.0 est désormais disponible dans les régions chinoises	Security Hub CSPM prend désormais en charge CIS AWS Foundations Benchmark v1.4.0 dans les régions chinoises.	18 novembre 2022
L'intégration de Jira Service Management Cloud est désormais disponible	Jira Service Management Cloud reçoit désormais les résultats du Security Hub CSPM dans toutes les régions disponibles, à l'exception de la Chine.	17 novembre 2022

AWS IoT Device Defender intégration désormais disponible	AWS IoT Device Defender envoie désormais les résultats au Security Hub CSPM dans toutes les régions disponibles.	17 novembre 2022
Support pour CIS AWS Foundations Benchmark v1.4.0	Security Hub CSPM fournit désormais des contrôles de sécurité compatibles avec CIS AWS Foundations Benchmark v1.4.0. Cette norme est disponible dans toutes les régions disponibles, à l'exception de la Chine.	9 novembre 2022
Prise en charge des annonces CSPM de Security Hub dans AWS GovCloud (US)	Vous pouvez désormais vous abonner aux annonces de Security Hub CSPM avec Amazon Simple Notification Service (Amazon SNS) dans AWS GovCloud () et AWS GovCloud (US-EastUS-West) pour recevoir des notifications concernant Security Hub CSPM.	3 octobre 2022
AWS Security Hub CSPM ajoute un nouveau contrôle de sécurité	Le nouveau contrôle Security Hub CSPM AutoScaling.9 est disponible pour les clients qui ont activé la norme FSBP. Les contrôles peuvent avoir des limites régionales.	1er septembre 2022

Abonnez-vous aux annonces du Security Hub CSPM	Vous pouvez désormais vous abonner aux annonces de Security Hub CSPM avec Amazon Simple Notification Service (Amazon SNS) pour recevoir des notifications concernant Security Hub CSPM.	29 août 2022
Expansion régionale pour l'agrégation interrégionale	Cross-Region l'agrégation est désormais disponible pour les résultats, les mises à jour et les informations sur l'ensemble de AWS GovCloud (US).	2 août 2022
Intégrations de nouveaux produits tiers	Fortinet - FortiCNP est une intégration tierce qui reçoit les résultats du Security Hub CSPM, et JFrog est une intégration tierce qui envoie les résultats au Security Hub CSPM.	26 juillet 2022
EC2.27 est retraité	Security Hub CSPM a été retiré EC2.27 . L'exécution d'instances EC2 ne doit pas utiliser de paires de clés, un ancien contrôle de la norme FSBP (AWS Foundational Security Best Practices).	20 juillet 2022

Lambda.2 ne supporte plus python3.6	Security Hub CSPM ne prend plus en charge python3.6 en tant que paramètre pour Lambda.2 - Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge, un contrôle de la norme FSBP (AWS Foundational Security Best Practices).	19 juillet 2022
AWS Security Hub CSPM ajoute de nouveaux contrôles de sécurité	Les nouveaux contrôles Security Hub CSPM sont disponibles pour les clients qui ont activé la norme FSBP. Certains contrôles ont des limites régionales.	22 juin 2022
AWS Security Hub CSPM soutient une nouvelle région	Security Hub CSPM est désormais disponible en Asie-Pacifique (Jakarta). Certaines commandes ne sont pas disponibles dans cette région.	7 juin 2022
Intégration améliorée entre AWS Security Hub CSPM et AWS Config	Les utilisateurs de Security Hub CSPM peuvent consulter les résultats des évaluations des AWS Config règles sous forme de résultats dans Security Hub CSPM.	6 juin 2022

Ajout de la possibilité de désactiver les normes activées automatiquement	Pour les utilisateurs qui ont intégré à AWS Organizations, cette fonctionnalité vous permet de vous connecter au compte administrateur CSPM de Security Hub et de désactiver les nouveaux comptes membres des normes activées automatiquement.	25 avril 2022
Agrégation interrégionale étendue	Ajout d'une agrégation interrégionale pour contrôler les statuts et les scores de sécurité.	20 avril 2022
CompanyName et ProductName sont désormais des attributs de premier niveau	Ajout de nouveaux attributs de niveau supérieur pour définir les noms de sociétés et de produits associés aux intégrations personnalisées	1er avril 2022
Ajout de nouveaux contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	Ajout de 5 nouveaux contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales.	31 mars 2022
Ajout de nouveaux objets de détails de ressources à ASFF	Type `AwsRdsDbSecurityGroup` de ressource ajouté à ASFF.	25 mars 2022
Ajout de détails sur les ressources supplémentaires dans ASFF	Ajout de détails supplémentaires à `AwsAutoScalingScalingGroup` `AwsElbLoadBalancer` ,`AwsRedshiftCluster` , et`AwsCodeBuildProject` .	25 mars 2022

Ajout de nouveaux contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	Ajout de 15 nouveaux contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales.	16 mars 2022
Ajout de nouveaux contrôles à la norme des meilleures pratiques AWS de sécurité fondamentales et à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)	Ajout de nouveaux contrôles pour Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing et CloudFront à la norme AWS Foundational Security Best Practices. Deux nouvelles commandes ont également été ajoutées pour le OpenSearch service à la norme PCI DSS.	15 février 2022
Ajout d'un nouveau champ à ASFF	Nouveau champ ajouté : Échantillon.	26 janvier 2022
Intégration ajoutée avec AWS Health	AWS Health utilise la messagerie d'événements service à service pour envoyer les résultats à Security Hub CSPM.	19 janvier 2022
Intégration ajoutée avec AWS Trusted Advisor	Trusted Advisor envoie les résultats de ses contrôles au Security Hub CSPM en tant que résultats du Security Hub CSPM. Security Hub CSPM envoie les résultats de ses contrôles des meilleures pratiques AWS de sécurité fondamentales à. Trusted Advisor	18 janvier 2022

Objets contenant les détails des ressources mis à jour dans ASFF	Ajout de `MixedInstancesPolicy` et `AvailabilityZones` à `AwsAutoScalingAutoScalingGroup`. Ajout de `MetadataOptions` à `AwsAutoScalingLaunchConfiguration`. Ajout de `BucketVersioningConfiguration` à `AwsS3Bucket`.	20 décembre 2021
Sortie mise à jour pour la documentation ASFF	Les descriptions des attributs ASFF étaient auparavant regroupées dans une seule rubrique. Chaque objet de niveau supérieur et chaque objet contenant des informations sur les ressources se trouvent désormais dans leur propre rubrique. La rubrique sur la syntaxe ASFF contient des liens vers ces rubriques.	20 décembre 2021
Ajout de nouveaux objets de détails de ressources à ASFF pour AWS Network Firewall	Pour AWS Network Firewall, les objets de détails des ressources suivants ont été ajoutés : `AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy`, et`AwsNetworkFirewallRuleGroup`.	20 décembre 2021

Ajout du support pour la nouvelle version d'Amazon Inspector	Security Hub CSPM est intégré à la nouvelle version d'Amazon Inspector ainsi qu'à Amazon Inspector Classic. Amazon Inspector envoie ses résultats au Security Hub CSPM.	29 novembre 2021
Modification de la sévérité de EC2.19	Le niveau de gravité de EC2.19 (Les groupes de sécurité ne doivent pas autoriser l'accès illimité aux ports présentant un risque élevé) passe de Élevé à Critique.	17 novembre 2021
Nouvelle intégration avec Sonrai Dig	Security Hub CSPM propose désormais une intégration avec. Sonrai Dig Sonrai Digsurveille les environnements cloud pour identifier les risques de sécurité. Sonrai Digenvoie les résultats au Security Hub CSPM.	12 novembre 2021
Vérification mise à jour pour CIS 2.1 et CloudTrail.1 contrôles	En plus de vérifier qu'au moins un CloudTrail sentier multirégional est en place, CIS 2.1 vérifie CloudTrail.1 désormais également que le `ExcludeManagementEventSources` paramètre est vide dans au moins un des sentiers multirégionaux CloudTrail .	9 novembre 2021

Ajout du support pour les points de terminaison VPC	Security Hub CSPM est désormais intégré aux points de terminaison VPC AWS PrivateLink et les prend en charge.	03 novembre 2021
Ajout de contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	Ajout de nouvelles commandes pour Elastic Load Balancing (ELB.2 et ELB.8) et AWS Systems Manager (SSM.4).	2 novembre 2021
Ports ajoutés à la vérification du EC2.19 contrôle	EC2.19 vérifie désormais également que les groupes de sécurité n'autorisent pas un accès d'entrée illimité aux ports suivants : 3000 (frameworks de développement Web Go et Ruby), 5000 (frameworks de développement Web Python), 8088 (port HTTP hérité) et 8888 (port HTTP alternatif) Node.js	27 octobre 2021
Ajout de l'intégration avec Logz.io Cloud SIEM	Logz.io est un fournisseur de Cloud SIEM qui fournit une corrélation avancée des données de journal et d'événements pour aider les équipes de sécurité à détecter, analyser et répondre aux menaces de sécurité en temps réel. Logz.io reçoit les résultats du Security Hub CSPM.	25 octobre 2021

Ajout de la prise en charge de l'agrégation interrégionale des résultats	Cross-Region l'agrégation vous permet de consulter tous vos résultats sans avoir à changer de région. Les comptes d'administrateur choisissent une région d'agrégation et des régions associées. Les résultats relatifs au compte administr ateur et à ses comptes membres sont agrégés à partir des régions liées à la région d'agrégation.	20 octobre 2021
Objets contenant les détails des ressources mis à jour dans ASFF	Les détails du certificat de visionnage ont été ajoutés à`AwsCloudFrontDistr ibution` . Des détails supplémentaires ont été ajoutés à`AwsCodeBu ildProject` . Des attributs d'équilibreur de charge ont été ajoutés à. `AwsElbV2L oadBalancer` L'identifiant du compte du propriétaire du compartiment S3 a été ajouté à`AwsS3Bucket` .	8 octobre 2021

Ajout de nouveaux objets de détails de ressources à ASFF	Les nouveaux objets de détails des ressources suivants ont été ajoutés à ASFF : `AwsEc2VpcEndpointService` `AwsEcrRepository` ,`AwsEksCluster` ,,`AwsOpenSearchServiceDomain` ,`AwsWafRateBasedRule` , `AwsWafRegionalRateBasedRule` `AwsXrayEncryptionConfig`	8 octobre 2021
Le runtime obsolète a été supprimé du contrôle Lambda.2	Dans la norme AWS Foundational Security Best Practices, le `dotnetcore2.1` runtime a été supprimé de [Lambda.2] Les fonctions Lambda doivent utiliser des environnements d'exécution pris en charge.	6 octobre 2021
Nouveau nom pour l'intégration de Check Point	L'intégration avec Check Point Dome9 Arc s'appelle désormais Check Point CloudGuard Posture Management. L'ARN d'intégration n'a pas changé.	1er octobre 2021
Suppression de l'intégration avec Alcide	L'intégration avec Alcide KAudit est interrompue.	30 septembre 2021

Modification de la sévérité de EC2.19	La sévérité de [EC2.19] Les groupes de sécurité ne devraient pas autoriser un accès illimité aux ports présentant un risque élevé passe de moyenne à élevée.	30 septembre 2021
L'intégration avec AWS Organizations est désormais prise en charge dans les régions de Chine	L'intégration du Security Hub CSPM aux organisations est désormais prise en charge en Chine (Pékin) et en Chine (Ningxia).	20 septembre 2021
Nouvelle AWS Config règle pour les PCI.S3.6 contrôles S3.1 et	Les deux S3.1 et PCI.S3.6 vérifiez que le paramètre Amazon S3 Block Public Access est activé. La AWS Config règle pour ces contrôles passe de `s3-account-level-public-access-blocks` à `s3-account-level-public-access-blocks-periodic` .	14 septembre 2021
Suppression des environnements d'exécution obsolètes du contrôle Lambda.2	Dans la norme AWS Foundational Security Best Practices, les fonctions Lambda ont été supprimées `nodejs10.x` et les `ruby2.5` runtimes de [Lambda.2] Lambda devraient utiliser des runtimes pris en charge.	13 septembre 2021

Modification de la sévérité du contrôle CIS 2.2	Dans la norme CIS AWS Foundations Benchmark, la sévérité de 2.2. — Assurez-vous que la validation du fichier CloudTrail journal est activée et passe de Faible à Moyen.	13 septembre 2021
Mise à jour ECS.1 et conforme SSM.1 à la norme des meilleures pratiques de sécurité AWS fondamentales Lambda.2	Dans la norme AWS Foundational Security Best Practices, un `SkipInactiveTaskDefinitions` paramètre est ECS.1 désormais défini sur. `true` Cela garantit que le contrôle vérifie uniquement les définitions de tâches actives. Pour Lambda.2, Python 3.9 a été ajouté à la liste des environnements d'exécution. SSM.1 vérifie désormais à la fois les instances arrêtées et en cours d'exécution.	7 septembre 2021
PCI.Lambda.2 le contrôle exclut désormais les ressources Lambda @Edge	Dans la norme PCI DSS (Payment Card Industry Data Security Standard), le PCI.Lambda.2 contrôle exclut désormais les ressources Lambda @Edge.	7 septembre 2021
Ajout de l'intégration avec HackerOne Vulnerability Intelligence	Security Hub CSPM propose désormais une intégration avec. HackerOne Vulnerability Intelligence L'intégration envoie les résultats au Security Hub CSPM.	7 septembre 2021

Objets contenant les détails des ressources mis à jour dans ASFF	Pour `AwsKmsKey`, ajouté `KeyRotationStatus`. Pour `AwsS3Bucket`, ajouté `AccessControlList` `BucketLoggingConfiguration`, `BucketNotificationConfiguration`, et `BucketWebsiteConfiguration`.	2 septembre 2021
Ajout de nouveaux objets de détails de ressources à ASFF	Les nouveaux objets de détails des ressources suivants ont été ajoutés à ASFF : `AwsAutoScalingLaunchConfiguration` `AwsEc2VpnConnection`, et `AwsEcrContainerImage`.	2 septembre 2021
Ajout de détails à l'`Vulnerabilities` objet en ASFF	Dans `Cvss`, ajouté `Adjustments` et `Source`. Dans `VulnerablePackages`, ont été ajoutés le chemin du fichier et le gestionnaire de packages.	2 septembre 2021
Systems Manager Explorer et son OpsCenter intégration sont désormais pris en charge dans les régions de Chine	L'intégration de Security Hub CSPM à SSM Explorer OpsCenter est désormais prise en charge en Chine (Pékin) et en Chine (Ningxia).	31 août 2021

Retrait du contrôle Lambda.4	Security Hub CSPM retire le contrôle [Lambda.4] Les fonctions Lambda devraient avoir une file d'attente de lettres mortes configurée. Lorsqu'un contrôle est retiré, il ne s'affiche plus sur la console et Security Hub CSPM n'effectue aucune vérification par rapport à celui-ci.	31 août 2021
Retrait du contrôle PCI.EC2.3	Security Hub CSPM retire le contrôle [PCI.EC2.3] Les groupes de sécurité EC2 non utilisés doivent être supprimés . Lorsqu'un contrôle est retiré, il ne s'affiche plus sur la console et Security Hub CSPM n'effectue aucune vérification par rapport à celui-ci.	27 août 2021
Modification de la façon dont Security Hub CSPM envoie les résultats aux actions personnalisées	Lorsque vous envoyez des résultats à une action personnalisée, Security Hub CSPM envoie désormais chaque résultat dans un événement distinct Security Hub Findings - Custom Action.	20 août 2021

Ajout d'un nouveau code de motif d'état de conformité pour les environnements d'exécution Lambda personnalisés	Ajout d'un nouveau code de motif d'état de `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` conformité. Ce code de raison indique que Security Hub CSPM n'a pas pu effectuer de vérification par rapport à un environnement d'exécution Lambda personnalisé.	20 août 2021
AWS Firewall Manager l'intégration est désormais prise en charge dans les régions chinoises	L'intégration de Security Hub CSPM à Firewall Manager est désormais prise en charge en Chine (Pékin) et en Chine (Ningxia).	19 août 2021
Nouvelles intégrations avec et Caveonix CloudForcepoint Cloud Security Gateway	Security Hub CSPM propose désormais des intégrations avec et. Caveonix Cloud Forcepoint Cloud Security Gateway Les deux intégrations envoient les résultats au Security Hub CSPM.	10 août 2021

Ajout de nouveaux `CompanyName` `Region` attributs et à ASFF `ProductName`	Les `Region` champs `CompanyName` `ProductName` , et ont été ajoutés au niveau supérieur de l'ASFF. Ces champs sont remplis automatiquement et, à l'exception des intégrations de produits personnalisées, ne peuvent pas être mis à jour à l'aide de `BatchImportFindings` ou`BatchUpdateFindings` . Sur la console, la recherche de filtres utilise ces nouveaux champs. Dans l'API, les `ProductName` filtres `CompanyName` et utilisent les attributs qui se trouvent sous`ProductFields` .	23 juillet 2021
Objets de détails de ressources ajoutés et mis à jour dans ASFF	Ajout d'un nouveau type de `AwsRdsEventSubscription` ressource et de détails sur la ressource . Ajout de détails sur les ressources pour le type de `AwsEcsService` ressource. Des attributs ont été ajoutés à l'objet `AwsElasticsearchDomain` des détails de la ressource.	23 juillet 2021

Ajout de contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	De nouveaux contrôles ont été ajoutés pour Amazon API Gateway (APIGatew ay.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 via ES.8), Amazon RDS (RDS.16 via RDS.23), Amazon Redshift (Redshift.4) et Amazon SQS (). SQS.1	20 juillet 2021
A déplacé une autorisation dans la politique de gestion des rôles liés aux services	L'`config:PutEvaluati ons` autorisation a été déplacée dans la politique `AWSSecurityHubServ iceRolePolicy` gérée afin qu'elle soit appliquée à toutes les ressources.	14 juillet 2021
Ajout de contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	De nouveaux contrôles ont été ajoutés pour Amazon API Gateway CloudFront (APIGateway.4), Amazon (CloudFront.5 et CloudFron t.6), Amazon EC2 (EC2.17 et EC2.18), Amazon ECS (ECS.1), Amazon OpenSearc h Service (ES.4), Gestion des identités et des accès AWS (IAM.21), Amazon RDS (RDS.15) et Amazon S3 (S3.8).	8 juillet 2021

Ajout de nouveaux codes de motif d'état de conformité pour les résultats des contrôles	`INTERNAL_SERVICE_ERROR` indique qu'une erreur inconnue s'est produite. `SNS_TOPIC_CROSS_ACCOUNT` indique que la rubrique SNS appartient à un autre compte. `SNS_TOPIC_INVALID` indique que la rubrique SNS associée n'est pas valide.	6 juillet 2021
Ajout de l'intégration avec Amazon Q Developer dans les applications de chat	Ajout de l'intégration avec Amazon Q Developer dans les applications de chat. Security Hub CSPM envoie les résultats à Amazon Q Developer via des applications de chat.	30 Juin 2021
Ajout d'une nouvelle autorisation à la politique de gestion des rôles liés aux services	Ajout d'une nouvelle autorisation à la politique gérée `AWSSecurityHubServiceRolePolicy` pour permettre au rôle lié au service de fournir des résultats d'évaluation à. AWS Config	29 juin 2021

Objets de détails de ressources nouveaux et mis à jour dans l'ASFF	Ajout de nouveaux objets de détails de ressources pour les clusters ECS et les définitions de tâches ECS. Mise à jour de l'objet d'instance EC2 pour répertorier les interfaces réseau associées. Ajout de l'ID de certificat client pour les étapes API Gateway V2. Ajout de la configuration du cycle de vie pour les compartiments S3.	24 juin 2021
Mise à jour du calcul des statuts de contrôle agrégés et des scores de sécurité standard	Security Hub CSPM calcule désormais l'état global des contrôles et le score de sécurité standard toutes les 24 heures. Pour les comptes administrateurs, le score indique désormais si chaque contrôle est activé ou désactivé pour chaque compte.	23 juin 2021
Informations mises à jour sur la gestion des comptes suspendus par Security Hub CSPM	Ajout d'informations sur la façon dont Security Hub CSPM gère les comptes suspendus dans. AWS	23 juin 2021

Ajout d'onglets pour afficher les commandes activées et désactivées pour le compte administrateur individuel	Pour le compte administrateur, les principaux onglets de la page de détails standard contiennent des informations agrégées sur tous les comptes. Les nouveaux onglets Activé pour ce compte et Désactivé pour ce compte répertorient les comptes qui sont activés ou désactivés pour le compte administrateur individuel.	23 juin 2021
Ajouté `java8.al2` aux paramètres pour `Lambda.2`	Dans la norme AWS Foundational Security Best Practices, ajoutée `java8.al2` aux environnements d'exécution pris en charge pour le `Lambda.2` contrôle.	8 juin 2021
Nouvelles intégrations avec NETSCOUT MicroFocus ArcSight Cyber Investigator	Ajout d'intégrations avec MicroFocus ArcSight et NETSCOUT Cyber Investigator. MicroFocus ArcSight reçoit les résultats du Security Hub CSPM. NETSCOUT Cyber Investigator envoie ses résultats au Security Hub CSPM.	7 juin 2021

Détails ajoutés pour `AWSSecurityHubServiceRolePolicy`	Mise à jour de la section des politiques gérées pour ajouter des détails sur la politique gérée existante `AWSSecurityHubServiceRolePolicy` , qui est utilisée par le rôle lié au service Security Hub CSPM.	4 juin 2021
Nouvelle intégration avec Jira Service Management	Le connecteur AWS de gestion des services pour Jira envoie les résultats à Jira et les utilise pour créer des problèmes avec Jira. Lorsque les problèmes de Jira sont mis à jour, les résultats correspondants dans Security Hub CSPM sont également mis à jour.	26 mai 2021
Mise à jour de la liste des contrôles pris en charge pour la région Asie-Pacifique (Osaka)	Mise à jour de la norme CIS AWS Foundations et de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) pour indiquer les contrôles qui ne sont pas pris en charge en Asie-Pacifique (Osaka).	21 mai 2021
Nouvelle intégration avec Sysdig Secure pour le cloud	Ajout d'une intégration avec Sysdig Secure pour le cloud. L'intégration envoie les résultats au Security Hub CSPM.	14 mai 2021

Ajout de contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	De nouveaux contrôles ont été ajoutés pour Amazon API Gateway AWS CloudTrail (APIGateway.2 CloudTrail.4 et APIGateway.3 CloudTrai l.5), Amazon EC2 (EC2.15 et EC2.16), AWS Elastic Beanstalk (ElasticBeanstalk.1 et ElasticBeanstalk.2), AWS Lambda (Lambda.4), Amazon RDS (RDS.12— RDS.14), Amazon Redshift (Redshift .7), AWS Secrets Manager (SecretsManager.3 et SecretsManager.4) et AWS WAF (WAF.1).	10 mai 2021
Mises à jour GuardDuty et contrôles Amazon RDS	La sévérité a été modifiée `GuardDuty.1` et est `PCI.GuardDuty.1` passée de Moyenne à Élevée. Un `databaseEngines` paramètre a été ajouté à`RDS.8`.	4 mai 2021
Ajout de nouvelles informati ons sur les ressources à l'ASFF	Dans`Resources.Details` , de nouveaux objets de détails de ressources ont été ajoutés pour les ACL réseau Amazon EC2, les sous-réseaux Amazon EC2 et les environne ments. AWS Elastic Beanstalk	3 mai 2021

Ajout de champs de console pour fournir des valeurs de filtre pour les EventBridge règles Amazon	Les nouveaux modèles de filtre prédéfinis pour les EventBridge règles CSPM de Security Hub fournissent des champs de console que vous pouvez utiliser pour spécifier des valeurs de filtre.	30 avril 2021
Ajout de l'intégration avec AWS Systems Manager Explorer et OpsCenter	Security Hub CSPM prend désormais en charge une intégration avec Systems Manager Explorer et. OpsCenter L'intégration reçoit les résultats de Security Hub CSPM et met à jour ces résultats dans Security Hub CSPM.	26 avril 2021
Nouveau type pour les intégrations de produits	Un nouveau type d'intégra tion`UPDATE_FINDINGS_IN _SECURITY_HUB` , indique qu'une intégration de produit met à jour les résultats qu'elle reçoit de Security Hub CSPM.	22 avril 2021
« Compte principal » est remplacé par « Compte administrateur »	Le terme « Compte principal » est remplacé par « Compte administrateur ». Le terme est également modifié dans la console et l'API Security Hub CSPM.	22 avril 2021

Mise APIGateway.1 à jour pour remplacer HTTP par Websocket	Mise à jour du titre, de la description et de la correctio n pour APIGateway.1. Le contrôle vérifie désormais la journalisation de l'exécution de l'API Websocket au lieu de la journalisation de l'exécution de l'API HTTP.	9 avril 2021
GuardDuty L'intégration d'Amazon est désormais prise en charge à Pékin et au Ningxia	L'intégration du Security Hub CSPM avec GuardDuty est désormais prise en charge dans les régions Chine (Pékin) et Chine (Ningxia).	5 avril 2021
Ajouté `nodejs14.x` aux runtimes pris en charge pour le contrôle Lambda.2	Le Lambda.2 contrôle de la norme Foundational Security Best Practices prend désormais en charge le `nodejs14.x` runtime.	30 mars 2021
Lancement du Security Hub CSPM en Asie-Pacifique (Osaka)	Security Hub CSPM est désormais disponible dans la région Asie-Pacifique (Osaka).	29 mars 2021
Ajout de champs de recherche de fournisseurs pour rechercher des détails	Dans le panneau des détails de la recherche, la nouvelle section Champs du fournisse ur de recherche contient les valeurs des fournisse urs de recherche en termes de confiance, de criticité, de résultats associés, de gravité et de types.	24 mars 2021

Ajout d'une option permettant de recevoir les résultats sensibles d'Amazon Macie	L'intégration avec Macie peut désormais être configurée pour envoyer des résultats sensibles à Security Hub CSPM.	23 mars 2021
Transition vers la AWS Organizations gestion des comptes	Pour les clients qui possèdent déjà un compte administrateur avec des comptes membres, de nouvelles informations ont été ajoutées sur la manière de passer de la gestion des comptes par invitation à la gestion des comptes via Organisations.	22 mars 2021
Nouveaux objets dans ASFF pour obtenir des informations sur la configuration du bloc d'accès public d'Amazon S3	Dans `Resources` , un nouveau type de `AwsS3AccountPublicAccessBlock` ressource et un nouvel objet de détails fournissent des informations sur la configuration du bloc d'accès public Amazon S3 pour les comptes. Dans l'objet `AwsS3Bucket` des détails de la ressource, l'`PublicAccessBlockConfiguration` objet fournit la configuration du bloc d'accès public pour le compartiment S3.	18 mars 2021

Nouvel objet dans ASFF pour permettre à la recherche de fournisseurs de mettre à jour des champs spécifiques	Le nouvel `FindingProviderFields` objet dans ASFF est utilisé `BatchImportFindings` pour fournir des valeurs pour `Confidence` `Criticality` , `RelatedFindings` `Severity`, et`Types`. Les champs d'origine ne doivent être mis à jour qu'à l'aide de`BatchUpdateFindings` .	18 mars 2021
Nouvel `DataClassification` objet pour les ressources dans ASFF	Le nouvel `Resources.DataClassification` objet dans ASFF est utilisé pour fournir des informations sur les données sensibles détectées sur la ressource.	18 mars 2021
`CONFIG_RETURNS_NOT_APPLICABLE` Valeur ajoutée aux codes de statut de conformité disponibles	Pour l'état de `NOT_AVAILABLE` conformité, vous avez supprimé le code de motif `RESOURCE_NO_LONGER_EXISTS` et ajouté le code de motif`CONFIG_RETURNS_NOT_APPLICABLE` .	16 mars 2021

Nouvelle politique gérée pour l'intégration avec AWS Organizations	Une nouvelle politique gérée fournit `AWSSecurityHubOrganizationsAccess` les autorisations d'organisation nécessaires au compte de gestion de l'organisation et au compte administrateur CSPM délégué de Security Hub.	15 mars 2021
Les informations relatives aux politiques gérées et aux rôles liés aux services ont été déplacées vers le chapitre Sécurité	Les informations sur les politiques gérées sont révisées et développées. Les informations sur les politiques gérées et les informations sur les rôles liés aux services ont été déplacées vers le chapitre Sécurité.	15 mars 2021
Sévérité révisée pour les témoins CIS 1.1 et CIS 3.1 — CIS 3.14	La sévérité des contrôles CIS 1.1 et CIS 3.1 — CIS 3,14 passe à Faible.	3 mars 2021
Suppression de la RDS.11 commande	Suppression du RDS.11 contrôle de la norme des meilleures pratiques de sécurité fondamentales.	3 mars 2021
Intégration mise à jour pour Turbot	L'intégration Turbot est mise à jour pour envoyer et recevoir des résultats.	26 février 2021

Ajout de contrôles à la norme des meilleures pratiques de sécurité fondamentales	Ajout de nouveaux contrôles pour Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 et EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 et ES.3), Elastic Load Balancing (ELB.6) et () AWS Key Management Service (AWS KMS) (KMS.3).	11 février 2021
`ProductArn` Filtre optionnel ajouté à l'`DescribeProducts` API	L'opération d'`DescribeProducts` API inclut désormais un `ProductArn` paramètre facultatif. Le `ProductArn` paramètre est utilisé pour identifier l'intégration de produit spécifique pour laquelle les détails doivent être renvoyés.	3 février 2021
Nouvelle intégration avec l'antivirus pour Amazon S3 depuis Cloud Storage Security	L'intégration avec Antivirus pour Amazon S3 envoie les résultats de l'analyse antivirus à Security Hub CSPM en tant que résultats.	27 janvier 2021
Mise à jour du processus de calcul du score de sécurité pour les comptes administrateurs	Pour un compte administrateur, Security Hub CSPM utilise un processus distinct pour calculer le score de sécurité. Le nouveau processus garantit que le score inclut des contrôles qui sont activés pour les comptes membres mais désactivés pour le compte administrateur.	21 janvier 2021

Nouveaux champs et objets dans l'ASFF	Ajout d'un nouvel `Action` objet pour suivre les actions effectuées sur une ressource. Ajout de champs à l'`AwsEc2NetworkInterface` objet pour suivre les noms DNS et les adresses IP. Un nouvel `AwsSsmPatchCompliance` objet a été ajouté aux détails de la ressource.	21 janvier 2021
Ajout de contrôles à la norme des meilleures pratiques de sécurité fondamentales	Ajout de nouveaux contrôles pour Amazon CloudFront (CloudFront.1 via CloudFront.4), Amazon DynamoDB (DynamoDB.1 via DynamoDB.3), Elastic Load Balancing (ELB.3 via ELB.5), Amazon RDS (RDS.9via RDS.11), Amazon Redshift (Redshift.1 via Redshift.3 et Redshift.6) et Amazon SNS (). SNS.1	15 janvier 2021

L'état du flux de travail est réinitialisé en fonction de l'état de l'enregistrement ou de l'état de conformité	Security Hub CSPM réinitialise automatiquement l'état du flux de travail à partir de `NOTIFIED` ou `RESOLVED` vers `NEW` si une découverte archivée est rendue active, ou si l'état de conformité d'une découverte passe de `PASSED` à`FAILED`, `WARNING` ou. `NOT_AVAILABLE` Ces modifications indiquent qu'une enquête supplémentaire est nécessaire.	7 janvier 2021
`ProductFields` Informations ajoutées pour les résultats basés sur le contrôle	Pour les résultats générés à partir des contrôles, des informations sur le contenu de l'`ProductFields` objet ont été ajoutées au format ASFF (AWS Security Finding Format).	29 décembre 2020
Mises à jour des informations gérées	Le titre d'insight 5 a été modifié. Ajout d'un nouvel aperçu, 32, qui permet de détecter les utilisateurs IAM présentant des activités suspectes.	22 décembre 2020
Mises à jour IAM.7 et Lambda.1 contrôles	Dans la norme des meilleures pratiques de sécurité AWS fondamentales, les paramètres ont été mis à jour pour IAM.7. Mise à jour du titre et de la description de Lambda.1.	22 décembre 2020

Intégration étendue à l' ServiceNow ITSM	L'intégration ServiceNow ITSM permet aux utilisateurs de créer automatiquement des incidents ou des problèmes lorsqu'un résultat CSPM de Security Hub est reçu. Les mises à jour de ces incidents ou problèmes entraînent la mise à jour des résultats dans Security Hub CSPM.	11 décembre 2020
Nouvelle intégration avec AWS Audit Manager	Security Hub CSPM propose désormais une intégration avec AWS Audit Manager. L'intégration permet à Audit Manager de recevoir des résultats basés sur les contrôles de Security Hub CSPM.	8 décembre 2020
Nouvelle intégration avec Aqua Security Kube-bench	Security Hub CSPM a ajouté une intégration avec Aqua Security. Kube-bench L'intégration envoie les résultats au Security Hub CSPM.	24 novembre 2020
Cloud Custodian est désormais disponible dans les régions de Chine	L'intégration avec Cloud Custodian est désormais disponible dans les régions Chine (Pékin) et Chine (Ningxia).	24 novembre 2020

BatchImportFindings peut désormais être utilisé pour mettre à jour des champs supplémentaires	Auparavant, vous ne pouviez pas l'utiliser BatchImportFindings pour mettre à jour les Types champs Confidence Criticality RelatedFindings Severity,, et. Désormais, si ces champs n'ont pas été mis à jour parBatchUpdateFindings , ils peuvent être mis à jour parBatchImportFindings . Une fois qu'ils sont mis à jour parBatchUpdateFindings , ils ne peuvent pas être mis à jour parBatchImportFindings .	24 novembre 2020
Security Hub CSPM est désormais intégré à AWS Organizations	Les clients peuvent désormais gérer les comptes des membres à l'aide de la configuration de leur compte d'organisation. Le compte de gestion de l'organisation désigne le compte administrateur Security Hub CSPM, qui détermine les comptes d'organisation à activer dans Security Hub CSPM. Le processus d'invitation manuel peut toujours être utilisé pour les comptes qui ne font pas partie d'une organisation.	23 novembre 2020

Suppression du format de liste de recherche distinct pour les commandes à volume élevé	La liste de résultats d'un contrôle n'utilise plus le format de page Résultats lorsqu'il existe un très grand nombre de résultats.	19 novembre 2020
Intégrations tierces nouvelles et mises à jour	Security Hub CSPM prend désormais en charge les intégrations avec cloudtame r.io, 3CoreSec, Prowler et Kubernetes Security. StackRox IBM QRadar n'envoie plus de résultats. Il ne reçoit que les résultats.	30 octobre 2020
Ajout d'une option permettant de télécharger la liste des résultats depuis la page des détails du contrôle.	Sur la page des détails du contrôle, une nouvelle option de téléchargement vous permet de télécharger la liste de recherche dans un fichier .csv. La liste téléchargée respecte tous les filtres qui s'y trouvent. Si vous avez sélectionné des résultats spécifiques, la liste téléchargée inclut uniquement ces résultats.	26 octobre 2020

Ajout d'une option permettant de télécharger la liste des contrôles depuis la page de détails standard.	Sur la page de détails standard, une nouvelle option de téléchargement vous permet de télécharger la liste de contrôle dans un fichier .csv. La liste téléchargée respecte tous les filtres qui s'y trouvent. Si vous avez sélectionné un contrôle spécifique, la liste téléchargée inclut uniquement ce contrôle.	26 octobre 2020
Intégrations de partenaires nouvelles et mises à jour	Security Hub CSPM est désormais intégré à. ThreatModeler Les intégrations partenaires suivantes ont été mises à jour pour refléter leurs nouveaux noms de produits. Twistlock Enterprise Edition s'appelle désormais Palo Alto Networks - Prisma Cloud Compute. Également issu de Palo Alto Networks, Demisto s'appelle désormais Cortex XSOAR et Redlock est désormais Prisma Cloud Enterprise.	23 octobre 2020
Lancement du Security Hub CSPM en Chine (Pékin) et en Chine (Ningxia)	Security Hub CSPM est désormais disponible dans les régions Chine (Pékin) et Chine (Ningxia).	21 octobre 2020

Format révisé pour les attributs ASFF et les intégrations tierces	Les listes d'attributs ASFF et d'intégrations de partenaires utilisent désormais un format basé sur des listes au lieu de tableaux. La syntaxe, les attributs et la taxonomie des types ASFF font désormais l'objet de rubriques distinctes.	15 octobre 2020
Page de détails des normes remaniée	La page de détails d'une norme activée affiche désormais une liste à onglets de contrôles. Les onglets filtrent la liste de contrôles en fonction de l'état des contrôles.	7 octobre 2020
CloudWatch Événements remplacés par EventBridge	Les références à Amazon CloudWatch Events ont été remplacées par Amazon EventBridge.	1er octobre 2020
Nouvelles intégrations avec Blue Hexagon pour AWS, Alcide KAudit et Palo Alto Networks. VM-Series	Security Hub CSPM est désormais intégré à Blue Hexagon pour AWS, Alcide KAudit et Palo Alto Networks. VM-Series Blue Hexagon for AWS et KAudit envoient leurs résultats au Security Hub CSPM. VM-Series reçoit les résultats du Security Hub CSPM.	30 septembre 2020

Objets de détails de ressources nouveaux et mis à jour dans ASFF	De nouveaux `Resources.Details` objets ont été ajoutés pour `AwsApiGatewayRestApi` `AwsApiGatewayStage` `AwsApiGatewayV2Api` `AwsApiGatewayV2Stage` ,`AwsCertificateManagerCertificate` ,`AwsElbLoadBalancer` ,`AwsIamGroup` , et`AwsRedshiftCluster` . Ajout de détails aux `AwsIamAccessKey` objets`AwsCloudFrontDistribution` , `AwsIamRole` et.	30 septembre 2020
Nouvel `ResourceRole` attribut pour les ressources dans ASFF permettant de savoir si une ressource est un acteur ou une cible.	L'`ResourceRole` attribut des ressources indique si la ressource est la cible de l'activité de recherche ou l'auteur de l'activité de recherche. Les valeurs valides sont `ACTOR` et `TARGET`.	30 septembre 2020
Ajout du gestionnaire de AWS Systems Manager correctifs aux intégrations AWS de services disponibles	AWS Systems Manager Patch Manager est désormais intégré à Security Hub CSPM. Patch Manager envoie les résultats à Security Hub CSPM lorsque les instances de la flotte d'un client ne sont pas conformes à sa norme de conformité des correctifs.	22 septembre 2020

Ajout de nouveaux contrôles à la norme des meilleures pratiques de sécurité AWS fondamentales	De nouvelles commandes ont été ajoutées pour les services suivants : Amazon EC2 (EC2.7 et EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 via RDS.8), Amazon S3 (S3.6) et AWS Secrets Manager (SecretsManager.1 et). SecretsManager.2	15 septembre 2020
Nouvelles clés contextuelles pour la politique IAM visant à contrôler l'accès aux champs `BatchUpdateFindings`	Les politiques IAM peuvent désormais être configurées pour restreindre l'accès aux champs et aux valeurs de champs lors de leur utilisati on`BatchUpdateFinding s` .	10 septembre 2020
Accès étendu aux comptes `BatchUpdateFindings` réservés aux membres	Par défaut, les comptes de membres ont désormais le même accès `BatchUpda teFindings` que les comptes d'administrateur.	10 septembre 2020
Nouveaux contrôles intégrés AWS KMS à la norme fondamentale sur les meilleure s pratiques de sécurité	Ajout de deux nouveaux contrôles (KMS.1 et KMS.2) à la norme des meilleure s pratiques de sécurité fondamentales. Les nouveaux contrôles vérifient si les politiques IAM limitent l'accès aux actions de AWS KMS déchiffrement.	9 septembre 2020

Suppression des résultats au niveau du compte pour les contrôles	Security Hub CSPM ne génère plus de résultats au niveau du compte pour un contrôle. Seuls les résultats au niveau des ressources sont générés.	1 septembre 2020
Nouvel PatchSummary objet dans ASFF	L'`PatchSummary` objet a été ajouté à l'ASFF. L'`PatchSummary` objet fournit des informations sur la conformité des correctifs d'une ressource par rapport à une norme de conformité sélectionnée.	1 septembre 2020
Page de détails des commandes redessinée	La page de détails des commandes a été repensée. La liste de recherche de contrôles comporte des onglets qui vous permettent de filtrer rapidement la liste en fonction de l'état de conformité. Vous pouvez également voir rapidement les résultats supprimés. Chaque entrée donne accès à des informations supplémentaires sur la ressource de recherche, la AWS Config règle et les notes de recherche.	28 août 2020

Nouvelles options de filtrage pour les résultats	Pour rechercher des filtres, vous pouvez utiliser le filtre is not pour rechercher des résultats pour lesquels la valeur d'un champ n'est pas égale à la valeur du filtre. Vous pouvez utiliser le paramètre ne commence pas par pour rechercher des résultats pour lesquels la valeur d'un champ ne commence pas par la valeur de filtre spécifiée.	28 août 2020
Une nouvelle ressource détaille les objets en ASFF	De nouveaux `Resources .Details` objets ont été ajoutés pour les types de ressources suivants : `AwsDynamoDbTable AwsEc2Eip AwsIamPol icy ,AwsIamUse r ,,AwsRdsDbC luster ,AwsRdsDbC lusterSna pshot ,AwsRdsDbS napshot , AwsSecret sManagerSecret`	18 août 2020
Nouvelle intégration avec RSA Archer	Security Hub CSPM est désormais intégré à RSA Archer. RSA Archer reçoit les résultats du Security Hub CSPM.	18 août 2020
Nouveau champ de descripti on pour AwsKmsKey	Un `Description` champ a été ajouté à l'`AwsKmsKey` objet ci-dessous`Resources .Details` .	18 août 2020

Champs ajoutés à AwsRdsDbInstance	Plusieurs attributs ont été ajoutés à l'`AwsRdsDbInstance` objet ci-dessous `Resources.Details` .	18 août 2020
Mise à jour de la façon dont Security Hub CSPM détermine l'état général d'un contrôle	Pour les contrôles qui n'ont aucun résultat, le statut est Aucune donnée au lieu de Inconnu. L'état du contrôle inclut à la fois les résultats au niveau du compte et au niveau des ressources. L'état du contrôle n'utilise pas l'état des résultats du flux de travail, sauf pour ignorer les résultats supprimés.	13 août 2020
Mise à jour de la façon dont Security Hub CSPM calcule le score de sécurité d'une norme	Lors du calcul du score de sécurité d'une norme, Security Hub CSPM ignore désormais les contrôles dont le statut est Aucune donnée. Le score de sécurité est la proportion des contrôles réussis par rapport aux contrôles activés, à l'exclusion des contrôles sans données.	13 août 2020
Nouvelle option pour activer automatiquement de nouveaux contrôles dans les normes activées	Ajout d'une option Paramètres pour activer automatiquement les nouveaux contrôles dans les normes qui sont activées. Vous pouvez également utiliser l'opération `UpdateSecurityHubConfiguration` API pour configurer cette option.	31 juillet 2020

Nouveaux contrôles pour la norme PCI DSS (Payment Card Industry Data Security Standard)	Ajout de nouvelles commandes à la norme PCI DSS. Les identificateurs des nouveaux contrôles sont PCI.DMS.1 PCI.EC2.5 , PCI.EC2.6, PCI.ELBV2.1 PCI.GuardDuty.1, PCI.IAM.7, PCI.IAM.8, PCI.S3.5, PCI.S3.6 PCI.SageMaker.1 PCI.SSM.2, et PCI.SSM.3.	29 juillet 2020
Contrôles nouveaux et mis à jour pour la norme des meilleures pratiques de sécurité fondamentales	De nouveaux contrôles ont été ajoutés à la norme des meilleures pratiques de sécurité fondamentales. Les identificateurs des nouveaux contrôles sont AutoScaling.1, DMS.1 EC2.4, EC2.6 S3.5, et SSM.3. Le titre du `daysToExpiration` paramètre a été mis à jour ACM.1 et sa valeur a été modifiée à 30.	29 juillet 2020
Nouvel `Vulnerabilities` objet dans l'ASFF	L'`Vulnerabilities` objet a été ajouté, qui fournit des informations sur les vulnérabilités associées à la découverte.	1er juillet 2020
Nouveaux `Resource.Details` objets dans l'ASFF pour les groupes Auto Scaling, les volumes EC2 et les VPC EC2	Les `AwsEc2Vpc` objets `AwsAutoScalingAutoScalingGroup` `AWSEc2Volume` , et ont été ajoutés à`Resource.Details` .	1er juillet 2020

Nouvel `NetworkPath` objet dans l'ASFF	L'`NetworkPath` objet a été ajouté, qui fournit des informations sur un chemin réseau lié à la découverte.	1er juillet 2020
Résolvez automatiquement les résultats quand `Compliance.Status` c'est `PASSED`	Pour les résultats des contrôles, si `Compliance.Status` c'est `PASSED` le cas, Security Hub CSPM passe automatiquement à. `Workflow.Status` `RESOLVED`	24 juin 2020
AWS Command Line Interface exemples	Ajout d' AWS CLI une syntaxe et d'exemples pour plusieurs tâches CSPM de Security Hub. Comprend l'activation de Security Hub CSPM, la gestion des informations, la gestion des normes et des contrôles, la gestion des intégrations de produits et la désactivation de Security Hub CSPM.	24 juin 2020
Nouvel `Severity.Original` attribut dans l'ASFF	Ajout de l'attribut `Severity.Original` , qui représente la gravité d'origine du fournisseur de résultat. Il remplace l'attribut obsolète `Severity.Product` .	20 mai 2020
Nouvel `Compliance.StatusReasons` objet dans l'ASFF pour plus de détails sur l'état d'un contrôle	Ajout de l'objet `Compliance.StatusReasons` , qui fournit un contexte supplémentaire pour l'état actuel d'un contrôle.	20 mai 2020

Nouvelle norme AWS fondamentale sur les meilleures pratiques de sécurité	Ajout de la nouvelle norme des meilleures pratiques de sécurité AWS fondamentales, qui est un ensemble de contrôles qui détectent les cas où vos comptes et ressources déployés s'écartent des meilleures pratiques de sécurité.	22 avril 2020
Nouvelle option de console permettant de mettre à jour l'état du flux de travail en fonction d'une découverte	Ajout d'informations sur l'utilisation de la console ou de l'API Security Hub pour définir l'état du flux de travail pour les conclusions.	16 avril 2020
Nouvelle `BatchUpdateFindings` API pour les mises à jour des résultats par les clients	Ajout d'informations pour utiliser `BatchUpdateFindings` pour mettre à jour les informations relatives au processus d'enquête sur un résultat. `BatchUpdateFindings` remplace `UpdateFindings` , qui est obsolète.	16 avril 2020

Mises à jour du format AWS de recherche de sécurité (ASFF)	Ajout de plusieurs nouveaux types de ressources. Ajout d'un nouvel attribut `Label` à l'objet `Severity`. `Label` est destiné à remplacer le champ `Normalized` . Ajout d'un nouvel objet `Workflow` pour suivre le processus d'enquête dans un résultat. `Workflow` contient un attribut `Status` qui remplace l'attribut `WorkflowsStatus` existant.	12 mars 2020
Mises à jour de la page Intégrations	Mise à jour reflétant les modifications apportées à la page Intégrations. Pour chaque intégration, la page affiche désormais la catégorie d'intégration et indique si chaque intégration envoie des résultats à Security Hub CSPM ou reçoit des résultats de celui-ci. Elle fournit également les étapes spécifiques requises pour activer chaque intégration.	26 février 2020
Intégrations de nouveaux produits tiers	Les nouvelles intégrations de produits suivantes ont été ajoutées : Cloud Custodian , FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security et Cognito Detect. Vectra.ai	21 février 2020

Nouvelle norme de sécurité pour la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)	Ajout de la norme de sécurité Security Hub CSPM pour la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Lorsque cette norme est activée, Security Hub CSPM effectue des vérifications automatisées par rapport aux contrôles liés aux exigences PCI DSS.	13 février 2020
Mises à jour du format AWS de recherche de sécurité (ASFF)	Ajout d'un champ pour les exigences connexes pour les contrôles des normes. Ajout de nouveaux types de ressources et de nouveaux détails de ressources. L'ASFF vous permet également de fournir jusqu'à 32 ressources.	5 février 2020
Nouvelle option pour désactiver les contrôles standard de sécurité individuels	Ajout d'informations sur la façon de contrôler si chaque contrôle de normes de sécurité individuel est activé.	15 janvier 2020
Mises à jour des concepts CSPM de Security Hub	Certaines descriptions ont été mises à jour et de nouveaux termes ont été ajoutés aux concepts CSPM de Security Hub.	21 septembre 2019
AWS Version de disponibilité générale de Security Hub CSPM	Mises à jour du contenu pour refléter les améliorations apportées à Security Hub CSPM pendant la période bêta.	25 juin 2019

Ajout d'étapes de correction pour les vérifications de CIS AWS Foundations	Ajout d'étapes de correction aux normes de sécurité prises en charge dans AWS Security Hub CSPM.	15 avril 2019
version bêta de AWS Security Hub CSPM	Publication de la version bêta du guide de l'utilisateur AWS de Security Hub CSPM.	18 novembre 2018

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.