aws

用户指南

AWS Security Hub



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

AWS Security Hub: 用户指南

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

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 Security Hub 和 Security Hub CSPM？ 1
AWS Security Hub 2
功能 2
集成 3
可访问性 3
定价 4
概念 4
成本估算器 8
按账户类型划分的访问权限 9
先决条件 9
设置跨账户访问 10
使用成本估算器 13
重要提示 20
相关信息 21
启用 Security Hub 21
为... 启用 Security Hub AWS Organization（组织） 21
在独立账户中启用 Security Hub 23
指定委派管理员 24
创建委派管理员策略 26
管理成员账户的配置 26
移除委派管理员 30
重新启用 Security Hub 31
建议 31
账户保障 32
账户覆盖范围页面 33
安全覆盖范围小组件 34
扩展计划 34
扩展套餐的权限 34
注册扩展计划合作伙伴 35
取消对合作伙伴的订阅 35
跨区域聚合 36
聚合的数据类型 36
聚合管理员账户和成员账户 37
自动化规则和跨区域聚合 38

启用聚合 38
查看聚合设置 39
更新聚合设置 39
删除聚合 40
摘要控制面板 41
注意事项 41
可用小组件 41
可用过滤器 53
在 Security Hub 中查看有关资源的详细信息 54
查找格式：OCSF 55
OCSF 概述 55
相关资源 55
AWS OCSF 的延期 56
覆盖范围调查发现 78
Sec AWS urity Hub CSPM 的报道结果 78
Amazon 的报道调查结果 GuardDuty 78
Amazon Inspector 的覆盖范围调查发现 79
Amazon Macie 的覆盖范围调查发现 79
隐瞒覆盖率调查结果 79
暴露调查发现 80
曝光结果如何运作 80
曝光调查结果的组成部分 81
严重性分类 82
暴露结果的好处 82
暴露来源调查结果 83
最佳实践 83
支持的资源 83
支持的特征 84
生成暴露调查发现 85
确定暴露调查发现的严重性级别 90
查看暴露调查发现 90
潜在攻击路径图 92
修复暴露调查发现 92
未使用的访问调查发现 140
未使用的访问分析的工作原理 140
未使用的访问权限查找类型 140

Service-linked 分析器 141
查看未使用的访问发现结果 141
暴露结果中未使用的访问权限 141
针对未使用权限的策略建议 142
定价 142
政策建议 142
政策建议如何运作 142
谁可以生成推荐 143
推荐生命周期 143
错误案例 143
使用控制台 143
API 参考 144
自动化 144
自动化规则 144
EventBridge 自动化规则 159
第三方集成 3
Jira Cloud 167
ServiceNow 172
KMS 工单集成的密钥政策 178
测试工单集成 181
监控使用情况和成本 183
谁可以访问 “使用情况” 页面 183
组织和账户成本汇总 184
“功能”视图 184
“账户”视图 185
成本优化策略 186
相关资源 186
禁用 Security Hub 186
为单个账户禁用 Security Hub 186
在整个组织中禁用 Security Hub 187
安全性 189
数据保护 189
Identity and access management 191
合规性验证 217
恢复能力 217
基础结构安全性 218

VPC 端点（AWS PrivateLink） 218
记录 API 调用 220
Security Hub 信息位于 CloudTrail 220
示例：Security Hub 日志文件条目 221
AWS Security Hub CSPM 224
Security Hub CSPM 的优点 225
访问 Security Hub CSPM 226
相关服务 227
Security Hub CSPM 免费试用、使用和定价 227
查看使用情况详情 227
定价详细信息 228
概念 228
启用 Security Hub CSPM 232
确认必要的权限 233
启用 Security Hub CSPM 与 Organizations 的集成 233
手动启用 Security Hub CSPM 235
后续步骤：状况管理和集成 236
正在配置 AWS Config 237
本地配置 242
中心配置 242
管理多个账户 279
使用管理账户 AWS Organizations 279
通过邀请手动管理账户 280
针对多账户环境的建议 281
使用管理账户 AWS Organizations 282
通过邀请管理账户 295
允许管理员账户和成员账户执行的操作 308
账户操作对数据的影响 312
跨区域聚合数据 314
聚合的数据类型 315
聚合管理员账户和成员账户 316
中心配置和聚合 317
启用聚合 318
查看聚合设置 320
更新聚合设置 321
停止聚合 323

标准 324
标准参考 325
启用标准 399
查看标准的详细信息 404
关闭自动启用的标准 406
禁用标准 407
控件 410
整合控件视图 410
控件的总体安全评分 411
控件参考 411
用于配置控件的权限 1121
启用控件 1121
禁用控件 1129
安全检查和评分 1138
控件类别 1208
查看控件的详细信息 1211
筛选和排序控件 1213
控制参数 1214
查看和管理控件调查发现 1226
集成 1253
查看集成列表 1254
启用来自集成的调查发现流 1256
禁用来自集成的调查发现流 1257
查看来自集成的调查发现 1258
AWS 服务 集成 1258
Third-party 集成 1277
自定义产品集成 1310
结果 1312
BatchImportFindings 用于寻找提供者 1314
BatchUpdateFindings 为顾客服务 1317
查看调查发现的详细信息和历史记录 1320
筛选调查发现 1324
对结果进行分组 1326
设置调查发现的工作流状态 1327
将结果发送到自定义操作 1329
调查发现格式：ASFF 1330

见解 1609
查看见解并对其采取行动 1609
托管见解 1612
自定义见解 1622
自动化 1629
自动化规则 1630
自动响应和补救 1654
摘要控制面板 1668
摘要控制面板的可用小组件 1668
筛选控制面板 1671
自定义 控制面板 1673
区域限制 1674
Cross-Region 聚合限制 1674
按区域划分的集成可用性 1674
按区域划分的标准的可用性 1677
按地区划分的控件可用性 1677
对控件的区域限制 1677
使用创建资源 CloudFormation 1896
Security Hub CSPM 和模板 CloudFormation 1896
了解更多关于 CloudFormation 1897
订阅公告 1897
Amazon SNS 消息格式 1903
禁用 Security Hub CSPM 1904
安全性 1906
数据保护 1907
Identity and access management 1908
合规性验证 1937
恢复能力 1937
基础结构安全性 1938
VPC 端点（AWS PrivateLink） 1938
记录 API 调用 1940
Security Hub CSPM 信息位于 CloudTrail 220
示例：Security Hub CSPM 日志文件条目 221
标注资源 1943
标签基础知识 1943
在 IAM policy 中使用标签 1944

将标签添加到资源 1945
编辑资源的标签 1947
查看资源的标签 1949
从资源中删除标签 1951
配额 1953
最大配额 1953
速率配额 1953
文档历史记录 1954
..... mmxxxviii

什么是 Security Hub 和 Security Hub CSPM？

AWS Security Hub 和 Sec AWS urity Hub CSPM AWS 服务 可以保护你的云环境。这些服务相辅相成。当它们一起使用时，它们可以提供有关您 AWS 环境安全状况的宝贵见解。

Security Hub CSPM 可让您全面了解您的安全状况，并帮助评估您的云环境是否符合安全行业标准和最佳实践。Security Hub 提供统一的体验，可帮助您优先处理和应对关键安全问题。Security Hub CSPM 调查发现会自动路由到 Security Hub，在那里它们与其他安全服务（例如 Amazon Inspector）的调查发现相关联，从而产生暴露。这有助于您识别自己环境中最严重的风险。Security Hub 还提供自动化工作流功能，帮助您将 Security Hub CSPM 调查发现融入到您的运营工作流中。

作为最佳实践，我们建议同时启用这两项服务。如果您的主要重点是识别错误配置和评估您的安全状况，则可以在不启用 Security Hub 的情况下启用 Security Hub CSPM。但是，如果您启用 Security Hub，但没有启用 Security Hub CSPM，则 Security Hub 无法使用 Security Hub CSPM 调查发现来提供有关您的 AWS 环境中的风险和暴露的信息。为了获得最佳体验，我们建议不仅要启用 Security Hub 和 Security Hub CSPM，还要启用其他安全服务：亚马逊、Amazon Insp ector 和 Amazon Mac ie。GuardDuty

简介 AWS Security Hub

AWS Security Hub 是一款统一的云安全解决方案，可对您的关键安全问题进行优先排序，并帮助您大规模做出响应。Security Hub 通过自动关联和丰富来自多个来源的安全信号来检测安全问题，例如状态管理、漏洞管理（Amazon Inspector）、敏感数据（Amazon Macie）和威胁检测（亚马逊）。GuardDuty这使得安全团队能够通过自动化分析和上下文见解优先处理云环境中的活跃风险。通过直观的可视化效果，Security Hub 将复杂的安全信号转化为切实可行的见解，从而使您能够快速做出明智的安全决策。Security Hub 还包括自动响应工作流，可帮助您修复风险、提高团队工作效率并最大限度地减少运营中断。

功能

统一的安全解决方案

通过统一云安全解决方案中的集中管理，在整个云环境中获得更广泛的可见性。

切实可行的安全见解

通过高级分析获取切实可行的安全见解，了解与您的环境关联的安全风险。

缩短响应时间

利用自动化工作流和集成的票证系统缩短响应时间。

暴露调查发现

Security Hub 关联来自 Security Hub CSPM 控制检查、Amazon Inspector 和其他检查的结果， AWS 服务 以检测与资源相关的风险。 AWS

未使用的访问权限分析

Security Hub 会自动识别在 90 天回顾期内未使用的 IAM 角色、用户、访问密钥和权限。当您启用 Security Hub 时，该服务会在您的账户中创建一个与服务关联的 IAM 访问分析器。未使用的访问发现通过突出显示过度配置的 IAM 委托人来帮助您实现最低权限访问。对于未使用的权限发现，Security Hub 可以生成最低权限策略建议，向您显示缩小范围的替换策略。

调查发现采用开放式网络安全架构框架（OCSF）格式。

Security Hub 在 OCSF 中生成调查结果，并在 OCSF 中接收来自 Security Hub CSPM 和其他机构的调查结果： AWS 服务

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

控制面板

Security Hub 控制台提供暴露、威胁、安全覆盖范围和资源的全面视图，以及一个称为攻击路径图的交互式可视化，显示潜在攻击者如何访问和控制与暴露调查发现关联的资源。

与第三方产品集成

您可以通过 Security Hub 集成来增强安全状况。例如，如果您使用 Jira Cloud 或 ServiceNow ITSM，则可以使用此功能根据调查发现创建票证。

集成

Security Hub 会从以下方面收到调查结果 AWS 服务。

- AWS Security Hub CSPM
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- IAM 访问分析器

可访问性

Security Hub 在大多数 AWS 地区都可用。有关当前已推出 Security Hub 的所有区域的列表，请参阅 AWS 一般参考 中的 Security Hub 端点和配额。有关管理 AWS 区域 您的账户的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》中的指定 AWS 区域 您的账户可以使用。

您可以为单个账户或组织内的账户启用 Security Hub。在每个区域，您可以通过以下任一方式访问和使用 Security Hub：

Security Hub 控制台

Security Hub 控制台是一个基于浏览器的界面，可用于创建和管理 AWS 资源。在此控制台中，您可以访问您的账户、数据和资源。

Security Hub API

Security Hub API 允许您以编程方式访问您的账户、数据和资源。您可以直接向 Security Hub 发送 HTTPS 请求。

AWS CLI

借助 AWS CLI，您可以在系统命令行中运行命令来执行任务和生成执行任务的脚本。在某些情况下， AWS CLI 可能比 Security Hub 控制台更有用。

AWS 软件开发工具包

AWS 软件开发工具包由适用于各种编程语言和平台（C++、Go、Java、.NET 和 Python）的库和示例代码组成。它们以您的首选语言提供对 Security Hub 和其他 AWS 服务 语言的编程访问权限，并可以帮助您管理错误、签署请求和重试请求等任务。

定价

Security Hub 的概念

在 Security Hub 中，我们建立在常用 AWS 概念和术语的基础上，并使用这些附加术语。

Account

包含您的 AWS 资源的标准 AWS 账户。 AWS 使用您的 AWS 帐户登录以启用 Security Hub。

如果您的帐户已注册 AWS Organizations，则您的组织会指定一个 Security Hub 管理员帐户。此账户可以启用其他组织账户作为成员账户。

一个组织只能有一个管理员账户。账户不能既是管理员账户又是成员账户。

Security Hub 支持以下账户：

- 组织管理 AWS 账户 — 管理 AWS 组织的账户。
- 委托管理员 AWS 账户 — 一种管理 AWS 组织使用情况 AWS 服务 的账户。
- 成员账户 — 作为 AWS AWS 组织成员的账户。
- 独立账户-未 AWS Organizations 启用的 AWS 账户

管理员账户

此类 AWS 账户可以查看关联成员账户的调查结果。

当组织管理 AWS 帐户将该帐户指定为 Security Hub 管理员帐户时，此类帐户将变为管理员帐户。Security Hub 管理员账户可以启用任何组织账户作为成员账户，还可以邀请其他账户成为成员账户。

一个组织只能有一个管理员账户。账户不能既是管理员账户又是成员账户。

聚合区域

聚合区域允许您在单个控制面板 AWS 区域 中查看来自多个区域的安全发现。

聚合区域是您查看和管理调查结果 AWS 区域 的地方。调查发现会从关联区域聚合到聚合区域中。更新后的调查发现会在各个区域之间复制。

在聚合区域中，控制面板和库存页包含来自所有关联区域的数据。自动化页面只能用于在聚合区域定义自动化规则。 Third-party 只能在聚合区域配置工单集成。

已存档的发现

状态为 ARCHIVED 的调查发现。这些调查发现表明，调查发现的调查发现提供者或客户认为该调查发现不再相关。

寻找提供者可以将他们创建的结果存档。客户可以使用 Security Hub API 的BatchUpdateFindingsV2操作或在 Security Hub 控制台中更新状态来存档他们认为不再相关的发现。

在 Security Hub 控制台中，默认筛选设置会将存档的调查发现从调查发现列表和表格中排除。您可以更新筛选条件以包括已存档的调查发现 如果使用 GetFindingsV2 操作检索查找结果，则该操作会同时检索存档和活动查找结果。以下示例说明了如何在结果中排除已存档的调查发现。

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

Cross-Region 聚合

将来自关联区域的调查发现和资源汇总到一个聚合区域。您可以查看聚合区域中的所有数据，并更新聚合区域中的调查发现。

委派管理员帐户

在中 AWS Organizations，服务的委派管理员帐户能够管理组织对服务的使用。

在 Security Hub 中，Security Hub 管理员账户也是 Security Hub 的委派管理员账户。当组织管理账户首次指定 Security Hub 管理员账户时，Security Hub 会调用 Organizations，将该账户设为委派管理员账户。

然后，组织管理账户必须选择委派管理员账户作为所有区域的 Security Hub 管理员账户。

曝光

风险是指安全控制、配置错误或其他可能被主动威胁利用的领域中更广泛的漏洞。

曝光的例子包括：

- Mis-configured 资源的控制平面。
- 存在极有可能被利用的软件漏洞。
- 可公开访问的资源（网络或 API）。

暴露调查发现

一种描述您的环境中存在的暴露情况的调查发现。暴露调查发现包括特征和信号。一个信号可以包含一种或多种类型的暴露特征。 AWS 当来自 Security Hub CSPM、Amazon Inspector、亚马逊、Amazon Macie AWS 或其他服务的信号表明存在风险时，Sec AWS urity Hub 会生成曝光结果。 GuardDuty一项或多项曝光调查结果可能涉及资源。如果资源没有任何暴露特征或特征不足，Security Hub 不会为该资源生成暴露调查发现。

曝光发现的一个例子是：一个可从互联网访问的 EC2 实例，该实例存在很有可能被利用的软件漏洞。

调查发现

安全检查或与安全相关的检测的可观察记录。Security Hub 通过与其他安全调查发现进行关联来生成和更新调查发现。这些被称为暴露调查发现。调查结果也可能来自与其他产品 AWS 服务 和第三方产品的集成。

正在寻找摄入量

将调查发现导入 Security Hub。调查发现摄取事件包括新调查发现和现有调查发现的更新。

关联区域

启用跨区域聚合后，关联区域是指将调查发现和资源清单聚合到聚合区域的区域。

在关联区域中，控制面板和库存页面仅包含相关调查结果 AWS 区域。

开放式网络安全架构框架（OCSF）

开放网络安全架构框架 (OCSF) 是由 AWS 网络安全行业的领先合作伙伴共同开发的开源项目。OCSF 为常见安全事件提供了标准架构，定义了版本控制标准以促进架构的演变，还包括安全日志生成者和使用者的自治流程。有关更多信息，请参阅 OCSF findings in Security Hub。

成员账户

授 AWS 账户 予管理员帐户查看其调查结果并对其采取行动的权限。当 Security Hub 管理员帐户将其启用为成员帐户时，此类帐户 AWS 账户 就会变成成员帐户。

信号

促成暴露调查发现的调查发现。信号可以被称为促成性调查发现。信号可以源自 Security Hub CSPM 或其他 AWS 服务信号 AWS Config，例如 Amazon Inspector。

Service-linked 配置记录器

一种 AWS Config 记录器，用于记录服务特定资源的配置数据。Security Hub 以事件驱动的方法使用这些记录器来获取风险分析覆盖范围、资源库存报告和状态管理控制评估的资源配置项目。此功能作为基本计划定价的一部分提供给所有 Security Hub 客户。启用 Security Hub 后，将在您的账户中创建以下与服务相关的配置记录器：

- 在每个 AWS 账户 和中 AWS 区域，都会创建一个名为`AWSConfigurationRecorderForSecurityHubAssets`的与服务相关的配置记录器。
- 对于全局资源类型，将在 us-east AWS 区域-1 中创建名`AWSConfigurationRecorderForSecurityHubAssetsGlobal`为的附加服务关联配置记录器。
- 如果在和中同时启用了 Security Hub AWS 账户 和 Security Hub CSPM AWS 区域，则会创建一个名为`AWSConfigurationRecorderForSecurityHubCSPM`的服务相关配置记录器。

有关更多信息，请参阅与服务相关的配置记录器的注意事项和录制区域和全球资源。

Service-linked 分析器

Security Hub 代表您创建和管理的 IAM 访问分析器。启用 Security Hub 后，它会自动创建一个与服务相关的未使用访问分析器，以识别在 90 天回顾期内未使用的 IAM 角色、用户、访问密钥和权

限。该分析器在美国东部（弗吉尼亚北部）运行，因为 IAM 是一项全球服务。Security Hub 会将未使用的访问结果复制到您已启用 Security Hub 的所有区域。您无需单独启用 IAM Access Analyzer 或采取任何其他操作。此功能作为基本计划定价的一部分提供给所有 Security Hub 客户。您可以在 IAM Access Analyzer 控制台中查看与服务相关的分析器，但在启用 Security Hub 后，您无法对其进行修改或删除。当您在的所有区域禁用分析器时，Security Hub 会删除该分析器 AWS 账户。有关更多信息，请参阅 the section called “未使用的访问调查发现”。

特质

导致暴露调查发现的安全偏差。特征类型包括假设性、错误配置、可访问性、敏感数据和漏洞。一个特征与一个信号相关联，一个信号可以包含多个特征。例如，Security Hub CSPM 控件表示客户管理型策略允许管理访问控制。此信号包含错误配置特征。

未使用的访问权限发现

一项发现，用于识别在 90 天回顾期内未使用的 IAM 角色、用户、访问密钥或一组权限。Security Hub 使用与服务关联的 IAM 访问分析器生成未使用的访问结果。未使用的访问发现有四种类型：未使用的 IAM 角色、未使用的 IAM 用户访问密钥、未使用的 IAM 用户密码和未使用的权限。

AWS Security Hub 成本估算器

Security Hub 成本估算器是一项控制台功能，可估算整个环境的功能。 AWS 成本估算器向您显示您在 Sec AWS urity Hub CSPM、Amazon Inspector和Amazon上的个人服务成本，以及使用Security Hub 的简化定价计划，您在Security Hub中的估计成本。 GuardDuty 您可以调整预估的使用量和资源数量以匹配您的 AWS 使用量，从而提高估算的准确性。成本估算器适用于所有可用 Security Hub 的区域。

成本估算器使用两种定价模型估算安全功能的每月成本：

- 个人服务定价 — 单独为每项安全功能付费（GuardDuty、Amazon Inspector、Security Hub CSPM）。
- S@@ ecurity Hub 简化了定价 — 3 种定价计划的统一定价、按资源定价的基本计划、按事件和每 GB 日志定价的威胁分析，以及按资源定价的 Lambda 代码扫描。

估算器使用可用 AWS Cost Explorer 数据。当 Cost Explorer 数据不可用时，您可以手动输入使用情况数据。成本估算基于观察到的和用户提供的使用情况以及公开定价信息。估算值可能无法反映企业折扣。

成本估算器的主要优点包括：

- 查看启用 Security Hub 时采用统一定价的成本与不启用 Security Hub 的单个服务的成本对比如何
- 在启用功能之前估算成本
- 调整使用参数以模拟不同的场景
- 将估算值导出为 PDF 以供利益相关者审查

按账户类型划分的访问权限

> **Note**
>
> 对于委托管理员和成员账户，默认情况下，成本估算器以编辑模式打开，允许您立即输入使用数据。当 Cost Explorer 数据可用时，管理账户和独立账户将在查看模式下打开。

此功能会自动检索有关过去实际使用情况的信息，以估算某些账户类型的费用。有关每种账户类型的详细信息以及每种账户类型的可用数据，请参阅下文。

按账户类型划分的访问权限

Account Type (账户类型)	Cost Explorer 数据	数据输入	Scope
管理账户 (MA)	自动填充	可手动超控	在整个组织范围内
委派管理员 (DA)	通过跨账户角色自动填充*	可手动超控	在整个组织范围内
会员账号	通过跨账户角色自动填充*	可手动超控	在整个组织范围内
独立账户 (SA)	自动填充	可手动超控	单一账户

* 需要在管理账户中配置跨账户 IAM 角色。参见以下设置跨账户访问章节。

先决条件

所需的 IAM 权限

要使用成本估算器的所有功能，您的 IAM 委托人必须具有以下权限：

成本估算器所需的 IAM 权限

API 操作	服务	用途
`ce:GetCostAndUsage`	AWS Cost Explorer	检索历史使用量和成本数据
`pricing:GetProducts`	AWS 定价	获取当前定价
`organizations:ListAccounts`	AWS 组织	计算组织中的账户数量
`organizations:DescribeOrganization`	AWS 组织	确定账户类型
`securityhub:ListOrganizationAdminAccounts`	Security Hub	列出组织管理员账号
`iam:GetRole`	IAM	检查是否存在跨账户角色（仅限管理账户）*
`sts:AssumeRole`	IAM	扮演跨账户角色（仅限委托 administrator/Member 账户）**

* 只有管理账户用户需要验证跨账户角色状态。

** 只有使用跨账户访问权限的授权管理员和组织成员账户才需要此选项。

其他要求

Cost Explorer 成本管理服务

必须启用自动数据填充（启用后处理延迟 24 小时）。

设置跨账户访问

委派的管理员和成员账户可以通过配置跨账户 IAM 角色从管理账户访问组织范围 AWS Cost Explorer 的数据。此配置允许这些账户在不切换到管理账户的情况下查看实际使用数据。

先决条件

在为成本估算器设置跨账户访问权限之前，需要以下项目和信息：

- 管理账户必须已 AWS Cost Explorer 启用。
- 在管理账户中创建角色的 IAM 权限。
- 了解将被授予跨账户访问权限的委托管理员或成员账户 ID。

设置步骤

成本估算器直接在控制台中提供指导性设置说明。要访问说明，请导航到组织管理账户中的 https://console.aws.amazon.com/securityhub/v2/Home#/ CosteStimator 的成本估算器页面。找到 “跨账户访问权限” 部分，然后按照概述的步骤设置跨账户角色。

角色配置

成本估算器的跨账户访问需要设置具有信任策略和权限策略的 IAM 角色。必须使用以下配置在管理账户中创建跨账户角色：

角色名称（需要确切的名称）- AwsSecurityHubCostEstimatorCrossAccountRole

推荐的信任政策：

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

通过替换策略示例中的以下值来编辑策略：

- *{ACCOUNT_ID}*替换为您授予跨账户访问权限的委派管理员或成员账户 ID。
- *{ROLE_NAME}*替换为您授予访问权限的委派管理员或成员账户中的 IAM 角色名称。

推荐的权限策略：

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

> **Note**
>
> 信任策略限制对特定账户和角色的访问权限。只有指定的 IAM 委托人可以担任此角色，从而防止未经授权的访问。

验证

在管理账户中创建角色后，使用以下步骤确认设置是否正常运行。

1. 登录委派管理员或成员账户。
2. 通过 v2/Home#/costeStimator 导航到 Security Hub 成本估算器 https://console.aws.amazon.com/securityhub/
3. 该页面应自动：
    a. 检测组织中的管理账户。
    b. 扮演跨账户角色。
    c. 加载组织范围内使用的 Cost Explorer 数据。

如果成功，您将看到实际使用情况数据，而不是手动输入字段。

问题排查

本节介绍设置跨账户访问权限时可能出现的常见问题和解决方案。

此账户没有组织使用情况数据

此警报表示无法访问跨账户角色。此警报可能导致的原因有：

1. 角色不存在：管理账户尚未创建角色。
   - 解决方案：请联系您的管理账户管理员，按照设置指南创建角色。
2. 角色名称不匹配：角色名称不完全匹配。
   - 解决方案：验证角色名为`AwsSecurityHubCostEstimatorCrossAccountRole`。
3. 信任政策不正确：信任政策不允许您的账户担任该角色。
   - 解决方案：验证信任策略包括您的账户 ID 和角色名称。
4. 缺少 AssumeRole 权限：您的 IAM 委托人缺少权限`sts:AssumeRole`。
   - 解决方案：请联系您的管理员添加`sts:AssumeRole`权限。

要查看详细的设置说明：单击警报中的 “查看说明” 链接，打开包含 step-by-step指导和策略模板的模式。

解决办法：您仍然可以通过在编辑模式下手动输入使用值来使用成本估算器。

使用成本估算器

访问成本估算器

从 Security Hub 登录页面访问成本估算器

1. 使用您的 AWS 组织管理或委派管理员 AWS 账户凭证登录您的账户。[在 v2/home 上打开 us-east-1 区域的 Security Hub 控制台。https://console.aws.amazon.com/securityhub/]
2. 在登录页面上，找到定价卡。
3. 选择估算成本。

在 Security Hub 启用和配置步骤中访问成本估算器

1. 在入门界面的新 Security Hub 卡片中找到定价。
2. 选择查看估算值。

要从 Amazon Inspector 或 Securit GuardDuty y Hub CSPM 控制台访问成本估算器

1. 导航到服务仪表板或摘要页面。
2. 在定价信息卡中选择 “比较价格”。

了解成本估算器接口

页面布局

成本估算器页面包含三个主要部分：

- 概述部分 — 解释统一安全管理和成本优化的好处。
- 定价信息-包含功能类别和定价等级的可扩展面板。
- 定价对比表 — Side-by-side 成本比较和功能详情。

定价对比表

表格标题包括 view/edit 模式控件和重置选项。该表分两列显示成本：

- 个人服务-单独安全服务的当前或估计成本。
- S@@ ecurity Hub — 使用简化的定价模型估算成本。

定价区域

第一列显示定价背景信息，包括关于估算值使用 us-east-1 定价进行计算的注释。徽章表示估算中不包括企业折扣。

查看成本估算

使用成本估算器时，您可以查看、编辑、重置和导出估算值。

默认情况下，成本估算器在视图模式下打开。

查看成本估算

1. 使用中描述的方法之一访问成本估算器。访问成本估算器
2. 查看摘要行中的每月总成本。
3. 查看能力组及其详细的成本明细。
4. 选择权能名称以在弹出框中查看描述。

视图模式下的数据源

估算器显示来自多个来源的数据，由标签表示：

- 默认-来自 AWS Cost Explorer （过去 30 天）的数据。
- $-/mo-成本数据不可用（当无法访问 Cost Explorer 时显示）。
- 自定义用法-用户输入的值。
- 未启用 — 在 Cost Explorer 权限不存在时显示。

特定于账户的行为

以下内容描述了成本估算器如何在不同类型的账户和配置中发挥作用。

委托管理员和成员账户

配置跨账户访问权限后：

- Cost Explorer 数据可在组织范围内使用。
- 默认情况下以查看模式打开（与管理账户相同）。可以切换到编辑模式来修改估计值。

未配置跨账户访问权限：

- 警报显示：“该账户的组织使用数据不可用”。
- 默认情况下以编辑模式打开，便于手动输入。
- 点击警报中的 “查看说明” 以获取设置指导。

管理账户

创建跨账户角色后：

- “跨账户访问” 部分显示配置状态。
- 显示推荐的验证策略。
- 提供在 IAM 控制台中查看角色的链接。

未创建跨账户角色：

- “跨账户访问” 部分显示设置指南。

- 提供带有预先填充策略的 step-by-step说明。
- 直接链接到 IAM 控制台以创建角色。

无法验证角色状态：

- 如果没有呼叫权限`iam:GetRole`，则控制台无法确定您是否创建了必要的角色。
- 显示 “无法验证” 以及相应的错误消息。

独立账户

未创建跨账户角色：

- 现有行为没有变化。
- Cost Explorer 数据在启用后可用。
- 默认情况下以视图模式打开。

编辑使用量值

编辑模式允许您修改维度值并查看实时成本更新。

编辑使用量值

1. 在表格标题中选择 “编辑”。
2. 在维度输入字段中输入值。
3. 自动查看更新的费用。
4. 选择 “查看” 可返回到查看模式。

> **Important**
>
> - 当您离开成本估算器页面时，编辑内容不会保存
> - 修改后的估算值使用 us-east-1（弗吉尼亚北部）定价，不包括企业折扣
> - 在 “仅显示当前成本” 模式下进行编辑会自动切换回预估模式

重置估算器

此操作会清除所有自定义值并从 Cost Explorer 中重新加载默认数据。

将所有值重置为默认值

1. 在表格标题中选择 “重置”。
2. 在确认对话框中，选择重置。

导出估计值

而在成本估算器中，您的估算数据可以导出为PDF文件。

导出成本估算

1. 确保您处于查看模式。
2. 在页眉中选择 “下载 PDF”。

PDF 会自动下载，文件名为:`SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`.

问题排查

本节介绍使用成本估算器时可能出现的常见问题和解决方案

没有可用的 Cost Explorer 数据

问题

提醒显示 “您的账户没有可用的费用数据”。

按账户类型划分的解决方案

解决方案取决于您的账户类型：

Cost Explorer 数据丢失的解决方案

Account Type (账户类型)	解决方案
管理账户	启用 Cost Explorer 并等待 24 小时进行数据处理

Account Type (账户类型)	解决方案
委托管理员	联系管理账户管理员申请访问权限
会员账号	请联系管理账户或授权管理员获取访问权限
独立账户	启用 Cost Explorer 并等待 24 小时进行数据处理

解决办法

在编辑模式下输入自定义值。

跨账户访问不起作用

问题

“授权的管理员或成员账户显示 “该账户的组织使用数据不可用” 警报。

可能的原因和解决方案

1. 管理账户中不存在跨账户角色。
    a. 解决方案：请联系管理账户管理员创建角色。
    b. 成本估算器为管理账户用户提供指导性设置说明。
2. 角色名称不完全匹配。
    a. 必填角色名:`AwsSecurityHubCostEstimatorCrossAccountRole`.
    b. 解决方案：验证 IAM 控制台中的角色名称是否完全匹配（区分大小写）。
3. 信任政策不允许您开设账户。
    a. 解决方案：验证信任策略主体包括您的账户 ID 和角色名称。
    b. 格式：`arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`。
4. 缺少 AssumeRole 权限。
    a. 解决方案：验证您的 IAM 委托人是否拥有`sts:AssumeRole`权限。
    b. 请联系您的 AWS 管理员添加此权限。

解决办法：

在编辑模式下输入自定义值，无需使用 Cost Explorer 数据即可手动估算成本。

获取详细说明

- 点击提醒中的 “查看说明” 链接，打开一个包含以下内容的模式：
  - Step-by-step 设置指南
  - 预先填充的策略模板
  - 针对您的错误的疑难解答提示

权限错误

问题

特定 API 操作出现 “访问被拒绝” 错误。

解决权限错误

1. 记下错误消息中被拒绝的操作（例如`ce:GetCostAndUsage`）。
2. 选择 “复制” 以复制错误详情。
3. 将错误详细信息发送给您的 AWS 管理员。
4. 请求中列出的必需 IAM 权限所需的 IAM 权限。

> **Note**
>
> 如果缺少权限，您仍然可以使用编辑模式手动输入值，除非定价 API 访问被拒绝（禁止所有成本估算）。

功能显示 “未启用”

问题

功能显示 “未启用” 状态。

说明

当您拥有 Cost Explorer 访问权限但该功能当前未处于活动状态时，就会显示此状态。如果您改为看到 $-/mo，则表示您的账户类型不可用 Cost Explorer 数据。

查看成本估算

1. 选择 “编辑” 进入编辑模式。
2. 输入权能的维度值。
3. 查看更新的成本估算。

能力显示 “不适用”

问题

能力在 “个人服务” 列中显示 “不适用”。

说明

此功能只能通过 Security Hub 的简化定价提供，不能作为独立服务提供。

修改后的费用与 Cost Explorer 不匹配

问题

编辑后的费用与最初的 Cost Explorer 值不同。

说明

修改后的估算值使用 us-east-1（弗吉尼亚北部）的定价率，不包括企业折扣。Cost Explorer 数据反映了实际成本和适用的折扣。

重要提示

- 估算基于观察到的使用情况和用户提供的使用情况以及公开定价信息 — 实际成本可能因使用模式和企业协议而异
- 30 天回顾 — Cost Explorer 数据反映了过去 30 天的使用情况
- 定价区域 — 所有估算值均使用 us-east-1（弗吉尼亚北部）费率
- 对@@ 设置没有影响 — 估算器中的更改不会影响您当前的 Security Hub 或服务配置
- 企业折扣-修改后的估算值不包括企业折扣；只有 Cost Explorer 数据反映了实际的折扣成本
- 数据刷新 — Cost Explorer 数据每天更新；刷新页面以查看最新数据

相关信息

- AWS Security Hub 定价
- AWS Cost Explorer 用户指南
- AWS 定价 API 参考
- 启用 Security Hub

启用 Security Hub

您可以为任何 AWS 账户启用 Security Hub。本文档的这一部分描述了为 AWS 组织或独立账户启用 Security Hub 所需的所有步骤。

有关如何启用 Security Hub 的简要演示，请观看以下视频：S ecurity Hub 入门演示和演示。

为... 启用 Security Hub AWS Organization（组织）

本节包括三个步骤：

- 在步骤 1 中， AWS 组织管理账户为其 AWS 组织指定委派管理员，创建委派管理员策略，并可选择为自己的账户启用 Security Hub。
- 在步骤 2 中，组织的委派管理员为自己的账户启用 Security Hub。

- 在步骤 3 中，组织的委派管理员为 Security Hub 和其他支持的安全服务配置组织中的所有成员帐户。

步骤 1：委派管理员帐户并可选择在中启用 Security Hub AWS 组织管理账户

> **Note**
>
> 此步骤只需要在组织管理账户的一个区域中完成。

为 Security Hub 分配委派管理员帐户时，您可以为委托管理员选择的帐户将取决于您如何为 Security Hub CSPM 配置委派管理员。如果您已为 Security Hub CSPM 配置了委托管理员，并且该帐户不是组织的管理帐户，则该帐户将自动设置为 Security Hub 的委托管理员，并且无法选择其他帐户。如果将 Security Hub CSPM 的委托管理员帐户设置为组织管理帐户或根本未设置，则可以选择哪个帐户将成为您的 Security Hub 委托管理员帐户，但组织管理帐户除外。

有关在 Security Hub 中指定委派管理员的信息，请参阅在 Security Hub 中指定委派管理员。有关在 Security Hub 中创建委派管理员策略的信息，请参阅在 Security Hub 中创建委派管理员策略。

为 Security Hub 指定管理员

1. 使用您的 AWS 组织管理 AWS 账户凭据登录您的账户。打开 Security Hub 控制台，网址为https://console.aws.amazon.com/securityhub/v2/home。
2. 在 Security Hub 主页上，选择 Security Hub，然后选择开始使用。
3. 在“授权管理员”部分，根据提供的选项选择管理员帐户。最佳做法是，建议对所有安全服务使用相同的委派管理员以实现一致的管理。
4. 选中“可信访问”复选框。选择此选项可使您的委托管理员帐户能够在成员帐户上配置某些功能，例如 GuardDuty 恶意软件防护。如果您取消选中此选项，Security Hub 将无法代表您启用这些功能，您需要直接通过与该功能关联的服务启用这些功能。
5. （可选）要启用帐户，请选中复选框以为您的 AWS 帐户启用 Security Hub。
6. 对于委派管理员策略，请选择以下选项之一来添加策略声明。

    a. （选项 1）选择为我更新此项。选中策略语句下方的框，以确认 Security Hub 将自动创建向委派管理员授予所有必需权限的委派策略。

    b. （选项 2）选择我想手动附加此项。选择复制并附加。在 AWS Organizations 控制台的“委派管理员”下 AWS Organizations，选择“委托”，然后将资源策略粘贴到委托策略编辑器中。选择创建策略。打开您当前在 Security Hub 控制台中的选项卡。

7. 选择配置。

步骤 2：在委派管理员账户中启用 Security Hub

委派管理员账户完成此步骤。在 AWS 组织管理账户为其组织指定委派管理员后，被授权的管理员必须为自己的账户启用 Security Hub，然后才能为整个 AWS 组织启用 Security Hub。

在委派管理员账户中启用 Security Hub

1. 使用您的委派管理员凭据登录您的 AWS 账户。打开 Security Hub 控制台，网址为https://console.aws.amazon.com/securityhub/v2/home。
2. 从 Security Hub 主页中选择 “开始”。
3. 安全功能部分概述了自动启用并包含在 Security Hub 每资源基本价格中的功能
4. （可选）对于标签，确定是否在账户设置中添加键值对。
5. 选择 “启用 Security Hub” 以完成对 Security Hub 的启用。
6. （推荐）从弹出窗口中选择 “配置我的组织”，然后继续执行步骤 3。

步骤 3：创建一个策略以在所有成员账户中启用 Security Hub

在组织的委托管理员账户中启用 Security Hub 后，您需要创建一个策略来定义在组织成员账户中启用哪些服务和功能。有关更多信息，请参阅使用策略类型启用配置。

启用 Security Hub 后，将在您的账户中创建以下资源：

- 一个名AWSServiceRoleForSecurityHubV2为的服务相关角色。
- Service-linked 配置记录器。有关更多详细信息，请参阅 S Service-linked ec urity Hub 概念文档中的记录器。
- Service-linked 分析器。有关更多详细信息，请参阅 Security Hub 概念文档中的Service-linked 分析器。

在独立账户中启用 Security Hub

此过程介绍了如何在独立账户中启用 Security Hub。独立账户是指 AWS 账户 尚未启用 AWS 组织的账户。

在独立账户中启用 Security Hub

1. 使用您的 AWS 账户凭证登录您的账户。打开 Security Hub 控制台，网址为https://console.aws.amazon.com/securityhub/v2/home。
2. 在 Security Hub 主页上，选择 “开始”。
3. 在 “安全功能” 部分中，执行以下任一操作：
   a. （选项 1）选择 “启用所有功能”。这将启用 Security Hub 的所有基本功能、威胁分析和其他功能。
   b. （选项 2）选择 “自定义功能”。选择应开启的威胁分析和其他功能。您不能取消选择 Security Hub 基本计划功能中的任何功能。
4. 在 “区域” 部分，选择 “启用所有区域” 或 “启用特定区域”。如果您选择启用所有区域，则可以决定是否自动启用新区域。如果选择 “启用特定区域”，则必须选择要启用的区域。
5. （可选）对于资源标签，将标签添加为键值对，以帮助您轻松识别配置。
6. 选择启用 Security Hub。

启用 Security Hub 后，将在启用该服务的每个账户中创建以下资源：

- 一个名AWSServiceRoleForSecurityHubV2为的服务相关角色。
- Service-linked 配置记录器。有关更多详细信息，请参阅 S Service-linked ec urity Hub 概念文档中的记录器。
- Service-linked 分析器。有关更多详细信息，请参阅 Security Hub 概念文档中的Service-linked 分析器。

在 Security Hub 中指定委派管理员

在 AWS 组织管理账户中，您可以为组织指定委派管理员。最佳做法是，建议对所有安全服务使用相同的委派管理员以实现一致的管理。

本主题中的过程介绍如何在 Security Hub 中指定委派管理员。它假设您之前已启用 Security Hub，但未在启用工作流中指定委派管理员。

注意事项

在 Security Hub 中指定委派管理员时，请考虑以下事项：

- AWS 组织管理账户可以将自己指定为 Security Hub CSPM 中的委托管理员。 AWS 组织管理账户无法在 Security Hub 中将自己指定为委托管理员。在这种情况下， AWS 组织管理账户必须在 Security Hub 中指定另一个账户 AWS 账户 作为委托管理员。最佳做法是，建议对所有安全服务使用相同的委派管理员以实现一致的管理。
- 如果 AWS 组织管理帐户在 Security Hub CSPM 中指定了委托管理员，则该授权管理员将自动成为 Security Hub 中的委托管理员。在这种情况下，Security Hub 仅允许该特定 AWS 账户 人员充当委派管理员。

> **Note**
>
> 如果 AWS 组织管理账户在 Security Hub 中使用与在 Security Hub CSPM 中相同的委托管理员，则通过 Security Hub CSPM 控制台或使用 AWS Organizations API 将其删除也会在 Security Hub 中将其删除。同样，通过 Security Hub 控制台或使用 Organizations AWS API 将其删除也会在 Security Hub CSPM 中将其删除。当从 Security Hub CSPM 中移除委派管理员时，中心配置将自动选择退出。

启用 Security Hub 后指定委派管理员

此过程需要 AWS 组织管理账户完成。它假设 AWS 组织管理账户之前启用了 Security Hub，但在启用工作流程中没有指定委派管理员。

> **Note**
>
> 完成此过程后，您必须创建一项策略，允许您组织的委派管理员配置 Security Hub 并在 AWS Organizations中执行特定操作。有关更多信息，请参阅在 Security Hub 中创建委派管理员策略。

在 Security Hub 中指定委派管理员

1. 使用您的组织管理 AWS 帐户凭据登录您的帐户，然后在 https://console.aws.amazon.com/securityhub/v2/ home 上打开 Security Hub 控制台。
2. 在导航窗格中，选择常规。
3. 在委派管理员中，选择配置。从提供的选项中选择一个 AWS 账户，或者输入要指定为组织委托管理员 AWS 账户 的 12 位 AWS 账户 数字。选择保存。

在 Security Hub 中创建委派管理员策略

AWS 组织管理账户可以创建策略，允许授权的管理员配置 Security Hub 并在中执行特定操作 AWS Organizations。本主题中的过程介绍如何创建策略。完成该过程时，您可以允许 Security Hub 为您创建策略，也可以手动创建策略。除非您想针对特定使用案例自定义策略，否则我们建议允许 Security Hub 为您创建策略。只有当 AWS 组织管理账户启用了 Security Hub 并指定了委派管理员，但在完成启用工作流程时跳过了创建策略时，组织管理账户才必须完成此过程。有关如何更新此策略的信息，请参阅《AWS Organizations 用户指南》中的使用 AWS Organizations更新基于资源的委派策略。

> **Note**
>
> 完成此过程后，委派管理员可以创建策略来允许其管理您组织内的成员账户。有关更多信息，请参阅以委派管理员身份创建策略来管理成员账户。

创建委派管理员策略

1. 使用您的组织管理 AWS 账户凭据登录您的账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 在导航窗格中，选择常规。
3. 对于委派管理员策略，请执行以下操作之一：

   a. （选项 1）选择创建策略。选中策略语句下方的框，以确认 Security Hub 将自动创建向委派管理员授予所有必需权限的委派策略。

   b. （选项 2）打开策略。选择复制并附加。在 AWS Organizations 控制台的 “委派管理员” 下 AWS Organizations，选择 “委托”，然后将资源策略粘贴到委托策略编辑器中。选择创建策略。打开您在 Security Hub 控制台中所处的选项卡，然后选择配置。

管理 AWS 组织中成员账户的配置

AWS 组织的委派管理员可以跨成员账户和区域配置安全功能。有两种类型的配置可用，即策略和部署。策略为 Sec AWS urity Hub 和 Amazon Inspector 的账户和区域生成 AWS 组织政策。部署是一次性操作，用于在 Amazon 和 Security Hub CSPM 的选定账户 GuardDuty 和区域中启用 AWS 安全功能。与策略不同，您无法查看或编辑部署，部署也不适用于新启用的账户。作为替代方案，亚马逊 GuardDuty 和Sec AWS urity Hub CSPM中提供了针对新成员账户的自动启用功能。

Security Hub 配置目录

Security Hub 的配置目录提供了多个选项，可帮助配置您的 AWS 组织帐户以使用提供的安全功能。

以下是 Security Hub 配置目录中可用的选项。

Security Hub（基本功能和附加功能）

这是为 Security Hub 部署的推荐配置。

类型：策略和部署

描述：此配置启用 Security Hub 的基本安全管理、状态管理、威胁分析和漏洞管理功能。它可以选择启用其他功能。

威胁分析来自 GuardDuty

类型：部署

描述：开启所选 Amazon GuardDuty 功能，持续监控、分析和处理 AWS 环境中的 AWS 数据源和日志。

来自 Sec AWS urity Hub 的状态管理 (CSPM)

类型：部署

描述：此配置启用 Security Hub CSPM 的标准和控件，这些标准和控件可检测您的 AWS 账户和资源何时偏离安全最佳实践。

Amazon Inspector 提供的漏洞管理

类型：政策

描述：此配置开启选定的 Amazon Inspector 功能，这些功能可自动发现工作负载、实例、容器映像等，并扫描它们是否存在漏洞和网络暴露。

启用具有某种策略类型的配置

以下过程介绍如何使用 AWS 组织账户的策略类型创建配置。要创建配置策略，需要在 AWS 组织管理账户中创建委派管理员策略。有关在 Security Hub 中创建委派管理员策略的信息，请参阅在 Security Hub 中创建委派管理员策略。

创建启用和禁用成员账户的策略

1. 使用带有委派管理员凭证的 AWS 账户登录。在 https://console.aws.amazon.com/securityhub/v2/home 中打开 Security Hub 控制台。
2. 从导航窗格中选择 “管理”，然后选择 “配置”。
3. 从配置目录中选择一个具有策略或策略类型的项目并进行部署。要完全配置 Security Hub，建议选择 Sec urity Hub（基本功能和附加功能）。
4. 在 “配置 Security Hub” 页面的 “详细信息” 部分，输入策略的名称和描述。
5. 在 “安全功能” 部分中，执行以下任一操作：
   a. （选项 1）选择 “启用所有功能”。这将启用 Security Hub 的所有基本功能、威胁分析和其他功能。
   b. （选项 2）选择 “自定义功能”。选择应开启的威胁分析和其他功能。您不能取消选择 Security Hub 基本计划功能中的任何功能。
6. 在账户选择部分，选择以下选项之一。如果要将配置应用于所有组织单位和帐户，请选择 “所有组织单位和帐户”。如果要将配置应用于特定的组织单位和帐户，请选择 “特定组织单位和帐户”。如果您选择此选项，请使用搜索栏或组织结构树来指定将应用该策略的组织单元和账户。如果您不想将配置应用于任何组织单位或帐户，请选择无组织单位或帐户。
7. 在 “区域” 部分，选择 “启用所有区域”、“禁用所有区域” 或 “指定区域”。如果您选择启用所有区域，则可以决定是否自动启用新区域。如果您选择禁用所有区域，则可以决定是否自动禁用新区域。如果选择指定区域，则必须选择要启用和禁用的区域。
8. （可选）有关高级设置，请参阅中的指南 AWS Organizations。
9. （可选）对于资源标签，将标签添加为键值对，以帮助您轻松识别配置。
10. 选择下一步。
11. 查看您的更改，然后选择应用。您的目标账户是根据策略进行配置的。您的策略的配置状态将显示在 “策略” 页面的顶部。每项功能都将显示其是否已配置或部署失败的状态。对于任何故障，请单击失败消息链接以查看更多详细信息。要查看账户级别的有效策略，您可以查看配置页面上的组织选项卡，可以在其中选择一个账户。

启用具有某种部署类型的配置

以下过程介绍如何为您的 AWS 组织账户创建具有部署类型的配置。

创建启用和禁用成员帐户的部署

1. 使用带有委派管理员凭证的 AWS 账户登录。在 https://console.aws.amazon.com/securityhub/v2/home 中打开 Security Hub 控制台。
2. 从导航窗格中选择 “管理”，然后选择 “配置”。
3. 从配置目录中选择具有部署类型的项目。要完全配置 Security Hub，建议选择 Sec urity Hub（基本功能和附加功能）。
4. 在 “安全功能” 部分中，选择应开启的安全功能。
5. 在账户选择部分，选择以下选项之一。如果要将配置应用于所有组织单位和帐户，请选择 “所有组织单位和帐户”。如果要将配置应用于特定的组织单位和帐户，请选择 “特定组织单位和帐户”。如果您选择此选项，请使用搜索栏或组织结构树来指定将应用该策略的组织单元和账户。如果您不想将配置应用于任何组织单位或帐户，请选择无组织单位或帐户。
6. 在 “区域” 部分，选择 “启用所有区域”、“禁用所有区域” 或 “指定区域”。如果您选择启用所有区域，则可以决定是否自动启用新区域。如果您选择禁用所有区域，则可以决定是否自动禁用新区域。如果选择指定区域，则必须选择要启用和禁用的区域。
7. 选择配置。

编辑配置策略

您可以编辑与具有某种策略类型的配置关联的权能、区域和账户。

以下内容介绍如何在 Security Hub 中编辑配置策略

要创建，请编辑配置策略

1. 使用带有委派管理员凭证的 AWS 账户登录。在 https://console.aws.amazon.com/securityhub/v2/home 中打开 Security Hub 控制台。
2. 从导航窗格中选择 “管理”，然后选择 “配置”。
3. 在 “已配置的策略” 选项卡中，选择要编辑的策略的单选按钮。选择 “编辑”。
4. 要在 “账户选择” 部分进行更改，请选择以下选项之一。如果要将配置应用于所有组织单位和帐户，请选择 “所有组织单位和帐户”。如果要将配置应用于特定的组织单位和帐户，请选择 “特定组织单位和帐户”。如果您选择此选项，请使用搜索栏或组织结构树来指定将应用该策略的组织单元和账户。如果您不想将配置应用于任何组织单位或帐户，请选择无组织单位或帐户。
5. 要在 “区域” 部分进行更改，请选择 “启用所有区域”、“禁用所有区域” 或 “指定区域”。如果您选择启用所有区域，则可以决定是否自动启用新区域。如果您选择禁用所有区域，则可以决定是否自动禁用新区域。如果选择指定区域，则必须选择要启用和禁用的区域。

6. 选择下一步。
7. 查看您的更改，然后选择更新。您的目标账户是根据策略进行配置的。

删除配置策略

您可以删除您拥有某种策略的配置。删除政策后，所有关联的账户和组织单位都将从该政策中删除。

下面介绍如何在 Security Hub 中删除配置策略。

要创建，请删除配置策略

1. 使用带有委派管理员凭证的 AWS 账户登录。在 https://console.aws.amazon.com/securityhub/v2/home 中打开 Security Hub 控制台。
2. 从导航窗格中选择 “管理”，然后选择 “配置”。
3. 在 “已配置的策略” 选项卡中，选择要编辑的策略的单选按钮。选择删除按钮。
4. 在确认框中键入删除。选择 “删除”。

在 Security Hub 中移除委派管理员账户

您可以随时在 Security Hub 控制台中移除委派管理员账户。但是，此操作不仅会从 Security Hub 中移除委派管理员，还会从 Security Hub CSPM 中移除委派管理员。我们建议您仅在通过安全账户确认此操作后才执行此操作。

> **Note**
>
> 如果您使用组织管理账户以外的账户作为 Security Hub CSPM 委托管理员，则通过 CSPM 控制台或 AWS Organizations API 将其删除也会将其从 Security Hub 中删除。
> 同样，如果您通过 Security Hub 控制台或 AWS Organizations API 移除 Security Hub 委托的管理员，则该管理员也将从 Security Hub CSPM 中删除。当从 CSPM 中移除委派管理员时，中心配置将自动选择退出。

移除委派管理员账户

1. 使用您的组织管理 AWS 账户凭据登录您的账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 在导航窗格中，选择常规。

3. 在委派管理员中，选择移除委派管理员。在弹出窗口中，输入移除，然后选择移除。

重新启用 Security Hub

在对以前使用 Security Hub 策略禁用的账户重新启用 Security Hub 之前，必须先取消禁用策略。如果您在账户或组织单位仍有禁用策略的情况下尝试重新启用 Security Hub，则禁用策略将覆盖启用，而 Security Hub 将保持禁用状态。

要移除 Security Hub，请禁用组织或账户的策略。

1. 使用您的 AWS 账户和组织管理账户凭据登录。在 https://console.aws.amazon.com/organizations/v2/ home 中打开 Security Hub 控制台。
2. 从导航面板中选择AWS 账户。
3. 如果当前的 Security Hub 禁用策略适用于您的整个组织，请在 “组织结构” 下选择 “根”。如果当前的 Security Hub 禁用策略适用于特定账户，请在组织结构下选择特定账户，然后按照每个账户的剩余步骤进行操作。
4. 在 “策略” 选项卡中，找到标题为 “Sec urity Hub 策略” 的部分
5. 选择禁用 Security Hub 的策略旁边的单选按钮。选择 “分离”。

从您的组织或账户中附加策略后，您可以重新启用 Security Hub。有关重新启用 S ecurity Hub 的详细信息，请参阅管理 AWS 组织中成员帐户的配置。

Security Hub 建议

中的以下安全服务以 OCSF 格式 AWS 将发现结果发送到 Security Hub。启用 Security Hub 后，我们建议启用这些功能 AWS 服务 以提高安全性。

Security Hub CSPM

启用 Security Hub CSPM 后，您将在 AWS中全面了解安全状态。这有助于您根据安全行业标准和最佳实践评测您的环境。虽然您可以不启用 Security Hub CSPM 即可开始使用 Security Hub，但我们建议启用 Security Hub CSPM，因为 Security Hub 会关联来自 Security Hub CSPM 的安全信号，以改善您的态势管理。

如果您启用 Security Hub CSPM，我们还建议您的账户启用 AWS 基础安全最佳实践标准。该标准由一组控件组成，用于检测您的 AWS 账户 和资源何时偏离安全最佳实践。当您为账户启用 AWS 基础安全最佳实践标准时，Sec AWS urity Hub CSPM 会自动启用其所有控件，包括对以下资源类型的控制：

- 账户控件
- Amazon DynamoDB 控件
- Amazon Elastic Compute Cloud 控件
- AWS Identity and Access Management (IAM) 控件
- AWS Lambda 控件
- Amazon Relational Database Service（Amazon RDS）控件
- Amazon Simple Storage Service 控制

您可以禁用此列表中的任意控件。但是，如果您禁用这些控件中的任何一个，则无法收到受支持资源的暴露调查发现。有关适用于基础安全最佳实践标准的控件的信息，请参阅 AWS AWS 基础安全最佳实践 v1.0.0 (FSBP) 标准。

GuardDuty

启用后 GuardDuty，您可以在 Security Hub 控制台的控制面板中查看所有威胁和安全覆盖结果。如果启用 GuardDuty，则 GuardDuty 会自动开始以 OCSF 格式向 Security Hub 发送数据。

Amazon Inspector

启用 Amazon Inspector 后，您可以在 Security Hub 控制台的控制面板中查看所有暴露和安全覆盖范围调查发现。如果启用 Amazon Inspector，Amazon Inspector 将自动开始以 OCSF 格式向 Security Hub 发送数据。

我们建议激活 Amazon EC2 扫描和 Lambda 标准扫描。激活 Amazon EC2 扫描后，Amazon Inspector 会扫描您账户中的 Amazon EC2 实例，查找是否存在程序包漏洞和网络可访问性问题。激活 Lambda 标准扫描后，Amazon Inspector 会扫描 Lambda 函数，查找程序包依赖项中是否存在软件漏洞。有关更多信息，请参阅《Amazon Inspector 用户指南》中的激活扫描类型。

Macie

启用 Macie 后，您可以检测 Amazon S3 存储桶的其他暴露。建议配置自动敏感数据发现，以便 Macie 可以每天评估您的 Amazon S3 存储桶清单。

Security Hub 中的账户覆盖范围

Security Hub 允许您通过策略和配置跨区域和组织账户启用多种功能。其中一些功能来自 Security Hub 以外的服务，包括亚马逊 Inspector、Amazon、Sec AWS ur GuardDuty ity Hub CSPM 和 Amazon Macie。您可以使用账户覆盖范围页面来跟踪这些功能涵盖了哪些账户和区域。

账户覆盖范围页面

账户覆盖范围页面可让您了解整个 AWS 账户的安全功能启用情况。此视图可帮助您识别安全覆盖范围中的差距，并跟踪整个组织的能力采用情况。

访问 Security Hub 账户覆盖范围页面

1. 在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 在导航窗格的 “设置” 下，选择 “账户覆盖范围”。

“概述”部分

概述部分显示所有受监控账户的汇总安全覆盖率指标。此高级可视化功能显示启用了每种安全功能的账户所占的百分比，可供您全面了解安全状况。您可以选择覆盖能力的每个百分比来筛选覆盖范围查找结果，以显示与该权能的覆盖范围相关的结果。

概述部分中的百分比是使用以下计算方法确定的：

```
(Count of number of accounts and regions the capability is enabled
in)/((Total number of accounts Security Hub is enabled in)*(Number of
regions the capability is available in))
```

“帐户” 选项卡

“账户” 选项卡通过按账户功能进行筛选，支持账户特定的覆盖范围分析。每项安全功能都显示一个覆盖百分比，选择该百分比后，将显示各个功能的详细细分及其在该功能中的覆盖百分比。当您选择这些百分比时，系统会筛选覆盖范围查找结果，以显示那些表示该权能和该行帐户的覆盖范围的结果。

“帐户” 选项卡中的百分比使用以下计算方法确定：

```
(Count of number of regions the capability is enabled in)/(Number of
regions the capability is available in)
```

在某些情况下，覆盖率可能显示为 0%：

- 账户中未启用 Security Hub，因此未采集任何覆盖结果。
- Security Hub 正在等待生成覆盖调查结果。

覆盖范围调查结果选项卡

覆盖范围调查结果选项卡显示安全功能检查检测到账户中已禁用的功能时生成的信息性调查结果。这些发现有助于确定可以增强安全覆盖范围的领域。每项保险调查结果都提供有关保险调查结果的标题、调查结果的叙述和区域以及调查结果的当前状态的信息。每个发现还具有一个配置链接，可将您带到可以管理该功能配置的单个服务，或者指向 Security Hub 配置页面，您可以在其中更新安全服务的当前配置。

有关覆盖结果的更多信息，请参阅 Sec urity Hub 中的覆盖率调查结果。

安全覆盖范围小组件

也可以通过 Security Hub 摘要控制面板中的安全覆盖范围控件查看账户覆盖范围。有关该控件的更多详细信息，请参阅安全覆盖范围小组件文档。

Security Hub 扩展计划

Security Hub 扩展计划通过以 Security Hub 为中心的集成安全运营体验，帮助保护您的整个企业资产，包括云、端点、网络、身份、数据、电子邮件和浏览器。 AWS 借助 Security Hub Extended 计划，您可以选择满足您的安全需求的合作伙伴解决方案，并注册灵活 pay-as-you-go定价，无需前期投资或长期承诺。您可以随着业务需求的变化添加或删除合作伙伴解决方案。

Security Hub 扩展计划适用于所有启用 Security Hub Essentials 计划的客户。Security Hub 扩展套餐的费用会显示在您的月度 AWS 账单上 AWS ，并且是登记在案的卖家。

所有解决方案的 Security Hub 扩展套餐定价可在 Sec urity Hub 定价详情页面的扩展计划选项卡上找到。

Security Hub 扩展套餐的权限

要订阅 Security Hub 扩展套餐中的合作伙伴产品，除了 Security Hub 权限外，还需要以下权限：

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

要取消订阅 Security Hub 扩展套餐中的合作伙伴产品，除了 Security Hub 权限外，还需要以下权限：

- `license-manager:ListReceivedLicenses`

- `aws-marketplace:ListAgreementCharges`
- `aws-marketplace:Unsubscribe`

有关 AWS Marketplace 权限的更多信息，请参阅 Marketplace 买家指南中的控制对AWS 商 AWS 城订阅的访问权限。

查看并注册扩展计划合作伙伴

Security Hub 扩展计划可通过 Security Hub 委托管理员账户或独立账户进行访问。在 Security Hub Extended 套餐页面上，您可以查看每个合作伙伴的详细信息，启动合作伙伴解决方案的订阅，以及通过合作伙伴的入职页面开始每个合作伙伴解决方案的入门流程。

访问 Security Hub 扩展计划并注册合作伙伴的产品

1. 使用您的委托管理员或独立账户凭证登录 AWS 管理控制台。
2. 在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
3. 在导航窗格中，选择管理，然后选择扩展套餐。
4. 对于您要注册的每个合作伙伴解决方案，请选择查看产品。
5. 查看产品定价详情，然后在准备好开始合作伙伴产品的入门流程时选择 “订阅”。
6. 订阅过程完成后，选择将您的账户设置为重定向到合作伙伴的注册页面。
7. 为合作伙伴注册页面提供必要的信息，然后按照合作伙伴提供的后续步骤完成入职步骤。

> **Important**
>
> 在您完成合作伙伴产品的入门流程之前，您无需为合作伙伴解决方案付费。

取消订阅扩展计划合作伙伴

如果您不想再使用扩展计划合作伙伴解决方案，可以取消订阅合作伙伴列表。

要取消订阅合作伙伴解决方案，请按照 Marketpl AWS ace 买家指南中的 “取消 SaaS 订阅” 中的指导进行操作。

> **Important**
>
> 除了取消订阅外，还要根据您为公司配置解决方案的方式，按照合作伙伴解决方案所需的任何其他离职步骤进行操作。

了解 Security Hub 中的跨区域聚合

跨区域聚合允许您将来自多个 AWS 区域的发现、资源和趋势汇总到一个主区域。然后，您可以从本地区域管理所有这些数据。

假设您将美国东部（弗吉尼亚州北部）设置为主区域，将美国西部（俄勒冈州）和美国西部（北加利福尼亚）设置为关联区域。在美国东部（弗吉尼亚州北部）查看调查发现页面时，您会看到所有三个地区的调查发现。这些调查发现的最新情况也反映在所有三个区域。

聚合的数据类型

在一个或多个关联区域中启用跨区域聚合后，Security Hub 会将以下数据从关联区域复制到主区域。每个启用了跨区域聚合的账户都会发生这种情况。

- 结果
- 资源
- Trends

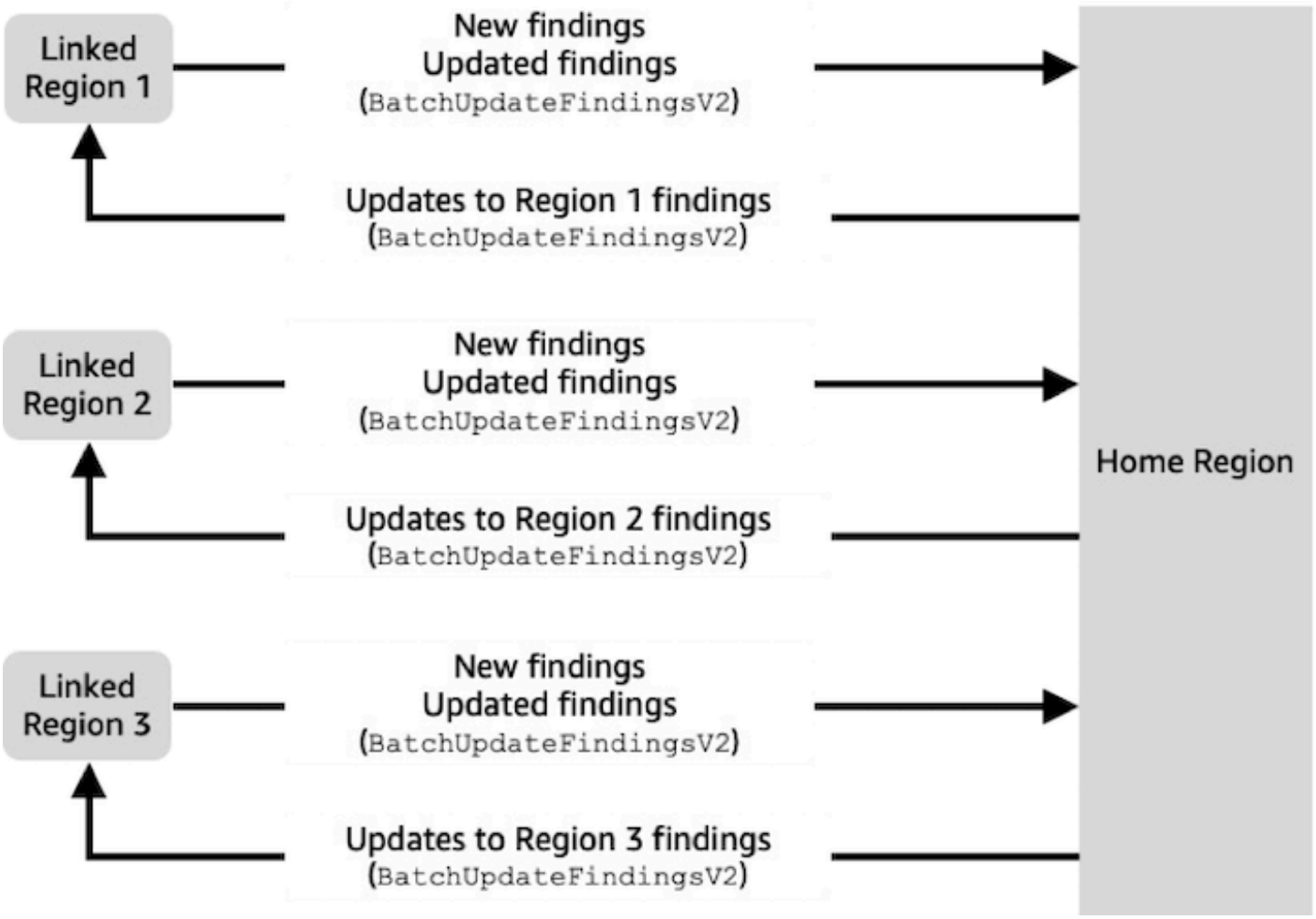
除了先前列表中的新数据之外，Security Hub 还会在关联区域和主区域之间复制对这些数据的更新。关联区域中进行的更新会被复制到主区域。主区域中进行的更新会被复制回关联区域。如果主区域和关联区域中的更新相互冲突，则使用最新的更新。

除非对发现结果进行更新，否则在某个区域成为关联区域时存在的任何发现都不会复制到原区域。将某个区域与主区域关联后，在关联区域中的发现结果更新或过时之前，主区域和关联区域之间的发现就会有所不同。

在某个区域成为关联区域时存在的任何资源都将复制到原区域，通常是在该区域与主区域关联后的 24-48 小时内。

移除关联区域时，该区域的所有发现或资源都将保留在本区域中，直到发现或资源失效。

趋势数据基于趋势所针对的区域内存在的发现和资源。主区域的趋势数据将反映已同步到原区域的发现和资源的当前状态。



跨区域聚合不会增加 Security Hub 的费用。Security Hub 复制新数据或更新时，您无需付费。

在主区域中，摘要页面提供了您在关联区域中的活跃发现和资源的视图。

Security Hub 仅汇总来自账户启用了 Security Hub 的地区数据。根据跨区域聚合配置，不会自动为账户启用 Security Hub。

可以在不选择任何关联区域的情况下启用跨区域聚合。在这种情况下，不会进行数据复制。

聚合管理员账户和成员账户

独立账户和管理员账户可以配置跨区域聚合。如果由管理员配置，则管理员账户的存在对于跨区域聚合在托管账户中发挥作用至关重要。如果管理员账户被移除或取消与成员账户的关联，则成员账户的跨区域聚合将停止，或者如果成员账户在与管理员关联之前具有跨区域聚合配置，则该聚合配置将再次对该账户生效。

管理员账户启用跨区域聚合后，Security Hub 会将管理员账户在所有关联区域中生成的数据复制到主区域。此外，Security Hub 会识别与该管理员关联的成员账户，并且每个成员账户都会继承管理员的跨区域聚合设置。Security Hub 会将成员账户在所有关联区域生成的数据复制到主区域。

管理员可以访问和管理托管区域内所有成员账户的安全调查发现。此外，管理员可以查看管理区域内所有成员账户的资源清单。

作为 Security Hub 成员账户，您必须登录到主区域才能查看您的账户和所有关联区域的聚合数据。成员账户无权查看来自其他成员账户的数据，也无权调用`CreateAggregatorV2`、`DeleteAggregatorV2`和`GetAggregatorV2` APIs。

自动化规则和跨区域聚合

启用跨区域聚合后，只能在定义的主区域创建自动化规则。除非您的规则标准适用于特定区域，否则您定义的任何规则都适用于所有关联区域。您必须为任何非关联区域的区域创建单独的自动化规则。

在启用跨区域聚合之前，在本地区创建的任何规则都将自动适用于关联区域。创建聚合器后，先前在关联区域中创建的规则将不再适用。删除聚合器或不再关联该区域后，在关联区域中定义的规则将恢复应用。

启用跨区域聚合

您必须从要指定为主 AWS 区域的区域启用跨区域聚合。

要启用跨区域聚合，您需要创建一项名为调查发现聚合器的 Security Hub 资源。调查发现聚合器资源指定主区域和关联区域（如果有）。

您不能使用默认禁用的 AWS 区域作为您的主区域。有关默认禁用的区域列表，请参阅《AWS 通用参考》中的 “启用区域”。

启用跨区域聚合时，如果需要，您可以选择指定一个或多个关联区域。启用跨区域聚合不会在该区域启用 Security Hub。要在某个区域启用 Security Hub，请参阅 Security Hub 用户指南中的以委托管理员身份创建策略来管理成员账户。

启用跨区域聚合（控制台）

1. 使用管理员帐户或独立账户在 https://console.aws.amazon.com/securityhub/v 2/home 上打开 Sec AWS urity Hub 控制台
2. 使用 AWS 区域选择器登录要用作聚合区域的区域。
3. 在 Security Hub 导航菜单中，选择设置，然后选择常规。

4. 在 “跨区域聚合” 部分中，选择 “配置”。
5. 默认情况下，主区域设置为无聚合区域。
6. 在 “主区域” 下，选择将当前区域指定为主区域的选项。
7. （可选）对于关联区域，选择要从中聚合数据的区域。
8. 选择保存。

查看跨区域聚合设置

您可以在 Sec AWS urity Hub 中使用管理员账户或独立账户从任何 AWS 区域查看当前的跨区域聚合配置。成员账户无法查看跨区域聚合配置。配置包括主区域和关联区域（如果有）。

按照步骤查看您当前的跨区域聚合设置

查看跨区域聚合设置（控制台）

1. 在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Sec AWS urity Hub 控制台。
2. 在导航窗格上，选择设置，然后选择常规。
3. 如果未启用跨区域聚合，则 “常规” 页面将显示启用跨区域聚合的选项。只有管理员账户和独立账户才能启用跨区域聚合。
4. 如果启用了跨区域聚合，则区域选项卡将显示以下信息：
   - 主区域
   - 是否自动汇总 Security Hub 支持且您选择加入的新区域的发现、资源和趋势
   - 关联区域列表（如果选择了任何区域）

更新跨区域聚合设置

您可以通过更改关联的区域或当前的主区域来更新 S AWS ecurity Hub 中当前的跨区域聚合设置。

只有在账户中启用可选区域后，才会对跨区域聚合进行更改。 AWS 在 2019 年 3 月 20 日当天或之后 AWS 推出的区域为可选区域。

当您停止聚合来自关联区域的数据时，Sec AWS urity Hub 不会从该区域中移除可在原区域访问的任何现有聚合数据。

您不能使用本节中的更新过程来更改主区域。要更改主区域，您必须执行以下操作：

1. 删除当前的跨区域聚合配置。有关说明，请参阅the section called “删除聚合”。
2. 更改为要作为新的主区域的区域。
3. 启用跨区域聚合。有关说明，请参阅the section called “删除聚合”。

您必须从当前主区域更新跨区域聚合配置。

更改关联区域（控制台）

1. 使用管理员帐户或独立帐户在 https://console.aws.amazon.com/securityhub/v2/ home 上打开 Sec AWS urity Hub 控制台。
2. 登录到当前聚合区域。
3. 在 Security Hub 导航菜单中，选择设置，然后选择常规。
4. 对于跨区域聚合，请选择编辑。
5. 对于关联区域，更新所选的关联区域。
6. 选择保存。

删除跨区域聚合

如果您不希望 S AWS ecurity Hub 聚合数据，则可以删除您的查找聚合器。或者，您可以将现有聚合器更新为不选择任何关联 AWS 区域，从而保留您的查找聚合器，但不将任何区域链接到主区域。

要更改主区域，您必须删除当前的调查发现聚合器并创建新的聚合器。

删除调查发现聚合器后，Security Hub 会停止聚合数据。它不会从主区域中移除任何现有的聚合数据。

删除调查发现聚合器（控制台）

您只能从当前的主区域中删除调查发现聚合器。

在主区域以外的区域中，Security Hub 控制台上的调查发现聚合面板会显示一条消息，提示您必须在主区域中编辑配置。选择此消息可显示切换到主区域的链接。

停止跨区域聚合（控制台）

1. 在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Sec AWS urity Hub 控制台。
2. 确保您已登录到当前主区域。
3. 在 Security Hub 导航菜单中，选择设置，然后选择常规。

4. 在 “跨区域聚合” 下，选择 “编辑”。
5. 在聚合区域下，选择无聚合区域。
6. 选择保存。
7. 在确认对话框的确认字段中，键入 **Confirm**。
8. 选择确认。

在 Security Hub 的摘要仪表板中工作

Security Hub 控制台中的 “摘要” 仪表板显示您在各个安全小组件中的风险敞口、威胁、资源和安全覆盖范围的概述。您可以通过添加和删除小组件以及创建和应用筛选器集来检索每个小组件中的数据来自定义仪表板。

注意事项

在与仪表板交互之前，请考虑以下几点：

- 诸如保存的过滤器集合或对小组件布局的更改之类的自定义项会自动保存。
- 每次打开仪表板时，数据都会自动刷新。
- 如果您配置跨区域聚合，则控制面板将包含所有关联区域的调查结果（在您所在区域查看仪表板时）。

如果您的账户是组织的委托管理员账户、组织中的成员账户或独立账户，请考虑以下几点。

- 委托管理员账户所做的自定义将独立于成员账户的自定义进行保存。自定义项可能包括已保存的过滤器集或对小组件布局的更改。
- 如果您的账户是某组织的委派管理员账户，则数据包括您的账户和成员账户的调查发现。
- 如果您的账户是组织中的成员账户或独立账户，则数据仅包含您账户的调查结果。

作为最佳实践，我们建议不要在已保存的筛选器集、自定义小组件或其他相关的自由格式文本字段中包含机密、敏感或个人身份信息 (PII)。

可用小组件

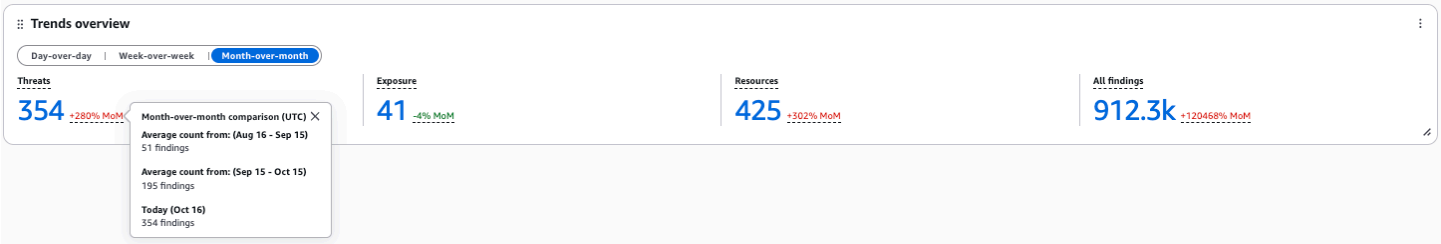
您可以在 “摘要” 仪表板的 “管理” 和 “会审” 选项卡中与不同的小组件进行交互。“Execut iv e” 选项卡包括显示您的风险敞口、威胁和资源的趋势数据的小组件，以及 “安全覆盖范围” 小部件，可帮助您在不

同的安全功能中跟踪您的账户覆盖范围。“分类” 选项卡包含显示您的风险、威胁和资源摘要的小部件。但是，您可以添加小部件、移除小组件以及管理每个小组件在两个选项卡中的位置，以自定义您的体验。

趋势小工具

以下小组件显示您的风险敞口、威胁和资源的趋势数据，因此您可以随着时间的推移对其进行分析。

趋势概述小工具



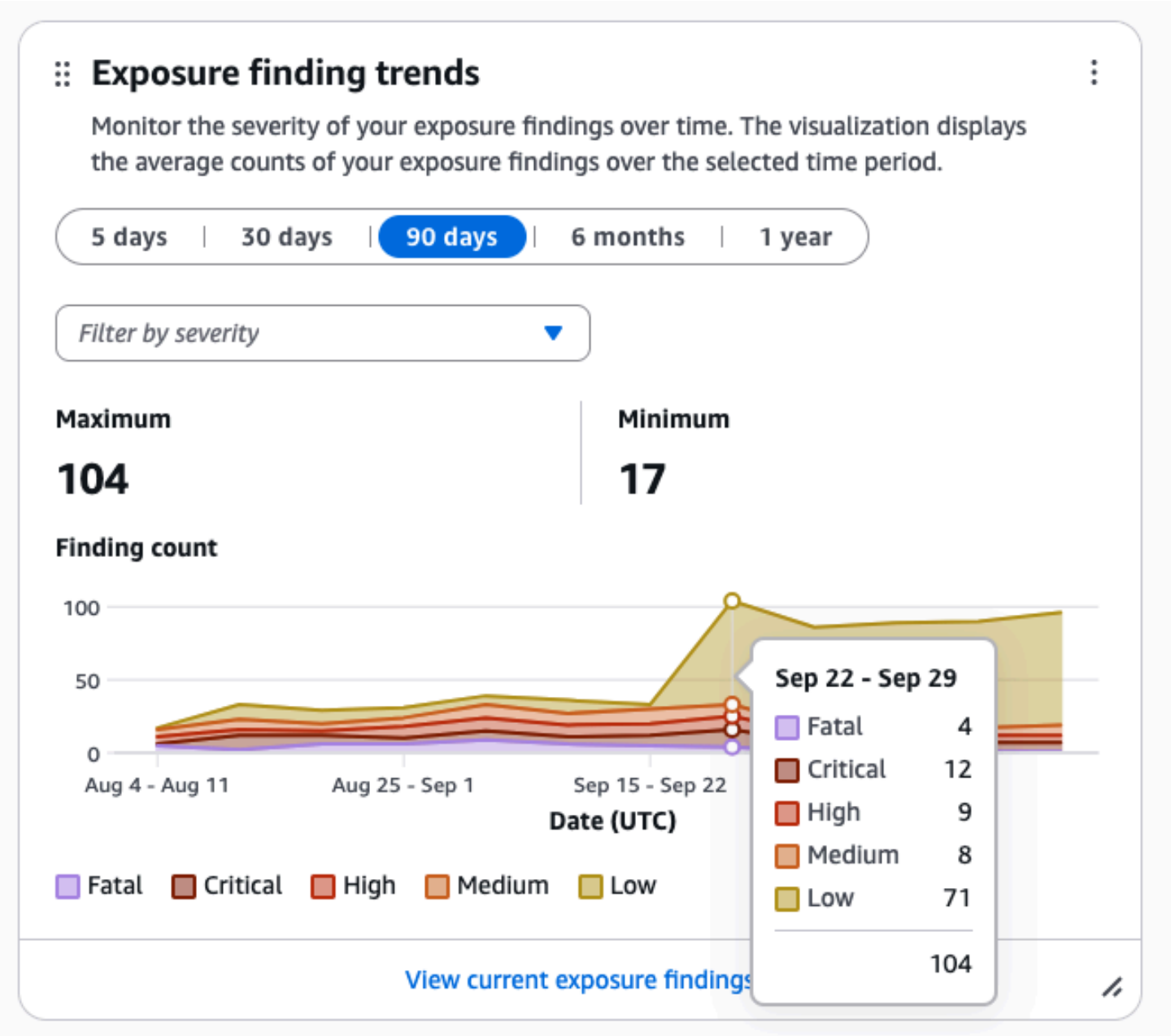
此小组件显示您在以下时间段内的暴露情况、威胁、资源和发现的概述：

- M onth-over-month 反映了最近两个月的 period-over-period计数。
- W eek-over-week 反映了过去两周的 period-over-period计数。
- D ay-over-day 反映了过去 2 天的 period-over-period计数。

百分比旁边的数字反映了迄今为止的平均 period-over-period数。选择此数字会将您定向到控制台中相应的仪表板。如果您导航到另一个显示趋势数据的仪表板，则该控制面板仅显示最近 90 天的趋势数据，或者如果您的账户不包含超过 30 天的调查结果或资源，则该控制面板仅显示最合适的时间段内的趋势数据。

> **Note**
>
> 要在此小组件中接收数据，必须启用以下安全服务：
>
> - AWS S@@ ecurity Hub CSPM — 接收有关暴露的数据
> - Amazon Inspector — 接收有关曝光的数据
> - GuardDuty— 接收有关威胁的数据

曝光度发现趋势小工具



此控件显示您在以下时间段内发现的暴露严重程度：

- 5 天
- 30 天
- 90 天
- 6 个月
- 1 年

可视化显示选定时间段内的平均发现次数。

严重性过滤器

您可以通过包括或排除以下严重性筛选器来更新图表：

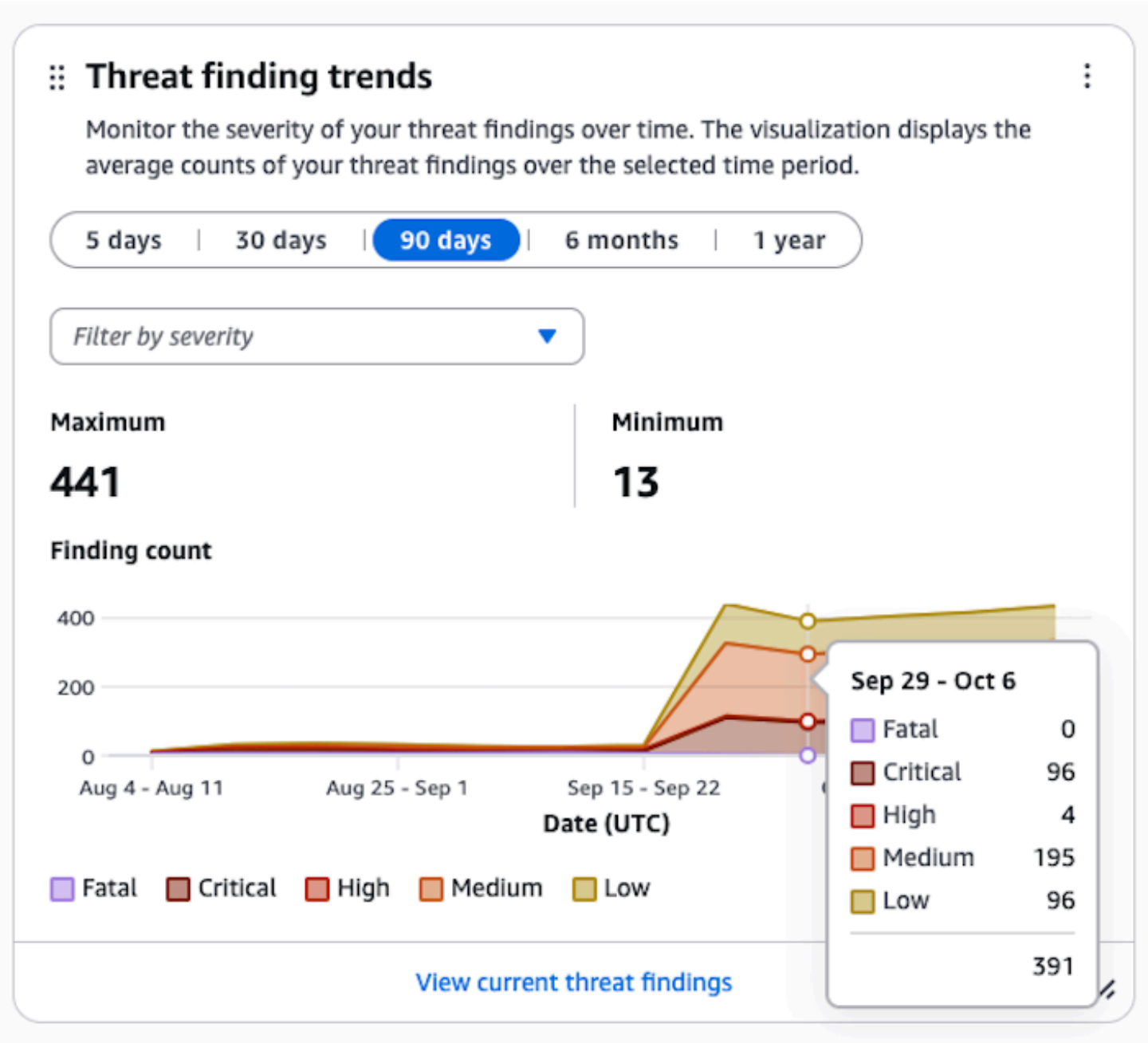
- 致命
- 重大
- 高
- 中等
- 低
- 信息性的
- 其他
- 未知

应用的严重性筛选器显示在可视化底部的不同框中。您可以将鼠标悬停在可视化图上，查看特定时间点的平均发现次数。您还可以查看与每个应用的严重性筛选条件相匹配的发现结果的平均数。

您可以选择 “查看所有当前曝光结果”，将其定向到 “曝光” 控制面板。默认情况下，曝光度控制面板仅显示过去 90 天的趋势数据。如果您的账户中不包含超过 30 天的曝光调查结果，则控制面板会根据最合适的时间段显示趋势数据。

> **Note**
>
> 要在此小组件中接收数据，您必须启用 Amazon Inspector 和 Sec urity Hub CSPM。

威胁发现趋势小工具



此小组件显示您在以下时间段内发现的威胁的严重性：

- 5 天
- 30 天
- 90 天
- 6 个月
- 1 年

可视化显示选定时间段内的平均发现次数。

严重性过滤器

您可以通过包括或排除以下严重性筛选器来更新图表：

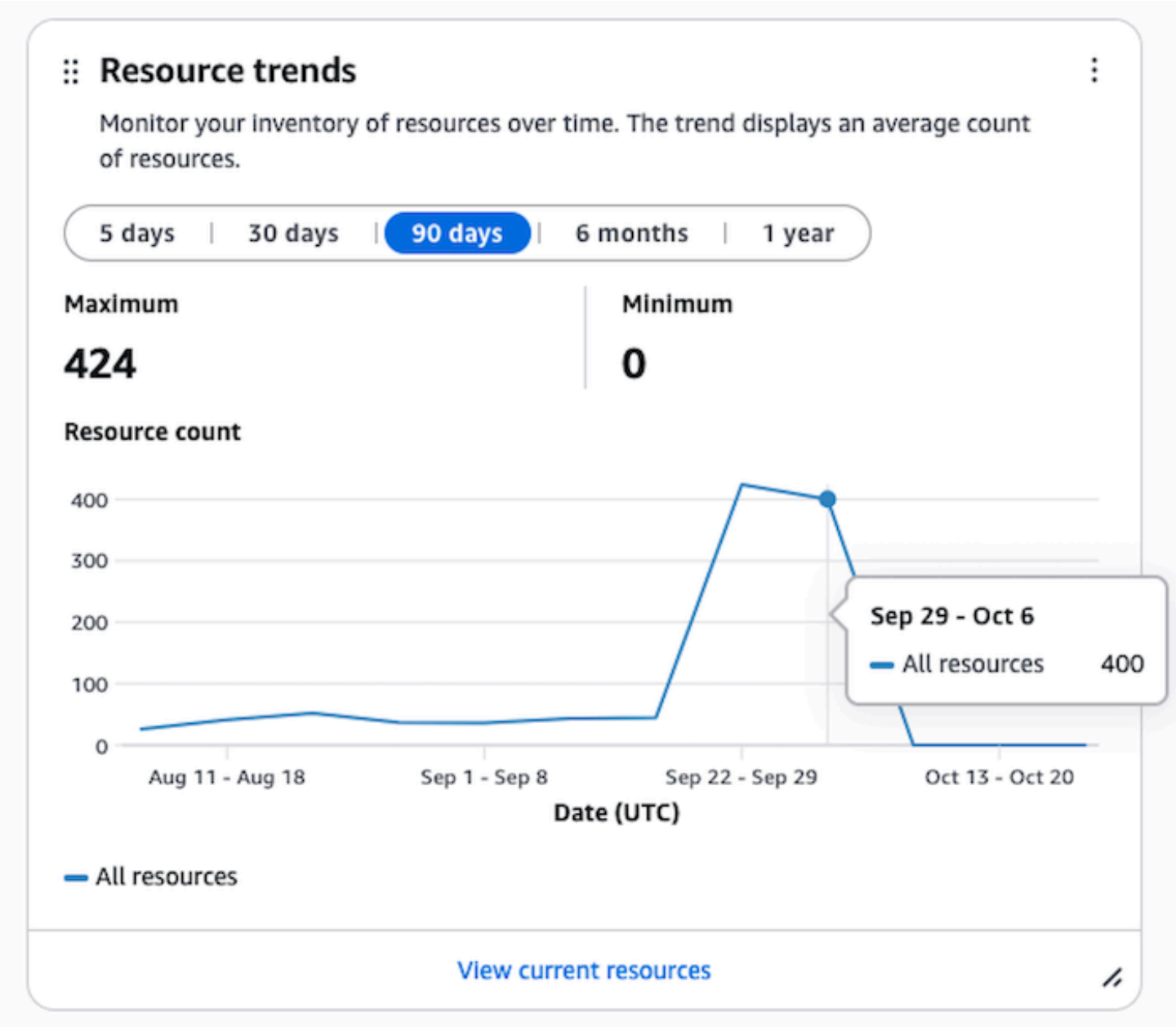
- 致命
- 重大
- 高
- 中等
- 低
- 信息性的
- 其他
- 未知

应用的严重性筛选器显示在可视化底部的不同框中。您可以将鼠标悬停在可视化图上，查看特定时间点的平均发现次数。您还可以查看与每个应用的严重性筛选条件相匹配的发现结果的平均数。

您可以选择 “查看所有当前威胁发现”，将其定向到 “曝光” 控制面板。默认情况下，“威胁” 控制面板仅显示过去 90 天的趋势数据。如果您的账户中未包含超过 30 天的威胁发现，则控制面板会根据最合适的时间段显示趋势数据。

> **Note**
>
> 要在此小组件中接收数据，必须启用GuardDuty。

资源趋势控件



此小组件显示您在以下时间段内的资源清单：

- 5 天
- 30 天
- 90 天
- 6 个月
- 1 年

可视化显示选定时间段内的平均资源数量。您可以将鼠标悬停在可视化项上，查看特定时间点的平均资源数量。

您可以选择 “查看当前资源”，将其定向到 “资源” 控制面板。默认情况下，资源控制面板仅显示过去 90 天的趋势数据。如果您的账户中没有超过 30 天的资源，则控制面板会根据最合适的时间段显示趋势数据。

此小组件显示您在以下时间段内的资源清单：

- 5 天
- 30 天
- 90 天
- 6 个月
- 1 年

保留数据以适应趋势

Security Hub 会将所有启用了 Security Hub 的 AWS 账户 位置的趋势数据保留一年。趋势数据保留一年后，将从 Security Hub 中删除。

在禁用 Security Hub 或帐户终止后，委托管理员和独立账户的趋势数据将被删除。

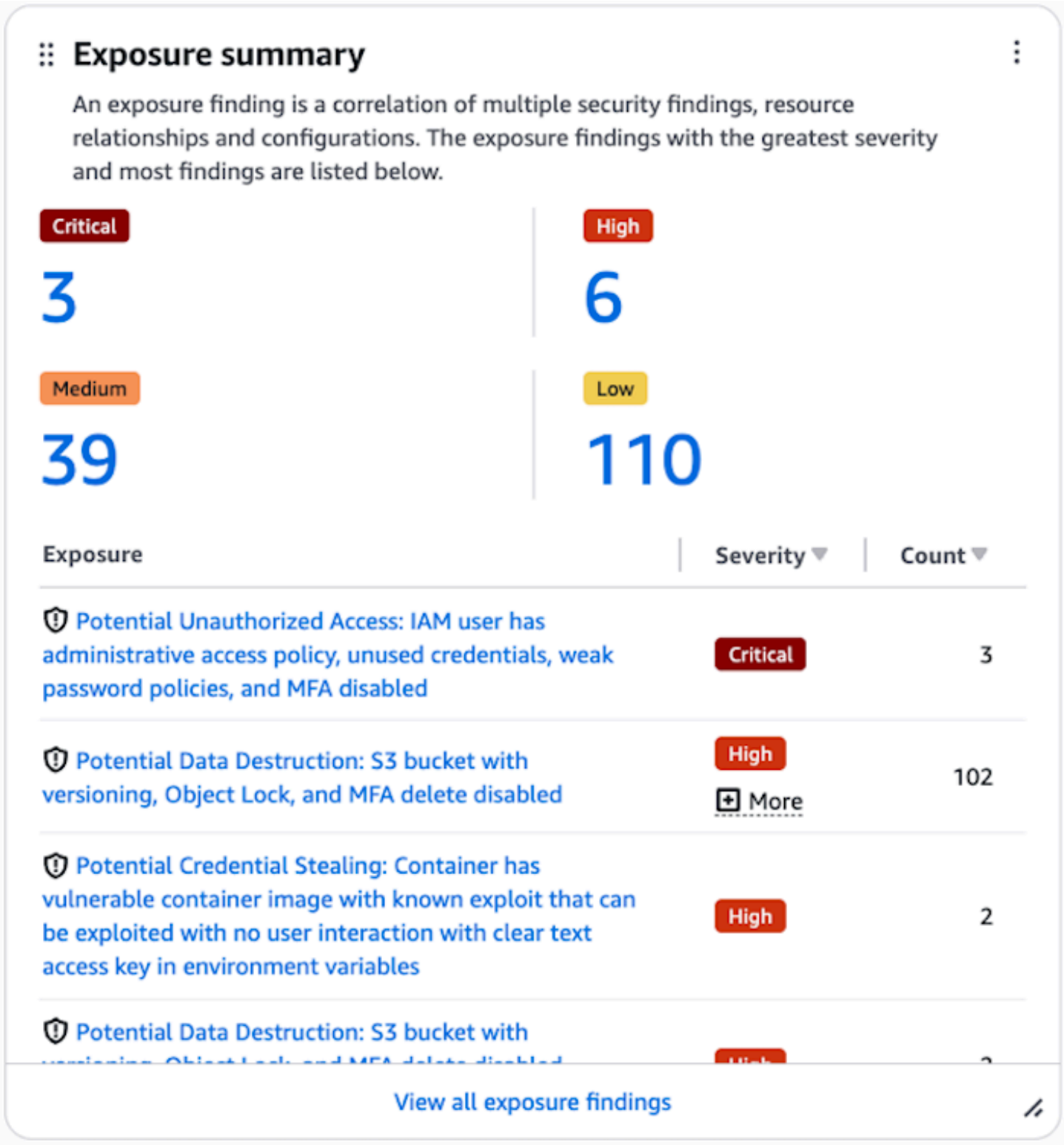
启用了 Security Hub 的成员账户的数据保留趋势方案：

- 如果成员账户离开其组织，Security Hub 仍会将趋势数据存储一年，直至该账户离开组织之时。
- 如果为成员账户禁用 Security Hub，则直到该账户被禁用时的趋势数据将保留一年。
- 如果成员账户被终止，趋势数据将与被终止的账户断开关联（例如，已终止的账户 ID 将被清除），其余的趋势数据将保留一年。

摘要小工具

以下小组件显示您的风险敞口、威胁和资源的摘要。

暴露摘要小组件

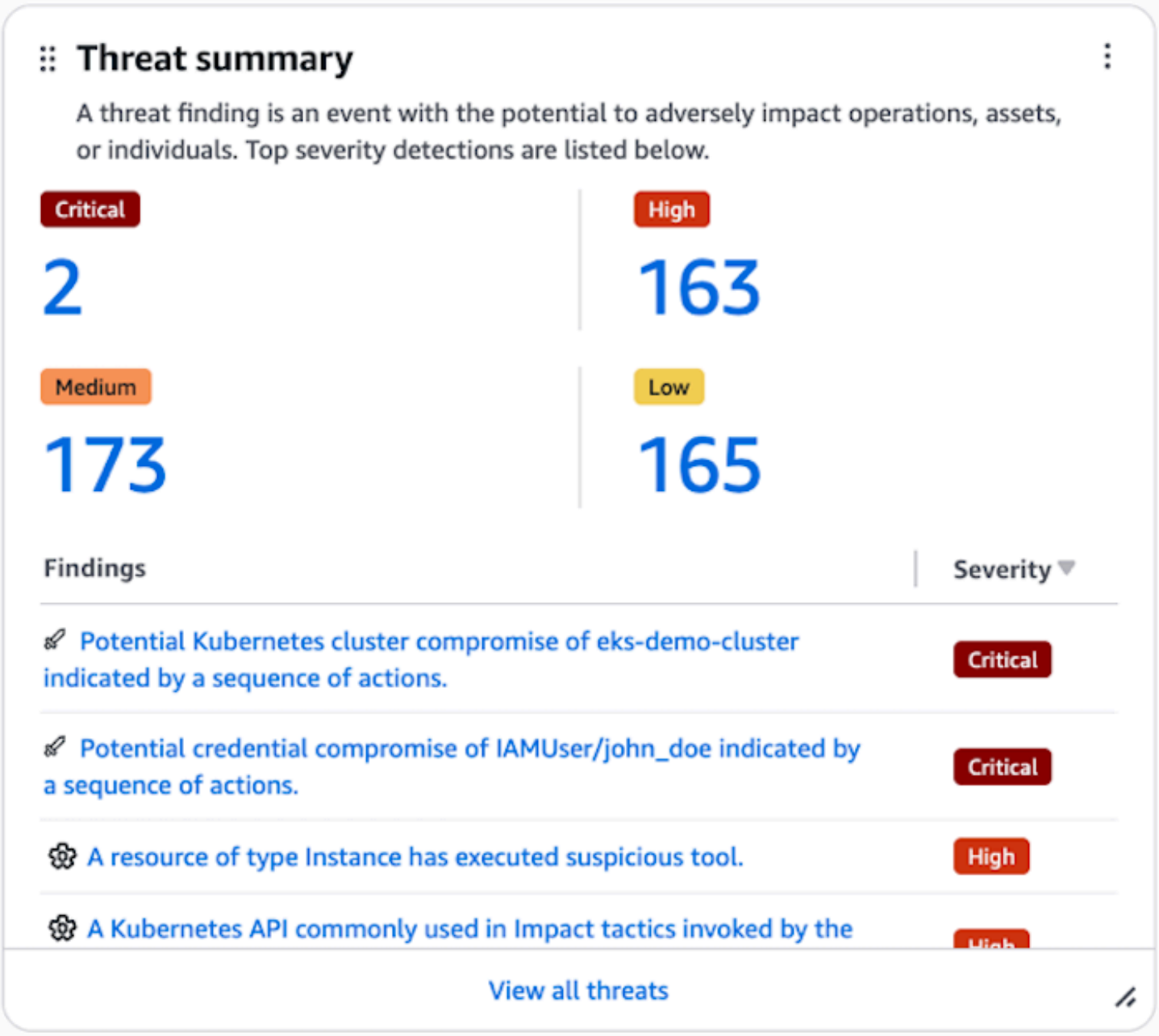


此控件按严重程度显示您的曝光情况。曝光基于对Security Hub和其他 AWS 安全服务（例如Amazon Inspector）的发现和特征的分析。此控件中的曝光列表仅限于严重程度最高的八次曝光。严重程度较

高的曝光出现在列表的首位。如果两次或更多次曝光的严重程度相同，则列表会自动将这些曝光分组到最近的曝光次数之后。选择 “查看所有曝光” 可将您定向到 “曝光” 控制面板。

> **Note**
>
> 要在此小组件中接收数据，您必须启用 Amazon Inspector 和 Sec urity Hub CSPM。

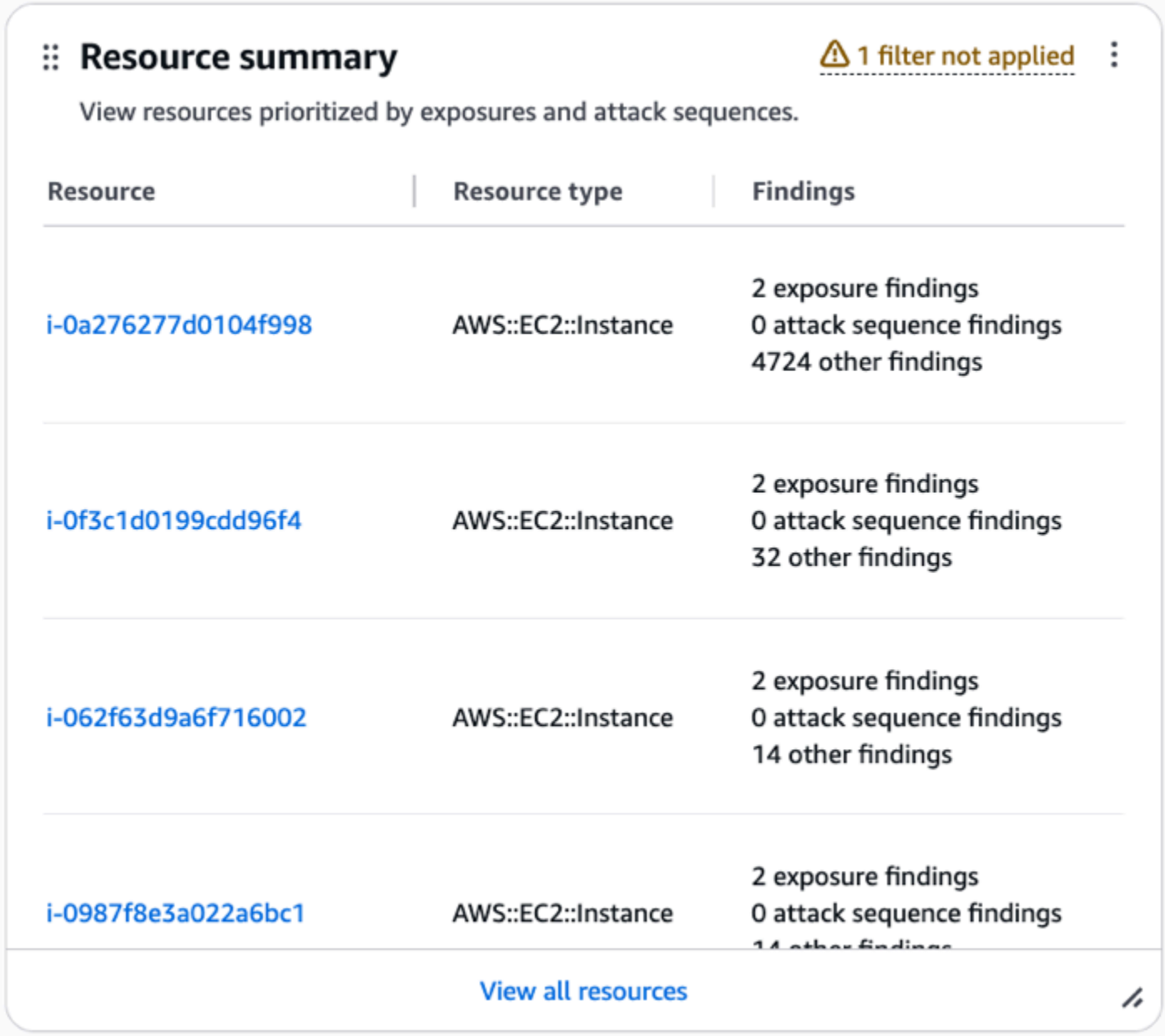
威胁摘要小组件



此小组件按严重程度显示您的威胁。威胁是指可能危及环境安全的恶意活动或可疑活动。此小组件中的威胁列表仅限于严重性最高的八个威胁。严重程度较高的威胁在列表中排在第一位。如果两个或两个以上威胁的严重性相同，则列表会自动将这些威胁归入最近的威胁背后。选择 “查看所有威胁” 会将您定向到 “威胁” 控制面板。

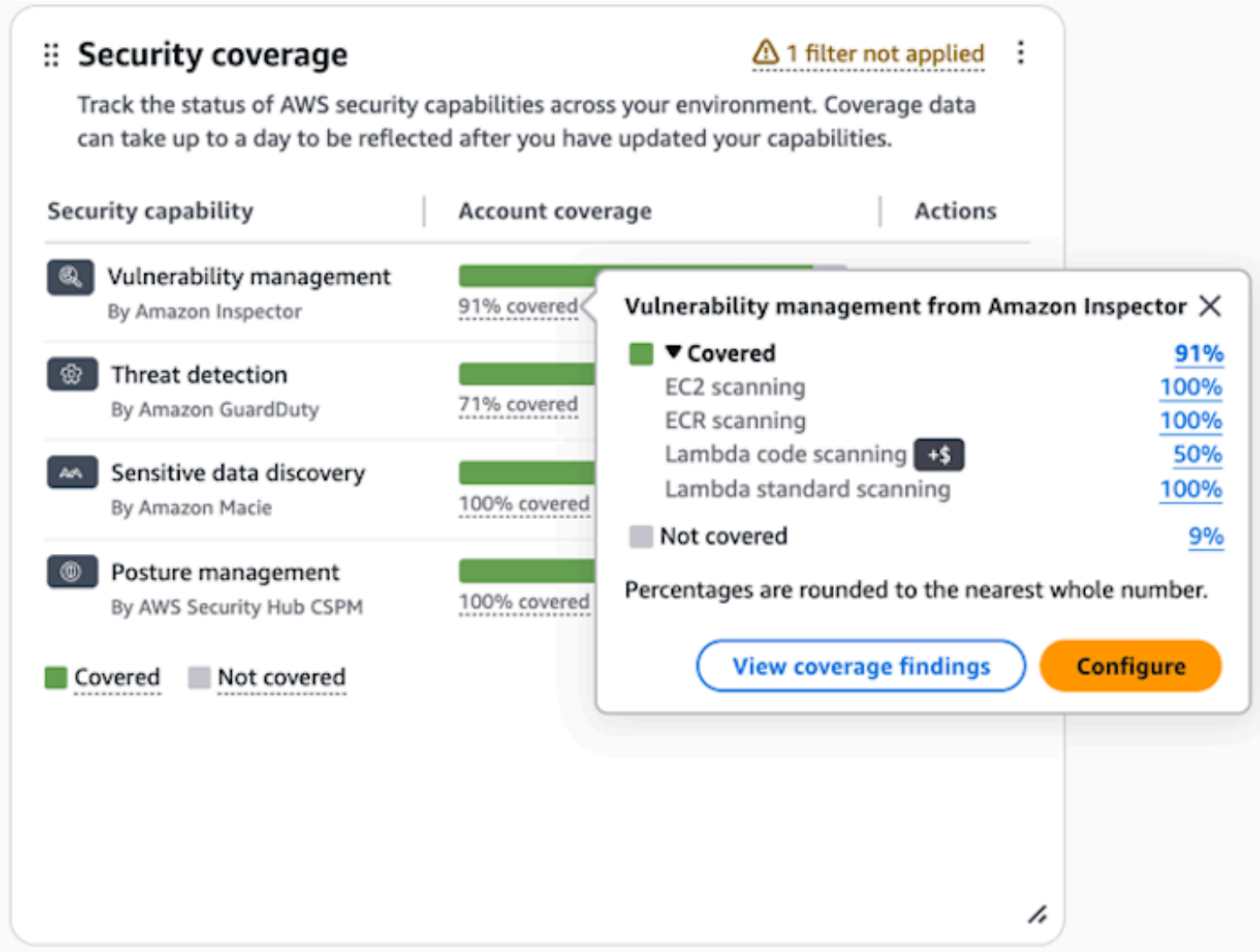
> **Note**
>
> 要在此小组件中接收数据，必须启用 GuardDuty。

资源摘要小组件



此小组件按类型显示资源以及与资源相关的调查结果。资源按照暴露和攻击序列确定优先级。选择 “查看所有资源” 会将您定向到资源控制面板。

安全覆盖范围小组件



该小组件显示您的账户覆盖范围摘要，包括以下安全功能：

- Amazon Inspector 的漏洞管理
- Amazon 的威胁检测 GuardDuty
- 亚马逊 Macie 发现敏感数据
- 由 Sec AWS urity Hub CSPM 进行状态管理

“账户覆盖率” 列中的百分比表示针对每项安全功能以及启用了 Security Hub 的覆盖率检查 AWS 区域 的通过 AWS 账户 和失败的次数。您可以通过选择百分比来查看安全功能的覆盖率检查通过和失

败。已覆盖表示覆盖范围检查已通过。未覆盖表示覆盖范围检查未通过。在查看通过和失败的覆盖范围检查数量的百分比时，“已覆盖” 下的每个百分比代表安全功能覆盖范围调查结果的百分比。在某些情况下，保险检查的百分比会四舍五入到最接近的整数。

隐蔽的报道结果

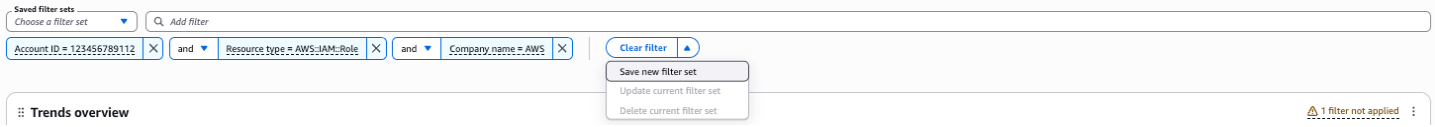
如果您在 Security Hub 中发现的任何覆盖范围被隐藏，则该小组件会显示一条消息，通知您已排除覆盖范围：

通过隐瞒的覆盖范围调查结果，已将安全功能的覆盖范围排除在外。

有关覆盖结果的更多信息，请参阅 Sec urity Hub 中的覆盖率调查结果。

可用过滤器

您可以使用添加筛选器栏将筛选器应用于安全小组件。



过滤器分为以下几类：

- 共享过滤器-适用于所有安全控件
- 查找过滤器-适用于显示查找数据的安全控件
- 资源筛选器-适用于显示资源数据的安全控件

您可以使用和/或运算符连接筛选器，然后在下拉列表中选择 “保存新过滤器集”，从而创建筛选器集。

应用于 “曝光度发现趋势” 小部件和 “威胁发现趋势” 控件的过滤器

目前，这些控件支持的过滤器包括以下内容：

- 账户 ID
- 正在查找类名
- 调查发现类型
- Product name
- 区域

- 状态

应用于 “资源趋势” 微件的筛选器

目前，此控件支持的过滤器包括以下内容：

- 账户 ID
- 区域
- 资源类别
- 资源类型

过滤器未应用于小部件



如果小组件不支持过滤器，则该过滤器不会应用于该小部件。在这种情况下，该小组件会显示一条警告消息，告知您有多少过滤器未被应用，并列出它不支持的过滤器的名称。

在 Security Hub 中查看有关资源的详细信息

资源页面跟踪您的账户和组织中的常用资源。您可以通过在导航窗格中选择资源来访问 Security Hub 控制台中的资源页面。资源页面的好处在于，它可以帮助您监控安全状况、组织资源并查看资源的详细信息。选择资源类型后，您可以查看与该资源类型关联的所有资源。您可以查看与资源关联的任何调查发现。“资源” 页面中可用的资源类型包括 AWS 安全服务所涵盖的账户中向 Security Hub 提供发现结果的所有资源。

> **Note**
>
> 委派管理员可以查看与成员账户关联的所有资源。如果您配置了主页 AWS 区域，则可以通过链接查看家 AWS 区域 中的所有资源 AWS 区域。

如果您选择某个资源，则可以查看该资源的详细信息。这些详细信息包括资源名称、ID、ARN、类型和类别。您可以查看与资源关联的账户 ID、资源的创建时间（时间戳）以及资源的创建位置（AWS 区

域）。您还可以查看有关该资源的其他配置详细信息。这些详细信息可以在您可以复制的 JSON 代码片段中找到。

如果从概览选项卡切换到调查发现选项卡，则可以查看与该资源关联的任何调查发现。调查发现选项卡显示每个调查发现的名称、每个调查发现的类型以及每个调查发现的严重性。您可以按不同字段对调查发现进行分组，并使用筛选条件搜索调查发现。如果您选择了某个调查发现，则可以查看该调查发现的概览，其中包括有关合规性以及如何修复与该调查发现关联的问题的信息。特征选项卡显示已识别的有关资源的每个特征。您可以查看用于为资源创建暴露调查发现的促成性特征。您还可以查看上下文特征，这些是为资源识别出的其他安全项，但不会直接导致任何暴露调查发现。如果返回到资源，则可以选择打开资源来在控制台中查看该资源的资源类型。例如，如果资源是 IAM 资源，则可以在 IAM 控制台中打开该资源。

资源页面为您提供了组织和搜索资源的不同方式。您可以按类型对资源进行分组。例如，您可以按账户 ID、查找类型、资源类别 AWS 区域、资源名称和资源类型对资源进行分组。快速筛选条件可帮助您按类别、账户和调查发现类型查看资源。

Security Hub 和开放网络安全调查结果格式 (OCSF)

OCSF 概述

Security Hub 的发现使用开源项目 OCSF 进行格式化，它提供了一个用于开发架构的可扩展框架以及不受供应商限制的核心安全架构。供应商和其他数据生成工具可以为其特定域采用和扩展架构。数据制作者可以映射不同的架构，以帮助安全团队简化数据摄取和标准化，以便数据科学家和分析师可以使用通用语言进行威胁检测和调查。其目标提供开放标准，可在任何环境、应用程序或解决方案中采用，同时补充现有的安全标准和流程。

该框架由一组数据类型、一个属性字典和分类法组成。它不仅限于网络安全领域也不局限于事件，但是该框架最初的重点是网络安全事件的架构。OCSF 不受存储格式、数据收集和 Extract-Transform-Load (ETL) 流程的约束。网络安全事件的核心架构旨在与实现无关。架构框架定义文件和生成的规范架构以 JSON 格式编写。

Security Hub 目前支持 OCSF 架构版本 1.6 中的发现。

相关资源

有关 OCSF 及其实现的更多信息，请参阅以下资源：

- OCSF 公开文档

- OCSF 扩展程序使用文档
- OCSF 核心架构参考
- OCSF 扩展注册表

AWS OCSF 的延期

可以通过添加新的属性、对象、类别、配置文件和事件类来扩展 OCSF 架构。架构是核心架构实体和扩展的聚合。

OCSF 的扩展允许特定的供应商或客户通过添加属性来增强现有架构，以提供特定于域的自定义，提高数据互操作性，并为安全分析添加更详细的上下文。

开放网络安全架构框架 AWS 扩展 (OCSF) 为 OCSF 事件中的云资源提供了属性定义。此扩展引入了一个新的`cloud_resources`配置文件，该配置文件扩展了标准 OCSF `resource_details` 对象，使其具有全面的云特定资源属性，使安全团队能够更深入地了解资源配置、潜在漏洞和关键元数据，这对于跨云环境进行有效的威胁检测和调查至关重要。

扩展**`resource_details`**对象

AWS 扩展模块使用下面的属性引用列表中提及的属性来扩展`resource_details`对象。这些属性可确保在标准化事件框架内对不同提供商的云资源进行正确识别和分类。

AWS OCSF 属性引用的扩展

基本属性和资源特定对象部分提供了每个属性的示例，这些属性是 resource_details 的 AWS OCSF 扩展的一部分。

每个属性定义都包含一个 OCSF 状态，概述了其与公共 OCSF 架构的当前关系：

- 现有：此属性已经存在于标准 OCSF resource_details 中，现在是扩展的一部分。 AWS
- 新增：该属性不是 OCSF 的一部分，是作为 AWS 扩展的一部分引入的。它不存在于核心 OCSF 架构中。
- 已添加到 resource_detail s：该属性是在 OCSF 中定义的，但不是 resource_details 的一部分。

基本属性

这些是用于资源识别、位置和基本元数据的基本属性。它们由简单的数据类型组成，例如字符串、时间戳和数组。

云分区

资源所在的云分区。

要求

推荐

Type

字符串

OCSF 状态

现有

示例

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

所有者账户 ID

资源所属的 12 位账户标识符。

要求

推荐

Type

字符串

OCSF 状态

现有

示例

```
{
```

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

资源类型

标识特定服务和资源的 AWS CloudFormation 资源类型。

要求

必需

Type

字符串

Format

必须遵循 AWS CloudFormation 资源类型命名惯例：`AWS::<Service>::<ResourceType>`

OCSF 状态

现有

示例

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

资源标识符

云资源的唯一标识符（例如 i-1234567890abcdef0）。

要求

推荐

Type

字符串

Format

必须是有效的资源标识符。最小长度为 1。最大长度为 768。

OCSF 状态

现有

示例

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

备用资源标识符

云资源的唯一标识符，通常是 Amazon 资源名称 (ARN)。

要求

推荐

Type

字符串

Format

应该是有效的 AWS ARN。常见模式包括：

- "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"

注意：某些服务（例如 S3）使用变体，例如 arn: aws: s3::: bucket-name（不含区域或账户 ID）。

OCSF 状态

现有

示例

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

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

资源名称

云资源的唯一名称。

要求

推荐

Type

字符串

Format

用户创建的名称，其值将取决于环境。

OCSF 状态

现有

示例

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

云区域

资源所在的 AWS 区域。

要求

推荐

Type

字符串

Format

有效的云区域标识符（例如 us-east-1、eu-west-1、ap-southeast-2）

OCSF 状态

现有

示例

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

资源创建时间

资源的创建时间。

要求

推荐

Type

Timestamp

Format

自纪元（1970 年 1 月 1 日，世界标准时间 00:00:00）以来的 Unix 时间戳（以毫秒为单位）

OCSF 状态

现有

示例

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

标签

资源元数据和组织的键值对。

要求

推荐

Type

键:值对象数组

Format

允许定义键:值对的通用对象。

OCSF 状态

现有

示例

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

IP 地址

以 IPv4 或 IPv6 格式与实例关联的 IP 地址。

要求

可选

Type

字符串

Format

有效 IPv4 或 IPv6 地址

OCSF 状态

现有

示例

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

```
    }
  ]
}
```

IP 地址

与设备关联的 IP 地址（IPv4 或 IPv6）数组。这些地址可能包括公有和私有 IP 地址。

要求

可选

Type

IP 地址数组

OCSF 状态

New

示例

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

VPC UID

资源所在的 VPC ID。

要求

可选

Type

字符串

Format

VPC 标识符（例如 vpc-12345678900）

OCSF 状态

已添加到 resource_details

示例

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

具有基本属性的资源对象示例

```
{
  "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"
    }
  ]
}
```

资源特定对象

这些是复杂的嵌套对象，可提供特定资源类型和服务的详细信息。每个对象都包含多个字段和子对象，其中包含服务特定的配置和元数据。

设备

增强了计算资源的云实例属性，包括加密详细信息、图像信息、实例配置文件和启动时间。

要求

可选

Type

对象

OCSF 状态

已添加到resource_details。请参阅 OCSF 设备对象定义。

AWS 扩展为该对象添加了以下属性：

- encryption_details-资源的加密详情
- image-图像信息
- instance_profile-要与实例关联的 IAM 实例配置文件
- launch_time-实例启动的时间
- uid_alt-资源的亚马逊资源名称 (ARN)

示例

```
{
  "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"
  }
}
```

网络接口

网络接口详细信息和配置，包括附件和安全组。

要求

可选

Type

对象

OCSF 状态

已添加到`resource_details`。请参阅 OCSF 网络接口对象定义。

AWS 扩展为该对象添加了以下属性：

- `attachments`-有关网络接口附件的信息
- `security_groups`-安全组唯一标识符数组
- `uid_alt`-资源的亚马逊资源名称 (ARN)

示例

```
{
  "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"
      }
    ]
  }
}
```

存储设备

存储设备详细信息，包括附件、加密和快照信息。

要求

可选

Type

对象

OCSF 状态

New

存储设备对象包括以下属性：

- name-存储设备的名称
- uid-存储设备的唯一标识符
- attachments-存储设备附件
- encryption_details-存储设备加密密钥
- is_encrypted-存储设备是否已加密（必填）
- snapshot_id-存储设备快照标识符
- uid_alt-资源的亚马逊资源名称 (ARN)

示例

```
{
  "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"
  }
}
```

数据库

数据库实例属性，包括引擎类型、端点和用户信息。

要求

可选

Type

对象

OCSF 状态

已添加到resource_details。请参阅 OCSF 数据库对象定义。

AWS 扩展为该对象添加了以下属性：

- cluster_uid-数据库集群标识符
- db_endpoint-数据库端点
- encryption_details-数据库加密详情
- engine-数据库引擎名称（例如 mysql）
- is_encrypted-数据库是否已加密
- is_iam_authentication-是否启用 IAM 身份验证
- is_public-数据库是否可公开访问
- port-数据库端口号
- security_groups-与数据库实例关联的 VPC 安全组数组
- snapshot_details-数据库快照详情
- status-数据库状态（例如可用）
- subnet_group-数据库子网组是 VPC 中子网的集合
- uid_alt-资源的亚马逊资源名称 (ARN)
- user-数据库用户
- version-数据库版本

示例

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

数据库集群

数据库实例属性，包括引擎类型、端点和用户信息。

要求

可选

Type

对象

OCSF 状态

New

数据库对象包括以下属性：

- uid-数据库集群的唯一标识符
- uid_alt-资源的亚马逊资源名称 (ARN)
- name-数据库集群的名称
- status-数据库集群状态
- engine-与集群关联的引擎
- version-数据库集群版本
- cluster_members-属于集群的数据库实例列表
- security_groups-与集群关联的安全组数组
- is_encrypted-数据库集群是否已加密
- is_iam_authentication-是否启用 IAM 身份验证
- encryption_details-数据库集群加密详情
- subnet_group-与集群关联的子网组
- port-数据库集群端口号
- zones-可用区列表
- db_endpoint-数据库集群终端节点
- snapshot_details-数据库快照的详细信息

示例

```
{
```

```
  "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
    }
  }
}
```

云端功能

无服务器函数的云函数属性，包括处理程序、层和运行时配置。

要求

可选

Type

对象

OCSF 状态

New

云函数对象包括以下属性：

- name-云函数的名称
- uid-云函数的唯一标识符
- uid_alt-资源的亚马逊资源名称 (ARN)
- encryption_details-云功能加密详情
- handler-函数代码中用于处理事件的方法
- layers-包含补充代码或数据的云函数层列表
- runtime-云功能语言特定的环境
- security_groups-与云功能关联的一系列安全组
- subnet_info_list-有关与云功能关联的子网的详细信息
- user-有关授予 cloud_function 访问服务的权限的 IAM 实体的详细信息
- version-云功能版本
- vpc_uid-如果云函数位于 VPC 中，则为 VPC 的唯一标识符

示例

```
{
  "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"
  }
}
```

数据桶

S3 存储桶或数据存储属性。

要求

可选

Type

对象

OCSF 状态

已添加到`resource_details`。请参阅 OCSF Databucket 对象定义。

注意：此对象由扩展程序添加到 resource_details 中。 AWS OCSF Databucket 的核心对象在没有其他属性的情况下使用。

示例

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

Image

计算资源的图像信息，包括平台和使用情况详细信息。

要求

可选

Type

对象

OCSF 状态

已添加到`resource_details`。请参阅 OCSF 图像对象定义。

AWS 扩展为该对象添加了以下属性：

- `platform`-镜像的操作系统平台
- `in_use_count`-使用此图像的资源计数

示例

```
{
  "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
  }
}
```

子网信息

有关资源所在子网的详细信息。

要求

可选

Type

对象

OCSF 状态

New

子网信息对象包括以下属性：

- uid-子网的唯一标识符
- uid_alt-资源的亚马逊资源名称 (ARN)
- name-子网的名称
- zone-可用区
- ip_count-子网中的 IP 地址数量
- cidr_block-子网的 CIDR 块
- is_default-这是否是默认子网
- is_public-子网是否可公开访问
- state-子网的状态
- vpc_uid-子网所在的 VPC ID

示例

```
{
  "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"
  }
}
```

用户

IAM 用户属性，包括实例配置文件和策略。

要求

可选

Type

对象

OCSF 状态

已添加到resource_details。请参阅 OCSF 用户对象定义。

用户对象包括以下属性：

- instance_profiles-附加到云实例的实例配置文件列表
- policies-为用户、群组、角色和资源分配权限的策略

示例

```
{
  "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"
      }
    ]
  }
}
```

Security Hub 中的覆盖范围调查发现

Security Hub 的覆盖范围调查结果可让您了解启用了哪些 AWS 安全功能，以及独立账户或组织成员账户的覆盖范围可能存在差距。覆盖范围调查结果目前支持报告亚马逊、Amazon Inspector GuardDuty、Amazon Macie和Sec AWS urity Hub CSPM启用了哪些服务和功能。这些调查发现显示在 Security Hub 控制面板的“安全覆盖范围”小组件中，可以按特定安全功能深入查看更详细的视图。

限制

- 对于成员账户，承保范围信息是跨关联账户汇总的 AWS 区域，但仅限于该成员账户。
- 对于未登录 Security Hub 的账户，不会显示承保范围信息。

Sec AWS urity Hub CSPM 的报道结果

Security Hub CSPM 覆盖范围调查发现评测账户中是否启用了合格的状况管理安全标准。启用任何 Security Hub CSPM 标准都符合资格，但 AWS Control Tower 和资源标记标准除外。

启用 Security Hub CSPM 时，可能需要长达 24 小时才能检测到默认启用的标准。

Amazon 的报道调查结果 GuardDuty

GuardDuty 覆盖率调查结果评估以下内容中 GuardDuty 是否已启用以及启用了哪些 GuardDuty 功能 AWS 账户：

- GuardDuty 亚马逊恶意软件防护 EC2 -扫描亚马逊 EC2 实例中是否存在潜在的恶意软件
- GuardDuty 亚马逊 EKS 保护 — 监控 Kubernetes 审计日志中是否存在亚马逊 EKS 集群中的威胁

- GuardDuty Lambda 保护 — 分析 Lambda 函数调用中是否存在潜在威胁
- GuardDuty Amazon S3 保护 — 分析数据事件是否存在对亚马逊 S3 存储桶的潜在威胁
- GuardDuty 亚马逊 RDS 保护 — 监控 Amazon RDS 数据库是否存在威胁
- GuardDuty 运行时监控 — 提供对 Amazon EC2 实例中运行时行为的实时监控
- GuardDuty 基础覆盖范围-启用后会自动开启 GuardDuty 的基准 GuardDuty 功能

> **Note**
>
> 对于 GuardDuty Foundational Coverage，显示该功能已关闭的覆盖率调查结果未在覆盖率调查结果的账户中启用。 GuardDuty

GuardDuty 覆盖范围的更新最多可能需要 24 小时才能反映到组织中的所有成员账户。

Amazon Inspector 的覆盖范围调查发现

Amazon Inspector 覆盖范围调查发现评测是否启用了 Amazon Inspector 以及账户中启用了哪些功能：

- Inspector 扫 EC2 描 — 扫描亚马逊 EC2 实例中是否存在漏洞
- Inspector ECR 扫描 – 扫描 Amazon ECR 容器映像是否存在漏洞
- Inspector Lambda 标准扫描 – 扫描 Lambda 函数是否存在漏洞
- Inspector Lambda 代码扫描 – 扫描 Lambda 代码函数是否存在代码漏洞

Amazon Macie 的覆盖范围调查发现

Macie 覆盖范围调查发现评测是否已在 AWS 账户中启用 Macie：

- Macie 自动敏感数据发现覆盖范围 – 持续评估您的 Amazon S3 数据资产是否包含敏感数据。

Macie 自动敏感数据发现的覆盖范围调查发现更新可能需要长达 24 小时才能反映到组织中的所有成员账户中。

隐瞒覆盖率调查结果

默认情况下，安全覆盖范围调查结果会评估账户和地区启用了哪些亚马逊 GuardDuty、Amazon Inspector、Amazon Macie和Sec AWS urity Hub CSPM功能。如果某些安全功能对您不适用或存在可

接受的风险，则可以使用抑制功能来隐藏与所有其他发现结果类似的覆盖范围调查结果。当覆盖率发现被抑制时，它不会包含在安全覆盖范围小部件的覆盖范围计算中，并且该小组件将显示一条消息：“已通过隐藏的覆盖范围发现排除安全功能，然后统计已抑制了多少发现结果。

隐藏 Security Hub 中发现的覆盖范围

1. 查看安全覆盖范围小部件时，选择覆盖百分比链接。
2. 从覆盖范围弹出窗口中选择 “查看覆盖率调查结果”。每项状态为 “新” 的发现都将是一个概述观察到的覆盖范围差距的发现。
3. 单击要取消的每个搜索结果旁边的复选框。
4. 在页面顶部，选择 “更新状态”，然后选择 “已禁止”。
5. 在 “将状态设置为已隐藏” 对话框中，可以选择输入注释，详细说明更改状态的原因。然后选择设置状态。

Security Hub 中的暴露调查发现

Security Hub 中的暴露发现表示多个安全信号之间的关联，这些信号可识别 AWS 环境中的潜在安全风险。暴露发现通过自动分析漏洞、配置、威胁和资源关系的组合，帮助您了解安全风险并确定其优先级。暴露调查发现包括特征和信号。一个信号可以包含一种或多种类型的暴露特征。当来自 Security Hub CSPM、Amazon Inspector、Macie 或其他 AWS 服务的信号表明存在风险时，Security Hub 会生成曝光结果。 GuardDuty一项资源最多可以是一项风险敞口发现的主要资源。如果资源没有任何暴露特征或特征不足，Security Hub 不会为该资源生成暴露调查发现。

曝光结果如何运作

Security Hub 通过以下方式生成曝光结果：

- 分析来自多个 AWS 安全服务的信号：Security Hub 持续收集和分析来自多个 AWS 安全服务的安全信号。它从中提取发现 GuardDuty 以进行威胁检测，从中提取用于漏洞评估的 Amazon Inspector，从中提取用于配置检查的 Security Hub CSPM，以及用于敏感数据泄露的 Macie。这些信号通过高级关联引擎进行处理，以识别潜在的安全风险。
- 评估资源配置和关系：系统根据安全最佳实践对资源配置进行详细评估。它检查特定于服务的设置、合规性要求和安全控制。此分析有助于识别与其他因素结合使用时可能导致安全漏洞的错误配置。
- 评估网络可访问性：风险暴露发现的关键组成部分是评估网络的可达性。该系统会评估互联网暴露和内部网络访问路径。它分析安全组配置和网络 ACL 设置，以确定潜在的攻击媒介。此分析有助于识别可能无意中暴露于未经授权访问的资源。

- 关联相关的安全问题：关联引擎映射 AWS 资源之间的关系，分析它们的交互方式并识别潜在的安全隐患。它检查 IAM 权限、角色和资源访问模式，以了解更广泛的安全背景。此过程有助于识别由于看似无害的个人配置组合而可能存在的安全风险。

曝光调查结果的组成部分

每项曝光发现包括：

- 潜在安全风险的标题和描述——每项风险发现都包括一个清晰的描述性标题，该标题可立即传达安全风险的性质。该描述提供了有关潜在安全影响、受影响的资源以及更广泛的暴露背景的详细信息。这些信息可以帮助安全团队快速了解和评估风险。
- 严重性分类（严重、高、中、低）：
  - 严重性严重性表示由于漏洞利用的可能性很高且潜在影响很大，因此需要立即采取行动。这些发现通常代表了容易发现和可利用的漏洞。
  - 严重程度高表示需要优先关注，漏洞利用的可能性为中到高，潜在影响很大。这些发现可能相对容易被利用，但可能需要特定的条件。
  - 中等严重性表示需要定期关注，利用漏洞的可能性较低，潜在影响适中。这些发现通常需要更复杂的利用方法。
  - 低严重性表示需要定期关注，漏洞利用的可能性有限，影响也很小。这些发现通常难以利用，风险也最小。
- 导致暴露的贡献特征：贡献特征是导致暴露发现的主要因素。这些漏洞包括直接安全漏洞、配置问题、网络泄露条件和资源权限设置。每个特征都提供了有关其如何导致整体安全风险的具体细节。
- 攻击路径可视化：攻击路径可视化提供了一个交互式图表，显示潜在攻击者如何利用已识别的漏洞。它绘制了资源关系、网络路径和潜在影响流图，帮助安全团队了解风险的全部范围并规划有效的补救策略。
- 详细的补救指南：每项暴露发现都包括详细的补救指南，以及针对已确定的风险的具体、可操作的步骤。本指南包括最佳实践建议、配置更正步骤和优先操作项目。该指南针对具体的暴露情景量身定制，并考虑了所涉及的 AWS 服务。
- 资源配置详情：创建调查结果时的资源配置以及 Security Hub 资源清单控制面板中资源的当前配置。
- 情境特征提供了额外的安全背景：上下文特征是由 Security Hub 识别但未用于创建暴露发现的其他安全标记。

来自 IAM Access Analyzer 的未使用的访问信息可以作为上下文特征出现在曝光结果中。当附加到资源的 IAM 角色具有未使用的权限时，Security Hub 会将此信息作为上下文特征包含在曝光详细信息视图中。例如，如果 Amazon EC2 实例存在软件漏洞，且其附加的 IAM 角色在 5 项服务中有 47 个未使用的权限，则暴露结果会将未使用的权限显示为补充上下文。这可以帮助您了解潜在的爆炸半径——具有过高权限的 IAM 角色的易受攻击的资源比权限最低的资源带来的风险更高，因为受感染的资源可能会使用这些未使用的权限来升级访问权限。

以下资源类型可以在其曝光结果中显示未使用的访问上下文特征：

- Amazon 弹性计算云实例
- AWS Lambda 函数
- Amazon 弹性容器服务服务
- 亚马逊 Elastic Kubernetes Service 集群
- IAM 用户（直接）

严重性分类

暴露结果的分类依据是：

- 易于发现
- 易于利用
- 被利用的可能性
- 公众意识
- 潜在影响

有关更多信息，请参阅暴露结果严重性分类。

暴露结果的好处

- 通过自动关联@@ 减少手动分析：通过自动关联和智能风险优先级划分，暴露发现显著减少了安全分析所需的时间和精力。Security Hub 持续监控您的 AWS 环境，通过手动审查自动识别和关联可能遗漏的安全风险。
- 安全风险的优先视图：Security Hub 采用复杂的风险评估算法，根据严重性、影响、资源重要性和漏洞利用可能性对风险进行优先排序。这有助于安全团队首先将精力集中在最重要的风险上，从而提高安全运营的效率。

暴露来源调查结果

暴露结果包含来自以下方面的数据：

- Amazon GuardDuty 集成在风险暴露结果中提供了持续的威胁检测功能。它可以监控恶意活动、潜在的账户泄露和行为异常。该系统将这些威胁发现纳入更广泛的风险暴露分析中，有助于确定威胁何时与其他安全问题结合而造成重大风险。
- Amazon Inspec tor 为暴露调查结果提供了重要的漏洞评估数据。它提供了有关网络可访问性、软件漏洞和违反安全最佳实践的详细信息。这种集成有助于了解漏洞是如何通过已确定的攻击路径被利用的。
- AWS S@@ ecurity Hub CSPM 确保在风险分析中考虑配置合规性和安全标准。它根据既定的安全控制措施和最佳实践评估资源，为了解基于配置的风险奠定基础。
- Amazon Macie 通过敏感数据发现和分类功能增强了暴露结果。它可以识别您 AWS 环境中存在的敏感数据的位置，并评估潜在的隐私风险，从而帮助了解已识别的风险暴露的潜在影响。

最佳实践

- 定期审查曝光结果：有效的风险敞口管理需要结构化的审查流程。Organizations 应对关键风险进行每日审查、每周评估总体风险暴露状态、每月趋势分析和季度安全态势评估。这种分层方法可确保适当关注眼前风险和长期安全趋势。
- 确定关键风险和高严重风险敞口的优先级：成功的风险敞口管理取决于有效的风险优先级划分。Organizations 应首先关注关键风险，同时考虑资源关键性和业务影响。这种基于风险的方法有助于确保安全措施与业务优先事项保持一致，并最大限度地降低风险。
- 实施建议的补救措施：暴露补救应遵循系统的方法。Organizations 应认真实施建议的补救措施，详细记录变更情况，对修改进行全面测试，并验证已实施修复的有效性。这种有条不紊的方法有助于确保成功降低风险，同时避免意想不到的后果。
- 配置自动响应规则：要最大限度地提高曝光结果的价值，需要有效的自动化。Organizations 应实施自动响应规则，配置适当的通知，建立高效的工作流程，并维护全面的审计跟踪。这种自动化有助于确保对已识别的暴露做出一致和及时的响应，同时减少人工操作。

Security Hub 中暴露调查发现支持的资源类型

AWS Security Hub 会生成以下类型 AWS 资源的暴露结果：

- `AWS::DynamoDB::Table`

- AWS::EC2::Instance
- AWS::ECS::Service
- AWS::EKS::Cluster
- AWS::IAM::User
- AWS::Lambda::Function
- AWS::RDS::DBInstance
- AWS::S3::Bucket

Security Hub 为每个主要资源生成一个曝光结果。如果资源没有任何暴露特征或特征不足，Security Hub 不会为该资源生成暴露调查发现。

Security Hub 中支持的特征类型

AWS 当 Security Hub CSPM 控制结果和其他受支持者（例如 Amazon Inspector）生成的发现包含资源的暴露特征时 AWS 服务，Sec AWS urity Hub 会生成暴露发现。下表提供了有关支持的特征类型的信息。

特征类型	说明	来源	受影响的资源
假设性	表示具有售 AWS Identity and Access Management 出权限的资源	资源配置来自 AWS Config	AWS 具有关联 AWS Identity and Access Management 角色的资源
错误配置	表示资源配置错误	AWS Security Hub CSPM 控制结果、Amazon GuardDuty 威胁发现以及有关资源确认的信息。AWS Config	所有资源类型
可访问性	表示资源的开放网络路径	AWS Security Hub CSPM 控制结果、亚马	亚马逊 EC2 实例、亚马逊 EKS 集群、Lambda

特征类型	说明	来源	受影响的资源
		逊 GuardDuty 威胁调查结果和 Amazon Inspector 网络可达性调查结果。	函数和亚马逊 S3 存储桶
敏感数据	表示资源包含敏感数据	Macie 敏感数据发现	Amazon S3 存储桶
脆弱性	表示资源存在可被威胁源利用的弱点。	Amazon Inspector 软件包漏洞调查结果和 GuardDuty 亚马逊 EC2 恶意软件发现。	Amazon EC2 实例、Amazon ECS 服务、Amazon EKS 集群和 Lambda 函数

每个特征可以与多个标题相关联，这些标题提供有关影响资源的暴露的详细信息。例如，您可能会在 EC2 暴露调查发现的详细信息中看到漏洞特征的攻击漏洞可用标题。

生成暴露调查发现

Security Hub 可以近乎实时地生成曝光结果。当新的安全发现被摄取并更新现有发现时，Security Hub 会近乎实时地生成或更新泄露结果。Security Hub 为每个资源 ID 生成一个曝光结果。

如果资源没有任何暴露特征或特征不足，Security Hub 不会为该资源生成暴露调查发现。Security Hub 不会为暴露调查发现不支持的资源类型发布暴露调查发现。当资源具有大量特征和特征组合时，Security Hub 会生成暴露调查发现。特征的数量和组合也决定暴露调查发现的严重性级别。

暴露调查发现示例

AWS Security Hub 对开放网络安全架构框架 (OCSF) 中的暴露发现进行标准化。

暴露调查发现示例

在以下样本暴露调查发现中，`related_events` 参数包含暴露调查发现所特有的详细信息，例如促成性调查发现。促成性调查发现是与暴露调查发现关联的特征和信号。单个促成性调查发现可以包含一

个或多个特征。observables 参数标识与促成性调查发现关联的资源。这可能与 resources 参数不同，后者标识与暴露调查发现关联的资源。


```
{
    "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,
    "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"
    }
}
```

确定暴露调查发现的严重性级别

AWS Security Hub 会为每个风险分配一个默认严重性为CRITICALHIGH、MEDIUM、或LOW。严重性为 INFORMATIONAL 的暴露调查发现不会发布。Security Hub 使用多个因素来确定暴露调查发现的默认严重性级别：

- 意识 – 暴露不是理论上的，而是具有公开可用或自动的漏洞利用。这适用于 EC2 实例和 Lambda 函数的暴露调查发现。
- 易于发现 – 是否有自动化工具（例如端口扫描或互联网搜索）可用于发现存在风险的资源。
- 易于利用 – 威胁参与者可以轻松利用暴露。例如，如果存在开放的网络路径或错误配置的元数据，则威胁参与者可以更轻松地利用暴露。
- 漏洞利用的可能性 – 未来 30 天内暴露被利用的可能性。此因素对应于攻击漏洞保护评分系统（EPSS），适用于对 Amazon EC2 实例和 Lambda 函数的暴露调查发现。
- 影响 – 实施漏洞利用所造成的危害。例如，暴露可能导致责任丧失、可用性丧失、数据泄露导致机密性丧失或者数据损坏导致完整性丧失。

查看暴露调查发现

您可以在 Security Hub 控制台中和使用 GetFindingsV2 API 中查看所有暴露调查发现。Security Hub 控制台中的暴露页面显示所有活跃暴露调查发现。暴露调查发现按严重程度降序列出。您可以通过使用添加筛选条件搜索栏添加和移除筛选条件来筛选暴露调查发现。您可以使用分组依据下拉菜单对暴露调查发现进行分组。您也可以使用快速筛选菜单筛选暴露调查发现。

暴露调查发现的详细信息

您可以查看暴露调查发现的许多详细信息。这些详细信息分布在 Security Hub 控制台的各个选项卡中。概述选项卡提供有关暴露调查发现的关键详细信息。特征选项卡列出与暴露调查发现关联的特征和信号。资源选项卡提供有关与暴露调查发现关联的资源和资源标签的详细信息。以下列表提供了暴露调查发现详细信息的描述。

- 调查发现标题：暴露调查发现的标题。
- 严重性级别 – 暴露调查发现的严重性级别。Security Hub 使用资源的特征数量和组合来确定暴露调查发现的严重性级别。严重性级别可以是 CRITICAL、HIGH、MEDIUM 或 LOW。Security Hub 不会发布严重性为 INFORMATIONAL 的暴露调查发现。您可以通过 Security Hub 控制台或 BatchUpdateFindingsV2 API 操作更新 Severity。
- 描述 – 暴露调查发现的描述。

- 类型 – 暴露调查发现类型的名称。例如，名称可能类似于 `Exposure/Potential Impact/Resource Hijacking`。
- 账户 – 生成暴露调查发现的 AWS 账户 的 ID。
- 期限– 表示暴露调查发现处于活跃状态的时长。
- 创建时间 – 指示暴露调查发现的创建时间的时间戳。
- 修改时间 – 指示暴露调查发现的上次更新时间的时间戳。
- 区域-产生曝光结果 AWS 区域 的地方。
- 产品名称 – 生成暴露调查发现的产品的名称。这将始终是 Security Hub 暴露检测。
- 公司名称 – 生成暴露调查发现的公司的名称。这将始终为 AWS。
- 活动名称 – 上次根据调查发现执行的活动的名称。
- 状态 – 此暴露调查发现的状态。
- 调查发现 ID – 与暴露调查发现关联的唯一标识符。
- 潜在攻击路径（仅限控制台） – 交互式可视化，显示潜在攻击者如何访问和控制与暴露调查发现关联的资源。有关更多信息，请参阅 使用潜在攻击路径图在 Security Hub 中查看暴露。
- 特征 – 识别与暴露调查发现关联的特征类型和特征标题。在 Security Hub 控制台中，您可以按特征类型或信号查看特征。这可以帮助您在相关暴露上下文中分析促成性调查发现。
- 修复 – 指向特定于暴露中发现的特征的修复文档的链接。
- 资源 – 识别与暴露调查发现关联的资源。

查看暴露调查发现的详细信息

本主题介绍如何在 AWS Security Hub 控制台中和使用 API 查看有关暴露调查发现的详细信息。

在 Security Hub 控制台中查看暴露调查发现的详细信息

在 Security Hub 控制台中查看暴露调查发现的详细信息

1. 使用您的凭据登录，然后在上打开 Security Hub 控制台https://console.aws.amazon.com/securityhub/v2/home。
2. 从导航窗格中选择暴露。
3. 选择要查看详细信息的暴露调查发现。

使用 API 查看暴露调查发现的详细信息

您可以使用 GetFindingsV2 API 或 AWS CLI查看暴露调查发现。您可以使用值为 `security-hub/Exposure` 的 `metadata.product.feature.uid` 字段筛选所有暴露调查发现。有关更多信息，请参阅 GetFindingsV2。

命令示例

以下是检索您账户中最近生成的 10 个曝光调查结果的 AWS CLI 示例。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

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

使用潜在攻击路径图在 Security Hub 中查看暴露

潜在攻击路径图是一种交互式可视化，显示潜在攻击者如何访问和控制与暴露调查发现关联的资源。您只能在 Security Hub 控制台中和从暴露页面访问此图表。当您查看暴露调查发现的详细信息时，概述选项卡包含名为潜在攻击路径的部分。

在概述选项卡的此部分中，您可以选择并拖动潜在攻击路径图中的 AWS 资源。您可以使用放大和缩小图标集中关注攻击路径图的特定区域。您可以通过全屏图标在全屏模式内外展开攻击路径图。图例按颜色对主要资源、涉及的资源和促成性特征计数进行编码，并在攻击路径图中显示特征类别和特征数量。您可以通过选择一个资源并选择查看资源详细信息来查看资源的详细信息。您也可以复制与资源关联的 ID 和 AWS 账户 号码。具有可访问性特征的暴露调查发现在攻击路径图中显示公共互联网和崩溃的网络路径。您可以通过选择折叠的网络路径节点来查看此详细信息。

修复暴露调查发现

本节中的主题描述了针对不同领域的暴露发现的补救步骤 AWS 服务。

OCSF 格式的 `Remediation` 字段包含两个字段：`remediation` 和 `references`。

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

```
    }
},
```

> **Note**
>
> 以下各节中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

修复 DynamoDB 表的暴露

AWS Security Hub 可以为 DynamoDB 表生成暴露结果。

在 Security Hub 控制台上，暴露调查发现中涉及的 DynamoDB 表及其识别信息列在调查发现详细信息的资源部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- DynamoDB 中的错误配置特征
  - DynamoDB 表已禁用恢复 point-in-time
  - DynamoDB 表不在备份计划的覆盖范围内
  - DynamoDB 表已禁用删除保护

DynamoDB 中的错误配置特征

下面介绍了 DynamoDB 表的错误配置特征和修复步骤。

DynamoDB 表已禁用恢复 point-in-time

启用 DynamoDB 恢复 point-in-time

Dynam point-in-time oDB 恢复为您的 DynamoDB 表数据提供持续的自动备份。有关如何将 DynamoDB 表还原到特定时间点的信息，请参阅《Amazon DynamoDB 开发人员指南》中的将 DynamoDB 表还原到某个时间点。

DynamoDB 表不在备份计划的覆盖范围内

AWS Backup 提供了一种集中式服务，用于配置、管理和自动执行跨 AWS 服务（包括 DynamoDB）的备份。如果没有备份计划，您的表就会缺少具有可自定义保留期的定时自动备份，从而造成严重的安全风险。攻击者可能会恶意破坏或删除您的表格数据。如果没有适当的备份，则可能在 “恢复” 窗口以外没有 Point-in-Time恢复选项（如果启用），这可能会导致数据永久丢失。根据数据保护最佳实践，我们建议您通过备份计划涵盖 DynamoDB。

创建备份计划

在创建备份计划之前，请为您的数据确定合适的备份频率和保留期。有关如何创建备份计划的信息，请参阅《Amazon DynamoDB 用户指南》中的将资源分配给备份计划。

DynamoDB 表已禁用删除保护

删除保护可防止意外删除 DynamoDB 表。在禁用删除保护后，DynamoDB 表很容易通过控制台操作、API 调用、CLI 命令或自动流程被意外删除。这可能会使您的 AWS 环境面临数据丢失风险，因为有权访问您的 AWS 环境的未经授权的实体可能会故意删除表，从而导致服务中断和永久丢失数据。根据数据保护最佳实践，我们建议为 DynamoDB 表启用数据保护。

启用删除保护

如果您管理多个表，请考虑 CloudFormation 使用批量更新表属性。您可以修改 CloudFormation 模板以包含`DeletionProtectionEnabled`属性并更新堆栈。完成修复后，请在表设置选项卡的其他信息下拉列表中验证是否已启用删除保护。

修复 EC2 实例的暴露

AWS Security Hub 可以生成亚马逊弹性计算云 (EC2) 实例的暴露结果。

在 Security Hub 控制台上，暴露调查发现中涉及的 EC2 实例及其识别信息列在调查发现详细信息的资源部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- EC2 实例的错误配置特征
  - EC2 实例允许使用版本 1 访问 IMDS
  - 与 Amazon EC2 实例关联的 IAM 角色具有管理访问策略
  - 与 Amazon EC2 实例关联的 IAM 角色具有服务管理员策略
  - Amazon EC2 实例具有允许 SSH 或 RDP 访问的安全组或网络 ACL
  - Amazon EC2 实例具有开放式安全组
- EC2 实例的可访问性特征
  - 可通过互联网访问 EC2 实例
- EC2 实例的漏洞特征
  - EC2 实例存在可通过网络利用的软件漏洞，被利用的可能性很高
  - Amazon EC2 实例存在软件漏洞
  - EC2 实例具有 End-Of-Life 操作系统
  - EC2 实例包含恶意软件包
  - EC2 实例包含恶意文件

EC2 实例的错误配置特征

以下是 EC2 实例的错误配置特征和建议的修复步骤。

EC2 实例允许使用版本 1 访问 IMDS

实例元数据是有关您的 Amazon EC2 实例的数据，可以用来配置或管理正在运行的实例。实例元数据服务（IMDS）是实例上的组件，在实例上进行编码，用于安全访问实例元数据。如果 IMDS 没有

得到妥善保护，它可能会成为潜在攻击向量，因为它提供了对临时凭证和其他敏感配置数据的访问权限。IMDSv2 通过面向会话的身份验证提供更强的防漏洞利用保护，要求对元数据请求使用会话令牌，并限制会话持续时间。按照标准安全原则， AWS 建议您将亚马逊 EC2 实例配置为使用 imdsv2 并禁用 imdsv1。

测试应用程序兼容性

在实施 IMDSv2 之前，请测试您的实例以确保其与 IMDSv2 兼容。某些应用程序或脚本可能需要 IMDSv1 来实现核心功能，并且需要额外配置。有关测试应用程序兼容性的工具和推荐路径的更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的转换为使用实例元数据服务版本 2。

更新实例以使用 IMDSv2

修改现有实例以使用 IMDSv2。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的为现有实例修改实例元数据选项。

将更新应用于自动扩缩组中的实例

如果您的实例属于某个自动扩缩组，请使用新配置更新您的启动模板或启动配置，并执行实例刷新。

与 Amazon EC2 实例关联的 IAM 角色具有管理访问策略

管理访问策略为 Amazon EC2 实例提供了广泛的访问权限 AWS 服务 和资源。这些策略通常包含实例功能不需要的权限。如果 Amazon EC2 实例遭到入侵，在 Amazon EC2 实例上提供具有管理访问策略的 IAM 身份（而不是附加到实例配置文件的角色所需的最低权限集）可能会扩大攻击范围。如果实例遭到入侵，攻击者可能会利用这些过多的权限在您的环境中横向移动、访问数据或操纵资源。根据标准安全原则，我们建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

查看和识别管理策略

在 IAM 控制面板中，找到具有角色名称的角色。查看附加到 IAM 角色的权限策略。如果该策略是 AWS 托管策略，请查找`AdministratorAccess`或`IAMFullAccess`。否则，请在策略文档中查找带有 `"Effect": "Allow", "Action": "*"` 和 `"Resource": "*"` 的语句。

实施最低权限访问

将管理策略替换为仅授予实例运行所需的特定权限的策略。有关 IAM 角色的安全最佳实践的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的应用最低权限许可。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的外部和未使用的访问的调查发现。或者，您可以创建一个新的 IAM 角色，以避免影响使用现有角色的其他应用程序。在这种情况下，请创

建一个新的 IAM 角色，然后将新的 IAM 角色与实例关联起来。有关如何替换实例的 IAM 角色的说明，请参阅《Amazon Elastic Compute Cloud 用户指南》中的将 IAM 角色附加到实例。

安全配置注意事项

如果实例需要服务级别的管理权限，请考虑实施以下额外安全控制措施来降低风险：

- 安全配置注意事项

  - Multi-factor 身份验证 (MFA) — MFA 要求使用其他形式的身份验证，从而增加了额外的安全层。即使凭证遭到泄露，这也有助于防止未经授权的访问。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的需要多重身份验证（MFA）。
  - IAM 条件 – 通过设置条件元素，您可以基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用 IAM 策略中的条件进一步限制访问权限。
  - 权限边界 – 权限边界规定了角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用权限边界在账户内委派权限管理。

将更新应用于自动扩缩组中的实例

对于 AWS 自动扩展组中的 Amazon EC2 实例，使用新的实例配置文件更新启动模板或启动配置，然后刷新实例。有关更新启动模板的信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的修改启动模板（管理启动模板版本）。有关更多信息，请参阅使用实例刷新更新自动扩缩组中的实例。有关将 IAM 角色与自动扩缩组结合使用的更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的在 Amazon EC2 实例上运行的应用程序的 IAM 角色。

与 Amazon EC2 实例关联的 IAM 角色具有服务管理员策略

服务访问策略为 Amazon EC2 实例提供了对 AWS 服务和资源的广泛权限。这些策略通常包含实例功能不需要的权限。如果实例遭到入侵，在 Amazon EC2 实例上提供具有管理访问策略的 IAM 身份（而不是附加到实例配置文件的角色所需的最低权限集）可能会扩大攻击范围。根据标准安全原则，我们建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

查看和识别管理策略

在 IAM 控制面板中，找到具有角色名称的角色。查看附加到 IAM 角色的权限策略。如果该策略是 AWS 托管策略，请查找`AdministratorAccess`或`IAMFullAccess`。否则，请在策略文档中查找带有 `"Effect": "Allow", "Action": "*"` 和 `"Resource": "*"` 的语句。

实施最低权限访问

将服务管理员策略替换为仅授予实例运行所需的特定权限的策略。有关 IAM 角色的安全最佳实践的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的应用最低权限许可。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的外部和未使用的访问的调查发现。或者，您可以创建一个新的 IAM 角色，以避免影响使用现有角色的其他应用程序。在这种情况下，请创建一个新的 IAM 角色，然后将新的 IAM 角色与实例关联起来。有关如何替换实例的 IAM 角色的信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的将 IAM 角色附加到实例。

安全配置注意事项

如果实例需要服务级别的管理权限，请考虑实施以下额外安全控制措施来降低风险：

安全配置注意事项

如果实例需要服务级别的管理权限，请考虑实施以下额外安全控制措施来降低风险：

- Multi-factor 身份验证 (MFA) — MFA 要求使用其他形式的身份验证，从而增加了额外的安全层。即使凭证遭到泄露，这也有助于防止未经授权的访问。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的需要多重身份验证（MFA）。
- IAM 条件 – 通过设置条件元素，您可以基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用 IAM 策略中的条件进一步限制访问权限。
- 权限边界 – 权限边界规定了角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用权限边界在账户内委派权限管理。

将更新应用于自动扩缩组中的实例

对于 AWS 自动扩展组中的 Amazon EC2 实例，使用新的实例配置文件更新启动模板或启动配置，然后刷新实例。有关更新启动模板的信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的修改启动模板（管理启动模板版本）。有关更多信息，请参阅使用实例刷新更新自动扩缩组中的实例。有关将 IAM 角色与自动扩缩组结合使用的更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的在 Amazon EC2 实例上运行的应用程序的 IAM 角色。

Amazon EC2 实例具有允许 SSH 或 RDP 访问的安全组或网络 ACL

SSH 和 RDP 等远程访问协议允许用户从外部位置连接和管理 Amazon EC2 实例。当安全组允许从互联网无限制地访问这些协议时，它们会允许通过互联网访问您的 Amazon EC2 实例，从而增加这些实例的攻击面。遵循标准的安全原则， AWS 建议您将远程访问限制在特定、可信的 IP 地址或范围内。

1. 修改安全组规则

   将对 Amazon EC2 实例的访问限制于特定的受信任 IP 地址。将 SSH 和 RDP 访问限制为特定的可信 IP 地址，或者使用 CIDR 表示法指定 IP 范围（例如 198.168.1）。 0/24)。要修改安全组规则，请参阅《Amazon Elastic Compute Cloud 用户指南》中的配置安全组规则。

Amazon EC2 实例具有开放式安全组

安全组充当 Amazon EC2 实例的虚拟防火墙以控制入站和出站流量。开放式安全组允许从任何 IP 地址进行不受限制的访问，这可能会使实例面临未经授权的访问。根据标准安全原则， AWS 建议将安全组的访问权限限制为特定 IP 地址和端口。

查看安全组规则并评测当前配置

评估哪些端口已开放且可从广泛的范围 IP 地址（例如 (`0.0.0.0/0 or ::/0`)）访问。有关查看安全组详细信息的说明，请参阅 .NET 移植助手 API 参考DescribeSecurityGroups中的。

修改安全组规则

修改您的安全组规则，将访问限制于特定的受信任 IP 地址或范围。更新安全组规则时，请考虑通过为每个所需的源 IP 地址范围创建规则或限制对特定端口的访问来区分不同网段的访问要求。要修改安全组规则，请参阅《Amazon EC2 用户指南》中的配置安全组规则。

EC2 实例的可访问性特征

以下是 EC2 实例的可访问性特征和建议的修复步骤。

可通过互联网访问 EC2 实例

带有可从互联网访问的端口的 Amazon EC2 实例可能会暴露您的实例。可访问性可通过 Internet 网关（包括应用程序负载均衡器或经典负载均衡器后面的实例）、VPC 对等连接或 VPN 虚拟网关实现。根据标准安全原则，我们建议通过将入站流量限制在仅必要的来源和端口来实施最低权限网络访问控制。

修改或移除安全组规则

在资源选项卡中，打开 Amazon EC2 安全组的资源。检查实例运行是否需要访问互联网。修改或移除允许无限制访问（`0.0.0.0/0` 或 `::/0`）的入站安全组规则。根据特定 IP 范围或安全组实施更严格的规则。如果需要有限的公开访问，请将访问限制于实例运行所需的特定端口和协议。有关管理安全组规则的说明，请参阅《Amazon EC2 用户指南》中的配置安全组规则。

更新网络 ACL

查看并修改与实例子网关联的网络访问控制列表（ACL）。验证 ACL 设置是否与安全组更改一致，并且不会无意中允许公开访问。有关修改网络 ACL 的说明，请参阅《Amazon VPC 用户指南》中的使用网络 ACL。

替代访问方法

请考虑以下替代访问方法选项：

- 使用 NAT 网关进行出站互联网连接 – 对于私有子网中需要访问互联网的实例（例如下载更新），请考虑使用 NAT 网关而不是分配公共 IP 地址。NAT 网关允许私有子网中的实例启动与互联网的出站连接，同时阻止来自互联网的入站连接。
- 使用 Systems Manager 会话管理器：会话管理器提供对 Amazon EC2 实例的 Secure Shell 访问，无需入站端口、管理 SSH 密钥或维护堡垒主机。
- 使用 WAF 和 Elastic Load Balancing 或应用程序负载均衡器 — 对于运行 Web 应用程序的实例，可以考虑将负载均衡与 AWS Web 应用程序防火墙 (WAF) 结合使用。LB 可以配置为允许您的实例在私有子网中运行，而 LB 在公共子网中运行并处理互联网流量。向负载均衡器添加 WAF 可提供额外保护来抵御 Web 漏洞和机器人。

EC2 实例的漏洞特征

以下是 EC2 实例的漏洞特征和建议的修复步骤。

EC2 实例存在可通过网络利用的软件漏洞，被利用的可能性很高

EC2 实例上安装的软件包可能会暴露于常见漏洞和暴露（CVE）。关键 CVE 会给您的 AWS 环境带来严重的安全风险。未经授权的主体可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。利用可能性较高的严重漏洞代表直接的安全威胁，因为漏洞利用代码可能已经公开并被攻击者或自动扫描工具积极使用。我们建议您修补这些漏洞以保护您的实例。

更新受影响的实例

查看特征的漏洞选项卡中的参考部分。供应商文档可能包括具体的修复指导。请按照以下一般准则进行适当的修复：

使用 Systems Manager 补丁管理器来应用操作系统和应用程序的补丁。补丁管理器可帮助您在大量实例上自动选择和部署操作系统和软件补丁。如果没有配置补丁管理器，请手动更新每个受影响实例上的操作系统。

按照供应商推荐的步骤，将受影响的应用程序更新到最新的安全版本。要管理多个实例中的应用程序更新，请考虑使用 Systems Manager 状态管理器使软件保持一致状态。如果没有更新可用，请考虑在补丁发布或采取其他缓解措施（例如，限制对应用程序的网络访问或禁用易受攻击的功能）之前移除或禁用易受攻击的应用程序。

遵循 Amazon Inspector 调查发现中提供的具体修复建议。这可能涉及更改安全组规则、修改实例配置或调整应用程序设置。

检查该实例是否属于 Auto Scaling 组。 AMI-replacement 通过更新配置为在 Auto Scaling 组中部署新 Amazon EC2 实例的 AMI ID，可以在不可变基础设施上进行修补。如果您使用的是 custom/golden AMI，请使用新 AMI 创建实例，然后自定义该实例并创建新的金色 AMI。有关更多信息，请参阅 AMI 更新修补（使用已修补的 AMI 用于 Auto Scaling 群组）。

未来注意事项

为防止未来再次发生，请考虑实施漏洞管理计划。可以将 Amazon Inspector 配置为自动扫描实例上的 CVE。Amazon Inspector 还可以与 Security Hub 集成以实现自动修复。请考虑使用 Systems Manager Maintenance Windows 实施定期修补计划，以尽量减少对实例的中断。

Amazon EC2 实例存在软件漏洞

安装在 Amazon EC2 实例上的软件包可能会暴露在常见漏洞和风险敞口 (CVE) 中。与严重 CVE 相比，非严重 CVE 代表安全隐患，其严重性或可利用性较低。虽然这些漏洞不会造成直接风险，但攻击者仍可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。按照安全最佳实践， AWS 建议修补这些漏洞以保护您的实例免受攻击。

更新受影响的实例

使用 AWS Systems Manager 补丁管理器为操作系统应用补丁。补丁管理器可帮助您在大量实例上自动选择和部署操作系统和软件补丁。如果没有配置补丁管理器，请手动更新每个受影响实例上的操作系统。

按照供应商推荐的步骤，将受影响的应用程序更新到最新的安全版本。要跨多个实例管理应用程序更新，请考虑使用 S AWS ystems Manager 状态管理器使您的软件保持一致状态。如果没有更新可用，请考虑在补丁发布或采取其他缓解措施（例如，限制对应用程序的网络访问或禁用易受攻击的功能）之前移除或禁用易受攻击的应用程序。

遵循 Amazon Inspector 调查发现中提供的具体修复建议。这可能涉及更改安全组规则、修改实例配置或调整应用程序设置。

检查该实例是否属于 Auto Scaling 组。 AMI-replacement 通过更新配置为在 Auto Scaling 组中部署新 Amazon EC2 实例的 AMI ID，可以在不可变基础设施上进行修补。如果您使用的是 custom/golden AMI，请使用新 AMI 创建实例，然后自定义该实例并创建新的金色 AMI。有关更多信息，请参阅 AMI 更新修补（使用已修补的 AMI 用于 Auto Scaling 群组）。

未来注意事项

为防止未来再次发生，请考虑实施漏洞管理计划。可以将 Amazon Inspector 配置为自动扫描实例上的 CVE。Amazon Inspector 还可以与 Security Hub 集成以实现自动修复。请考虑使用 Systems Manager Maintenance Windows 实施定期修补计划，以尽量减少对实例的中断。

EC2 实例具有 End-Of-Life 操作系统

EC2 实例运行的操作系统已过期，不再由原始开发人员支持或维护。这会使实例面临安全漏洞和潜在攻击。当操作系统寿命结束时，供应商通常会停止发布新的安全公告。现有的安全公告也可以从供应商 Feed 中删除。因此，Amazon Inspector可能会停止为已知的CVE生成调查结果，从而在安全覆盖方面造成进一步的漏洞。

请参阅《亚马逊检查员用户指南》中的已停产操作系统，了解有关亚马逊检查员可以检测到的已使用寿命终止的操作系统的信息。

更新到支持的操作系统版本

我们建议更新到支持的操作系统版本。在风险调查结果中，打开资源以访问受影响的资源。在更新实例上的操作系统版本之前，请查看 Amazon Inspector 用户指南中支持的操作系统中的可用版本，了解当前支持的操作系统版本列表。

EC2 实例包含恶意软件包

恶意软件包是包含有害代码的软件组件，旨在危害系统和数据的机密性、完整性和可用性。恶意软件包会对您的实例构成严重威胁，因为攻击者可以在不利用漏洞的情况下自动执行恶意代码。按照安全最佳实践， AWS 建议移除恶意软件包，以保护您的实例免受潜在攻击。

移除恶意软件包

在特征的 “漏洞” 选项卡的 “参考” 部分中查看恶意软件包的详细信息，以了解威胁。使用相应的软件包管理器删除已识别的恶意软件包。有关示例，请参阅《亚马逊 Linux 2023 用户指南》中的 Pack age 管理工具。删除恶意软件包后，可以考虑执行扫描，确保所有可能由恶意代码安装的软件包都已删除。有关更多信息，请参阅 GuardDuty中的启动 On-demand 恶意软件扫描。

EC2 实例包含恶意文件

恶意文件包含有害代码，旨在危害系统和数据的机密性、完整性和可用性。恶意文件会对您的实例构成严重威胁，因为攻击者可以在不利用漏洞的情况下自动执行恶意代码。遵循安全最佳实践， AWS 建议删除恶意文件以保护您的实例免受潜在攻击。

移除恶意文件

要识别包含恶意文件的特定亚马逊 Elastic Block Store (Amazon EBS) 卷，请查看该特征发现详情的“资源” 部分。识别出带有恶意文件的卷后，请移除已识别的恶意文件。删除恶意文件后，请考虑执行扫描，以确保可能由恶意文件安装的所有文件都已删除。有关更多信息，请参阅 GuardDuty中的启动 On-demand 恶意软件扫描。

修复 Amazon ECS 服务的暴露

AWS Security Hub 可以生成亚马逊弹性容器服务 (Amazon ECS) 服务 (Amazon ECS) 服务的曝光调查结果。

暴露调查发现中涉及的 Amazon ECS 服务及其识别信息列在调查发现详细信息的资源部分中。您可以在 Security Hub 控制台上检索这些资源详细信息，也可以通过 Security Hub CSPM AP GetFindingsV2I 的操作以编程方式检索这些资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- Amazon ECS 服务的错误配置特征
  - Amazon ECS 服务使用允许容器访问根文件系统的任务定义
  - Amazon ECS 服务使用配置为共享主机的进程命名空间的任务定义
  - Amazon ECS 服务使用在环境变量中配置了明文凭证的任务定义

  - Amazon ECS 服务具有开放的安全组
  - Amazon ECS 服务有公有 IP 地址
  - Amazon ECS 服务使用已配置且启用了主机联网模式的任务定义
  - 与 Amazon ECS 服务关联的 IAM 角色具有管理访问策略
  - 与 ECS 服务关联的 IAM 角色具有服务管理员策略
- Amazon ECS 服务的可访问性特征
  - 可以通过互联网访问 Amazon ECS 服务
- Amazon ECS 服务的漏洞特征
  - Amazon ECS 服务的一个容器存在可通过网络利用的软件漏洞，被利用的可能性很高
  - Amazon ECS 服务的一个容器存在软件漏洞
  - Amazon ECS 服务有一个装有 End-Of-Life 操作系统的容器
  - Amazon ECS 服务有一个装有恶意软件包的容器

Amazon ECS 服务的错误配置特征

以下是 Amazon ECS 服务的错误配置特征和建议的修复步骤。

Amazon ECS 服务使用允许容器访问根文件系统的任务定义

有权访问主机根文件系统的 Amazon ECS 容器可能会读取、修改或执行主机系统上的关键文件。这种配置增加了遭入侵容器可能被用于访问或修改其预期范围之外的资源的风险，从而可能暴露主机文件系统上的敏感数据。根据标准安全原则， AWS 建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

查看和修改具有主机文件系统访问权限的容器

在暴露调查发现中，识别任务定义 ARN。在 Amazon ECS 控制台中打开任务定义。在定义主机路径映射的任务定义中查找卷部分。查看任务定义，确定容器功能是否需要主机文件系统访问权限。如果不需要访问主机文件系统，请创建一个新的任务定义修订版，并移除任何使用主机路径的卷定义。如果需要访问主机文件系统，请考虑将容器配置为使用只读文件系统，以防止未经授权的修改。

Amazon ECS 服务使用配置为共享主机的进程命名空间的任务定义

使用公开的命名空间运行的 Amazon ECS 容器可能会访问主机系统资源和其他容器命名空间。这种配置可能会允许遭入侵的容器逃离其隔离边界，从而可能导致访问其预期范围外的进程、网络接口或其他资源。进程 ID（PID）命名空间提供了进程之间的分离。它防止系统进程可见，并允许重复使用 PID，

包括 PID 1。如果主机的 PID 命名空间与容器共享，则容器可以看到主机系统上的所有进程。这降低了主机和容器之间进程级分离的好处。这些因素可能导致未经授权访问主机本身的进程，包括操纵和终止这些进程的能力。遵循标准的安全原则， AWS 建议为容器保持适当的命名空间隔离。

使用公开的命名空间更新任务定义

打开暴露的资源选项卡，识别具有公开的命名空间的任务定义。在 Amazon ECS 控制台中打开任务定义。查找值为 host 的 PidMode 设置，该设置将与主机共享进程 ID 命名空间。从任务定义中移除 PidMode: host 设置，以确保容器以正确的命名空间隔离运行。

Amazon ECS 服务使用在环境变量中配置了明文凭证的任务定义

环境变量中包含明文凭证的 Amazon ECS 容器会暴露敏感的身份验证信息，如果攻击者获得任务定义、容器环境或容器日志的访问权限，这些信息可能会被泄露。这会造成严重的安全风险，因为泄露的凭据可能被用来访问其他 AWS 服务或资源。

替换明文凭证

在暴露调查发现中，识别具有明文凭证的任务定义。在 Amazon ECS 控制台中打开任务定义。在容器定义中查找包含敏感值（例如 AWS 访问密钥、数据库密码或 API 令牌）的环境变量。

考虑采用以下替代方法来传递凭证：

- 与其使用 AWS 访问密钥，不如使用 IAM 任务执行角色和任务角色向容器授予权限。
- 将凭证作为机密存储在中， AWS Secrets Manager 并在任务定义中引用它们。

更新任务定义

创建一个新的可安全地处理凭证的任务定义修订版。然后对 Amazon ECS 服务进行更新，以使用新的任务定义修订版。

Amazon ECS 服务具有开放的安全组

安全组充当 Amazon ECS 任务的虚拟防火墙以控制入站和出站流量。允许从任何 IP 地址进行不受限制访问的开放式安全组可能会使您的容器面临未经授权的访问，从而增加暴露于自动扫描工具和针对性攻击的风险。根据标准安全原则， AWS 建议将安全组的访问权限限制为特定 IP 地址和端口。

查看安全组规则并评测当前配置

打开 Amazon ECS 安全组的资源。评估哪些端口已开放且可从广泛的范围 IP 地址（例如 `(0.0.0.0/0 or ::/0)`）访问。

修改安全组规则

修改您的安全组规则，将访问限制于特定的受信任 IP 地址或范围。更新安全组规则时，请考虑通过为每个所需的源 IP 地址范围创建规则或限制对特定端口的访问来区分不同网段的访问要求。

修改安全组规则

请考虑以下替代访问方法选项：

- 会话管理器提供对 Amazon EC2 实例的 Secure Shell 访问，无需入站端口、管理 SSH 密钥或维护堡垒主机。
- NACL 在子网级别提供额外安全保护。与安全组不同，NACL 是无状态的，需要明确定义入站和出站规则。

Amazon ECS 服务有公有 IP 地址

具有分配给其任务的公有 IP 地址的 Amazon ECS 服务可以直接从互联网访问。虽然这对于需要公开提供的服务来说可能是必要的，但这会增加攻击面和未经授权访问的可能性。

识别具有公有 IP 地址的服务

在暴露调查发现中，识别为其任务分配了公有 IP 地址的 Amazon ECS 服务。在服务配置中查找值为 ENABLED 的 `assignPublicIp` 设置。

更新任务定义

创建可禁用公有 IP 地址的任务定义新修订版。然后对 Amazon ECS 服务进行更新，以使用新的任务定义修订版。

实施私有网络访问模式

对于运行 Web 应用程序的实例，请考虑使用负载均衡器（LB）。LB 可以配置为允许您的实例在私有子网中运行，而 LB 在公共子网中运行并处理互联网流量。

Amazon ECS 服务使用已配置且启用了主机联网模式的任务定义

以主机联网模式运行的 Amazon ECS 容器与主机共享网络命名空间，从而可以直接访问主机的网络接口、端口和路由表。此配置绕过了容器提供的网络隔离，可能会将容器上运行的服务直接暴露给外部网络，并允许容器修改主机网络设置。遵循标准的安全原则， AWS 建议为容器保持适当的网络隔离。

禁用主机联网模式

在暴露调查发现中，识别具有主机联网模式的任务定义。在 Amazon ECS 控制台中打开任务定义。在任务定义中查找值为 host 的 NetworkMode 设置。

请考虑使用以下选项来禁用主机联网模式：

- awsvpc 网络模式通过为每个任务提供自己的弹性网络接口来提供最强的网络隔离级别。
- bridge 网络模式提供隔离，同时允许端口映射将特定的容器端口暴露给主机。

更新任务定义

创建一个新的具有更新的网络模式配置的任务定义修订版。然后对 Amazon ECS 服务进行更新，以使用新的任务定义修订版。

与 Amazon ECS 服务关联的 IAM 角色具有管理访问策略

具有附加到 Amazon ECS 任务的管理访问策略的 IAM 角色提供了超出容器操作通常所需的广泛权限。这种配置会增加被入侵的容器被用来访问或修改整个 AWS 环境中的资源的风险。遵循标准的安全原则， AWS 建议通过仅授予任务运行所需的权限来实现最低权限访问权限。

查看和识别管理策略

在资源 ID 中，识别 IAM 角色名称。前往 IAM 控制面板，然后选择已识别的角色。查看附加到 IAM 角色的权限策略。如果该策略是 AWS 托管策略，请查找AdministratorAccess。否则，在策略文档中，查找同时包含 "Effect": "Allow", "Action": "*", and "Resource": "*" 语句的语句。

实施最低权限访问

将管理策略替换为仅授予实例运行所需的特定权限的策略。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。或者，您可以创建一个新的 IAM 角色，以避免影响使用现有角色的其他应用程序。在这种情况下，请创建一个新的 IAM 角色，然后将新的 IAM 角色与实例关联起来。

安全配置注意事项

如果实例需要服务级别的管理权限，请考虑实施以下额外安全控制措施来降低风险：

- MFA 通过要求其他形式的身份验证来增加额外安全保障。即使凭证遭到泄露，这也有助于防止未经授权的访问。
- 通过设置条件元素，您可以基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。

更新任务定义

创建一个新的引用新增或更新的 IAM 角色的任务定义修订版。然后对 Amazon ECS 服务进行更新，以使用新的任务定义修订版。

与 ECS 服务关联的 IAM 角色具有服务管理员策略

服务管理策略为 Amazon ECS 任务和服务提供了在特定 AWS 服务中执行所有操作的权限。这些策略通常包括 Amazon ECS 任务功能所需的权限。为一个 IAM 角色提供用于 Amazon ECS 任务的服务管理策略（而不是所需的最低权限集）可能会在容器遭到入侵时扩大攻击范围。遵循标准的安全原则，AWS 建议您授予最低权限，这意味着仅授予执行任务所需的权限。

查看和识别管理策略

在资源 ID 中，标识 Amazon ECS 任务角色和执行角色名称。前往 IAM 控制面板并选择已识别的角色。查看附属于这些 IAM 角色的权限策略。查找授予服务完全访问权限的政策声明（例如`"s3": "*", "ecr": "*"`）。有关编辑 IAM 策略的说明，请参阅 IAM 用户指南中的编辑 IAM 策略。

实施最低权限访问

将服务管理策略替换为仅授予 Amazon ECS 任务运行所需的特定权限的策略。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。或者，您可以创建一个新的 IAM 角色，以避免影响使用现有角色的其他应用程序。在这种情况下，请创建一个新的 IAM 角色，然后将新的 IAM 角色与实例关联起来。

安全配置注意事项

如果 Amazon ECS 任务需要服务级别的管理权限，请考虑实施以下额外的安全控制：

- IAM 条件 — 设置条件元素，根据 VPC 终端节点或特定的 Amazon ECS 集群等因素限制何时以及如何使用管理权限。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 策略中的条件进一步限制访问权限。
- 权限边界-确定角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。有关更多信息，请参阅 IAM 用户指南中的使用权限边界委派账户内的权限管理。

更新任务定义

创建一个新的引用新增或更新的 IAM 角色的任务定义修订版。然后对 Amazon ECS 服务进行更新，以使用新的任务定义修订版。

Amazon ECS 服务的可访问性特征

以下是 Amazon ECS 服务的可访问性特征和建议的补救措施。

可以通过互联网访问 Amazon ECS 服务

在公有子网上运行任务的 Amazon ECS 服务可以直接从互联网访问。这会增加攻击面和未经授权访问的风险。遵循标准的安全原则， AWS 建议您在私有子网上运行任务，并且仅允许您的服务所需的互联网接入。

在私有子网上运行任务

要将任务移出公有子网，请更新启动类型的网络配置：

- 对于 Fargate，请在您的 Amazon ECS 服务的网络配置中指定私有子网并将其设置为。`assignPublicIp` `DISABLED`Amazon ECS 将每项任务托管在私有子网上，并通过您与该子网关联的 NAT 网关路由其出站流量。
- 对于 EC2，启动在私有子网上为您的集群提供容量的容器实例。任务使用主机的私有网络，通过 NAT 网关路由出站流量。

使用 NAT 网关进行出站访问

对于私有子网上需要出站互联网访问的任务，请使用 NAT 网关。您可以使用 NAT 网关让任务启动互联网的出站连接，并阻止来自互联网的入站连接。有关更多信息，请参阅《亚马逊 ECS 开发人员指南》中的将 Amazon ECS 应用程序连接到互联网。

使用负载均衡器进行入站访问

对于需要接受 Internet 流量的服务，请在公有子网上运行的负载均衡器后面的私有子网上运行任务。要添加针对 Web 漏洞和机器人的防护，请将 AWS Web 应用程序防火墙 (WAF) 与您的负载均衡器关联。有关更多信息，请参阅 Amazon ECS 开发人员指南中的使用负载平衡来分配 Amazon ECS 服务流量。

Amazon ECS 服务的漏洞特征

以下是 Amazon ECS 的漏洞特征和建议的修复步骤。

Amazon ECS 服务的一个容器存在可通过网络利用的软件漏洞，被利用的可能性很高

1. 了解暴露

程序包漏洞调查发现可识别 AWS 环境中暴露于常见漏洞和风险（CVE）的程序包。攻击者可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。ECR 容器映像可能具有程序包漏洞调查发现。

2. 修复暴露

   a. 更新软件包版本

      查看 ECR 容器映像的程序包漏洞调查发现。按照 Amazon Inspector 的建议更新软件包版本。有关更多信息，请参阅《Amazon Inspector 用户指南》中的查看 Amazon Inspector 调查发现的详细信息。Amazon Inspector 控制台中的调查发现详细信息的修复部分会指明您可以运行哪些命令来更新软件包。

   b. 更新基本容器映像

      定期重建和更新基础容器映像，使您的容器保持最新状态。重建映像时，请不要包括不必要的组件以减少攻击面。有关重建容器映像的说明，请参阅 Rebuild your images often。

Amazon ECS 服务的一个容器存在软件漏洞

Amazon ECS 容器上安装的软件包可能会暴露于常见漏洞和暴露（CVE）。与高优先级漏洞相比，低优先级漏洞表示严重性或可利用性较低的安全隐患。虽然这些漏洞不会造成直接风险，但攻击者仍可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。

更新受影响的容器映像

查看特征的漏洞选项卡中的参考部分。供应商文档可能包括具体的修复指导。

请按照以下一般准则进行适当的修复：

- 更新您的容器映像以使用受影响软件包的修补版本。
- 将应用程序中受影响的依赖项更新为其最新的安全版本。

更新容器映像后，请将其推送到您的容器注册表，并更新 Amazon ECS 任务定义以使用新映像。

未来注意事项

为进一步增强容器映像的安全状态，请考虑遵循 Amazon ECS 任务和容器安全最佳实践。可以将 Amazon Inspector 配置为自动扫描容器上的 CVE。Amazon Inspector 还可以与 Security Hub 集成以实现自动修复。请考虑使用 Systems Manager Maintenance Windows 实施定期修补计划，以尽量减少对容器的中断。

Amazon ECS 服务有一个装有 End-Of-Life 操作系统的容器

Amazon ECS 容器依赖的是已停产的操作系统，该操作系统不再由原始开发者支持或维护。这会使容器面临安全漏洞和潜在攻击。当操作系统寿命结束时，供应商通常会停止发布新的安全公告。现有的安全公告也可以从供应商 Feed 中删除。因此，Amazon Inspector可能会停止为已知的CVE生成调查结果，从而在安全覆盖方面造成进一步的漏洞。

请参阅《亚马逊检查员用户指南》中的已停产操作系统，了解有关亚马逊检查员可以检测到的已使用寿命终止的操作系统的信息。

更新到支持的操作系统版本

我们建议更新到支持的操作系统版本。在风险调查结果中，打开资源以访问受影响的资源。在更新容器映像中的操作系统版本之前，请查看 Amazon Inspector 用户指南中支持的操作系统中的可用版本，了解当前支持的操作系统版本列表。更新容器映像后，请将其推送到您的容器注册表，并更新 Amazon ECS 任务定义以使用新映像。

Amazon ECS 服务有一个装有恶意软件包的容器

恶意软件包是包含有害代码的软件组件，旨在危害系统和数据的机密性、完整性和可用性。恶意软件包会对您的 Amazon ECS 容器映像构成活跃而严重的威胁，因为攻击者可以在不利用漏洞的情况下自动执行恶意代码。按照安全最佳实践， AWS 建议移除恶意软件包，以保护您的容器免受潜在攻击。

移除恶意软件包

在特征的 “漏洞” 选项卡的 “参考” 部分中查看恶意软件包的详细信息，以了解威胁。从您的容器镜像中移除已识别的恶意软件包，然后对其进行重建。有关更多信息，请参阅 AWS Amazon ECS API 参考中的 ContainerDependency。更新容器映像后，请将其推送到您的容器注册表，并更新 Amazon ECS 任务定义以使用新映像。有关更多信息，请参阅 Amazon ECS 开发人员指南中的使用控制台更新AWS Amazon ECS 任务定义。

修复 Amazon EKS 集群的暴露

AWS Security Hub 可以生成亚马逊 Elastic Kubernetes Service（亚马逊 EKS）集群的曝光结果。

暴露调查发现中涉及的 Amazon EKS 集群及其识别信息列在调查发现详细信息的资源部分中。您可以在 Security Hub 控制台上检索这些资源详细信息，也可以通过 Security Hub CSPM AP GetFindingsV2I 的操作以编程方式检索这些资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- Amazon EKS 集群的错误配置特征
  - Amazon EKS 集群允许公开访问
  - Amazon EKS 集群使用不受支持的 Kubernetes 版本
  - Amazon EKS 集群使用未加密的 Kubernetes 密钥
- Amazon EKS 集群的漏洞特征
  - Amazon EKS 集群的一个容器存在可通过网络利用的软件漏洞，被利用的可能性很高
  - Amazon EKS 集群的一个容器存在软件漏洞
  - Amazon EKS 集群有一个装有 End-Of-Life 操作系统的容器
  - Amazon EKS 集群有一个装有恶意软件包的容器
  - EKS 集群有恶意文件

Amazon EKS 集群的错误配置特征

以下是 Amazon EKS 集群的错误配置特征和建议的修复步骤。

Amazon EKS 集群允许公开访问

Amazon EKS 集群端点是您用来与集群的 Kubernetes API 服务器进行通信的端点。默认情况下，此端点对互联网是公开的。公共端点会增加您的攻击面和未经授权访问您的 Kubernetes API 服务器的风险，从而可能允许攻击者访问或修改集群资源或访问敏感数据。遵循安全最佳实践， AWS 建议将对 EKS 集群终端节点的访问限制为仅必要的 IP 范围。

修改端点访问

在暴露调查发现中，打开资源。这将打开受影响的 Amazon EKS 集群。您可以将集群配置为使用私有访问、公开访问或两者兼而有之。通过私有访问，源自集群 VPC 内的 Kubernetes API 请求将使用私有 VPC 端点。通过公开访问，源自集群 VPC 外部的 Kubernetes API 请求将使用公有端点。

修改或移除对集群的公开访问

要修改现有集群的端点访问，请参阅《Amazon Elastic Kubernetes Service 用户指南》中的修改集群端点访问。根据特定 IP 范围或安全组实施更严格的规则。如果需要有限的公开访问，请将访问限制于特定 CIDR 数据块范围或使用前缀列表。

Amazon EKS 集群使用不受支持的 Kubernetes 版本

Amazon EKS 对每个 Kubernetes 版本的支持时间都是有限的。使用不受支持的 Kubernetes 版本运行集群可能会使您的环境面临安全漏洞，因为过时的版本将不再发布 CVE 补丁。不受支持的版本可能包含攻击者可以利用的已知安全漏洞，并且缺少新版本中可能提供的安全功能。遵循安全最佳实践，AWS 建议您不断更新您的 Kubernetes 版本。

更新 Kubernetes 版本

在暴露调查发现中，打开资源。这将打开受影响的 Amazon EKS 集群。在更新集群之前，请查看《Amazon Elastic Kubernetes Service 用户指南》中的标准支持上的可用版本，了解当前支持的 Kubernetes 版本列表。

Amazon EKS 集群使用未加密的 Kubernetes 密钥

默认情况下，Kubernetes 密钥以未加密形式存储在 API 服务器的底层数据存储（etcd）中。任何具有 API 访问权限或 etcd 访问权限的人都可以检索或修改密钥。为防止发生这种情况，您应该对 Kubernetes 密钥进行静态加密。如果 Kubernetes 密钥未加密，一旦 etcd 遭到入侵，它们就很容易受到未经授权的访问。由于密钥通常包含密码和 API 令牌等敏感信息，因此泄露密钥可能会导致未经授权访问其他应用程序和数据。按照安全最佳实践， AWS 建议对存储在 Kubernetes 密钥中的所有敏感信息进行加密。

加密 Kubernetes 密钥

Amazon EKS 支持使用 KMS 密钥通过信封加密对 Kubernetes 密钥进行加密。要为您的 EKS 集群启用 Kubernetes 密钥加密，请参阅《Amazon EKS 用户指南》中的在现有集群上使用 KMS 加密 Kubernetes 密钥。

Amazon EKS 集群的漏洞特征

以下是 Amazon EKS 集群的漏洞特征。

Amazon EKS 集群的一个容器存在可通过网络利用的软件漏洞，被利用的可能性很高

EKS 集群上安装的软件包可能会暴露于常见漏洞和暴露（CVE）。关键 CVE 会给您的 AWS 环境带来严重的安全风险。未经授权的用户可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。利用可能性较高的严重漏洞代表直接的安全威胁，因为漏洞利用代码可能已经公开并

被攻击者或自动扫描工具积极使用。按照安全最佳实践， AWS 建议修补这些漏洞以保护您的实例免受攻击。

更新受影响的实例

将容器映像更新到包含已识别漏洞的安全修复的较新版本。这通常包括使用更新的基础映像或依赖项重建容器映像，然后将新映像部署到 Amazon EKS 集群。

Amazon EKS 集群的一个容器存在软件漏洞

Amazon EKS 集群上安装的软件包可能会暴露于常见漏洞和暴露（CVE）。与严重 CVE 相比，非严重 CVE 代表安全隐患，其严重性或可利用性较低。虽然这些漏洞不会造成直接风险，但攻击者仍可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。按照安全最佳实践， AWS 建议修补这些漏洞以保护您的实例免受攻击。

更新受影响的实例

将容器映像更新到包含已识别漏洞的安全修复的较新版本。这通常包括使用更新的基础映像或依赖项重建容器映像，然后将新映像部署到 Amazon EKS 集群。

Amazon EKS 集群有一个装有 End-Of-Life 操作系统的容器

Amazon EKS 容器映像依赖于已停产的操作系统，该操作系统不再由原始开发者支持或维护。这会使容器面临安全漏洞和潜在攻击。当操作系统寿命结束时，供应商通常会停止发布新的安全公告。现有的安全公告也可以从供应商 Feed 中删除。因此，Amazon Inspector可能会停止为已知的CVE生成调查结果，从而在安全覆盖方面造成进一步的漏洞。

请参阅《亚马逊检查员用户指南》中的已停产操作系统，了解有关亚马逊检查员可以检测到的已使用寿命终止的操作系统的信息。

更新到支持的操作系统版本

我们建议更新到支持的操作系统版本。在风险调查结果中，打开资源以访问受影响的资源。在更新容器映像中的操作系统版本之前，请查看 Amazon Inspector 用户指南中支持的操作系统中的可用版本，了解当前支持的操作系统版本列表。更新容器映像后，重新构建容器并将其重新部署到 Amazon EKS 集群。

Amazon EKS 集群有一个装有恶意软件包的容器

恶意软件包是包含有害代码的软件组件，旨在危害系统和数据的机密性、完整性和可用性。恶意软件包会对您的 Amazon EKS 集群构成严重威胁，因为攻击者可以在不利用漏洞的情况下自动执行恶意代码。按照安全最佳实践， AWS 建议移除恶意软件包，以保护您的集群免受潜在攻击。

移除恶意软件包

在特征的 “漏洞” 选项卡的 “参考” 部分中查看恶意软件包的详细信息，以了解威胁。从您的容器镜像中移除已识别的恶意软件包。然后，删除带有受损图像的 pod。更新您的 Kubernetes 部署以使用更新的容器镜像。然后，部署您的更改并重新部署 pod。

EKS 集群有恶意文件

恶意文件包含有害代码，旨在危害系统和数据的机密性、完整性和可用性。恶意文件会对您的集群构成严重威胁，因为攻击者可以在不利用漏洞的情况下自动执行恶意代码。按照安全最佳实践， AWS 建议删除恶意文件以保护您的集群免受潜在攻击。

移除恶意文件

要识别包含恶意文件的特定亚马逊 Elastic Block Store (Amazon EBS) 卷，请查看该特征发现详情的 “资源” 部分。识别出带有恶意文件的卷后，请移除已识别的恶意文件。删除恶意文件后，请考虑执行扫描，以确保可能由恶意文件安装的所有文件都已删除。有关更多信息，请参阅 GuardDuty中的启动 On-demand 恶意软件扫描。

修复 IAM 用户的暴露

AWS Security Hub 可以为 AWS Identity and Access Management (IAM) 用户生成曝光结果。

在 Security Hub 控制台上，暴露调查发现中涉及的 IAM 用户及其识别信息列在调查发现详细信息的资源部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

IAM 最佳实践建议您创建 IAM 角色或使用与身份提供商的联合身份验证，以便使用临时凭证访问 AWS ，而不是创建单独的 IAM 用户。如果这对您的组织和使用案例来说是一个选择，我们建议您切换到角色或联合身份验证，而不是使用 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的 IAM 用户。

目录

- IAM 用户的错误配置特征
  - IAM 用户拥有具有管理访问权限的策略
  - IAM 用户未启用 MFA
  - IAM 用户拥有拥有管理权限的策略 AWS 服务
  - 这些区域有： AWS IAM 用户的账户的密码策略较弱
  - IAM 用户拥有未轮换的访问密钥
  - IAM 用户有一个策略允许不受限制地访问 KMS 密钥解密
- IAM 用户未使用的访问特征

IAM 用户的错误配置特征

以下是 IAM 用户的错误配置特征和建议的修复步骤。

IAM 用户拥有具有管理访问权限的策略

IAM 策略在 IAM 用户访问资源时会向其授予一组权限。管理策略为 IAM 用户提供了访问 AWS 服务和资源的广泛权限。如果凭证遭到泄露，提供完整的管理权限而不是用户所需的最低权限，可能会扩大攻击范围。根据标准安全原则， AWS 建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

1. 查看和识别管理策略 – 在资源 ID 中，识别 IAM 角色名称。前往 IAM 控制面板，然后选择已识别的角色。查看附加到 IAM 用户的权限策略。如果该策略是 AWS 托管策略，请查找`AdministratorAccess`或`IAMFullAccess`。否则，在策略文档中，查找包含具有 `"Action": "*"` 而不是 `"Resource": "*"` 的 `"Effect": "Allow"` 语句的语句。
2. 实施最低权限访问 – 将服务管理策略替换为仅授予用户运行所需的特定权限的策略。有关 IAM 策略的安全最佳实践的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的应用最低权限许可。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的外部和未使用的访问的调查发现。
3. 安全配置注意事项 – 如果实例需要服务管理权限，请考虑实施以下额外安全控制措施来降低风险：
   - Multi-factor 身份验证 (MFA) — MFA 要求使用其他形式的身份验证，从而增加了额外的安全层。即使凭证遭到泄露，这也有助于防止未经授权的访问。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的需要多重身份验证（MFA）。

- IAM 条件 – 通过设置条件元素，您可以基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用 IAM 策略中的条件进一步限制访问权限。
- 权限边界 – 权限边界规定了角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用权限边界在账户内委派权限管理。

IAM 用户未启用 MFA

Multi-factor 身份验证 (MFA) 在用户名和密码之上增加了一层额外的保护。启用 MFA 并且 IAM 用户登录 AWS 网站后，系统会提示他们输入用户名、密码和来自其 MFA AWS 设备的身份验证码。身份验证委托人必须拥有发放具有时效性的密钥的设备，并且必须知道凭证。如果没有 MFA，如果用户的密码被泄露，攻击者就会获得对用户权限的 AWS 完全访问权限。按照标准安全原则， AWS 建议为所有具有 AWS 管理控制台 访问权限的账户和用户启用 MFA。

查看 MFA 类型

AWS 支持以下 MFA 类型：

- 通行密钥和安全密钥
- 虚拟身份验证器应用程序
- 硬件 TOTP 令牌

虽然使用物理设备进行身份验证通常能提供更严格的安全保护，但使用任何类型的 MFA 比禁用 MFA 更安全。

启用 MFA

要启用符合您要求的 MFA 类型，请参阅《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。请按照要实施的特定 MFA 类型的步骤进行操作。对于管理许多用户的组织，您可能需要强制使用 MFA，要求访问敏感资源时必须进行 MFA 验证。

IAM 用户拥有拥有管理权限的策略 AWS 服务

服务管理员策略为 IAM 用户提供了在特定 AWS 服务中执行所有操作的权限。这些策略通常包含用户履行其工作职能不需要的权限。如果向 IAM 用户提供服务管理员权限，而不是所需的最低权限集，一旦凭证遭到泄露，就会扩大攻击范围。根据标准安全原则， AWS 建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

查看和识别服务管理员策略

在资源 ID 中，识别 IAM 角色名称。前往 IAM 控制面板，然后选择已识别的角色。查看附加到 IAM 用户的权限策略。如果策略是 AWS 托管式策略，请查找 `AdministratorAccess` 或 `IAMFullAccess`。否则，在策略文档中，查找包含 `"Effect": "Allow" with "Action": "*" over "Resource": "*"` 语句的语句。

实施最低权限访问

将服务管理策略替换为仅授予用户运行所需的特定权限的策略。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。

安全配置注意事项

如果实例需要服务管理权限，请考虑实施以下额外安全控制措施来降低风险：

- MFA 通过要求其他形式的身份验证来增加额外安全保障。即使凭证遭到泄露，这也有助于防止未经授权的访问。
- 使用条件元素基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。
- 使用权限边界规定角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。

这些区域有： AWS IAM 用户的账户的密码策略较弱

密码策略通过强制执行 IAM 用户密码的最低复杂度要求，帮助防止未经授权的访问。如果没有严格的密码策略，用户账户可能因密码猜测或暴力攻击而遭到入侵的风险就会增加。遵循标准的安全原则，AWS 建议实施严格的密码策略，以确保用户创建难以猜测的复杂密码。

配置严格的密码策略

前往 IAM 控制面板并导航到“账户设置”。查看账户的当前密码策略设置，包括最小长度、所需的字符类型以及密码过期设置。

在设置密码策略时， AWS 建议至少遵循以下最佳实践：

- 至少需要一个大写字符。
- 至少需要一个小写字符。
- 至少需要一个符号。
- 至少需要一个数字。

- 至少需要八个字符。

其它安全注意事项

除了严格的密码策略外，请考虑以下其他安全措施：

- MFA 通过要求其他形式的身份验证来增加额外安全保障。即使凭证遭到泄露，这也有助于防止未经授权的访问。
- 设置条件元素基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。

IAM 用户拥有未轮换的访问密钥

访问密钥由访问密钥 ID 和允许以编程方式访问 AWS 资源的私有访问密钥组成。如果访问密钥长时间保持不变，一旦遭到泄露，就会增加未经授权访问的风险。遵循安全最佳实践， AWS 建议每 90 天轮换一次访问密钥，以最大限度地减少攻击者使用受损凭证的机会。

轮换访问密钥

在暴露调查发现中，打开资源。这将打开用户详细信息窗口。要轮换访问密钥，请参阅《IAM 用户指南》中的管理 IAM 用户的访问密钥。

IAM 用户有一个策略允许不受限制地访问 KMS 密钥解密

AWS KMS 使您能够创建和管理用于保护数据的加密密钥。如果 IAM 用户的证书遭到泄 AWS KMS 露，则允许对所有 KMS 密钥拥有不受限制的解密权限（例如`kms:Decrypt`或`kms:ReEncryptFrom`）的 IAM 策略可能会导致未经授权的数据访问。如果攻击者获得对这些凭证的访问权限，他们就有可能解密您环境中的任何加密数据，其中可能包括敏感数据。遵循安全最佳实践， AWS 建议通过将 AWS KMS 解密权限限制为仅限用户履行其工作职能所需的特定密钥来实现最低权限。

实施最低权限访问

在暴露调查发现中，打开资源。此时将打开 IAM 策略窗口。查找 KMS 中允许 kms:Decrypt 或 `kms:ReEncryptFrom` 或 `KMS:*` 且资源规范为 `"*"` 的权限。更新政策，将 AWS KMS 解密权限限制为仅限所需的特定密钥。修改策略，将`"*"`资源替换为所需 AWS KMS 密钥的特定 ARN。

安全配置注意事项

请考虑添加条件来进一步限制何时可以使用这些权限。例如，您可以将解密操作限制在特定 VPC 端点或源 IP 范围。您还可以配置密钥策略，进一步限制哪些人可以使用特定的 KMS 密钥。

IAM 用户未使用的访问特征

当 IAM 用户拥有未使用的权限、访问密钥或密码时，Security Hub 可能会将这些作为上下文特征包含在该用户的曝光结果中。这些特征由服务托管的 IAM Access Analyzer 生成，可提供有关用户安全状况的其他背景信息。未使用的访问特征不是暴露发现的主要原因，但它们表明用户拥有的权限超出了所需的权限，如果用户的凭据遭到泄露，这会增加潜在的影响。

具体而言，对于未使用的权限，您可以生成最低权限策略建议，向您显示缩小范围的替换策略。有关更多信息，请参阅 the section called “政策建议”。

修复 Lambda 函数的暴露

AWS Security Hub 可以为 AWS Lambda (Lambda) 函数生成暴露结果。

在 Security Hub 控制台上，暴露调查发现中涉及的 Lambda 函数及其识别信息列在调查发现详细信息的资源部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- Lambda 函数的错误配置特征
  - Lambda 函数部署在 Amazon VPC 之外
  - 与 Lambda 函数关联的 IAM 角色具有管理访问策略
  - 与 Lambda 函数关联的 IAM 角色具有对服务的管理访问权限的策略 AWS
  - 无需授权即可通过 API Gateway 访问 Lambda 函数
- Lambda 函数的可访问性特征
  - 可以公开调用 Lambda 函数

- Lambda 函数的漏洞特征
  - Lambda 函数存在可通过网络利用的软件漏洞
  - Lambda 函数存在软件漏洞
  - Lambda 函数包含恶意软件包
  - Lambda 函数存在代码漏洞

Lambda 函数的错误配置特征

以下是 Lambda 函数的错误配置特征和建议的修复步骤。

Lambda 函数部署在 Amazon VPC 之外

默认情况下，部署 Lambda 函数时可以访问公共互联网。此默认配置使 Lambda 函数能够访问 AWS 服务端点和外部端点 APIs，但也使它们面临潜在的安全风险。具有互联网访问权限的函数可能会被用来泄漏数据、与未经授权的服务器进行通信，或者在遭到入侵后成为外部行为者的入口点。Amazon VPC 通过限制 Lambda 函数只能与您定义的私有网络内的资源通信来提供网络隔离。根据标准安全原则，我们建议在 VPC 内部署 Lambda 函数以通过网络隔离提高安全性。

将函数附加到 VPC

在暴露调查发现中，通过超链接打开资源。此时将打开 Lambda 函数窗口。要通过限制其网络访问权限来保护 Lambda 函数，请将其附加到具有适当网络控制的 VPC。在将您的函数附加到 VPC 之前，请规划其可能需要的任何 AWS 服务访问权限，因为没有 NAT 网关或 VPC 终端节点的私有子网中的函数将无法 AWS 访问服务。 APIs有关如何将 Lambda 函数附加到您账户中的 Amazon VPC 的信息，请参阅将 Lambda 函数附加到您的 AWS 账户中的 Amazon VPC。如果您的功能需要从私有子网内访问服务，请考虑使用 VPC 终端节点进行 AWS 服务连接，无需访问 Internet。如果您需要从私有子网进行出站互联网连接，请配置 NAT 网关。

与 Lambda 函数关联的 IAM 角色具有管理访问策略

管理访问策略为 Lambda 函数提供了对 AWS 服务和资源的广泛权限。这些策略通常包含功能不需要的权限。如果在 Lambda 函数上提供具有管理访问策略的 IAM 身份，而不是执行角色所需的最低权限集，则当函数遭到入侵时，可能会扩大攻击范围。根据标准安全原则， AWS 建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

1. 查看和识别管理策略

   在暴露调查发现中，识别角色名称。前往 IAM 控制面板，找到具有先前识别的角色名称的角色。查看附加到 IAM 角色的权限策略。如果该策略是 AWS 托管策略，请查

找AdministratorAccess或IAMFullAccess。否则，在策略文档中，查找同时包含 "Effect": "Allow", "Action": "*" 和 "Resource": "*" 语句的语句。

2. 实施最低权限访问

   将管理策略替换为仅授予函数运行所需的特定权限的策略。有关 IAM 角色的安全最佳实践的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的应用最低权限许可。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的外部和未使用的访问的调查发现。或者，您可以创建一个新的 IAM 角色，以避免影响使用现有角色的其他 Lambda 函数。在这种情况下，请创建一个新的 IAM 角色。然后将新角色与实例关联起来。有关替换函数的 IAM 角色的信息，请参阅《AWS Lambda 开发人员指南》中的更新函数的执行角色。

3. 安全配置注意事项

   如果实例需要管理访问权限，请考虑实施以下额外安全控制措施来降低风险：

   - 多重身份验证（MFA）– MFA 通过要求其他形式的身份验证来增加额外安全保障。即使凭证遭到泄露，这也有助于防止未经授权的访问。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的需要多重身份验证（MFA）。
   - IAM 条件 – 通过设置条件元素，您可以基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 策略中的条件进一步限制访问权限。
   - 权限边界 – 权限边界规定了角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用权限边界在账户内委派权限管理。

与 Lambda 函数关联的 IAM 角色具有对服务的管理访问权限的策略 AWS

服务管理策略允许 Lambda 函数在特定 AWS 服务中执行所有操作。这些策略通常会授予比函数运行所需更多的权限。如果带有服务管理策略的 Lambda 函数遭到入侵，攻击者可能会利用这些权限访问或修改您 AWS 环境中的敏感数据或服务。根据标准安全原则，我们建议您授予最低权限，这意味着您仅授予执行任务所需的权限。

1. 查看和识别管理策略

   在暴露调查发现中，识别 ARN 中的角色名称。前往 IAM 控制面板，找到角色名称。查看附加到角色的权限策略。如果该策略是 AWS 托管策略，请查找AdministratorAccess或IAMFullAccess。否则，在策略文档中，查找包含 "Effect": "Allow", "Action": "*" 和 "Resource": "*" 语句的语句。

2. 实施最低权限访问

   将管理策略替换为仅授予函数运行所需的特定权限的策略。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的应用最低权限许可。要识别不必要的权限，您可以使用 IAM Access Analyzer 来了解如何基于访问历史记录修改策略。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的外部和未使用的访问的调查发现。或者，您可以创建一个新的 IAM 角色，以避免影响使用现有角色的其他 Lambda 函数。在这种情况下，请创建一个新的 IAM 角色，然后将新的 IAM 角色与实例关联起来。有关替换函数的 IAM 角色的说明，请参阅《AWS Lambda 开发人员指南》中的更新函数的执行角色。

3. 安全配置注意事项

   如果实例需要服务级别的管理权限，请考虑实施以下额外安全控制措施来降低风险：

   - 多重身份验证（MFA）– MFA 通过要求其他形式的身份验证来增加额外安全保障。即使凭证遭到泄露，这也有助于防止未经授权的访问。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的需要多重身份验证（MFA）。
   - IAM 条件 – 通过设置条件元素，您可以基于源 IP 或 MFA 期限等因素限制何时以及如何使用管理权限。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用 IAM 策略中的条件进一步限制访问权限。
   - 权限边界 – 权限边界规定了角色可以拥有的最大权限，为具有管理访问权限的角色提供防护。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的使用许可边界委派权限管理。

无需授权即可通过 API Gateway 访问 Lambda 函数

未经授权的 API Gateway 方法允许任何有权访问 API 网关的调用者无需身份验证即可调用集成的 Lambda 函数。这种配置会带来安全风险，因为调用者可以在未经适当授权的情况下调用 Lambda 函数，从而可能导致滥用函数功能、消耗资源、访问敏感数据或未经授权的操作。虽然 API Gateway 可能具有网络级别的访问控制，但由于缺乏方法级授权，任何有权访问 API Gateway 的调用者都可以免费调用该函数。遵循安全最佳实践， AWS 建议为与 Lambda 函数集成的 API Gateway 方法实施适当的授权机制。

配置 API Gateway 身份验证

在曝光的 “资源” 选项卡中，单击 “打开资源” 超链接以访问 API Gateway 方法。查看当前的授权配置并实施适当的身份验证机制。API Gateway 支持多种身份验证选项，包括 AWS IAM、Amazon Cognito 用户池、Lambda 授权者和 API 密钥。选择最适合您的安全要求和用例的身份验证方法。有关配置身

份验证的详细说明，请参阅《API Gatew ay 开发者指南》中的 API Gateway 中控制和管理对 REST API 的访问权限。

Lambda 函数的可访问性特征

以下是 Lambda 函数的可访问性特征和建议的修复步骤。

可以公开调用 Lambda 函数

Lambda 基于资源的策略决定了谁可以调用您的函数。如果函数的资源策略包含 “*” 作为委托人（或者根本不包含委托人），则允许任何经过身份验证的 AWS 用户调用该函数。这会带来重大风险，特别是对于处理敏感数据、修改资源或拥有提升权限的函数。未经授权的用户可以利用此配置执行不需要的操作，从而可能暴露数据、操纵资源或滥用函数功能。根据安全最佳实践，我们建议仅允许授权主体访问 Lambda 函数。

修改函数的基于资源的策略

在暴露的资源选项卡中，通过超链接打开资源。此时将打开 Lambda 函数窗口。通过在基于资源的策略中仅指定授权 AWS 账户 IDs 或特定的 IAM 委托人（用户、角色或服务），限制对您的 Lambda 函数的访问。您只能以编程方式修改基于资源的策略。

Lambda 函数的漏洞特征

以下是 Lambda 函数的漏洞特征和建议的修复步骤。

Lambda 函数存在可通过网络利用的软件漏洞

Lambda 函数代码中使用的软件包可能包含很有可能被利用的常见漏洞和漏洞 (CVEs)。 CVEs 危急会给您的 AWS 环境带来严重的安全风险。攻击者可以利用这些未修补的漏洞来破坏数据的保密性、完整性或可用性，或访问其他系统。利用可能性较高的严重漏洞代表直接的安全威胁，因为漏洞利用代码可能已经公开并被攻击者或自动扫描工具积极使用。根据安全最佳实践，我们建议修补这些漏洞以保护您的函数免受攻击。

更新受影响的函数

查看特征的漏洞选项卡中的参考部分。供应商文档可能包括具体的修复指导。按照供应商推荐的过程，将易受攻击的库更新到其最新的安全版本。通常，修复工作流取决于您是通过上传 zip 文件来部署 Lambda 包，还是通过创建带有容器映像的 Lambda 函数来部署 Lambda 包。更新库后，请更新 Lambda 函数代码以使用修复后的版本。之后，请部署更新后的版本。

Lambda 函数存在软件漏洞

Lambda 函数通常使用第三方库和依赖项，这些库和依赖项可能包含安全漏洞，与严重漏洞相比，其严重性或可利用性较低。 CVEs虽然这些非关键漏洞可能不会立即被利用，但它们仍然代表着安全隐患，这些隐患可能会与其他漏洞关联在一起，从而危及您的函数。随着时间推移，还可能会出现新的漏洞利用技术，从而增加这些漏洞的风险。根据标准安全原则，我们建议修补这些漏洞以维护安全的环境。

查看特征的漏洞选项卡中的参考部分。供应商文档可能包括具体的修复指导。按照供应商推荐的过程，将易受攻击的库更新到其最新的安全版本。通常，修复工作流取决于您是通过上传 zip 文件来部署 Lambda 包，还是通过创建带有容器映像的 Lambda 函数来部署 Lambda 包。更新库后，请更新 Lambda 函数代码以使用修复后的版本。之后，请部署更新后的版本。

Lambda 函数包含恶意软件包

恶意软件包是包含有害代码的软件组件，旨在危害系统和数据的机密性、完整性和可用性。恶意软件包会对您的 Lambda 函数构成严重威胁，因为攻击者可以在不利用漏洞的情况下自动执行恶意代码。按照安全最佳实践， AWS 建议移除恶意软件包，以保护您的 Lambda 函数免受潜在攻击。

移除恶意软件包

在特征的 “漏洞” 选项卡的 “参考” 部分中查看恶意软件包的详细信息，以了解威胁。从您的函数代码和依赖项中移除已识别的恶意软件包。对于使用图层的函数，请检查是否在任何层中安装了恶意软件包，然后将其删除。更新您的部署包或容器映像以排除恶意软件包，然后部署更新的版本。有关说明，请参阅将 Lambda 函数部署为.zip 文件存档的.zip 文件存档或使用容器映像创建容器映像的 Lambda 函数。

Lambda 函数存在代码漏洞

Lambda 函数应用程序代码包含可能被威胁行为者利用的安全漏洞。代码漏洞包括数据泄露、注入缺陷、缺少加密以及通过自动代码分析发现的弱加密。这些漏洞会给您的 AWS 环境带来安全风险，因为攻击者可以利用它们来破坏数据的机密性、完整性或可用性，或者访问其他系统。代码漏洞代表安全漏洞，这些漏洞可能与其他攻击向量链接在一起，从而危害您的功能。遵循安全最佳实践， AWS 建议修复这些代码漏洞，以保护您的函数免受攻击。

更新受影响的函数

查看特征的漏洞选项卡中的参考部分。Amazon Inspector 的调查结果可能包括具体的补救指南和显示漏洞代码位置的代码片段。使用提供的代码块或实施安全编码实践，解决函数 plug-and-play代码中已确定的安全问题。在采用代码补救建议之前，请务必对其进行审查，因为您可能需要对其进行编辑以确保代码按预期执行。修复漏洞后，更新 Lambda 函数代码以使用更正后的版本。有关说明，请参阅《AWS Lambda 开发人员指南》中的更新函数代码。之后，请部署更新后的版本。有关说明，请参阅将 Lambda 函数部署为.zip 文件存档的.zip 文件存档或使用容器映像创建容器映像的 Lambda 函数。

有关亚马逊 Inspector 代码扫描的更多信息，请参阅亚马逊 Inspector 用户指南中的亚马逊 Inspector Lambda 代码扫描。

修复 Amazon RDS 实例和集群面临的风险

AWS Security Hub 可以为 Amazon RDS 实例和集群生成暴露调查结果。

在 Security Hub 控制台上，暴露发现中涉及的 Amazon RDS 实例或集群及其识别信息列在发现详情的“资源” 部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- Amazon RDS 实例和集群的配置错误特征
  - Amazon RDS 数据库实例配置为公开访问
  - Amazon RDS 数据库集群有一个公开共享的快照
  - Amazon RDS 数据库实例有一个公开共享的快照
  - Amazon RDS 数据库实例具有未进行静态加密的快照
  - Amazon RDS 数据库集群具有未进行静态加密的快照
  - Amazon RDS 数据库实例具有开放式安全组
  - Amazon RDS 数据库实例已禁用 IAM 数据库身份验证
  - Amazon RDS 数据库实例使用默认管理员用户名
  - Amazon RDS 数据库集群使用默认管理员用户名
  - Amazon RDS 数据库实例已禁用自动次要版本升级
  - Amazon RDS 数据库实例已禁用自动备份
  - Amazon RDS 数据库实例已禁用删除保护

- Amazon RDS 数据库集群已禁用删除保护
- Amazon RDS 数据库实例对数据库引擎使用默认端口
- Amazon RDS 数据库实例不在备份计划的覆盖范围内

Amazon RDS 实例和集群的配置错误特征

下面介绍了 Amazon RDS 实例和集群的错误配置特征和补救步骤。

Amazon RDS 数据库实例配置为公开访问

具有公开访问权限的 Amazon RDS 实例可能通过其端点从互联网进行访问。虽然有时实例功能需要公开访问，但这种配置可能会成为尝试访问您的数据库的未经授权用户的潜在攻击向量。可公开访问的数据库可能遭受端口扫描、暴力攻击和漏洞利用尝试。根据标准安全原则，我们建议您限制数据库资源的公开暴露。

1. 修改公开访问设置

   在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。根据您的应用程序架构，评估数据库实例是否需要公开访问。有关更多信息，请参阅 Setting up public or private access in Amazon RDS。

Amazon RDS 数据库集群有一个公开共享的快照

任何人都可以访问公共快照 AWS 账户，这可能会将敏感数据暴露给未经授权的用户。任何人 AWS 账户 都有权复制这些公共快照并从中创建数据库实例，这可能会导致数据泄露或未经授权的数据访问。按照安全最佳实践，我们建议仅允许受信任 AWS 账户 的组织访问您的 Amazon RDS 快照。

1. 配置 Amazon RDS 快照以实现私有访问

在暴露调查发现中，通过超链接打开资源。有关如何修改快照共享设置的信息，请参阅 Amazon Aurora 用户指南中的共享快照。有关如何停止共享快照的信息，请参阅《Amazon Aurora 用户指南》中的停止快照共享。

Amazon RDS 数据库实例有一个公开共享的快照

任何人都可以访问公共快照 AWS 账户，这可能会将敏感数据暴露给未经授权的用户。任何人 AWS 账户 都有权复制这些公共快照并从中创建数据库实例，这可能会导致数据泄露或未经授权的数据访问。按照安全最佳实践，我们建议仅允许受信任 AWS 账户 的组织访问您的 Amazon RDS 快照。

配置 Amazon RDS 快照以实现私有访问

在暴露调查发现中，通过超链接打开资源。有关如何修改快照共享设置的信息，请参阅 Amazon R DS 用户指南中的共享数据库快照。有关如何停止共享快照的信息，请参阅 Amazon R DS 用户指南中的停止共享数据库快照。 。

Amazon RDS 数据库实例具有未进行静态加密的快照

如果未经授权访问存储层，则未加密的 Amazon RDS 数据库实例快照可能会泄露敏感数据。如果没有加密，快照中的数据可能会因未经授权访问而泄露。这会带来数据泄露和合规性违规的风险。根据安全最佳实践，我们建议对所有数据库资源及其备份进行加密以保持数据机密性。

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的快照。您无法直接加密现有的未加密快照。相反，请创建未加密快照的加密副本。有关详细说明，请参阅《Amazon Aurora 用户指南》中的数据库集群快照复制和加密 Amazon RDS 资源。

Amazon RDS 数据库集群具有未进行静态加密的快照

如果未经授权访问存储层，则未加密的 Amazon RDS 数据库集群快照可能会泄露敏感数据。如果没有加密，快照中的数据可能会因未经授权访问而泄露。这会带来数据泄露和合规性违规的风险。根据安全最佳实践，我们建议对所有数据库资源及其备份进行加密以保持数据机密性。

1. 创建快照的加密副本

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的快照。您无法直接加密现有的未加密快照。相反，请创建未加密快照的加密副本。有关详细说明，请参阅《Amazon Aurora 用户指南》中的数据库集群快照复制和加密 Amazon RDS 资源。

Amazon RDS 数据库实例具有开放式安全组

安全组充当 Amazon RDS 实例的虚拟防火墙以控制入站和出站流量。开放式安全组允许从任何 IP 地址进行不受限制的访问，这可能会使数据库实例遭受未经授权的访问和潜在工具。根据标准安全原则，我们建议将安全组访问限制在特定 IP 地址和端口，以维护最低权限原则。

查看安全组规则并评测当前配置

在暴露调查发现中，打开数据库实例安全组的资源。评估哪些端口已开放且可从广泛的范围 IP 地址（例如 (`0.0.0.0/0 or ::/0`)）访问。有关查看安全组详细信息的信息，请参阅DescribeSecurityGroups《亚马逊弹性计算云 API 参考》。

修改安全组规则

修改您的安全组规则，将访问限制于特定的受信任 IP 地址或范围。更新安全组规则时，请考虑通过为每个所需的源 IP 地址范围创建规则或限制对特定端口的访问来区分不同网段的访问要求。要修改安全

组规则，请参阅《Amazon EC2 用户指南》中的配置安全组规则。要修改现有 Amazon RDS 数据库实例的默认端口，请参阅《Amazon Aurora 用户指南》中的使用控制台、CLI 和 API 修改数据库集群。

Amazon RDS 数据库实例已禁用 IAM 数据库身份验证

IAM 数据库身份验证允许您使用 IAM 凭证（而不是数据库密码）对 Amazon RDS 数据库进行身份验证。这提供了多项安全优势，例如集中式访问管理、临时凭证以及无需在应用程序代码中存储数据库密码。IAM 数据库身份验证允许使用身份验证令牌而不是密码对数据库实例进行身份验证。因此，进出数据库实例的网络流量使用 SSL 进行加密。如果没有 IAM 身份验证，数据库通常依赖基于密码的身份验证，这可能会导致密码重复使用和弱密码。根据安全最佳实践，我们建议启用 IAM 数据库身份验证。

启用 IAM 数据库身份验证

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。您可以在数据库选项中启用 IAM 数据库身份验证。有关更多信息，请参阅《Amazon RDS 用户指南》中的启用和禁用 IAM 数据库身份验证。启用 IAM 身份验证后，请更新数据库实例，使其使用 IAM 身份验证而不是基于密码的身份验证。

Amazon RDS 数据库实例使用默认管理员用户名

对数据库实例使用默认用户名（例如“admin”、“root”）会增加安全风险，因为这些用户名广为人知，并且经常是暴力攻击的目标。默认用户名是可预测的，这使得未经授权的用户更容易尝试访问您的数据库。使用默认用户名时，攻击者只需要获取密码，而无需同时获取用户名和密码即可访问您的数据库。根据安全最佳实践，我们建议对数据库实例使用唯一管理员用户名，以通过模糊机制来增强安全性并降低未经授权访问尝试的风险。

配置唯一管理员用户名

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。请考虑哪些备份频率、保留期和生命周期规则最适合您的应用程序。

Amazon RDS 数据库集群使用默认管理员用户名

对数据库实例使用默认用户名（例如“admin”、“root”）会增加安全风险，因为这些用户名广为人知，并且经常是暴力攻击的目标。默认用户名是可预测的，这使得未经授权的用户更容易尝试访问您的数据库。使用默认用户名时，攻击者只需要获取密码，而无需同时获取用户名和密码即可访问您的数据库。根据安全最佳实践，我们建议对数据库实例使用唯一管理员用户名，以通过模糊机制来增强安全性并降低未经授权访问尝试的风险。

配置唯一管理员用户名

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。您无法更改现有 Amazon RDS 数据库实例的管理员用户名。要创建唯一的管理员名称，您需要创建一个具有自定义用户名的新数据库实例并迁移您的数据。

Amazon RDS 数据库实例已禁用自动次要版本升级

自动次要版本升级可确保您的 Amazon RDS 实例在次要引擎版本升级可用时自动接收升级。这些升级通常包括重要的安全补丁和错误修复，有助于维护数据库的安全性和稳定性。您的数据库面临运行已知安全漏洞的风险，这些漏洞已在较新的次要版本中修复。如果没有自动更新，数据库实例可能会在发现新 CVEs 漏洞时积累安全漏洞。根据安全最佳实践，我们建议为所有 Amazon RDS 实例启用自动次要版本升级。

启用自动次要版本升级

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。您可以在维护和备份选项卡中查看自动次要升级设置。有关更多信息，请参阅 Amazon RDS for MySQL 的自动次要版本升级。您也可以将维护时段配置为在数据库活动较少的时期内进行。

Amazon RDS 数据库实例已禁用自动备份

自动备份为您的 Amazon RDS 实例提供 point-in-time恢复，使您可以将数据库还原到保留期内的任意点。如果禁用自动备份，则当发生恶意删除、数据损坏或其他数据丢失情况时，您将面临数据丢失的风险。如果发生勒索软件攻击、数据库表删除或损坏等恶意活动，则由于能够恢复到事件发生之前的时间点，因此可以减少从事件恢复所需的时间。根据安全最佳实践，我们建议对所有生产数据库启用自动备份并设置适当的保留期。

Amazon RDS 数据库实例已禁用删除保护

数据库删除保护是一项有助于防止数据库实例被删除的功能。如果禁用删除保护，任何拥有足够权限的用户都可以删除您的数据库，这可能会导致数据丢失或应用程序停机时间。攻击者可以删除您的数据库，导致服务中断、数据丢失和恢复时间增加。根据安全最佳实践，我们建议为 RDS 数据库实例启用删除保护以防止恶意删除。

为 Amazon RDS 数据库集群启用删除保护

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库集群。

Amazon RDS 数据库集群已禁用删除保护

数据库删除保护是一项有助于防止数据库实例被删除的功能。如果禁用删除保护，任何拥有足够权限的用户都可以删除您的数据库，这可能会导致数据丢失或应用程序停机时间。攻击者可以删除您的数据

库，导致服务中断、数据丢失和恢复时间增加。根据安全最佳实践，我们建议为 RDS 数据库集群启用删除保护以防止恶意删除。

为 Amazon RDS 数据库集群启用删除保护

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库集群。

Amazon RDS 数据库实例对数据库引擎使用默认端口

对数据库引擎使用默认端口的 Amazon RDS 实例可能会面临更高的安全风险，因为这些默认端口广为人知，并且经常是自动扫描工具的目标。将数据库实例修改为使用非默认端口时会通过模糊机制增加额外安全层，使未经授权的用户更难对您的数据库执行自动或针对性攻击。默认端口经常会被未经授权的人员扫描，这可能会导致您的数据库实例成为攻击目标。根据安全最佳实践，我们建议将默认端口更改为自定义端口以降低自动攻击或定向攻击的风险。

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。

更新应用程序连接字符串

更改端口后，请更新所有连接到 Amazon RDS 实例的应用程序和服务，以使用新的端口号。

Amazon RDS 数据库实例不在备份计划的覆盖范围内

AWS Backup 是一项完全托管的备份服务，可集中和自动备份数据。 AWS 服务如果您的数据库实例不在备份计划的覆盖范围内，则在发生恶意删除、数据损坏或其他数据丢失情况时，您可能会丢失数据。如果发生勒索软件攻击、数据库表删除或损坏等恶意活动，则由于能够恢复到事件发生之前的时间点，因此可以减少从事件恢复所需的时间。根据安全最佳实践，我们建议将 Amazon RDS 实例纳入备份计划以确保数据保护。

为数据库实例创建和分配备份计划

在暴露调查发现中，通过超链接打开资源。此时将打开受影响的数据库实例。请考虑哪些备份频率、保留期和生命周期规则最适合您的应用程序。

修复 Amazon S3 存储桶的暴露

AWS Security Hub 可以生成亚马逊简单存储服务 (S3) 存储桶的风险调查结果。

在 Security Hub 控制台上，暴露调查发现中涉及的 Amazon S3 存储桶及其识别信息列在调查发现详细信息的资源部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行更多咨询。

目录

- Amazon S3 存储桶的错误配置特征
  - Amazon S3 存储桶已禁用版本控制
  - Amazon S3 存储桶已禁用对象锁定
  - Amazon S3 存储桶未使用 AWS KMS 密钥进行静态加密
  - 受版本控制的 Amazon S3 存储桶上已禁用多重身份验证（MFA）删除
  - Amazon S3 存储桶允许其他 AWS 账户的委托人修改存储桶权限
- Amazon S3 存储桶的可访问性特征
  - Amazon S3 存储桶具有公共读取权限
  - Amazon S3 存储桶具有公共写入权限
- Amazon S3 存储桶的敏感数据特征
  - Amazon S3 存储桶的敏感数据特征

Amazon S3 存储桶的错误配置特征

以下是 Amazon S3 存储桶的错误配置特征和建议的修复步骤。

Amazon S3 存储桶已禁用版本控制

Amazon S3 版本控制可帮助您在同一个存储桶中保存对象的多个变体。禁用版本控制后，Amazon S3 只存储每个对象的最新版本，这意味着如果对象被意外或恶意删除或覆盖，则无法恢复。启用版本控制的存储桶可防止意外删除、应用程序故障以及勒索软件攻击等安全事件，在这些情况下可能会发生未经授权的数据修改或删除。根据安全最佳实践，我们建议对包含重要数据的存储桶启用版本控制，因为这些数据如果丢失则将难以或无法重新创建。

1. 启用版本控制 – 要在存储桶上启用 Amazon S3 版本控制，请参阅《Amazon Simple Storage Service 用户指南》中的在存储桶上启用版本控制。启用版本控制时，请考虑实施生命周期规则来管理存储，因为版本控制会维护对象的多个副本。

Amazon S3 存储桶已禁用对象锁定

Amazon S3 对象锁定为 Amazon S3 对象提供了 write-once-read-many (WORM) 模型，可防止它们在固定期限内或无限期地被删除或覆盖。禁用对象锁定后，您的对象可能容易遭受意外或恶意删除、修改或勒索软件加密。对象锁定对于遵守监管要求（需要不可变数据存储）以及防范勒索软件等可能试图加密数据的复杂威胁尤为重要。启用对象锁定后，您可以强制执行保留策略作为额外数据保护层，并为您的关键数据创建不可变的备份策略。根据安全最佳实践，我们建议启用对象锁定以防止恶意修改对象。

1. 请注意，只能在创建新的存储桶时启用对象锁定，因此您需要创建一个启用对象锁定的新存储桶。对于大型迁移，请考虑使用批量操作将对象复制到新存储桶。在锁定任何对象之前，您还必须在存储桶上启用 Amazon S3 版本控制和对象锁定。由于只能在新存储桶上启用对象锁定，因此您需要将现有数据迁移到已启用对象锁定的新存储桶。配置 Amazon S3 对象锁 — 有关如何在存储桶上配置对象锁的信息，请参阅亚马逊简单存储服务用户指南中的配置 Amazon S3 对象锁。设置对象锁定后，请根据您的环境选择合适的保留模式。

Amazon S3 存储桶未使用 AWS KMS 密钥进行静态加密

Amazon S3 应用具有 Amazon S3 托管式密钥的服务器端加密作为所有新存储桶的默认加密级别。虽然 Amazon S3 托管密钥提供强大的加密保护，但它提供的访问控制和审计功能级别与 AWS Key Management Service 密钥不同。使用 KMS 密钥时，访问对象需要同时拥有 Amazon S3 存储桶和加密该对象的 KMS 密钥的权限。这对于敏感数据尤其重要，在这些数据中，您需要精细控制谁可以访问加密对象，并对加密密钥使用情况进行全面的审核记录。根据安全最佳实践，我们建议使用 KMS 密钥对包含敏感数据的存储桶进行加密，或者将其用于具有严格合规性要求的环境。

1. 配置 Amazon S3 存储桶密钥

   要将存储桶配置为对新对象使用 Amazon S3 存储桶密钥，请参阅《Amazon Simple Storage Service 用户指南》中的将存储桶配置为将 Amazon S3 存储桶密钥与 SSE-KMS 结合使用于新对象。有关如何加密现有对象的信息，请参阅 AWS 存储博客中的使用 Amazon S3 批处理操作加密对象。

实施 AWS KMS 加密时，请考虑以下几点：

- 密钥管理-决定使用 AWS 托管密钥还是客户托管密钥 (CMK)。 CMKs 让客户完全控制密钥的生命周期和使用情况。有关这两种密钥之间区别的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 AWS KMS keys。
- 密钥轮换 – 要采取其他安全措施，请为您的 KMS 密钥启用自动密钥轮换。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 Enable automatic key rotation。

受版本控制的 Amazon S3 存储桶上已禁用多重身份验证（MFA）删除

多重身份验证（MFA）删除可为您的 Amazon S3 存储桶提供额外安全保护层。它对于破坏性 Amazon S3 操作需要多重身份验证。禁用 MFA 删除后，具有适当权限的用户无需额外身份验证即可永久删除对象版本或暂停存储桶上的版本控制。启用 MFA 删除有助于防止未经授权或意外删除您的数据，从而增强对勒索软件攻击、内部威胁和操作错误的防护。MFA 删除对于包含关键数据或合规性敏感数据的存储桶尤其有价值，这些数据必须防止未经授权的删除。根据安全最佳实践，我们建议为 Amazon S3 存储桶启用 MFA。

1. 查看 MFA 类型

   AWS 支持以下 MFA 类型。虽然使用物理设备进行身份验证通常能提供更严格的安全保护，但使用任何类型的 MFA 比禁用 MFA 更安全。

2. 在资源策略级别强制执行 MFA

   在存储桶策略中使用 `aws:MultiFactorAuthAge` 条件键，以要求对敏感操作进行 MFA。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的需要 MFA。

3. 启用 MFA

   要启用 MFA 删除，请确保在 Amazon S3 存储桶上启用版本控制。仅已启用版本控制的存储桶支持 MFA 删除。有关如何启用 Amazon S3 版本控制的信息，请参阅《Amazon Simple Storage Service 用户指南》中的在存储桶上启用版本控制。无法通过 Amazon S3 控制台启用 MFA 删除。您必须使用 Amazon S3 API 或 AWS CLI。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中配置 MFA 删除。

Amazon S3 存储桶允许其他 AWS 账户的委托人修改存储桶权限

Amazon S3 存储桶策略控制对存储桶和对象的访问。当存储桶策略允许其他 AWS 账户的委托人修改存储桶权限时，未经授权的用户可以重新配置您的存储桶。如果外部委托人凭证遭到泄露，未经授权的用户可以控制您的存储桶，从而导致数据泄露或服务中断。遵循标准的安全原则， AWS 建议您将权限管理操作仅限于受信任的委托人。

1. 查看和识别存储桶策略

   在曝光中，在 ARN 字段中标识 Amazon S3 存储桶。在 Amazon S3 控制台中，选择存储桶，然后导航至权限选项卡以查看存储桶策略。查看附加到存储桶的权限策略。查找授予 `s3:PutBucketPolicy`, `s3:PutBucketAcl`, `s3:DeleteBucketPolicy`, `s3:*` 等操作的策略语句，或者允许访问您账户之外的主体的策略语句，如主体语句中所述。

2. 修改存储桶策略

   修改存储桶策略以删除或限制授予其他 AWS 账户的操作：

   - 移除向外部账户授予权限管理操作的策略语句。
   - 如果需要跨账户访问，请将宽泛权限 (`s3:*`) 替换为不包含存储桶权限管理的特定操作。

   有关修改存储桶策略的信息，请参阅《亚马逊简单存储服务用户指南》中的使用 Amazon S3 控制台添加存储桶策略。

Amazon S3 存储桶的可访问性特征

以下是 Amazon S3 存储桶的可访问性特征和建议的修复步骤。

Amazon S3 存储桶具有公共读取权限

具有公共读取权限的 Amazon S3 存储桶允许互联网上的任何人查看您的存储桶内容。虽然这对于公开访问的网站或共享资源来说可能是必要的，但如果存储桶包含敏感数据，则可能会造成安全风险。公共读取权限可能导致未经授权的查看和下载，如果敏感数据存储在这些存储桶中，则可能导致数据泄露。遵循标准安全原则， AWS 建议限制必要的用户和系统才能访问 Amazon S3 存储桶。

1. 在存储桶级别阻止公开访问

   Amazon S3 提供阻止公共访问设置，无论存储桶策略如何，都可以在存储桶和账户级别进行配置，以防止公开访问或 ACLs。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的阻止对 Amazon S3 存储的公共访问。阻止公开访问后，请检查您的存储桶访问控制配置，以确保其符合您的访问要求。然后查看您的 Amazon S3 存储桶策略，明确定义谁可以访问您的存储桶。有关存储桶策略的示例，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 存储桶策略的示例。

2. 替代访问方法

   如果需要公共读取权限，请考虑以下更安全的替代方案：

   - CloudFront— CloudFront 与原始访问身份 (OAI) 或源访问控制 (OAC) 一起使用，以允许从私有 Amazon S3 存储桶进行读取访问。这种替代方案限制了对您的 Amazon S3 存储桶的直接访问，

同时允许通过 CloudFront公开访问内容。有关更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amaz on S3 来源的访问。

- 预签名 URLs-使用预签名 URLs 来临时访问特定对象。有关更多信息，请参阅《Amazon CloudFront 开发者指南》 URLs中的使用预签名共享对象。

Amazon S3 存储桶具有公共写入权限

具有公共写入权限的 Amazon S3 存储桶允许互联网上的任何人上传、修改或删除您的存储桶中的对象。这会造成严重的安全风险，包括有人可能上传恶意文件、修改现有文件和删除数据。公共写入权限会造成可被攻击者利用的安全漏洞。遵循标准安全原则， AWS 建议将对 Amazon S3 存储桶的写入权限限制为仅限必要的用户和系统。

1. 在账户和存储桶级别阻止公开访问

   Amazon S3 提供了封锁公有访问设置，可以在存储桶和账户级别配置这些设置，无论存储桶策略如何，都可防止公开访问或 ACLs。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的阻止对 Amazon S3 存储的公共访问。

2. 修改存储桶策略

   要更精细地移除公共写入权限，请查看存储桶策略。您可以查找 `s3:PutObject`、`s3:DeleteObject` 或 `s3:*`。有关管理存储桶策略的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 的存储桶策略。

3. 替代访问方法

   如果需要公共读取权限，请考虑以下更安全的替代方案：

   - CloudFront— CloudFront 与原始访问身份 (OAI) 或源访问控制 (OAC) 一起使用，以允许从私有 Amazon S3 存储桶进行读取访问。这种替代方案限制了对您的 Amazon S3 存储桶的直接访问，同时允许通过 CloudFront公开访问内容。有关更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amaz on S3 来源的访问。
   - 预签名 URLs-使用预签名 URLs 来临时访问特定对象。有关更多信息，请参阅 Amazon 简单存储服务用户指南 URLs中的使用预签名共享对象。

Amazon S3 存储桶的敏感数据特征

以下是 Amazon S3 存储桶的敏感数据特征和建议的修复步骤。

Amazon S3 存储桶的敏感数据特征

当 Macie 在您的 Amazon S3 存储桶中识别出敏感数据时，它会指明需要立即注意的潜在安全和合规风险。

敏感数据可能包括：

- 凭据
- 个人身份信息
- 财务信息
- 需要保护的机密内容

如果敏感数据因错误配置或未经授权的访问而暴露，则可能会导致合规性违规、数据泄露、身份盗用或经济损失。遵循安全最佳实践， AWS 建议对数据进行适当分类，并持续监控 Amazon S3 存储桶中的敏感数据。

对敏感数据实施控制

在暴露调查发现中，选择打开资源。查看检测到的敏感数据类型及其在存储桶中的位置。如需帮助解读 Macie 调查发现，请参阅《Amazon Macie 用户指南》中的 Types of Macie findings。

根据发现的敏感数据类型，实施适当的安全控制：

- 限制对存储桶的访问 – 查看存储桶权限，确保其遵循最低权限原则。使用 IAM 策略、存储桶策略和 ACLs 来限制访问权限。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 的身份和访问管理。
- 启用服务器端加密 – 启用具有 KMS 密钥的服务器端加密以获得额外保护。有关更多信息，请参阅《亚马逊简单存储服务用户指南》中的使用 AWS KMS 密钥的服务器端加密 (SSE-KMS)。
- 用途 AWS Glue DataBrew-Glue DataBrew 用于数据准备和清理。有关更多信息，请参阅《AWS Glue DataBrew 开发人员指南》中的 What is AWS Glue DataBrew。

修复 Ama SageMaker zon 笔记本实例的风险敞口

AWS Security Hub 可以生成亚马逊 SageMaker 笔记本实例的暴露结果。

在 Security Hub 控制台上，暴露发现中涉及的笔记本实例及其识别信息列在发现详情的 “资源” 部分中。通过编程方式，您可以通过 Security Hub CSP GetFindingsV2M API 的操作来检索资源详细信息。

在确定暴露调查发现中涉及的资源后，如果不需要该资源，您可以将其删除。删除不必要的资源可以减少您的曝光概况和 AWS 成本。如果资源至关重要，请按照这些建议的修复步骤进行操作以帮助降低风险。修复主题根据特征的类型进行划分。

单个暴露调查发现包含在多个修复主题中发现的问题。相反，您只需解决一个修复主题即可解决暴露调查发现并降低其严重性级别。您的风险修复方法取决于您的组织要求和工作负载。

> **Note**
>
> 本主题中提供的补救指南可能需要在其他 AWS 资源中进行进一步的咨询。

目录

- Amazon SageMaker 笔记本实例的配置错误特征
  - Amazon SageMaker 笔记本实例已启用直接互联网接入
  - Amazon SageMaker 笔记本实例已启用根访问权限
  - 与 Amazon SageMaker 笔记本实例关联的角色具有管理访问策略
  - 与 Amazon SageMaker 笔记本实例关联的角色具有服务级别管理访问策略

Amazon SageMaker 笔记本实例的配置错误特征

以下是 Amazon SageMaker 笔记本实例的配置错误特征和建议的补救步骤。

Amazon SageMaker 笔记本实例已启用直接互联网接入

在 Amazon SageMaker 笔记本实例上启用后，出站流量将通过 SageMaker-managed 网络地址转换 (NAT) 网关路由到互联网。`DirectInternetAccess`这提供了一个出口路径，可用于数据泄露，或者在笔记本电脑遭到入侵时用作命令和控制通道。遵循安全最佳实践， AWS 建议禁用直接互联网访问，并将笔记本实例放置在具有 VPC 终端节点的 VPC 中，以 AWS 提供所需服务。

禁用直接 Internet 访问

创建笔记本实例后，无法更改该`DirectInternetAccess`设置。要将其禁用，请在 VPC 内的私有子网`Disabled`中创建一个`DirectInternetAccess`设置为的新笔记本实例，然后从现有实例迁移您的笔记本和数据。有关说明，请参阅《Amazon SageMaker 开发者指南》中的将 VPC 中的笔记本实例连接到外部资源。

配置 VPC 端点

禁用直接互联网访问后，笔记本实例需要 VPC 终端节点才能访问 Amazon S3 和 Amazon SageMaker API 等 AWS 服务。为您的笔记本电脑所需的服务创建接口 VPC 终端节点。有关 VPC 终端节点的信息，请参阅什么是 AWS PrivateLink？ 在AWS PrivateLink 指南中。

Amazon SageMaker 笔记本实例已启用根访问权限

在 RootAccess Amazon SageMaker 笔记本实例上启用后，用户将拥有完全的 OS-level 根权限。root 访问权限允许进行任意系统修改、永久后门程序和不受限制的软件包安装。按照安全最佳实践， AWS 建议禁用笔记本实例的根访问权限，除非您的工作流程明确要求这样做。

禁用 root 访问权限

您无法更改正在运行的笔记本实例上的RootAccess设置。要将其禁用，请停止该实例，然后将实例配置更新RootAccess为设置Disabled。大多数笔记本工作流程，包括安装带有生命周期配置的软件包pip和运行生命周期配置，都可以在没有 root 访问权限的情况下继续运行。有关说明，请参阅《亚马逊 SageMaker 开发者指南》中的控制对亚马逊 SageMaker 笔记本实例的根访问权限。

其他注意事项

如果特定任务需要根访问权限，可以考虑改用 Amazon SageMaker Studio 笔记本，它为基于容器的隔离环境提供了更精细的访问控制。您还可以在创建实例时使用生命周期配置预安装所需的软件包，从而减少正常使用期间对 root 访问权限的需求。

与 Amazon SageMaker 笔记本实例关联的角色具有管理访问策略

附加到 notebook 实例的执行角色具有一项策略，该策略可向您的 AWS 账户授予管理访问权限。如果笔记本遭到入侵，攻击者可以利用角色凭据访问和修改账户中的任何资源。遵循安全最佳实践， AWS 建议将最低权限原则应用于笔记本执行角色。

缩小执行角色的范围

查看笔记本执行角色所附的 IAM 政策。移除AdministratorAccess或过于宽泛的策略，取而代之的是仅授予笔记本工作流程所需权限的策略。有关创建限定范围的亚马逊 SageMaker 角色的指导，请参阅《亚马逊 SageMaker 开发者指南》中的亚马逊 SageMaker 角色。

与 Amazon SageMaker 笔记本实例关联的角色具有服务级别管理访问策略

附加到 notebook 实例的执行角色具有授予对一项或多项 AWS 服务的完全访问权限的策略（例如，s3:*或ec2:*）。如果笔记本遭到入侵，攻击者可以利用角色凭据访问或修改这些服务中的资源。遵循安全最佳实践， AWS 建议将服务权限范围仅限于所需的特定操作和资源。

限制服务级别权限

查看笔记本执行角色所附的 IAM 政策。将通配符服务操作（例如`s3:*`）替换为工作流程所需的特定操作（例如`s3:GetObject`和`s3:PutObject`针对特定存储桶 ARN）。有关创建范围策略的指导，请参阅 IAM 用户指南中的创建 IAM 策略。

了解 Security Hub 中未使用的访问发现结果

Security Hub 使用 IAM 访问分析器来识别您账户中未使用的 IAM 权限、角色、访问密钥和密码。这些发现通过突出显示未被积极使用的 IAM 委托人和权限，帮助您实施最低权限访问的安全最佳实践。向所有 Security Hub 客户提供此功能，无需支付额外费用。

未使用的访问分析的工作原理

当您启用 Security Hub 时，该服务会自动在您的账户中创建与服务关联的 IAM 访问分析器。此分析器根据 AWS CloudTrail 活动数据评估所有 IAM 委托人（角色和用户），以确定哪些委托人和权限在 90 天回顾期内未被使用。回顾期不可配置。

IAM Access Analyzer 每 24 小时重新评估所有活跃的调查结果。当以前未使用的委托人或权限变为活动状态时，相应的发现会自动得到解决。

未使用的访问分析器在美国东部（弗吉尼亚北部）运行，因为 IAM 是一项全球服务。Security Hub 会将发现结果复制到您已启用 Security Hub 的所有区域。您无需在美国东部（弗吉尼亚北部）启用 Security Hub 即可运行分析器。

未使用的访问权限查找类型

Security Hub 会生成四种类型的未使用访问发现结果：

调查发现类型	说明	资源已评估
unuseDiamRole	在 90 天回顾期内未担任的 IAM 角色。	IAM 角色
UnusedIAM UserAccessKey	在 90 天回顾期内未用于签署 API 请求的 IAM 用户访问密钥。	IAM 用户
UnusedIAM UserPassword	在 90 天回顾期内未用于控制台登录的 IAM 用户密码。	IAM 用户
UnusedPermission	授予角色或用户但在 90 天回顾期内未被调用的特定 IAM 操作。	IAM 角色或 IAM 用户

Service-linked 分析器

Security Hub 创建的 IAM 访问分析器是一个与服务相关的分析器。您可以在 IAM Access Analyzer 控制台中查看它，但在启用 Security Hub 后，您无法对其进行修改或删除。

当您在所有区域禁用 Security Hub 时，服务关联分析器将自动删除。如果自动删除失败，您可以通过调用 IAM Access Analyzer `DeleteServiceLinkedAnalyzer` API 操作来删除分析器。只有在您的账户完全禁用 Security Hub 之后，此操作才会成功。

服务关联分析器与您可能在 IAM Access Analyzer 中独立创建的任何客户管理的分析器是分开的。创建或删除客户管理的分析器不会影响与服务相关的分析器，反之亦然。

查看未使用的访问发现结果

未使用的访问发现与其他 Security Hub 发现一起显示在 Security Hub 控制台中。您可以按类型筛选查找结果，以便仅查看未使用的访问结果。未使用的访问结果采用开放网络安全架构框架 (OCSF) 的格式，与所有 Security Hub 调查结果使用的格式相同。

对于 UnusedPermission 发现，如果您从过于宽松的策略中移除一些未使用的权限，但不是全部权限，Security Hub 将关闭现有发现结果，并在修订后的策略仍然过于宽松的情况下为其创建新的发现。

也可以从 IAM Access Analyzer 控制台访问未使用的访问发现结果。IAM Access Analyzer 控制台中未使用的访问发现是只读的，并且仅在美国东部（弗吉尼亚北部）区域可见。

暴露结果中未使用的访问权限

未使用的访问信息可以作为上下文特征显示在 Security Hub 暴露结果中。当附加到资源的 IAM 角色具有未使用的权限时，曝光结果会将其作为补充上下文包括在内。这可以帮助您了解漏洞的潜在爆炸半径——具有过高权限的 IAM 角色的资源比权限最低的资源面临更高的风险。

以下资源类型可以在其曝光结果中显示未使用的访问上下文特征：

- Amazon 弹性计算云实例
- AWS Lambda 函数
- Amazon 弹性容器服务服务
- 亚马逊 Elastic Kubernetes Service 集群
- IAM 用户（直接）

有关暴露结果的更多信息，请参阅Security Hub 中的暴露调查发现。

针对未使用权限的策略建议

对于 UnusedPermission 调查结果，Security Hub 可以生成最低权限策略建议。这些建议向您展示了范围缩小的替换策略，该策略仅保留您的委托人实际使用的权限。有关更多信息，请参阅 为未使用的访问发现生成策略建议。

定价

与服务相关的 IAM 访问分析器免费提供给所有 Security Hub 客户。您无需为分析器或未使用的访问发现单独付费。

为未使用的访问发现生成策略建议

对于未使用的权限发现，Security Hub 可以生成最低权限策略建议，向您显示缩小范围的替换策略。该建议会评估附加到 IAM 委托人的每个策略，并生成一个仅保留委托人实际使用的权限的替代策略。向所有 Security Hub 客户提供此功能，无需支付额外费用。

政策建议如何运作

策略建议生成是一种异步操作。要生成和检索推荐，请执行以下操作：

1. 使用 GetFindingsV2 API 操作从 Security Hub 中检索未使用的权限。请注意调查结果中的metadata.uid字段。
2. 致GenerateRecommendedPolicyV2电了解调查结果metadata.uid。这将启动建议生成，该生成通常在 20 秒内完成。
3. GetRecommendedPolicyV2用同样的方法进行轮询，metadata.uid直到status字段返回SUCCEEDED。
4. 响应包含一个或多个建议步骤。每个步骤都指定一个 recommendedActionCREATE_POLICY（创建并附加范围缩小范围的替换策略）或DETACH_POLICY（分离超权限的原始策略）。对于CREATE_POLICY步骤，响应中同时包含 existingPolicy JSON 和 JS recommendedPolicy ON，因此您可以对它们进行比较。

GetRecommendedPolicyV2如果GenerateRecommendedPolicyV2之前没有针对该发现生成建议，则必须在致电之前致电。

谁可以生成推荐

账户所有者和委托管理员都可以调用以下 API 操作：

- 账户所有者可以在自己的账户中生成和查看针对未使用权限发现的建议。
- 授权管理员可以针对任何成员账户在其组织内发现的未使用权限生成和查看建议。

如果您不是委派管理员并且发现的结果属于不同的账户，则 API 操作会返回`AccessDeniedException`错误。

推荐生命周期

- 推荐将缓存 90 天，只要搜索结果处于活动状态（未关闭），推荐就会一直可用。但是，`GenerateRecommendedPolicyV2`多次调用会使缓存失效，并启动一个新的作业，该任务将取代缓存的策略。建议您在每次发现时只致电`GenerateRecommendedPolicyV2`一次。
- 该建议遵循拆卸和连接模式。它不会修改您现有的 IAM 策略。您可以查看推荐的策略，然后在 IAM 控制台或通过 IAM API 手动应用该策略。
- 如果发现得到解决（例如，因为现在正在使用以前未使用的权限），则该建议将不再可用。

错误案例

在以下情况下，API 操作会返回错误：

- 该发现已得到解决 — `InvalidInputException` (HTTP 400)。
- 该发现不是未使用的权限调查结果—— `InvalidInputException` (HTTP 400)。
- IAM 委托人是通过 IAM 身份中心权限集创建的。无法直接修改权限集主体的策略。该建议返回带有解释的`FAILED`状态。
- 来电者不是委派的管理员，结果属于不同的账户—— `AccessDeniedException` (HTTP 403)。
- 尚未生成任何建议，您`GetRecommendedPolicyV2`无需先致电即可拨打电话 `GenerateRecommendedPolicyV2` — `ResourceNotFoundException` (HTTP 404)。

使用控制台

在 Security Hub 控制台中，您可以通过查看未使用的权限查找结果并选择 “修复” 选项卡来生成策略建议。创建推荐时，控制台会显示一个正在加载的微调器。建议准备就绪后，您可以选择 “预览”，查看当前策略和推荐的最低权限替代策略的并排比较。您可以以 JSON 格式复制推荐的策略。

API 参考

- GenerateRecommendedPolicyV2— 针对未使用的权限查找启动异步生成最低权限策略建议。将调查结果`metadata.uid`作为输入。成功时返回 HTTP 200，主体为空。
- GetRecommendedPolicyV2— 检索生成的策略建议。将调查结果`metadata.uid`作为输入。支持使用 `maxResults` (1—100) 和参数进行分页。`nextToken`返回建议状态（`IN_PROGRESS`、`SUCCEEDED`或`FAILED`）、推荐步骤、资源 ARN 和任何错误。

如需详细的 API 文档，请参阅 S ecurity Hub API 参考。

Security Hub 中的自动化

Security Hub 包括根据您的规范自动修改调查发现并对其采取行动的功能。

Security Hub 目前支持以下几种自动化类型：

- 自动化规则：根据定义的标准近乎实时地自动更新和隐藏调查发现，并将调查发现发送到票证工具。
- 自动响应和补救 — 创建自定义 Amazon EventBridge 规则，定义针对特定发现和见解采取的自动操作。

当您想要自动更新开放式网络安全架构框架（OCSF）中的调查发现字段时，自动化规则非常有用。例如，您可以使用自动化规则来更新具有特定标签的资源的调查发现的严重级别。使用自动化规则，无需再手动更新与特定标签相关的每个调查发现的严重性级别。您可以配置自动化规则，以便在调查发现与特定属性匹配时，在 Jira Cloud 和 ServiceNow 等工具中创建票证。这样，只要将调查发现发送到 Security Hub 或在 Security Hub 中创建调查发现，就可以将其创建到票证中。

EventBridge 当你想在 Security Hub CSPM 之外就特定发现采取措施或将特定发现发送给第三方工具进行补救或进行额外调查时，规则会很有用。这些规则可用于触发支持的操作，例如调用 AWS Lambda 函数或将特定发现通知亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题。

自动化规则在应用 EventBridge 规则之前生效。也就是说，在 EventBridge 收到查找结果之前，会触发自动化规则并更新结果。 EventBridge 然后，规则适用于更新的调查结果。

Security Hub 中的自动化规则

借助 Security Hub，您可以自动执行诸如更新调查发现详细信息和为第三方集成创建票证之类的任务。

自动化规则和 AWS 区域

自动化规则可以合而为一，AWS 区域 然后应用于所有已配置的规则 AWS 区域。使用区域聚合时，您只能在主区域中创建规则。在主区域创建规则时，除非规则条件排除特定的关联区域，否则您定义的任何规则都将应用于所有关联区域。对于任何非关联区域，您必须创建自动化规则。

规则操作和条件

Security Hub 中的自动化规则使用条件来引用 Security Hub 调查发现中的 OCSF 属性。例如，`CreateAutomationRuleV2` 中的 `Criteria` 参数支持的筛选条件与 `GetFindingsV2` 中的 `Criteria` 参数支持的筛选条件相匹配。这意味着可以使用自动化规则中的筛选条件来获取调查发现。Security Hub 支持以下 OCSF 字段作为自动化规则条件。

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
activity_name	Activity name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
class_name	Finding class name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.account.uid	Account ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.provider	Cloud provider	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
cloud.region	Region	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
comment	Comment	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.category	Assessment category	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.name	Assessment name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control	Security control ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.standards	Applicable standards	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
compliance.status	Compliance status	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.desc	Finding description	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.product.uid	Related findings product ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.title	Related findings title	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.uid	Related findings ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.src_url	Source URL	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
finding_info.types	Finding type	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.uid	Provider ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.feature.uid	Generator ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.name	Product name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.uid	Product ARN	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.vendor_name	Company name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
metadata.uid	Finding ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.desc	Recommendation text	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.references	Recommendation URL	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.cloud_partition	Resource partition	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.name	Resource name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.region	Resource region	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
resources.type	Resource type	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.uid	Resource ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
severity	Severity	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
status	Status	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.fix_coverage	Software vulnerabilities coverage	EQUALS, PREFIX, NOT_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)

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
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)
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean
vulnerabilities.is_exploit_available	Software vulnerabilities with exploit available	True, False	Boolean
vulnerabilities.is_fix_available	Software vulnerabilities with fix available	True, False	Boolean
activity_id	Activity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

OCSF 字段	控制台筛选条件值	筛选条件运算符	字段类型
confidence_score	Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
severity_id	Severity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
status_id	Status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.related_events_count	Related findings count	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
resources.tags	Resource tags	EQUALS	Map

对于标记为字符串字段的条件，在同一字段上使用不同的筛选运算符会影响评估逻辑。有关更多信息，请参阅 Sec urity Hub API 参考StringFilter中的。

每个标准都支持可用于筛选匹配调查发现的最大值数。有关每个标准的限制，请参阅 Sec urity Hub API 参考OcsfFindingFilters中的

可以更新的 OCSF 字段

以下是可以使用自动化规则更新的 OCSF 字段。

- Comment

- SeverityId
- StatusId

自动化规则如何评估调查发现

自动化规则会评估 Security Hub 在您创建规则后生成或提取的新的和更新后的调查发现。

自动化规则会评估提供者提供的原始调查发现。提供者可以通过与 Security Hub 的集成来提供新的调查发现并更新现有调查发现。通过 BatchUpdateFindingsV2 操作创建规则后，更新调查发现字段不会触发规则。如果您创建的自动化规则和进行的 BatchUpdateFindingsV2 更新都会影响同一个调查发现字段，则上次更新会设置该字段的值。请参见以下示例：

您可以使用 BatchUpdateFindingsV2 将调查发现的 Status 字段从 New 更新为 In Process。如果您调用了 GetFindingsV2，则 Status 字段现在的值为 In Process。您创建了一条自动化规则，该规则会将调查发现的 Status 字段从 New 更改为 Suppressed（请注意，规则会忽略使用 BatchUpdateFindingsV2 进行的更新）。调查发现提供者会更新调查发现，并将 Status 字段更改为 New。如果您调用了 GetFindingsV2，则 Status 字段现在的值为 Suppressed，因为应用了自动化规则，而该规则是对调查发现执行的最后一个操作。

在 Security Hub 控制台中创建或编辑规则时，控制台会显示符合规则条件的调查发现的预览。虽然自动化规则会评估调查发现提供者发送的原始调查发现，但控制台预览会反映最终状态的调查发现，就像它们在响应 GetFindingsV2 API 操作时所显示的那样（即在对调查发现应用规则操作或其他更新之后）。

自动化规则如何排序

每条自动化规则都分配了规则顺序。这决定了 Security Hub 应用您的自动化规则的顺序，当多个规则与同一个调查发现或调查发现字段相关时，这变得非常重要。

当多个规则操作与同一个调查发现或调查发现字段相关时，规则顺序数值最高的规则将应用于最后并产生最终效果。

在 Security Hub 控制台中创建规则时，Security Hub 会根据规则的创建顺序自动分配规则顺序。您创建的第一条规则的规则顺序为 1。当存在多条规则时，后续创建的每条规则都将具有下一个可用的最高数值作为规则顺序值。

当您通过 CreateAutomationRuleV2API 或创建规则时 AWS CLI，Security Hub 会RuleOrder首先应用数值最低的规则。然后它按升序应用后续规则。如果多个调查发现具有相同的 RuleOrder，则

Security Hub 会先为 UpdatedAt 字段应用具有较早值的规则（也就是说，最近编辑的规则应用在最后）。

您可以随时修改规则顺序。

规则顺序示例：

规则 A（规则顺序为 **1**）：

- 规则 A 条件
  - ProductName = Security Hub CSPM
  - Resources.Type 是 S3 Bucket
  - Compliance.Status = FAILED
  - RecordState 是 NEW
  - Workflow.Status = ACTIVE
- 规则 A 操作
  - Confidence 更新为 95
  - Severity 更新为 CRITICAL
  - Comment 更新为 This needs attention

规则 B（规则顺序为 **2**）：

- 规则 B 条件
  - AwsAccountId = 123456789012
- 规则 B 操作
  - Severity 更新为 INFORMATIONAL

首先，规则 A 操作应用于符合规则 A 条件的 Security Hub 调查发现。然后，规则 B 操作应用于具有指定账户 ID 的 Security Hub 调查发现。在此示例中，由于规则 B 最后适用，因此调查发现中来自指定账户 ID 的 Severity 的最终值为 INFORMATIONAL。根据规则 A 操作，在匹配调查发现中 Confidence 的最终值为 95。

第三方集成

您可以使用自动化规则来为与 Jira Cloud 和 ServiceNow ITSM 的集成创建票证。有关更多信息，请参阅创建用于第三方集成的规则。

自动化规则无法正常工作的场景

以下是自动化规则无法正常工作的场景。

- 独立账户成为具有委派管理员的组织的成员
- 组织管理账户移除委派管理员并设置新的委派管理员
- 当未关联的区域变为关联区域时，委派管理员账户或独立账户的聚合器配置会发生变化

在这些场景中，组织成员可以在 AWS CLI 或中通过列出、获取和删除操作来管理自动化规则 APIs。

当未关联的区域变为关联区域时，委派管理员或独立账户可以通过列出、获取和删除操作来管理关联区域中的资源。

在 Security Hub 中创建自动化规则

本主题介绍如何创建自动化规则。您可以使用自动化规则来更新调查发现的详细信息，或者为第三方集成创建票证。您必须单独创建自动化规则，并按您想要的应用 AWS 区域 位置创建这些规则。然而，如果您在聚合区域中创建自动化规则，则该规则将应用于所有区域。否则，如果您在非关联区域创建自动化规则，则该规则将仅在该区域应用。

创建用于更新调查发现详细信息的规则

以下过程介绍了如何创建用于更新调查发现详细信息的规则。

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 从导航窗格中，在管理下，选择自动化。
3. 选择 Create rule（创建规则）。
4. 在详细信息下，输入自动化规则的名称。
   - （可选）输入自动化规则的描述。
5. 在操作下，选择更新调查发现详细信息。您可以在搜索栏中搜索条件和添加条件。要检查是否有任何调查发现符合您的条件，请选择预览匹配调查发现。
6. 在更新调查发现详细信息下，选择至少一个调查发现详细信息，以便在调查发现符合您的条件时进行更新。您可以选择严重性、状态或注释。
7. 在规则设置下，选择已启用或已禁用。如果选择已启用，则自动化规则将启用并会处理新的调查发现。如果选择已禁用，则自动化规则将被禁用，并且不会处理任何调查发现。
8. （可选）在标签下，选择添加新标签以输入要应用于您的自动化规则的键值对。

9. 选择 Create rule（创建规则）。

创建用于第三方集成的规则

以下过程介绍了如何为第三方集成创建票证的规则。有关 Security Hub CSPM 支持的集成的信息，请参阅 Security Hub CSPM 的第三方集成。

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 从导航窗格中，在管理下，选择自动化。
3. 选择 Create rule（创建规则）。
4. 在详细信息下，输入自动化规则的名称。
   - （可选）输入自动化规则的描述。
5. 在操作下，选择创建票证。您可以在搜索栏中搜索条件和添加条件。要检查是否有任何调查发现符合您的条件，请选择预览匹配调查发现。
6. 在创建票证下，从下拉列表中选择 IT 票证集成，然后选择添加集成。
7. 在规则设置下，选择已启用或已禁用。如果选择已启用，则自动化规则将启用并会处理新的调查发现。如果选择已禁用，则自动化规则将被禁用，并且不会处理任何调查发现。
8. （可选）在标签下，选择添加新标签以输入要应用于您的自动化规则的键值对。
9. 选择 Create rule（创建规则）。

在 Security Hub 中查看自动化规则的详细信息

本主题介绍如何查看自动化规则的详细信息。您可以查看自动化规则的以下详细信息：

- 名称和描述
- 操作和条件
- 规则状态和现有调查发现
- 标签

查看自动化规则的详细信息

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。

2. 从导航窗格中，在管理下，选择自动化。此屏幕显示您创建的所有自动化规则。
3. 选择要查看的自动化规则。请选择查看详细信息。或者，您可以选择要查看的自动化规则的名称。

在 Security Hub 中更新规则顺序

本主题介绍如何在控制台中更新自动化规则的规则顺序。如果要编辑自动化规则的条件，请参阅在 Security Hub 中编辑自动化规则。

不能只更新一条自动化规则的规则顺序，而不更新其他自动化规则的规则顺序。例如，您有四条自动化规则：规则 A（1）、规则 B（2）、规则 C（3）和规则 D（4）。您希望首先应用规则 D。为此，您将它的数字从 4 改为 1。结果，规则 A 得到 2，规则 B 得到 3，规则 C 得到 4。

更新自动化规则的规则顺序

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 从导航窗格中，在管理下，选择自动化。
3. 选择要编辑的自动化规则。在顺序下，选择顺序编号旁边的铅笔图标。使用箭头确定新的顺序编号。选择 ✓ 图标进行确认。选择 X 图标进行取消。或者，您可以选择更改顺序，将自动化规则向下、向上移动或移至列表顶部。

在 Security Hub 中禁用自动化规则

本主题介绍了如何禁用自动化规则。当您禁用自动化规则时，Security Hub 会停止应用这些规则。您可以随时在创建自动化规则 AWS 区域 的地方禁用这些规则。

删除规则

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 从导航窗格中，在管理下，选择自动化。
3. 选择要禁用的自动化规则。在状态下，选择已启用旁边的铅笔图标。选择下拉列表，然后选择已禁用。选择 ✓ 图标进行确认。选择 X 图标进行取消。您也可以从操作下拉列表中选择禁用。

在 Security Hub 中启用自动化规则

本主题介绍如何启用自动化规则。启用自动化规则后，Security Hub 会恢复应用这些规则。您可以随时在创建自动化规则 AWS 区域 的地方启用这些规则。

启用规则

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 从导航窗格中，在管理下，选择自动化。
3. 选择要启用的自动化规则。在状态下，选择已禁用旁边的铅笔图标。选择下拉列表，然后选择已启用。选择 ✓ 图标进行确认。选择 X 图标进行取消。您也可以从操作下拉列表中选择启用。

在 Security Hub 中复制自动化规则

本主题介绍如何复制自动化规则。如果您想避免从头开始创建自动化规则，复制自动化规则可以帮助您节省时间。复制自动化规则时，您可以更新详细信息、操作、规则设置和标签。您可以在创建自动化规则 AWS 区域 的地方对其进行编辑。

复制规则

1. 登录您的 AWS 帐户，然后在 https://console.aws.amazon.com/securityhub/v2/ home 上打开 Security Hub 控制台。
2. 从导航窗格中选择管理，然后选择自动化。
3. 选择要复制的自动化规则。选择操作，然后选择复制。
4. 进行更改并查看它们，然后选择创建规则。

在 Security Hub 中编辑自动化规则

本主题介绍如何编辑自动化规则。您可以在创建自动化规则 AWS 区域 的地方对其进行编辑。

您可以编辑自动化规则的以下内容：

- 名称和描述
- 操作
- 规则设置

您无法编辑自动化规则的标签。

编辑规则

1. 登录您的 AWS 账户。在 https://console.aws.amazon.com/securityhub/v2/ home 中打开 Security Hub 控制台。
2. 从导航窗格中，在管理下，选择自动化。
3. 选择要编辑的自动化规则。选择操作，然后选择编辑。
4. 进行编辑并查看它们。
5. 选择保存更改。

在 Security Hub 中删除自动化规则

本主题介绍如何删除自动化规则。您可以在创建自动化规则 AWS 区域 的地方将其删除。

删除规则

1. 登录您的 AWS 帐户，然后在 https://console.aws.amazon.com/securityhub/v2/ home 上打开 Security Hub 控制台。
2. 从导航窗格中选择管理，然后选择自动化。
3. 选择要删除的自动化规则。选择操作，然后选择删除。
4. 选择删除。

中的自动化规则 EventBridge

您可以使用亚马逊中的自动化规则 EventBridge 来响应 Security Hub 的调查结果。Security Hub 几乎实时地将发现结果 EventBridge 作为事件发送。您可以编写基本规则来指示在事件与规则匹配时要执行的自动化操作。可自动触发的操作包括：

- 在中配置 API 目的地 EventBridge。
- 调用 Amazon EC2 运行命令
- 调用 Lambda 函数
- 调用 Step Functions 状态机
- 通知 Amazon SNS 主题或 Amazon SQS 队列
- 将事件中继到 Kinesis Data Streams

- 将结果发送到第三方票证、聊天、SIEM 或事件响应和管理工具
- 使用其他 AWS 账号向 EventBridge 公交车发送事件

Security Hub 将新发现和更新的发现 EventBridge 作为事件发送到。然后，您可以配置 EventBridge 规则以响应每个 Security Hub 事件。有关更多信息，请参阅什么是 EventBridge？ 在《EventBridge 用户指南》中。

> **Note**
>
> 如果您在 Securit EventBridge y Hub CSPM 中为搜索结果定义了规则，则这些规则可能会与为 Security Hub 定义的规则重叠。为避免发送重复的搜索结果，请评估您为 Security Hub CSPM 定义的规则，以确定它们是否与您为 Security Hub 定义的规则重叠。如果适用，请禁用所有被 Security Hub 规则取代的 Security Hub CSPM 规则。

> **Note**
>
> 作为最佳实践，请确保拥有访问权限的用户 EventBridge 使用授予最低所需权限的 AWS Identity and Access Management 策略。有关更多信息，请参阅《EventBridge 用户指南》AWS Identity and Access Management中的EventBridge 和。

EventBridge 事件类型

Security Hub 使用以下亚马逊 EventBridge 事件类型进行集成 EventBridge。

在 Security Hub 的 EventBridge 控制面板上，“所有事件” 包括所有这些事件类型。

导入的调查发现 V2

Security Hub 会自动将所有新发现和现有发现的所有更新 EventBridge 作为Findings Imported V2事件发送到。每个 Findings Imported V2 事件都包含一个调查发现。

导入的每个调查发现以及通过 `BatchUpdateFindingsV2` 请求更新的每个调查发现都会触发 Findings Imported V2 事件。

对于管理员账户，中的事件源 EventBridge 包括来自其账户和成员账户的调查结果的事件。

在聚合区域中，事件源包括来自聚合区域和关联区域的调查发现的事件。跨区域调查发现几乎实时地包含在事件源中。

您可以在中定义规则 EventBridge ，自动将发现结果传送到修复工作流程、第三方工具或其他支持的 EventBridge 目标。这些规则可以包括筛选条件，使仅在调查发现具有特定属性值时才应用规则。

您可以使用此方法自动将所有调查发现或具有特定特征的所有调查发现发送到响应或补救工作流。

> **Note**
>
> Security Hub 和 Security Hub CSPM 都将调查结果发送给 EventBridge 以下来源。`aws.securityhub`确保您的 EventBridge 规则使用特定于 Security Hub 的详细信息类型，以避免与 Security Hub CSPM 发现结果相关的重复通知。

EventBridge 事件格式

Findings Imported V2 事件类型使用以下事件格式。

示例

当 Security Hub 向发送事件时，将使用这种格式 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>
       }]
   }
}
```

每个事件都会发送一项调查发现。*<finding content>* 是事件发送的调查发现的 JSON 内容。

有关调查发现属性的完整列表，请参阅 Security Hub 中的 OCSF 调查发现。

为配置规则 EventBridge

您可以在 Amazon 中创建规则 EventBridge ，定义在收到Findings Imported V2事件时要采取的操作。Findings Imported V2事件由更新触发BatchUpdateFindingsV2。

每条规则都包含一个事件模式，用于标识触发规则的事件。事件模式始终包含事件源（aws.securityhub）和事件类型（导入的调查发现 V2）。事件模式还可以指定筛选条件来识别规则适用的调查发现。

然后，该事件规则用于确定规则目标。目标是在 EventBridge 收到 Findings Importe d V2 事件并且结果与过滤器匹配时要采取的操作。

此处提供的说明使用 EventBridge 控制台。当您使用控制台时， EventBridge会自动创建所需的基于资源的策略， EventBridge 以允许写入 Amazon CloudWatch Logs。

您也可以使用 EventBridge API 的PutRule操作。但是，如果您使用 EventBridge API，则必须创建基于资源的策略。有关所需策略的信息，请参阅 Amazon EventBridge 用户指南中的CloudWatch 日志权限。

事件模式的格式

导入的调查发现 V2 事件的事件模式格式如下：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- source 将 Security Hub 标识为生成事件的服务。
- detail-type 标识事件的类型。
- detail 是可选的，它提供了事件模式的筛选条件值。如果事件模式不包含 detail 字段，则所有调查发现都会触发规则。

您可以根据任何调查发现属性筛选调查发现。您可以为每个属性提供一个或多个值的逗号分隔的数组。

```
"<attribute name>": [ "<value1>", "<value2>"]
```

如果您为一个属性提供多个值，则这些值将通过 OR 连接在一起。如果调查发现包含任何列出的值，则该调查发现与单个属性的筛选条件相匹配。例如，如果您同时提供 INFORMATIONAL 和 LOW 作为 Severity.Label 的值，则如果调查发现的严重性标签为 INFORMATIONAL 或 LOW，则调查发现将匹配。

属性的连接方式为 AND。如果调查发现与所有提供的属性的筛选条件相匹配，则该调查发现与之匹配。

当您提供属性值时，它必须反映该属性在 AWS 开放网络安全架构框架 (OCSF) 结构中的位置。

在以下示例中，事件模式为 ProductArn 和 Severity.Label 提供了筛选值，因此，如调查发现由 Amazon Inspector 生成，并且其严重性标签为 INFORMATIONAL 或 LOW，则调查发现与之匹配。

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

创建事件规则

您可以使用预定义的事件模式或自定义的事件模式在中创建规则 EventBridge。如果您选择预定义的图案，则 EventBridge 会自动填充source和detail-type。 EventBridge 还提供了用于为以下查找结果属性指定筛选值的字段：

- cloud.account.uid

- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

创建 EventBridge 规则（控制台）

1. 打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 使用以下值创建监控查找事件的 EventBridge 规则：
   - 对于规则类型，选择具有事件模式的规则。
   - 选择如何构建事件模式。

使用...构建事件模式	请执行此操作...	
一个模板	在事件模式部分中，选择以下选项： • 对于事件源，选择AWS 服务。 • 对于AWS 服务，选择 Security Hub。 • 对于事件类型，选择导入的调查发现 V2。 • （可选）要使规则更具体，请添加筛选条件值。例如，要将规则限制为具有活动记录状态的调查发现，请在特定记录状态下选择活动。	
自定义事件模式 （如果要根据 EventBridge 控制台中未显示的属性筛	• 在事件模式部分中，选择自定义模式（JSON 编辑器），然后将以下事件模式粘贴到文本区域中：	

使用...构建事件模式	请执行此操作...

选结果，请使用自定义模式。）	<pre>{
	  "source": [
	  "aws.securityhub"
	  ],
	  "detail-type": [
	  "Findings Imported V2"
	  ],
	  "detail": {
	  "findings": {
	  "<attribute name> ":
	  ["<value1>",
	  "<value2>"]
	  }
	  }
	}</pre>
	• 更新事件模式以包含要用作筛选器的属性和属性值。
	
	例如，要将规则应用于严重性为 Critical 的调查发现，请使用以下模式示例：
	
	<pre>{
	  "source":
	["aws.securityhub"
	],
	  "detail-type":
	["Findings Imported
	 V2"],
	  "detail":{
	  "findings":
	{</pre>

使用...构建事件模式	请执行此操作...
	"Severity ": ["Critical"] } } }

- 对于目标类型，选择AWS 服务，在选择目标中，选择目标，例如 Amazon SNS 主题或 AWS Lambda 函数。在收到与规则中定义的事件模式匹配的事件时将触发目标。

有关创建规则的详细信息，请参阅《亚马逊 EventBridge 用户指南 EventBridge》中的创建对事件做出反应的 Amazon 规则。

> **Note**
>
> 如果您在 Securit EventBridge y Hub CSPM 中为搜索结果定义了规则，则这些规则可能会与为 Security Hub 定义的规则重叠。为避免发送重复的搜索结果，请评估您为 Security Hub CSPM 定义的规则，以确定它们是否与您为 Security Hub 定义的规则重叠。如果适用，请禁用所有被 Security Hub 规则取代的 Security Hub CSPM 规则。

Security Hub 的第三方集成

您可以通过 Security Hub 的第三方集成来增强您的 AWS 安全状况。借助此功能，您可以启用从 Security Hub 获取调查发现的集成，从而将您的运营、调查和响应工具与 Security Hub 整合在一起。目前，Security Hub 支持与 Jira Cloud 和 ServiceNow 集成。

主题

- 的集成 AWS Security Hub Jira Cloud
- 的集成 ServiceNow
- Security Hub 票务集成的 KMS 密钥策略
- 测试已配置的工单集成

的集成 AWS Security Hub Jira Cloud

本主题介绍如何与集成Jira Cloud。在完成本主题中的任何过程之前，您必须购买 Jira Cloud 订阅计划。有关订阅计划的信息，请参阅 Atlassian 网站上的定价。

这种集成允许您手动或自动将 Security Hub 调查结果发送到 Jira Cloud，这样您就可以将其作为操作工作流程的一部分进行管理。例如，您可以将所有权分配给需要调查和修复的问题。

对于组织内的账户，只有委派管理员才能配置集成。委派管理员可以手动为任何成员账户调查发现使用创建票证功能。此外，委派管理员可以使用自动化规则自动为与成员账户关联的任何调查发现创建票证。在定义自动化规则时，委派管理员可以设置条件，这些条件可以包括所有成员账户或特定成员账户。有关设置委派管理员的信息，请参阅在 Security Hub 中设置委派管理员账户。

对于非组织账户，此功能的所有方面均可使用。

先决条件

在将 Security Hub 与您的Jira Cloud环境连接之前，您必须确保在 Jira 环境中完成以下配置步骤。

- 安装 Sec AWS urity Hub for Jira 云端应用程序。
- 至少有一个由公司管理的软件开发项目。
- 将 AWS 应用程序分配给您想要从 Security Hub 接收发现结果的软件开发项目。

下面列出了每个先决条件的步骤。

1. 安装 AWS 适用于 Security Hub Jira Cloud 应用程序

Security Hub 有一款支持其与 Jira 集成的应用程序。此应用程序安装自定义字段和自定义问题类型，允许 Security Hub b 填充有关 Security Hub 发现的特定属性。

1. 以管理员身份登录您的 Atlassian 站点。
2. 选择设置，然后选择应用程序。
3. 如果定向到市场页面，请选择查找新应用程序。如果定向到应用程序页面，请选择浏览应用程序，然后搜索 AWS Security Hub for Jira Cloud。然后选择立即获取。

2. 创建项目或验证现有项目

如果您尚未创建项目，则需要执行此步骤。有关如何创建项目的信息，请参阅 Jira Cloud Support 文档中的创建新项目。

创建项目的要求

创建新项目时，请务必执行以下操作：

- 为项目模板选择软件开发。
- Company-managed为项目类型选择。

现有项目的要求

您的 Jira 环境中任何将与 Security Hub 集成的现有项目都必须是项目类型。Company-managed

3. 将您的项目添加到 AWS 适用于 Security Hub Jira Cloud 应用程序

为了让 Security Hub 能够成功地将发现结果发送到您的 Jira 环境，您要与 Security Hub 一起使用的每个项目都必须与Jira Cloud应用程序的 Sec AWS urity Hub 相关联。将 Jira 项目与应用程序关联可确保必需的自定义字段与项目相关联，并且可以在 Security Hub 向项目发送调查结果时填充这些字段。

1. 以管理员身份登录您的 Atlassian 站点。
2. 选择设置，然后选择应用程序。
3. 从应用程序列表中，选择 AWS Security Hub for Jira Cloud。
4. 选择连接器设置选项卡。
5. 在已启用的项目下，选择添加 Jira 项目。
    a. 从下拉列表中选择全部添加，或选择一个项目。如果要添加多个项目，但不是全部项目，请重复此部分步骤。
    b. 选择保存。

您可以从安装管理器选项卡验证已成功安装了哪些项目。您还可以从安装管理器选项卡验证字段、屏幕、状态和工作流的配置。

有关 Jira Cloud 的更多信息，请参阅 Atlassian 网站上的 Jira Cloud 资源。

建议

为您的 Jira 环境创建专用的系统帐户

Security Hub 的集成Jira Cloud使用与你的 Jira 实例中的特定用户关联的 OAuth 连接。出于以下原因，建议为连接创建专用的系统帐户以用于 Security Hub OAuth 连接：

- 专门的系统用户可确保该连接与员工无关，该员工对 Jira 环境的权限可能会随着时间的推移而发生变化，从而影响 Security Hub 与您的 Jira 环境集成的能力。
- Security Hub 在 Jira 中创建的每个议题都将显示一个创建者，即用于创建 OAuth 连接的用户名。使用系统帐户进行 OAuth 连接将导致该系统帐户显示为工单创建者，这有助于让人们知道发现结果是通过 Security Hub 集成创建的，而不是由其他 Jira 用户手动创建的。

在 Security Hub 和之间配置集成 Jira Cloud

对于要向其发送 Security Hub 调查结果的每个Jira Cloud项目，都需要完成以下步骤。

> **Note**
>
> 创建Jira Cloud连接器时，您会从当前连接器重定向 AWS 区域到"`https://3rdp.oauth.console.api.aws`"，因此您可以完成连接器注册。之后，您将返回到创建连接器 AWS 区域 的位置。

为以下各项配置集成 Jira Cloud

1. 使用您的凭据登录您的 AWS 账户，然后打开 Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/v2/home？region=us-east-1。
2. 在导航窗格中，选择管理，然后选择集成。
3. 选择添加Jira Cloud。
4. 对于详细信息，为集成输入唯一描述性名称，并确定是否为集成输入了可选描述。
5. 对于加密，请选择您想要在 Security Hub 中加密集成凭据的方式。
   - 使用 AWS 自有密钥-使用此选项，将使用 Security Hub 拥有的服务密钥来加密您在 Security Hub 中的集成凭证数据。
   - 选择其他 KMS 密钥（高级）-使用此选项 AWS KMS key ，您可以选择自己创建的密钥，用于在 Security Hub 中加密集成凭证数据。有关如何创建 AWS KMS 密钥的信息，请参阅《 AWS Key Management Service 开发者指南》中的创建 AWS KMS 密钥。如果您选择使用自己的密钥，则必须在 KMS 密钥中添加策略声明，以允许 Security Hub 访问该密钥。有关必要策略的详细信息，请参阅 Security Hub 票务集成的AWS KMS 关键政策。

> **Note**
>
> 配置完成后，您将无法更改这些设置。但是，如果您选择自定义密钥，则可以随时编辑您的自定义密钥策略。

6. （可选）对于标签，请创建标签并将其添加到您的集成。最多可以添加 50 个标签。
7. 对于授权，请选择创建连接器并授权。此时将出现一个弹出窗口，您可以在其中选择允许以完成授权。完成授权后，将出现一个复选框，告知您授权成功。
8. 对于配置，输入 Jira Cloud 项目 ID。
9. 选择完成配置。完成配置后，您可以在已配置的集成选项卡中查看已配置的集成。

配置与 Jira 的集成后，您可以测试连接，以确认您的 Jira 环境和 Security Hub 中的所有配置是否正确。有关更多详细信息，请参阅测试已配置的工单集成。

其他 Jira 集成详情

速率限制注意事项

Jira 强制执行 API 速率限制，以维护服务稳定性并确保其平台的公平使用。将 S AWS ecurity Hub 与 Jira 集成使用时，这些速率限制可能会影响 Security Hub 调查结果的处理，尤其是在生成大量调查结果的环境中。这可能会导致工单创建延迟，并且在查找量极高的场景中，某些发现可能根本无法处理到 Jira 工单中。要优化集成，可以考虑在 Security Hub 中对自动化规则实施筛选器，以确定最重要发现的工单优先级，通过管理员控制台监控 Jira API 的使用情况，并根据 Jira 许可等级的特定速率限制规划工作流程。对于业务关键型实施，请联系您的 Jira 管理员以查看您的速率限制分配。

有关 Jira API 速率限制的详细信息，请参阅《Atlassian 开发者指南》网站上的速率限制文档。

身份验证和安全

Jira API 身份验证需要正确的 OAuth 2.0 配置才能进行安全访问。确保您的应用程序遵循 Atlassian 的 API 集成安全最佳实践。

资源：

- Jira Rest api v3：https://developer.atlassian.com/cloud/jira/platform/rest/v3/intro/
- 实现 OAuth 2.0 (3LO)：https://developer.atlassian.com/cloud/oauth/getting-started/implementing-oauth-3lo/

- 管理 Jira Cloud 应用程序：https://support.atlassian.com/jira-cloud-administration/resources/
- 管理 Jira 权限：https://support.atlassian.com/jira-cloud-administration/docs/manage-project-permissions/

为某人创建票证 Jira Cloud 集成

在创建与 Jira Cloud 的集成之后，您可以为调查发现创建票证。

> **Note**
>
> 在整个生命周期中，每个调查发现始终与一个票证关联。自初始创建以来对调查发现的所有后续更新都将发送到同一票证。如果与自动化规则关联的连接器发生更改，则更新后的连接器将仅用于符合规则条件的新调查发现和传入调查发现。

为调查发现创建票证

1. 使用您的凭据登录您的 AWS 账户，然后打开 Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/v2/home？region=us-east-1。
2. 在导航窗格中的清单下，选择调查发现。
3. 选择一个调查发现。在调查发现中，选择创建票证。
4. 对于集成，打开下拉菜单，然后选择一个集成。此集成是您之前在配置 Jira Cloud 项目时创建的集成。选择要将调查发现发送到的集成。
5. 选择创建。

查看门票 Jira Cloud 集成

为调查发现创建票证后，您可以在您的 Jira Cloud 实例上打开票证。

要查看您的调查结果 Jira Cloud 实例

1. 使用您的凭据登录您的 AWS 账户，然后打开 Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/v2/home？region=us-east-1。
2. 在导航窗格中的清单下，选择调查发现。
3. 选择您在其中创建票证的调查发现。
4. 在调查发现中，选择票证 ID 以在您的 Jira Cloud 实例上查看票证或查看 JSON。

的集成 ServiceNow

本主题介绍如何访问 Security Hub 控制台以为 ServiceNow ITSM 配置集成。在完成本主题中的任何过程之前，必须先订阅 ServiceNow ITSM，然后才能添加此集成。有关更多信息，请参阅 ServiceNow 网站上的定价页面。

对于组织内的账户，只有委派管理员才能配置集成。委派管理员可以手动为任何成员账户调查发现使用创建票证功能。此外，委派管理员可以使用自动化规则自动为与成员账户关联的任何调查发现创建票证。在定义自动化规则时，委派管理员可以设置条件，这些条件可以包括所有成员账户或特定成员账户。有关设置委派管理员的信息，请参阅在 Security Hub 中设置委派管理员账户。

对于非组织账户，此功能的所有方面均可使用。

先决条件-配置 ServiceNow 环境

在为 ServiceNow ITSM 配置集成之前，您必须先完成以下先决条件。否则，ServiceNow ITSM 和 Security Hub 之间的集成将无法正常工作。

1. 安装用于 IT 服务管理（ITSM）的 Security Hub 调查发现集成

以下过程介绍如何安装 Security Hub 插件。

1. 登录您的 ServiceNow ITSM 实例，然后打开应用程序导航器。
2. 导航到ServiceNow 商店。
3. 搜索用于 IT 服务管理（ITSM）的 Security Hub 调查发现集成，然后选择获取以安装应用程序。

> **Note**
>
> 在 Security Hub 应用程序的设置中，选择当新的 Security Hub 调查发现发送到您的 ServiceNow ITSM 环境时要执行的操作。您可以选择 “什么都不做”、“创建事件”、“创建问题” 或 “两者兼而有之” (incident/problem)。

2. 配置入站 OAuth 请求的客户端凭证授权类型

您必须为入站 OAuth 请求配置此授权类型。有关更多信息，请参阅 ServiceNow Support 网页上的 Client Credentials grant type for Inbound OAuth is supported。

3. 创建 OAuth 应用程序

如果您已经创建了 OAuth 应用程序，则可以跳过此先决条件。有关创建 OAuth 应用程序的信息，请参阅 Setting up OAuth。

先决条件-配置 AWS Secrets Manager

要使用 Security Hub 的集成 ServiceNow，您的 ServiceNow OAuth 应用程序的凭据必须存储在 Secrets Manager 中。将您的证书存储在 Secrets Manager 中允许您控制和查看凭证的使用，同时还允许 Security Hub 使用这些证书与您的 ServiceNow 实例集成。要将您的凭据存储在 Secrets Manager 中，您必须使用客户管理的密 AWS KMS 钥来保护机密。此密 AWS KMS 钥允许您在静态存储时保护机密，还允许在密钥上附加策略，从而授予 Security Hub 访问保护该密钥的权限。

使用以下步骤为您的 ServiceNow 证书配置 Secrets Manager。

第 1 步：将策略附加到您的 AWS KMS 键

要成功配置您的 ServiceNow 集成，您必须首先向 Security Hub 授予使用将在 Secrets Manager 中与您的 ServiceNow 凭据关联的密 AWS KMS 钥的权限。

要修改 AWS KMS Security Hub 访问您的 ServiceNow 凭证的密钥策略

1. 打开 AWS KMS 控制台，网址为https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 选择现有 AWS KMS 密钥或执行《AWS KMS 开发者指南》中创建新密钥的步骤。
4. 在 Key policy（密钥策略）部分，选择 Edit（编辑）。
5. 如果显示 “切换到策略视图”，请选择它以显示密钥策略，然后选择 “编辑”。
6. 将以下策略块复制到您的 AWS KMS 密钥策略中，以授予 Security Hub 使用您的密钥的权限。

```
{
    "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. 通过替换策略示例中的以下值来编辑策略：
   - *your-account-id*替换为您的 AWS 账户 ID。
   - *your-region*替换为您 AWS 所在的地区（例如，us-east-1）。
8. 如果在最后一条语句之前添加了策略语句，请在添加该语句之前添加一个逗号。确保 AWS KMS 密钥策略的 JSON 语法有效。
9. 选择保存。
10. （可选）将密钥 ARN 复制到记事本中，以便在后续步骤中使用。

第 2 步：在 Secrets Manager 中创建密钥

在 Secrets Manager 中创建一个用于存储您的 ServiceNow 凭据的密钥。与您的 ServiceNow 环境交互时，Security Hub 将访问此密钥。

按照《AWS Secrets Manager 用户指南》中的步骤创建密钥。创建密钥后，复制密钥 ARN，因为在创建 Security Hub 连接器时需要使用它。

创建密钥时，请确保配置以下内容：

密钥类型

其他密钥类型

Key/value 对（纯文本格式）

```
{
    "ClientId": "your-servicenow-client-id",
    "ClientSecret": "your-servicenow-client-secret"
    }
```

> **Note**
>
> 字段名称必须完全相同`ClientId`和`ClientSecret`（区分大小写）。Security Hub 需要这些确切的名称才能检索凭证。

加密密钥

使用您在步骤 1 中配置的 AWS KMS 密钥

资源政策

请使用以下资源策略：

```
{
    "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:*"
            }
        }
        }
    ]
```

```
    }
```

现在，您的密钥已配置完毕，您可以使用 CreateConnector V2 API 或 AWS 控制台创建 Security Hub 连接器。你需要提供：

- InstanceName: 您的 ServiceNow 实例 URL（例如，`your-instance.service-now.com`）
- SecretArn: 您在此过程中创建的密钥的 ARN

为以下各项配置集成 ServiceNow ITSM

Security Hub 可以自动在 ServiceNow ITSM 中创建事件或问题。

为以下各项配置集成 ServiceNow ITSM

1. 使用您的凭据登录您的 AWS 账户，然后打开 Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/v2/home？region=us-east-1。
2. 在导航窗格中，选择管理，然后选择集成。
3. 在 ServiceNow ITSM 下，选择添加集成。
4. 对于详细信息，为集成输入名称，并确定是否为集成输入了可选描述。
5. 对于加密，请选择您想要在 Security Hub 中加密集成凭据的方式。

   - 使用 AWS 自有密钥-使用此选项，将使用 Security Hub 拥有的服务密钥来加密您在 Security Hub 中的集成凭证数据。
   - 选择其他 KMS 密钥（高级）-使用此选项 AWS KMS key ，您可以选择自己创建的密钥，用于在 Security Hub 中加密集成凭证数据。有关如何创建 AWS KMS 密钥的信息，请参阅《AWS Key Management Service 开发者指南》中的创建 AWS KMS 密钥。如果您选择使用自己的密钥，则必须在 KMS 密钥中添加允许 Security Hub 访问该密钥的策略声明。有关必要策略的详细信息，请参阅 Security Hub 票务集成的AWS KMS 关键政策。

   > **Note**
   >
   > 配置完成后，您将无法更改这些设置。但是，如果您选择自定义密钥，则可以随时编辑您的自定义密钥策略。

6. 对于证书，请输入您ServiceNow ITSM的 URL 以及在先决条件部分生成的 AWS Secrets Manager 密钥的 ARN。

7. 对于标签，确定是否创建可选标签并将其添加到您的集成中。
8. 选择添加集成。完成配置后，您可以在已配置的集成选项卡中查看已配置的集成。

配置完与的集成后， ServiceNow 您可以测试连接，以确认您的 ServiceNow 环境和 Security Hub 中的所有配置是否正确。有关更多详细信息，请参阅测试配置的工单集成。

为 a 创建票证 ServiceNow ITSM 集成

在创建与 ServiceNow ITSM 的集成之后，您可以为调查发现创建票证。

> **Note**
>
> 在整个生命周期中，每个调查发现始终与一个票证关联。自初始创建以来对调查发现的所有后续更新都将发送到同一票证。如果与自动化规则关联的连接器发生更改，则更新后的连接器将仅用于符合规则条件的新调查发现和传入调查发现。

为调查发现创建票证

1. 使用您的凭据登录您的 AWS 账户，然后打开 Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/v2/home？region=us-east-1。
2. 在导航窗格中的清单下，选择调查发现。
3. 选择一个调查发现。在调查发现中，选择创建票证。
4. 对于集成，打开下拉菜单，然后选择一个集成。
5. 选择创建。

查看门票 ServiceNow ITSM 集成

为调查发现创建票证后，您可以在您的 ServiceNow ITSM 实例上打开票证。

要查看您的调查结果 ServiceNow ITSM 实例

1. 使用您的凭据登录您的 AWS 账户，然后打开 Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/v2/home？region=us-east-1。
2. 在导航窗格中的清单下，选择调查发现。
3. 选择您在其中创建票证的调查发现。

4. 在调查发现中，选择票证 ID 以在您的 ServiceNow ITSM 实例上查看票证或查看 JSON。

Security Hub 票务集成的 KMS 密钥策略

将客户管理的 KMS 密钥与 Security Hub 票证集成一起使用时，需要向 KMS 密钥添加其他策略，以允许 Security Hub 与该密钥进行交互。此外，还需要添加策略，允许将密钥添加到 Security Hub 连接器的委托人访问密钥。

Security Hub 权限策略

以下策略概述了 Security Hub 访问和使用与您的 Jira 和 ServiceNow 连接器关联的 KMS 密钥所需的权限。需要将此策略添加到与 Security Hub 连接器关联的每个 KMS 密钥中。

该策略包含以下权限：

- 允许 Security Hub 使用密钥保护、临时访问或刷新用于与您的票务集成进行通信的令牌。权限仅限于与特定 Security Hub 连接器相关的操作，通过检查源 ARN 和加密上下文的条件块来实现。
- 通过允许`DescribeKey`操作，允许 Security Hub 读取有关 KMS 密钥的元数据。此权限是 Security Hub 验证密钥状态和配置所必需的。访问权限通过源 ARN 条件限制为特定 Security Hub 连接器。

```
{
    "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/*"
        }
    }
}
```

通过替换策略示例中的以下值来编辑策略：

- 替换*CloudProviderName*为JIRA_CLOUD或 SERVICENOW
- *AccountId*替换为您在其中创建 Security Hub 连接器的账户 ID。
- *Region*替换为您 AWS 所在的地区（例如，us-east-1）。

Security Hub 操作的 IAM 主体

任何要向 Security Hub 连接器分配客户管理的 KMS 密钥的委托人都需要拥有对要添加到连接器的密钥执行密钥操作（描述、生成、解密、重新加密和列出别名）的权限。这适用于CreateConnectorV2和CreateTicketV2 APIs。以下政策声明应作为任何将与之互动的委托人的政策的一部分包括在内 APIs。

```
{
    "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"
            ]
        }
    }
}
```

通过替换策略示例中的以下值来编辑策略：

- *RoleName*替换为正在调用 Security Hub 的 IAM 角色的名称。
- 将 *CloudProviderName* 替换为 JIRA_CLOUD 或 SERVICENOW。
- *AccountId*替换为您在其中创建 Security Hub 连接器的账户 ID。

- *Region*替换为您 AWS 所在的地区（例如，us-east-1）。

测试已配置的工单集成

对于已配置的 Jira 和 ServiceNow 集成，您可以测试连接，以确保 Security Hub 和 Jira 或 ServiceNow 环境中的所有配置都已完成。

测试票证功能将创建标题为的票证TESTING Test CreateTicketV2 Finding。测试票证中填充了示例数据，例如账户 ID 和执行测试的账户区域、示例资源详细信息以及 Finding JSON AWS 示例。

使用控制台测试集成

使用以下步骤来测试您的集成：

1. 在 Security Hub 导航面板中，选择集成。
2. 在“已配置的集成”选项卡中，选择要测试的集成。
3. 在集成的概述页面中，选择创建测试票证。
4. 如果测试成功，将显示一条成功消息以及指向测试票证的链接。如果测试不成功，则会显示测试错误。根据错误消息解决 Security Hub 或 Jira 或 Service Now 环境中的配置问题。

> **Note**
>
> 测试票证功能旨在帮助验证设置新连接或更改现有连接时的端到端功能。每次使用此功能时，都会在您的 Jira 或 Service Now 环境中创建一个新票证，并且不打算用于定期验证您的连接。

使用进行测试 AWS CLI

要使用测试您的集成 AWS CLI，请使用带--mode DRYRUN参数的create-ticket-v2命令：

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

示例

以下示例显示了如何测试集成：

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

成功响应

成功的响应将返回以下内容：

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

响应`TicketSrcUrl`中的提供了在您的 Jira 或 ServiceNow 环境中查看测试票证的直接链接。

如果测试失败，将显示一条错误消息，指出需要解决的配置问题。

对 Jira 云集成错误进行故障排除

在测试从 Security Hub 与 Jira Cloud 的集成时，可能会返回以下错误消息。这些错误消息可以让人们深入了解连接器的配置问题可能出在哪里以及如何解决。

Jira Cloud 集成错误消息

错误	错误消息	可能的原因和解决方案
ConflictException	找不到 jira 项目	可能的原因：连接器上的项目不正确，或者我们无法访问该项目 credentials/permissions 的问题。 可能的解决方案：将正确的项目添加到连接器中，或者使用正确的凭据重新对 Jira 进行身份验证。

错误	错误消息	可能的原因和解决方案
ConflictException	未找到 Security Hub 问题类型	可能的原因：应用程序安装问题或问题类型与项目无关。 可能的解决方案：执行必备步骤，将 Jira 应用程序安装到您的 Jira 环境中，并将该应用程序与项目关联。

在 Security Hub 中监控使用情况和成本

“用量”页面有助于您了解和管理在整个组织中运行 Security Hub 的成本。在此页面上，您可以查看当前成本，查看预计的每月费用，按功能或账户浏览使用情况，并找到优化支出的策略。

谁可以访问 “使用情况” 页面

任何启用了 Security Hub 的账户都可以访问使用情况页面。要访问它，请打开 Security Hub 控制台，然后在导航窗格的 “设置” 下选择 “使用情况”。

> **Important**
>
> 如果您的账户是 AWS 组织中的成员账户，并且尚未指定 Security Hub 委派管理员，则使用数据不可用。要查看使用情况数据，贵组织的管理账户必须指定委派管理员。有关更多信息，请参阅 the section called “指定委派管理员”。

根据您的账户类型，体验会有所不同：

- 委派管理员或管理帐户-您可以看到完整的使用情况页面，其中包含组织成本摘要、按权能划分的使用情况、按账户划分的使用情况以及成本优化策略。
- 成员账户或独立账户 — 您会看到账户费用摘要，其中仅包含您账户按功能划分的使用情况。“按账户” 选项卡不可用，因为您查看的是单个账户。

组织和账户成本汇总

> **Note**
>
> 组织成本摘要部分只能从委派的管理员账户或管理账户中看到。成员账户和独立账户将改为查看账户费用摘要。

当您通过委派的管理员或管理账户打开 “使用情况” 页面时，“组织成本摘要” 部分会显示贵组织在当前计费周期内的 Security Hub 成本的高级概览。本节包含以下内容：

- 上次刷新数据-Security Hub 上次刷新贵组织的使用情况数据的日期。Security Hub 会定期刷新这些数据。如果您访问 “使用情况” 页面时数据已超过 24 小时，Security Hub 会自动触发刷新。刷新将在几个小时内完成，具体取决于您的组织规模。刷新数据时，会出现一条警报，并显示一条消息，告知数据将很快可用。
- 当前成本 — 从当前计费周期开始到上次刷新数据之日，贵组织因使用 Security Hub 而产生的总金额。
- 预计每月费用（30 天）— 根据最近 7 天的使用情况，推断为整整 30 天的计费周期，估算出每月费用。该预测包括付费和免费试用两种用量，可让您对每月的费用做出真实的估计。预计成本不包括您与 AWS之协商的任何折扣 (EDP)。如果您的预计费用似乎低于当前费用，则意味着您的使用量一直在减少，并且根据过去 7 天的使用情况，30 天的账单将低于当前账单周期中的账单。

“功能”视图

能力视图按安全功能显示整个组织的成本和使用情况。权能分为三个可扩展组。您可以展开或折叠每个组，以查看其中的各个使用类型。每种使用类型都直接映射到 Cost Explorer 中 AWS 相应的使用类型。

Sec@@ urity Hub 基本计划 — 监控您的 EC2 实例、ECR 容器映像、Lambda 函数、IAM 用户和 IAM 角色。涵盖风险和暴露分析、漏洞管理（由 Amazon Inspector 提供支持）、安全态势管理（由 Security Hub CSPM 提供支持）和安全响应。所有这些功能都包含在基本计划中，按资源单一价格收费，您无需单独启用 Amazon Inspector 或 Sec AWS urity Hub CSPM 或为其付费，也无需为基础服务使用量收取双重费用。

威胁分析-包括 CloudTrail 管理事件和数据事件、网络活动和其他日志。这些功能涵盖由 Amazon 支持的威胁检测 GuardDuty。

其他功能-包括 Lambda 函数代码扫描。这是一项由 Amazon Inspector 提供支持的可选增强功能，用于分析 Lambda 函数应用程序代码中是否存在安全漏洞。

有关每项功能定价的更多信息，请参阅 Sec urity Hub 定价。

此视图中的表格包括每种使用类型的以下各列：

- 当前使用量-从账单周期开始到上次刷新数据之日，该使用类型在所有账户和所有地区的总使用量。
- 免费使用量-当前处于免费试用期的账户中该使用类型的总使用量。免费使用量值显示为绿色。
- 当前成本 — 从账单周期开始到上次刷新数据之日，该使用类型在所有账户和所有地区的总成本。
- 免费试用价值 — 如果当前处于免费试用期的账户不在试用期，则此使用类型所产生的费用。这可以帮助您了解免费试用的价值。
- 预计每月费用（30 天）— 此使用类型的估计每月费用，根据所有账户和所有地区的过去 7 天使用量推算得出。这包括付费和免费试用，以提供估计的每月费用。

“账户”视图

> **Note**
>
> 账户视图只能通过委派管理员账户或管理账号获取。

选择账户视图，查看按所有地区的个人成员账户整理的费用。此视图可帮助您确定哪些账户带来的成本最高。

该表列出了每个账户，其中包含以下各列：

- 帐户- AWS 账户 ID，显示为可点击的链接。选择一个账户会打开一个详细的细分面板。
- 当前成本 — 该账户从账单周期开始到上次刷新数据之日止的所有地区的总成本。
- 免费试用价值 — 如果不在免费试用期内，此账户可能产生的费用。
- 预计每月费用（30 天）— 此账户的估计每月费用，从所有地区最近 7 天的使用量推断为整整 30 天的账单周期。该预测包括付费和免费试用两种用量，以对您的每月费用进行具有代表性的估算。预计成本不包括您与之协商的任何折扣 AWS （eDP）。

  如果在过去 7 天内为此账户启用了 Security Hub，则预测基于启用后的天数。7 天后，预测将使用最近 7 天的全部使用量。“使用情况” 页面当前无法检测账户何时禁用 Security Hub。如果最近在一个

或多个账户上禁用了 Security Hub，则这些账户将继续出现在预测中，直到其使用量耗尽。在进行这些更改后，请等待 7 天，以便预测反映组织的最新状态。

账户详情视图

当您从列表中选择一个账户时，页面右侧会打开一个详细信息面板。此面板显示的能力级别细分与 “能力” 视图相同，但已筛选到该特定帐户。您可以查看该账户中所有地区每种使用类型的当前使用量、免费使用量、当前费用、免费试用价值和预计每月费用。

成本优化策略

在 “使用情况” 页面上选择成本优化策略，进入专门页面，其中包含可行的方法来管理成本，同时保持安全保障。

每种策略都以独立选项的形式呈现，您可以根据组织的需求对其进行评估和应用。首先列出了没有安全权衡的选项。应用任何策略后，更改通常需要 24 到 48 小时才能反映在您的账单中。

相关资源

- Security Hub 定价
- AWS Cost Explorer 用户指南

禁用 Security Hub

为单个账户禁用 Security Hub

如果您的账户不属于某个组织，则可以随时在 Security Hub 控制台中禁用 Security Hub 或使用 DisableSecurityHubV2 API。禁用 Security Hub 后，它会停止从检测引擎获取发现，您也将无法访问现有发现、集成和配置。

当您在所有区域为账户禁用 Security Hub 时，Security Hub 还会删除您在启用服务时创建的与服务相关的 IAM 访问分析器。如果自动删除失败，您可以通过调用 IAM Access Analyzer `DeleteServiceLinkedAnalyzer` API 操作来删除分析器。只有在您的账户完全禁用 Security Hub 之后，此操作才会成功。如果您在单个区域禁用 Security Hub，但在其他区域仍处于启用状态，则未使用的访问分析器将继续运行，发现的结果将继续复制到剩余已启用的区域。

禁用 Security Hub

1. 使用您的凭据登录您的 AWS 账户，然后在上打开 Security Hub 控制台https://console.aws.amazon.com/securityhub/v2/home。
2. 在导航窗格中，选择常规。
3. 在 Security Hub 中，选择 “禁用”。在弹出窗口中**`Disable`**，输入并选择 “禁用”。

在整个组织中禁用 Security Hub

如果您是 AWS 组织的委托管理员，则有两个选项可用于跨成员账户禁用 Security Hub。

选项 1：使用检测引擎禁用 Security Hub

您可以利用委托管理员账户中策略目录中的 Sec urity Hub（基本和额外功能）部署和策略，为特定组织单位、账户或区域禁用 Security Hub 和 Amazon Inspector。

使用策略在成员账户中禁用 Security Hub 和 Amazon Inspector

1. 使用带有委派管理员凭证的 AWS 账户登录。打开 Security Hub 控制台，网址为https://console.aws.amazon.com/securityhub/v2/home。
2. 从导航窗格中选择 “管理”，然后选择 “配置”。
3. 从配置目录中选择 Sec urity Hub（基本功能和附加功能）。
4. 在详细信息部分的配置 Security Hub 页面上，输入策略的名称和描述（例如，“Security Hub 禁用策略”）。
5. 在 “账户选择” 部分，选择以下选项之一。如果要将禁用功能应用于所有组织单位和帐户，请选择 “所有组织单位和帐户”。如果要将禁用功能应用于特定的组织单位和帐户，请选择 “特定组织单位和帐户”。如果选择此选项，请使用搜索栏或组织结构树来指定目标组织单位和帐户。
6. 在 “区域” 部分，选择 “禁用所有区域” 以在所有区域中禁用 Security Hub。（可选）选择是否自动禁用新区域。选择 “指定区域”，选择要禁用的特定区域。
7. （可选）有关高级设置，请参阅中的指南 AWS Organizations。
8. （可选）对于资源标签，将标签添加为键值对，以帮助您轻松识别配置。
9. 选择下一步。
10. 查看您的更改，然后选择应用。您的目标账户是根据策略进行配置的。您的策略的配置状态将显示在 “策略” 页面的顶部。

禁用 Amazon GuardDuty 和 AWS Security Hub CSPM

对于 GuardDuty 和 Security Hub CSPM 功能，您必须手动禁用相应委派管理员帐户的权能。GuardDuty 而且 Security Hub CSPM 使用部署（一次性操作）而不是策略，因此必须从各自的控制台手动执行禁用。

选项 2：仅禁用 Security Hub

如果您已有 Security Hub 策略，并且只想在不影响 Amazon Inspector 或 Security Hub CSPM 的情况下禁用 Security Hub，请按照以下步骤操作。 GuardDuty

仅在成员账户中禁用 Security Hub

1. 使用带有委派管理员凭证的 AWS 账户登录。打开 Security Hub 控制台，网址为https://console.aws.amazon.com/securityhub/v2/home。
2. 从导航窗格中选择 “管理”，然后选择 “配置”。
3. 从 “已配置” 策略中选择您的任何 Security Hub 策略。
4. 单击 “编辑政策”，然后在 “账户选择” 部分，选择以下选项之一。如果要将禁用功能应用于所有组织单位和帐户，请选择 “所有组织单位和帐户”。如果要将禁用功能应用于特定的组织单位和帐户，请选择 “特定组织单位和帐户”。如果选择此选项，请使用搜索栏或组织结构树来指定目标组织单位和帐户。
5. 在 “区域” 部分，选择 “禁用所有区域” 以在所有区域中禁用 Security Hub。（可选）选择是否自动禁用新区域。选择 “指定区域”，选择要禁用的特定区域。
6. （可选）有关高级设置，请参阅 Organizations AWS 中的指南。
7. （可选）对于资源标签，将标签添加为键值对，以帮助您轻松识别配置。
8. 选择下一步。
9. 查看您的更改，然后选择应用。您的目标账户是根据策略进行配置的。您的策略的配置状态将显示在 “配置” 页面的顶部。

对其他安全服务的影响

通过 Security Hub 策略禁用 Security Hub 不会对 Security Hub CSPM 和 Amazon Inspector 的配置产生任何影响。 GuardDuty

如果您只需要在成员账户中禁用 Amazon Inspector，则可以使用 Security Hub 配置目录中的漏洞管理策略。导航到 Security Hub 配置页面，从 Amazon Inspector 中选择漏洞管理，然后按照与上述 Security Hub 禁用过程类似的步骤创建禁用策略。

Security Hub 中的 AWS 安全

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Security Hub 的合规计划，请参阅按合规计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Security Hub 时应用责任共担模型 以下主题说明如何配置 Security Hub 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Security Hub 资源。

主题

- 中的数据保护 AWS Security Hub
- AWS Security Hub 的身份和访问管理
- 的合规性验证 AWS Security Hub
- Sec AWS urity Hub 中的弹性
- Security Hub 中的基础设施 AWS 安全
- AWS Security Hub 和接口 VPC 终端节点 (AWS PrivateLink)

中的数据保护 AWS Security Hub

责任 AWS 共担模式分适用于 Sec AWS urity Hub 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题解答AWS条款。 有关欧洲数据保护的信息，请参阅通用数据保护条例（GDPR）中心。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务 使用控制台、API 或软件开发工具包与 AWS Security Hub 或其他人合作时。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

Security Hub 是一种多租户服务产品。为了帮助保护您的数据，Security Hub 对静态数据和组件服务之间传输的数据进行加密。

选择不使用您的数据来改进服务

> **Note**
>
> 本文档页面仅适用于 2025 年 12 月 2 日推出的增强版 Sec AWS urity Hub。如果您是最初的 Sec AWS urity Hub（现为 Sec AWS urity Hub CSPM）的客户，则只有在启用增强型 AWS 安全中心之后，才会适用下述的数据使用量。

通过使用 AWS 组织选择退出政策，您可以选择不将您的数据（在 Security Hub 服务条款中定义为“Security Hub 内容”）用于开发和改进 AWS Security Hub 和其他 AWS 安全服务。即使 Security Hub 目前未收集任何此类内容，您也可以选择退出。有关如何选择退出的更多信息，请参阅《AWS Organizations 用户指南》中的 AI 服务选择退出政策。

> **Note**
>
> 要使用选择退出政策，您的 AWS 账户必须由 Organizations 集中管理。 AWS 如果您尚未为自己的 AWS 账户创建组织，请参阅《AWS Organizations 用户指南》中的创建和管理组织。

选择退出会带来以下影响：

- 在您选择退出（如果有）之前，Security Hub 将删除出于服务改进目的而收集和存储的内容。
- 在您选择退出后，Security Hub 将不再出于服务改进目的收集或存储此内容。

以下部分介绍了 Security Hub 将如何处理您的内容以改进服务。

AWS Security Hub 数据使用情况

目前，Sec AWS urity Hub 不会出于服务改进目的收集或存储任何 Security Hub 内容。但是，将来，Security Hub 可能会收集和使用您在 Security Hub 和其他形式的 Security Hub 内容（Security Hub 为提供 Security Hub 功能而从您或上游服务那里收到的）中汇总的第三方安全发现来改进 Security Hub 和其他 AWS 安全服务功能。

您的信任、隐私和内容安全是我们的首要任务。如果 Security Hub 将来出于服务改进目的开始收集 Security Hub 内容，则此页面将进行更新以反映这些更改，并提供有关收集哪些数据以及如何使用这些数据的详细信息。您可以使用上述 Organizations 的选择退出政策，随时选择退出此 S AWS ecurity Hub 内容集。有关 AWS 数据隐私惯例的更多信息，请参阅数据隐私常见问题解答。

参考

有关其他 AWS 安全服务中类似的选择退出程序，请参阅：

- 在《亚马逊 GuardDuty 用户指南》中选择不使用您的数据来改善服务。
- 在《Amazon Security Lake 用户指南》中，选择不使用您的数据来改善服务。

AWS Security Hub 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Security Hub 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Security Hub 如何与 IAM 协同工作
- 基于身份的策略示例 AWS Security Hub CSPM
- Service-linked 的角色 AWS Security Hub
- AWS Security Hub 的托管策略
- 对 Sec AWS urity Hub 身份和访问进行故障排除

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 Sec AWS urity Hub 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅Security Hub 如何与 IAM 协同工作）
- IAM 管理员：编写用于管理访问权限的策略（请参阅基于身份的策略示例 AWS Security Hub CSPM）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Security Hub 如何与 IAM 协同工作

在使用 AWS Identity and Access Management (IAM) 管理对 Sec AWS urity Hub 的访问权限之前，请先了解哪些 IAM 功能可用于 Security Hub。

你可以在 Sec AWS urity Hub 上使用的 IAM 功能

IAM 功能	Security Hub 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	否
策略条件键	是
访问控制列表 (ACLs)	否
基于属性的访问权限控制（ABAC）：策略中的标签	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
服务关联角色	是

有关 Security Hub 和其他 AWS 服务 功能如何与大多数 IAM 功能配合使用的高级视图 AWS 服务 ，请参阅 IAM 用户指南中的如何与 IAM 配合使用。

Security Hub 基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Security Hub 支持基于身份的策略。有关更多信息，请参阅 基于身份的策略示例 AWS Security Hub CSPM。

Security Hub 基于资源的策略

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Security Hub 不支持基于资源的策略。您不能将 IAM 策略直接附加到 Security Hub 资源。

Security Hub 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

Security Hub 中的策略操作在操作前使用以下前缀：

```
securityhub:
```

例如，要授予用户启用 Security Hub 的权限（该操作对应于 Security Hub API 的 `EnableSecurityHubV2` 操作），请在其策略中包含 `securityhub:EnableSecurityHubV2` 操作。策略语句必须包含 `Action` 或 `NotAction` 元素。Security Hub 定义了一组自己的操作，以描述您可以使用该服务执行的任务。

```
"Action": "securityhub:EnableSecurityHubV2"
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。例如：

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

您也可以使用通配符（*）指定多项操作。例如，要指定以单词 Get 开头的所有操作，包括以下操作：

```
"Action": "securityhub:Get*"
```

但作为最佳实践，您应创建遵循最低权限 原则的策略。换句话说，您应创建仅包含执行特定任务所需的权限的策略。

有关 Securit y Hub 操作的列表，请参阅《服务授权参考》中的 Sec AWS urity Hub 定义的操作。有关指定 Security Hub 操作的策略示例，请参阅基于身份的策略示例 AWS Security Hub CSPM。

Security Hub 的策略资源

支持策略资源：否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

Security Hub 定义了以下资源类型：

- 中心
- 产品
- 调查发现聚合器，也称为跨区域聚合器
- 自动化规则

您可以使用在策略中指定这些类型的资源 ARNs。

有关 Security Hub 资源类型列表以及每种资源类型的 ARN 语法，请参阅《服务授权参考》中的 S ec AWS urity Hub 定义的资源。要了解您可以为每种类型的资源指定哪些操作，请参阅《服务授权参考》

中的 Sec AWS urity Hub 定义的操作。有关指定资源的策略示例，请参阅 基于身份的策略示例 AWS Security Hub CSPM。

Security Hub 的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

有关 Security Hub 条件键的列表，请参阅《服务授权参考》中的 Sec AWS urity Hub 条件密钥。要了解可以将条件键与哪些操作和资源一起使用，请参阅 Sec AWS urity Hub 定义的操作。有关使用条件密钥的策略示例，请参阅 基于身份的策略示例 AWS Security Hub CSPM。

Security Hub 中的访问控制列表 (ACLs)

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Security Hub 不支持 ACLs，这意味着你无法将 ACL 附加到 Security Hub 资源。

用于 Security Hub 的基于属性的访问权限控制（ABAC）

支持 ABAC（策略中的标签）：是

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/`*`key-name`*`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

您可以将标签附加到 Security Hub 资源。您还可以通过在策略的 `Condition` 元素中提供标签信息，控制对资源的访问权限。

有关标记 Security Hub 资源的信息，请参阅标记 Security Hub 资源。有关基于标签控制资源访问权的基于身份的策略示例，请参阅 基于身份的策略示例 AWS Security Hub CSPM。

将临时凭证与 Security Hub 一起使用

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 AWS STS API 操作来获取临时安全证书GetFederationToken。

Security Hub 支持使用临时凭证。

Security Hub 的转发访问会话

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

例如， AWS 服务 当您将 Security Hub 与 Organiations 中的组织集成 AWS Organizations 以及为组织中的组织指定委派的 Security Hub 管理员帐户时，Security Hub 会向下游发出 FAS 请求。

对于其他任务，Security Hub 使用服务相关角色来代表您执行操作。有关此角色的详细信息，请参阅Service-linked 的角色 AWS Security Hub。

Security Hub 的服务角色

Security Hub 不代入或使用服务角色。要代表您执行操作，Security Hub 使用服务相关角色。有关此角色的详细信息，请参阅Service-linked 的角色 AWS Security Hub。

> **Warning**
>
> 更改服务角色的权限可能会在您使用 Security Hub 时导致操作问题。仅当 Security Hub 提供相关指导时才编辑服务角色。

Security Hub 的服务相关角色

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

要代表您执行操作，Security Hub 使用服务相关角色。有关此角色的详细信息，请参阅Service-linked 的角色 AWS Security Hub。

基于身份的策略示例 AWS Security Hub CSPM

默认情况下，用户和角色无权创建或修改 Security Hub CSPM 资源。他们也无法使用 AWS 管理控制台 AWS CLI、或 AWS API 执行任务。管理员必须创建 IAM policy，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的在 JSON 选项卡上创建策略。

主题

- 策略最佳实践
- 使用 Security Hub CSPM 控制台
- 示例：允许用户查看自己的权限
- 示例：允许用户查看调查发现
- 示例：允许用户创建和管理自动化规则

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Security Hub 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Security Hub CSPM 控制台

要访问 AWS Security Hub CSPM 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Security Hub CSPM 资源的详细信息。 AWS 账户如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保这些用户和角色可以使用 Security Hub CSPM 控制台，还要将以下 AWS 托管策略附加到实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

JSON

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

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

示例：允许用户查看自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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": "*"
        }
    ]
}
```

示例：允许用户查看调查发现

此示例说明如何创建允许用户查看 Security Hub CSPM 发现结果的 IAM 策略。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}
```

示例：允许用户创建和管理自动化规则

此示例说明如何创建允许用户创建、查看、更新和删除 Security Hub CSPM 自动化规则的 IAM 策略。要使此 IAM 策略发挥作用，用户必须是 Security Hub CSPM 管理员。要限制权限（例如，允许用户仅查看自动化规则），您可以移除创建、更新和删除权限。

```
{
            "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 的角色 AWS Security Hub

AWS Security Hub 使用名`AWSServiceRoleForSecurityHubV2`为的 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Security Hub 直接关联的 IAM 角色。它由 Security Hub 预定义，它包括 Security Hub 代表你调用其他资源 AWS 服务 和监控 AWS 资源所需的所有权限。Security Hub 在所有可用 Security Hub AWS 区域 的地方都使用此服务相关角色。

您可以使用服务相关角色轻松设置 Security Hub，因为您不必手动添加所需的权限。Security Hub 定义其服务相关角色的权限，除非另有定义，否则只有 Security Hub 可以代入该角色。定义的权限包括信任策略和权限策略，您不能将该权限策略附加到任何其他 IAM 实体。

要查看服务相关角色的详细信息，您可以使用 Security Hub 控制台。在导航窗格中的设置下，选择常规。然后，在服务权限部分，选择查看服务权限。

您必须首先在启用了 Security Hub 的所有区域中禁用它，然后才能删除 Security Hub 服务相关角色。这会保护您的 Security Hub 资源，因为您不会无意中删除这些资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅AWS IAM 用户指南中的与 IAM 配合使用的服务，并在Service-linked 角色列中找到标有 “是” 的服务。选择带有链接的是可以查看该服务的服务相关角色文档。

主题

- Service-linked Security Hub 的角色权限
- 为 Security Hub 创建服务相关角色
- 为 Security Hub 编辑服务相关角色
- 为 Security Hub 删除服务相关角色

Service-linked Security Hub 的角色权限

Security Hub 使用名为 AWSServiceRoleForSecurityHubV2 的服务相关角色。这是 Sec AWS urity Hub 访问您的资源所需的服务相关角色。此服务相关角色允许 Security Hub 执行任务，例如从他人那里接收调查结果 AWS 服务 和配置必要的 AWS Config 基础架构以运行安全检查以进行控制措施。AWSServiceRoleForSecurityHubV2 服务关联角色信任 securityhub.amazonaws.com 服务来代入角色。

AWSServiceRoleForSecurityHubV2 服务相关角色使用托管策略 AWSSecurityHubV2ServiceRolePolicy。

必须授予权限，允许 IAM 身份（如角色、组或用户）创建、编辑或删除服务相关角色。为了成功创建 AWSServiceRoleForSecurityHubV2 服务相关角色，用于访问 Security Hub 的 IAM 身份必须具有所需的权限。要授予所需的权限，请将以下策略附加到 IAM 身份。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

为 Security Hub 创建服务相关角色

当您首次启用 Security Hub 或在之前未启用过 Security Hub 的区域启用它时，系统会自动创建 `AWSServiceRoleForSecurityHubV2` 服务相关角色。您还可以使用 IAM 控制台、IAM API 或 IAM API 创建 `AWSServiceRoleForSecurityHubV2` 服务相关角色。有关手动创建角色的更多信息，请参阅 IAM 用户指南中的创建服务相关角色。

> **Important**
>
> 为 Security Hub 管理员账户创建的服务相关角色不适用于关联的 Security Hub 成员账户。

为 Security Hub 编辑服务相关角色

Security Hub 不允许您编辑 `AWSServiceRoleForSecurityHubV2` 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

为 Security Hub 删除服务相关角色

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

禁用 Security Hub 时，Security Hub 不会自动为您删除 `AWSServiceRoleForSecurityHubV2` 服务相关角色。如果再次启用 Security Hub，该服务就可以再次开始使用现有的服务相关角色。如果您不再需要使用 Security Hub，则可以手动删除服务相关角色。

> **Important**
>
> 在删除 `AWSServiceRoleForSecurityHubV2` 服务相关角色之前，您必须先在启用了 Security Hub 的所有区域禁用它。有关更多信息，请参阅 禁用 Security Hub。如果在您尝试删除服务相关角色时未禁用 Security Hub，删除将失败。

要删除 AWSServiceRoleForSecurityHubV2 服务相关角色，您可以使用 IAM 控制台、IAM CLI 或 IAM API。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

AWS Security Hub 的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：AWSSecurityHubFullAccess

您可以将 AWSSecurityHubFullAccess 策略附加到 IAM 身份。

此策略授予管理权限，允许主体完全访问所有 Security Hub 操作。在主体为其账户手动启用 Security Hub 之前，必须将此策略附加到主体。例如，拥有这些权限的主体可以查看和更新调查发现的状态。他们还可以配置自定义见解、启用集成以及启用和禁用标准和控件。管理员账户的主体也可以管理成员账户。

权限详细信息

该策略包含以下权限：

- securityhub：允许主体访问所有 Security Hub 操作。
- guardduty— 允许委托人在 Amazon GuardDuty 中获取有关账户状态的信息。
- iam— 允许委托人为 Security Hub 创建服务相关角色。
- inspector：允许主体在 Amazon Inspector 中获取有关账户状态的信息。
- pricing— 允许校长获取 AWS 服务 和产品的价目表。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubFullAccess。

AWS 托管策略：AWSSecurityHubReadOnlyAccess

您可以将 AWSSecurityHubReadOnlyAccess 策略附加到 IAM 身份。

此策略授予只读权限，允许用户查看 Security Hub 中的信息。附加了此策略的主体无法在 Security Hub 中进行任何更新。例如，拥有这些权限的主体可以查看与其账户关联的调查发现列表，但不能改变调查发现的状态。他们可以查看见解的结果，但不能创建或配置自定义见解。他们无法配置控件或产品集成。

权限详细信息

该策略包含以下权限：

- securityhub：允许用户执行返回项目列表或项目详细信息的操作。这包括以Get、List 或 Describe 开头的 API 操作。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubReadOnlyAccess。

AWS 托管策略：AWSSecurityHubOrganizationsAccess

您可以将 AWSSecurityHubOrganizationsAccess 策略附加到 IAM 身份。

此策略授予管理权限，以便为中的组织启用和管理 Security Hub AWS Organizations。此策略的权限允许组织管理账户为 Security Hub 指定委托管理员帐户。它们还允许委派管理员账户将组织账户启用为成员账户。

此策略仅为提供权限 AWS Organizations。组织管理账户和委派管理员账户也需要关联操作的权限。这些权限可以使用 AWSSecurityHubFullAccess 管理策略来授予。

权限详细信息

该策略包含以下权限：

- organizations:ListAccounts：允许主体检索属于某个组织的账户列表。
- organizations:DescribeOrganization：允许主体检索有关组织的信息。
- organizations:ListRoots：允许主体列出组织的根。
- organizations:ListDelegatedAdministrators：允许主体列出组织的委派管理员。
- organizations:ListAWSServiceAccessForOrganization— 允许委托人列出组织使用 AWS 服务 的。

- organizations:ListOrganizationalUnitsForParent：允许主体列出父组织单元（OU）的子 OU。
- organizations:ListAccountsForParent：允许主体列出父 OU 的子账户。
- organizations:ListParents – 列出根或组织单元（OU），它们作为指定子 OU 或账户的直接父级。
- organizations:DescribeAccount – 让委托人可以检索有关企业中某个账户的信息。
- organizations:DescribeOrganizationalUnit：允许主体检索有关组织中某个 OU 的信息。
- organizations:ListPolicies – 检索指定类型的组织中所有策略的列表。
- organizations:ListPoliciesForTarget – 列出直接附加到指定的目标根、组织单元（OU）或账户的策略。
- organizations:ListTargetsForPolicy – 列出指定的策略附加到的所有根、组织单元（OU）和账户。
- organizations:EnableAWSServiceAccess – 允许主体启用与 Organions 的集成。
- organizations:RegisterDelegatedAdministrator – 允许主体指定委派管理员账户。
- organizations:DeregisterDelegatedAdministrator – 允许主体移除委派管理员账户。
- organizations:DescribePolicy – 检索有关策略的信息。
- organizations:DescribeEffectivePolicy – 返回指定的策略类型和账户的有效策略的内容。
- organizations:CreatePolicy— 创建指定类型的策略，您可以将其附加到根帐户、组织单位 (OU) 或个人 AWS 账户。
- organizations:UpdatePolicy – 使用新的名称、描述或内容更新现有策略。
- organizations:DeletePolicy – 从您的组织中删除指定的策略。
- organizations:AttachPolicy – 将策略附加到根、组织单元（OU）或单个账户。
- organizations:DetachPolicy – 将策略从目标根、组织单元（OU）或账户分离。
- organizations:EnablePolicyType – 在根中启用一种策略类型。
- organizations:DisablePolicyType – 在根中禁用一种组织策略类型。
- organizations:TagResource – 将一个或多个标签添加到指定的资源。
- organizations:UntagResource – 从指定的资源中移除具有指定密钥的任何标签。
- organizations:ListTagsForResource – 列出附加到指定资源的标签。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubOrganizationsAccess。

AWS 托管策略：AWSSecurityHubV2ServiceRolePolicy

此策略允许 Security Hub 代表您管理组织中的 AWS Config 规则和 Security Hub 资源。此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到 IAM 身份。有关更多信息，请参阅 the section called “Service-linked 角色”。

权限详细信息

该策略包含以下权限：

- `access-analyzer`— 当客户启用或禁用 Security Hub 时，创建和删除与服务相关的 IAM 访问分析器，列出分析器以验证分析器状态是否与启用状态一致，并针对未使用的访问发现生成和检索策略建议。
- `cloudwatch`— 检索指标数据以支持 Security Hub 资源和 Connector 运行状况指标的计量功能。
- `config`— 管理 Security Hub 资源的与服务相关的配置记录器和第三方服务关联的配置记录器，包括对全局 Config 记录器的支持。列出配置记录器并获取连接器信息，以支持第三方云集成。
- `ecr`— 检索有关 Amazon Elastic Container Registry 镜像和存储库的信息，以支持
- `iam`— 创建以下与服务相关的角色： AWS Config、客户账户中的 IAM Access Analyzer 和用于第三方扫描的 Amazon Inspector。检索账户信息以支持计量功能。检索现有 IAM 策略，以便客户可以查看其当前策略与建议的最低权限替代策略的比较。
- `inspector2`— 创建、更新、删除和列出 Amazon Inspector 连接器和连接器扫描配置，以支持第三方云集成。
- `lambda`— 检索 AWS Lambda 功能信息以支持计量功能。
- `organizations`：检索组织的账户和组织单元（OU）信息。
- `securityhub` – 管理 Security Hub 配置。创建、更新和删除 Security Hub 连接器以支持第三方云集成。
- `sts`— 获取用于出站身份联合的 Web 身份令牌，以支持第三方云集成。
- `tag`：检索有关资源标签的信息。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubV2ServiceRolePolicy。

Security Hub 更新至 AWS 托管策略

下表提供了自该服务开始跟踪这些更改以来对 S AWS ecurity Hub AWS 托管策略的更新的详细信息。有关策略更新的自动提醒，请订阅 Security Hub 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSSecurityHubV2ServiceRolePolicy - 更新的策略	Security Hub 更新了政策以支持第三方集成。此更新增加了以下权限：管理第三方配置记录器、创建和管理 Security Hub 和 Amazon Inspector 连接器、从中检索连接器运行状况指标 CloudWatch、创建用于第三方扫描的 Amazon Inspector 服务关联角色以及获取用于联合身份验证的网络身份令牌。	2026 年 6 月 30 日
AWSSecurityHubV2ServiceRolePolicy - 更新的策略	Security Hub 更新了策略，添加了 IAM 访问分析器权限。此更新允许 Security Hub 创建和管理服务托管分析器，列出分析器以验证分析器配置是否与启用状态一致，生成和检索未使用的访问结果的策略建议，以及检索 IAM 策略以显示建议。	2026年5月10日
AWSSecurityHubOrganizationsAccess - 更新的策略	Security Hub 更新了策略，添加了描述支持 Security Hub 功能的资源策略的权限。Security Hub 目前为预览版，可能会发生变化。	2025 年 11 月 12 日
AWSSecurityHubFullAccess - 更新的策略	Security Hub 更新了政策，增加了管理 GuardDuty、Amazon Inspector 和账户管理方面的功能，以支持 Security Hub 的功能。Security Hub 目前为预览版，可能会发生变化。	2025 年 11 月 17 日

更改	描述	日期
AWSSecurityHubV2ServiceRolePolicy - 更新的策略	Security Hub 更新了政策，增加了亚马逊弹性容器注册表 AWS Lambda、亚马逊的计量功能 CloudWatch，并 AWS Identity and Access Management 支持 Security Hub 的功能。此更新还增加了对全局 AWS Config 录音机的支持。Security Hub 目前为预览版，可能会发生变化。	2025 年 11 月 5 日
AWSSecurityHubOrganizationsAccess：对现有策略的更新	Security Hub 为策略添加了新的权限。这些权限允许组织管理层为组织启用和管理 Security Hub 和 Security Hub CSPM。	2025 年 6 月 17 日
AWSSecurityHubFullAccess：对现有策略的更新	Security Hub CSPM 新增了权限，允许主体为 Security Hub 创建服务相关角色。	2025 年 6 月 17 日
AWSSecurityHubV2ServiceRolePolicy：新策略	Security Hub 添加了一项新政策，允许 Security Hub 代表客户组织管理 AWS Config 规则和 Security Hub 资源。Security Hub 目前为预览版，可能会发生变化。	2025 年 6 月 17 日
AWSSecurityHubFullAccess— 更新现有政策	Security Hub CSPM 更新了政策，以获取 AWS 服务 和产品的定价详情。	2024 年 4 月 24 日
AWSSecurityHubReadOnlyAccess— 更新现有政策	Security Hub CSPM 通过添加 `Sid` 字段更新了此托管策略。	2024 年 2 月 22 日

更改	描述	日期
AWSSecurityHubFullAccess— 更新现有政策	Security Hub CSPM 更新了政策，因此它可以确定账户中是否启用了亚马逊 GuardDuty 和亚马逊 Inspector。这可以帮助客户汇集来自多个 AWS 服务与安全相关的信息。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess— 更新现有政策	Security Hub CSPM 更新了授予额外权限的策略，允许以只读方式访问 AWS Organizations 委派管理员功能。这包括根、组织单元（OU）、账户、组织结构和服务访问权限等详细信息。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess— 新政策	Security Hub CSPM 添加了一项新策略，该策略授予 Security Hub CSPM 与 Organizations 集成所需的权限。	2021 年 3 月 15 日
Security Hub CSPM 开始跟踪更改	Security Hub CSPM 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 15 日

对 Sec AWS urity Hub 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Sec AWS urity Hub 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Security Hub 中执行操作
- 我无权执行 iam：PassRole
- 我想以编程方式访问 Security Hub
- 我是管理员并希望允许其他人访问 Security Hub
- 我想允许我以外的人访问我的 S AWS 账户 ecurity Hub 资源

我无权在 Security Hub 中执行操作

如果 AWS 管理控制台 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当用户mateojackson尝试使用控制台查看有关某的详细信息*widget*但没有securityhub:*GetWidget*权限时，就会出现以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 securityhub:*GetWidget* 操作访问 *my-example-widget* 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Security Hub。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Security Hub 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想以编程方式访问 Security Hub

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS 管理控制台。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
IAM	（推荐）使用控制台凭证作为临时凭证，签署对 AWS CLI AWS SDKs、或的编程请求 AWS APIs。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》中的“登录 AWS 本地开发”。 • 有关信息 AWS SDKs，请参阅《工具参考指南》AWS SDKs 和《工具参考指南》中的登录进行 AWS 本地开发。
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关工具和 AWS SDKs AWS APIs，请参阅《工具参考指南》中的 IAM 身份中心身份验证AWSSDKs 和工具参考指南。
IAM	使用临时证书签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。
IAM	（不推荐使用）	按照您希望使用的界面的说明进行操作。

哪个用户需要编程式访问权限？	目的	方式
	使用长期凭证签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。	• 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDKs 和工具，请参阅《工具参考指南》AWS SDKs 和《工具参考指南》中的使用长期凭证进行身份验证。 • 有关信息 AWS APIs，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

我是管理员并希望允许其他人访问 Security Hub

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

我想允许我以外的人访问我的 S AWS 账户 ecurity Hub 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Security Hub 是否支持这些功能，请参阅 Security Hub 如何与 IAM 协同工作。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的合规性验证 AWS Security Hub

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

Sec AWS urity Hub 中的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。各区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

Security Hub 中的基础设施 AWS 安全

作为一项托管服务，Sec AWS urity Hub 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Security Hub。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

AWS Security Hub 和接口 VPC 终端节点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点在您的 VPC 和 Sec AWS urity Hub 之间建立私有连接。接口端点由一项技术提供支持 AWS PrivateLink，该技术使您 APIs 无需互联网网关、NAT 设备、VPN 连接或 Di AWS rect Connect 连接即可私密访问 Security Hub。您的 VPC 中的实例不需要公有 IP 地址即可与 Security Hub 通信 APIs。VPC 和 Security Hub 之间的流量不会脱离 Amazon 网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。有关更多信息，请参阅《Amazon Virtual Private Cloud 指南》中的AWS 服务 使用接口 VPC 终端节点访问和。

Security Hub VPC 端点的注意事项

在为 Security Hub 设置接口 VPC 端点之前，请务必查看《Amazon Virtual Private Cloud 指南》中的先决条件和其他信息。

Security Hub 支持从 VPC 调用它的所有 API 操作。

为 Security Hub 创建接口 VPC 端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 Security Hub 服务创建 VPC 终端节点。有关更多信息，请参阅《Amazon Virtual Private Cloud 指南》中的创建 VPC 端点。

使用以下服务名称为 Security Hub 创建 VPC 端点：

```
com.amazonaws.region.securityhub
```

适*region*用的地区代码在哪里 AWS 区域。

如果为端点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 Security Hub 发出 API 请求，例如，美国东部（弗吉尼亚州北部）区域为 `securityhub.us-east-1.amazonaws.com`。

为 Security Hub 创建 VPC 端点策略

您可以为 VPC 端点附加控制对 Security Hub 的访问的端点策略。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon Virtual Private Cloud 指南》中的使用端点策略控制对 VPC 端点的访问。

示例：Security Hub 操作的 VPC 端点策略

下面是用于 Security Hub 的端点策略示例。当附加到端点时，此策略会向所有资源上的所有主体授予对列出的 Security Hub 操作的访问权限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

共享子网

您无法在与您共享的子网中创建、描述、修改或删除 VPC 端点。但是，您可以在与您共享的子网中使用 VPC 端点。有关 VPC 共享的信息，请参阅《Amazon Virtual Private Cloud 指南》中的与其他账户共享 VPC 子网。

使用记录 Security Hub API 调用 CloudTrail

与一项服务集成 AWS CloudTrail，该服务提供用户、角色或 AWS 服务在 Security Hub 中执行的操作的记录。 CloudTrail 将 Security Hub 的 API 调用捕获为事件。捕获的调用包含来自 Security Hub 控制台和代码的 Security Hub API 操作调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Security Hub 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 主机上的事件历史记录中查看最新的事件。使用 CloudTrail 收集到的信息，您可以确定向 Security Hub 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，包括如何配置和启用它，请参阅《AWS CloudTrail 用户指南》。

Security Hub 信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Security Hub 中出现支持的事件活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

要持续记录账户中的事件（包括 Security Hub 的事件），请创建跟踪记录。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。在控制台创建跟踪时，跟踪默认应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

Security Hub 支持将所有 Security Hub API 操作作为事件 CloudTrail 记录在日志中。要查看 Security Hub 操作的列表，请参阅 Security Hub API 参考。

将以下操作的活动记录到时 CloudTrail，的值将设置`responseElements`为`null`。这样可以确保 CloudTrail 日志中不包含敏感信息。

- `GetFindingsV2`

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户证书还是 AWS Identity and Access Management (IAM) 用户凭证发出
- 请求是使用角色还是联合用户的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

示例：Security Hub 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该`CreateAutomationRuleV2`操作的 CloudTrail 日志条目。在此示例中，创建了一条名`TestAutomationRule`为的自动化规则。`Severity`和`Account ID`属性被指定为标准。匹配规则后，将更新`Severity`为 “高”。有关自动化规则的更多信息，请参阅Security Hub 中的自动化规则。

```
{
    "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"
}
```

简介 AWS Security Hub CSPM

AWS Security Hub 云AWS 安全态势管理 (Security Hub CSPM) 可让您全面了解自己的安全状态，AWS 并帮助您根据安全行业标准和最佳实践评估您的 AWS 环境。

AWS Security Hub CSPM 收集跨 AWS 账户第三方产品和支持的第三方产品的安全数据，并帮助您分析安全趋势并确定优先级最高的安全问题。 AWS 服务

为了帮助您管理组织的安全状态，Security Hub CSPM 支持多种安全标准。其中包括由互联网安全中心 (CIS) AWS、支付卡行业数据安全标准 (PCI DSS) 和美国国家标准与技术研究院 (NIST) 制定的 AWS 基础安全最佳实践 (FSBP) 标准和外部合规框架。每个标准都包含多个安全控件，每种控件都代表一种安全最佳实践。Security Hub CSPM 对安全控件进行检查并生成控件调查发现，以帮助您评测您是否符合安全最佳实践。

除了生成控制结果外，Security Hub CSPM还会收到来自其他产品 AWS 服务（例如亚马逊、Amazon Insp GuardDuty ector和Amazon Macie）和支持的第三方产品的调查结果。这使您可以通过单一窗格来解决各种与安全相关的问题。您还可以将 Security Hub CSPM 调查发现发送到其他 AWS 服务 和受支持的第三方产品。

Security Hub CSPM 提供自动化功能，可帮助您对安全问题进行分类和修复。例如，当安全检查失败时，您可以使用自动化规则自动更新关键调查发现。您还可以利用与 Amazon 的集成 EventBridge 来触发对特定发现的自动响应。

主题

- Security Hub CSPM 的优点
- 访问 Security Hub CSPM
- 相关服务
- Security Hub CSPM 免费试用和定价
- Security Hub CSPM 中的概念和术语
- 启用 Security Hub CSPM
- 管理 Security Hub CSPM 中的管理员账户和成员账户
- 了解 Security Hub CSPM 中的跨区域聚合
- 了解 Security Hub CSPM 中的安全标准
- 了解 Security Hub CSPM 中的安全控件
- 了解 Security Hub CSPM 中的集成

- 在 Security Hub CSPM 中创建和更新调查发现
- 在 Security Hub CSPM 中查看见解
- 自动修改 Security Hub CSPM 中的调查发现并对其采取行动
- 使用 Security Hub CSPM 中的控制面板
- Security Hub CSPM 的区域限制
- 使用创建 Security Hub CSPM 资源 CloudFormation
- 通过 Amazon SNS 订阅 Security Hub CSPM 公告
- 禁用 Security Hub CSPM
- 中的安全性 AWS Security Hub CSPM
- 使用记录 Security Hub API 调用 CloudTrail

Security Hub CSPM 的优点

以下是 Security Hub CSPM 帮助您监控整个环境中的合规性和安全状况的一些主要方法。 AWS

减少了收集结果并确定其优先次序的工作

Security Hub CSPM 减少了收集来自集成产品和 AWS 合作伙伴产品的各个账户的安全发现 AWS 服务 并确定其优先顺序的工作量。Security Hub CSPM 使用 AWS 安全查找格式 (ASFF) (一种标准查找格式) 处理查找数据。这样就无需管理来自多种来源的多种格式的调查发现。Security Hub CSPM 还将各提供商的调查发现相关联，以帮助您确定最重要几项的优先级。

根据最佳实践和标准进行自动安全检查

Security Hub CSPM 根据 AWS 最佳实践和行业标准自动运行持续的账户级配置和安全检查。Security Hub CSPM 使用这些检查的结果来计算安全分数，并识别需要关注的特定账户和资源。

跨账户和提供商的结果的综合视图

Security Hub CSPM 将合并账户和提供商产品的安全调查发现，然后在 Security Hub CSPM 控制台上显示结果。你也可以通过 Security Hub CSPM API 或软件开发工具包检索发现。 AWS CLI通过全面了解您当前的安全性状态，您可以发现趋势、识别潜在问题并采取必要的补救措施。

自动调查发现更新和修复的能力

您可以创建自动化规则，根据您定义的标准修改或隐藏调查发现。Security Hub CSPM 还支持与亚马逊的集成。 EventBridge要自动修复特定调查发现，您可以定义在生成调查发现时要执行的自定义操作。例如，您可以配置自定义操作，将结果发送到票证系统或自动修复系统。

访问 Security Hub CSPM

Security Hub CSPM 在大多数版本中都可用。 AWS 区域有关当前已推出 Security Hub CSPM 的所有区域的列表，请参阅 AWS 一般参考 中的 AWS Security Hub CSPM 端点和配额。有关管理 AWS 区域您的账户的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》中的指定 AWS 区域 您的账户可以使用。

在每个区域，您可以通过以下任一方式访问和使用 Security Hub CSPM：

Security Hub CSPM 控制台

AWS 管理控制台 是一个基于浏览器的界面，可用于创建和管理 AWS 资源。作为该控制台的一部分，Security Hub CSPM 控制台提供对您的 Security Hub CSPM 账户、数据和资源的访问权限。您可以使用 Security Hub CSPM 控制台执行 Security Hub CSPM 任务，包括查看调查发现、创建自动化规则、创建聚合区域等。

Security Hub CSPM API

Security Hub CSPM API 允许您以编程方式访问您的 Security Hub CSPM 账户、数据和资源。使用该 API，您可以直接向 Security Hub CSPM 发送 HTTPS 请求。有关 API 的信息，请参阅 AWS Security Hub API 参考。

AWS CLI

借助 AWS CLI，您可以在系统的命令行上运行命令来执行 Security Hub CSPM 任务。与使用控制台相比，在某些情况下使用命令行更快、更方便。如果要构建执行任务的脚本，命令行也会十分有用。有关安装和使用的信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》。

AWS 软件开发工具包

AWS 提供由各种编程语言和平台（例如 Java、Go、Python、C++ 和.NET）的库和示例代码组成的软件开发工具包。这些软件开发工具包以您的首选语言提供对 Security Hub CSPM 和其他 AWS 服务 语言的便捷编程访问。它们可以执行多种任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求等。有关安装和使用 AWS 软件开发工具包的信息，请参阅构建工具。 AWS

Important

Security Hub CSPM 仅检测和整合启用 Security Hub CSPM 后生成的调查发现。它不会以追溯方式检测和整合在启用 Security Hub CSPM 前生成的安全调查发现。
Security Hub CSPM 仅接收和处理您在账户中启用 Security Hub CSPM 的区域中的调查发现。

要完全符合 CIS AWS 基金会基准安全检查，您必须在所有支持的 AWS 区域启用 Security Hub CSPM。

相关服务

为了进一步保护您的 AWS 环境，可以考虑将其他与 Secur AWS 服务 ity Hub CSPM 结合使用。有些人 AWS 服务 将调查结果发送给 Security Hub CSPM，而 Security Hub CSPM 则将调查结果标准化为标准格式。有些人 AWS 服务 还可以从 Security Hub CSPM 那里收到调查结果。

有关发送或接收 Secur AWS 服务 ity Hub CSPM 发现结果的其他人的列表，请参阅。AWS 服务 与 Security Hub CSPM 集成

Security Hub CSPM 使用中的服务相关规则 AWS Config 对大多数控件进行安全检查。控件是指特定 AWS 服务 和 AWS 资源。有关 Security Hub CSPM 控件列表，请参阅 Security Hub CSPM 控件参考。您必须启用 AWS Config 并记录资源， AWS Config 以便 Security Hub CSPM 生成大部分控制结果。有关更多信息，请参阅 启用和配置前的注意事项 AWS Config。

Security Hub CSPM 免费试用和定价

当你首次在中启用 Security Hub CSPM 时，该账户将自动注册 AWS 账户 为期 30 天的 Security Hub CSPM 免费试用。

在免费试用期间使用 Security Hub CSPM 时，您需要为使用 Security Hub CSPM 与之交互的其他服务（例如项目）付费。 AWS Config 对于仅通过 Security Hub CSPM 安全标准激活的 AWS Config 规则，您无需支付任何费用。

在免费试用期结束之前，您不必为使用 Security Hub CSPM 付费。

查看使用情况详情

Security Hub CSPM 提供使用信息，包括您的账户处理的安全检查次数和发现次数。使用详情还包括免费试用的剩余时间。这些信息可以帮助你了解免费试用期结束后的 Security Hub CSPM 使用情况。免费试用结束后，还会提供使用信息。免费试用结束后，还可以查看使用信息。

显示使用信息（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中的设置下，选择使用情况。

使用信息仅适用于当前账户和当前区域。在聚合区域中，使用情况信息不包括关联区域。有关关联区域的更多信息，请参阅 the section called “聚合的数据类型”。

要查看您账户的费用明细，请使用AWS 账单控制台。

定价详细信息

有关 Security Hub CSPM 如何对提取调查发现和安全检查收费的更多信息，请参阅 Security Hub CSPM 定价。

Security Hub CSPM 中的概念和术语

在 S AWS ecurity Hub CSPM 中，我们建立在常用 AWS 概念和术语的基础上，并使用这些附加术语。

Account

包含您的 AWS 资源的标准亚马逊 Web Services (AWS) 账户。你可以 AWS 使用自己的账户登录并启用 Security Hub CSPM。

一个账户可以邀请其他账户启用 Security Hub CSPM，并在 Security Hub CSPM 中与该账户建立关联。接受成员资格邀请是可选的。如果邀请被接受，该账户成为管理员账户，而被添加的账户成为成员账户。管理员账户可以在其成员账户中查看调查发现。

如果您已注册 AWS Organizations，则您的组织将为该组织指定一个 Security Hub CSPM 管理员帐户。Security Hub CSPM 管理员账户可以启用其他组织账户作为成员账户。

账户不能既是管理员账户又是成员账户。一个账户只能有一个管理员账户。

有关更多信息，请参阅 管理 Security Hub CSPM 中的管理员账户和成员账户。

管理员账户

Security Hub CSPM 中被授予查看相关成员账户调查发现权限的账户。

账户通过以下方式之一成为管理员账户：

- 该账户邀请其他账户在 Security Hub CSPM 中与其建立关联。当这些账户接受邀请时，它们就会成为成员账户，发送邀请的账户则成为他们的管理员账户。
- 该账户由组织管理账户指定为 Security Hub CSPM 管理员账户。Security Hub CSPM 管理员账户可以启用任何组织账户作为成员账户，还可以邀请其他账户成为成员账户。

一个账户只能有一个管理员账户。账户不能既是管理员账户又是成员账户。

聚合区域

设置聚合区域允许您在单个控制面板 AWS 区域 中查看来自多个区域的安全发现。

聚合区域是您从中查看和管理调查发现的区域。调查发现将从关联区域汇总到聚合区域。调查发现的更新会跨区域复制。

在聚合区域中，安全标准、见解和调查发现页面包含来自所有关联区域的数据。

有关更多信息，请参阅 the section called “跨区域聚合数据”。

存档的调查发现

其记录状态（`RecordState`）为 `ARCHIVED` 的调查发现。将调查发现存档表明调查发现提供者认为该调查发现已不再相关。记录状态与工作流状态不同，其跟踪调查发现的调查状态。

调查发现提供者可以使用 Security Hub CSPM API 的 BatchImportFindings 操作来存档他们创建的调查发现。Security Hub CSPM 会自动存档符合特定条件的控件调查发现。有关更多信息，请参阅生成、更新和存档控件调查发现。

在 Security Hub CSPM 控制台上，默认筛选设置会将存档的调查发现从调查发现列表和表格中排除。您可以更新设置以包括存档的调查发现。如果使用 Security Hub CSPM API 的 GetFindings 操作检索调查发现，则该操作会检索已存档的调查发现和活跃调查发现。要排除已存档的调查发现，您可以对结果进行筛选。例如：

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS 安全调查结果格式 (ASFF)

Security Hub CSPM 聚合或生成的调查发现内容的标准化格式。 AWS 安全调查结果格式使您可以使用 Security Hub CSPM 来查看和分析由 AWS 安全服务、第三方解决方案或 Security Hub CSPM 本身在运行安全检查时生成的发现。有关更多信息，请参阅 AWS 安全调查结果格式 (ASFF)。

控件

为信息系统或组织规定的一种保护措施或对策，旨在保护信息的机密性、完整性和可用性并满足一组已定义的安全性要求。安全标准与控件集合相关联。

“安全控件”一词是指各类标准的具有单一控件 ID 和标题的控件。标准控制一词是指具有特定标准控件 IDs 和标题的控件。目前，Security Hub CSPM 仅在中国区域和 AWS GovCloud (US) Regions 支持标准控件。所有其他区域均支持安全控件。

自定义操作

一种 Security Hub CSPM 机制，用于将选定的结果发送到。 EventBridge在 Security Hub CSPM 中创建一个自定义操作。然后将其链接到 EventBridge 规则。该规则定义在收到与自定义操作 ID 关联的调查发现时执行的特定操作。例如，可以使用自定义操作将特定调查发现或一小部分调查发现发送到响应或修复工作流。有关更多信息，请参阅 the section called “创建自定义操作”。

委派管理员账户（Organizations）

在中 AWS Organizations，服务的委派管理员帐户能够管理组织对服务的使用。

在 Security Hub CSPM 中，Security Hub CSPM 管理员账户也是 Security Hub CSPM 的委派管理员账户。当组织管理账户首次指定 Security Hub CSPM 管理员账户时，Security Hub CSPM 会调用 Organizations，将该账户设为委派管理员账户。

然后，组织管理账户必须选择委派管理员账户作为所有区域的 Security Hub CSPM 管理员账户。

调查发现

安全检查或与安全相关的检测的可观察记录。完成控件的安全检查后，Security Hub CSPM 会生成并更新调查发现。这些被称为控件调查发现。调查结果也可能来自与其他产品 AWS 服务 和第三方产品的集成。

有关更多信息，请参阅 the section called “结果”。

跨区域聚合

将关联区域的调查发现、见解、控件合规状态和安全评分汇总到聚合区域。然后，您可以查看聚合区域中的所有数据，并更新聚合区域的发现和见解。

有关更多信息，请参阅 the section called “跨区域聚合数据”。

调查发现摄取

将来自其他 AWS 服务和第三方合作伙伴提供商的调查结果导入 Security Hub CSPM。

调查发现摄取事件包括新调查发现和现有调查发现的更新。

见解

由聚合语句和可选的筛选器定义的相关调查发现的集合。见解确定了需要注意和干预的安全区域。Security Hub CSPM 提供了一些您无法修改的托管（默认）见解。您还可以创建自定义

Security Hub CSPM 见解，以跟踪您的 AWS 环境和使用情况所特有的安全问题。有关更多信息，请参阅 the section called “见解”。

关联区域

启用跨区域聚合时，关联区域是将调查发现、见解、控件合规状态和安全评分汇总到聚合区域的区域。

在关联区域中，调查发现和见解页面仅包含该区域的调查发现。

有关更多信息，请参阅 the section called “跨区域聚合数据”。

成员账户

已授予管理员账户查看和处理其调查发现的权限的账户。

账户通过以下方式之一成为成员账户：

- 该账户接受来自其他账户的邀请。
- 对于组织账户，Security Hub CSPM 管理员账户将该账户启用为成员账户。

相关要求

与某个控件对应的一组行业或监管要求。

规则

一组自动化标准，用于评测是否已坚持使用控件。在评估规则时，评估结果可能是通过或失败。如果评估无法确定规则是通过还是失败，则规则将处于警告状态。如果无法评估规则，则规则会处于不可用状态。

安全检查

针对单一资源对规则 point-in-time进行具体评估，结果为PASSEDFAILED、WARNING、或NOT_AVAILABLE状态。运行安全检查将生成一个调查发现。

Security Hub CSPM 管理员账户

管理组织的 Security Hub CSPM 成员资格的组织账户。

组织管理账户在每个区域指定 Security Hub CSPM 管理员账户。组织管理账户必须在所有区域选择相同的 Security Hub CSPM 管理员账户。

Security Hub CSPM 管理员账户也是 Organizations 中 Security Hub CSPM 的委派管理员账户。

Security Hub CSPM 管理员账户可以启用任何组织账户作为成员账户。Security Hub CSPM 管理员账户还可以邀请其他账户成为成员账户。

安全标准

发布的关于某一主题的声明，该声明指定了必须满足或实现才能获得合规性的特征（通常为可衡量的控制措施）。安全标准可以基于监管框架、最佳实践或内部公司策略。控件可能与 Security Hub CSPM 中一个或多个支持的标准相关联。要了解有关 Security Hub CSPM 中的安全标准的更多信息，请参阅了解 Security Hub CSPM 中的安全标准。

严重性

分配给 Security Hub CSPM 控件的严重性确定该控件的重要性。控件的严重性，可以为严重、高、中等、低或信息性。分配给控件调查发现的“严重性”等于控件本身的“严重性”。要了解 Security Hub CSPM 如何为控件分配严重性，请参阅控件调查发现的严重性级别。

工作流状态

对发现的调查状态。这使用 `Workflow.Status` 属性进行跟踪。

工作流状态初始为 `NEW`。如果已通知资源所有者对调查发现执行操作，可以将工作流状态设置为 `NOTIFIED`。如果调查发现没有问题，不需要执行任何操作，可以将工作流状态设置为 `SUPPRESSED`。查看并修复调查发现后，可以将工作流状态设置为 `RESOLVED`。

默认情况下，大多数调查发现列表仅包含工作流状态为 `NEW` 或 `NOTIFIED` 的调查发现。控件的发现列表还包括 `RESOLVED` 发现。

要进行 GetFindings 操作，您可以包含工作流状态筛选器。

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Security Hub CSPM 控制台提供了一个选项来设置调查发现的工作流状态。客户（或 SIEM、票证、事件管理或代表客户更新调查发现提供商的调查发现的 SOAR 工具）也可以使用 BatchUpdateFindings 更新工作流状态。

启用 Security Hub CSPM

有两种方法可以启用 Sec AWS urity Hub CSPM，即与集成 AWS Organizations 或手动集成。

在多账户和多区域环境中，我们强烈建议与 Organizations 集成。如果您有独立账户，则需要手动设置 Security Hub CSPM。

确认必要的权限

在注册 Amazon Web Services（AWS）之后，您必须启用 Security Hub CSPM 才能使用其功能和特性。要使用 Security Hub CSPM，您必须设置权限来允许访问 Security Hub CSPM 控制台和 API 操作。为此，您或您的 AWS 管理员可以使用 AWS Identity and Access Management (IAM) 将名为的 AWS 托管策略附加`AWSSecurityHubFullAccess`到您的 IAM 身份。

要通过 Organizations 集成启用和管理 Security Hub CSPM，还应附加名为的 AWS 托管策略。`AWSSecurityHubOrganizationsAccess`

有关更多信息，请参阅 AWS Security Hub 的托管策略。

启用 Security Hub CSPM 与 Organizations 的集成

要开始使用 Security Hub CSPM AWS Organizations，组织的 AWS Organizations 管理账户需要将一个账户指定为该组织委派的 Security Hub CSPM 管理员帐户。Security Hub CSPM 会在当前区域的委派管理员账户中自动启用。

选择您的首选方法，然后按照步骤指定委派管理员账户。

Security Hub CSPM console

在注册时指定 Security Hub CSPM 委派管理员

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 选择转到 Security Hub CSPM。系统会提示您登录到组织管理账户。
3. 在指定委派管理员页面的委派管理员账户部分，指定委派管理员账户。我们建议选择您为其他 AWS 安全与合规服务设置的相同委派管理员。
4. 选择设置委派管理员。

Security Hub CSPM API

从组织管理账户调用 `EnableOrganizationAdminAccount` API。提供 Security Hub CSPM 委派管理员账户的 AWS 账户 ID。

AWS CLI

从 Organizations 管理账户运行 `enable-organization-admin-account` 命令。提供 Security Hub CSPM 委派管理员账户的 AWS 账户 ID。

命令示例：

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

有关与 Organizations 集成的更多信息，请参阅将 Security Hub CSPM 与 AWS Organizations。

中心配置

在集成 Security Hub CSPM 和 Organizations 时，您可以选择使用一项名为中心配置的功能来为组织设置和管理 Security Hub CSPM。我们强烈建议使用中心配置，因为其可让管理员为组织自定义安全范围。在适当情况下，委派管理员可以允许成员账户配置自己的安全范围设置。

中央配置允许授权的管理员跨账户、 OUs和配置 Security Hub CSPM。 AWS 区域委派管理员通过创建配置策略来配置 Security Hub CSPM。在配置策略中，您可以指定以下设置：

- 启用还是禁用 Security Hub CSPM
- 哪些安全标准已启用和禁用
- 哪些安全控件已启用和禁用
- 是否自定义所选控件的参数

作为委托管理员，您可以为整个组织创建单一的配置策略，也可以为不同的账户创建不同的配置策略 OUs。例如，测试账户和生产账户可以使用不同的配置策略。

使用配置策略的成员账户是集中管理的，只能由授权的管理员进行配置。 OUs 授权的管理员可以将特定的成员帐户指定 OUs 为自我管理帐户，从而使成员能够 Region-by-Region根据需要配置自己的设置。

如果您不使用中心配置，则必须主要在每个账户和区域中单独配置 Security Hub CSPM。这称为本地配置。在本地配置下，委派管理员可以在当前区域的新组织账户中自动启用 Security Hub CSPM 和一组有限的安全标准。本地配置不适用于现有组织账户或当前区域以外的其他区域。本地配置也不支持使用配置策略。

手动启用 Security Hub CSPM

如果您有独立账户或未与集成，则必须手动启用 Security Hub CSPM。 AWS Organizations独立账户无法集成 AWS Organizations ，必须使用手动启用。

手动启用 Security Hub CSPM 时，您可以指定一个 Security Hub CSPM 管理员账户并邀请其他账户成为成员账户。当潜在成员账户接受邀请时，管理员与成员的关系即已建立。

选择您喜欢的方法，然后按照以下步骤启用 Security Hub CSPM。从控制台中启用 Security Hub CSPM 时，您还可以选择启用支持的安全标准。

Security Hub CSPM console

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 首次打开 Security Hub CSPM 控制台时，选择前往 Security Hub CSPM。
3. 在欢迎页面上，安全标准部分列出了 Security Hub CSPM 支持的安全标准。

   选中标准的复选框即可将其启用，取消选中该复选框即可将其禁用。

   您可以随时启用或禁用标准或其各个控制。有关管理安全标准的信息，请参阅了解 Security Hub CSPM 中的安全标准。
4. 选择启用 Security Hub。

Security Hub CSPM API

调用 `EnableSecurityHub` API。从 API 中启用 Security Hub CSPM 时，它会自动启用以下默认安全标准：

- AWS 基础安全最佳实践
- 互联网安全中心 (CIS) AWS 基金会基准测试 v1.2.0

如果您不想启用这些标准，请将 `EnableDefaultStandards` 设置为 `false`。

您也可以使用 `Tags` 参数为 hub 资源分配标签值。

AWS CLI

运行 enable-security-hub 命令。要启用默认标准，请包括 --enable-default-standards。若不启用默认标准，请包括 --no-enable-default-standards。默认安全标准如下：

- AWS 基础安全最佳实践
- 互联网安全中心 (CIS) AWS 基金会基准测试 v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

示例

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

多账户启用脚本

> **Note**
>
> 我们建议不要使用此脚本，而是使用中心配置在多个账户和区域中启用和配置 Security Hub CSPM。

中的 S ecurity Hub CSPM 多账户启用脚本 GitHub允许您跨账户和地区启用 Security Hub CSPM。该脚本还自动执行向成员账户发送邀请并启用 AWS Config的流程。

该脚本会自动为所有区域的所有资源（包括全球资源）启用 AWS Config 资源记录。它不会将全局资源的记录限制在单个区域。为了节省成本，我们建议仅在一个区域内记录全局资源。如果您使用中心配置或跨区域聚合，则这应是您的主区域。有关更多信息，请参阅 在中录制资源 AWS Config。

有一个相应的脚本可以跨账户和区域禁用 Security Hub CSPM。

后续步骤：状况管理和集成

启用 Security Hub CSPM 后，我们建议启用安全标准和控件以监控您的安全状况。启用控制后，Security Hub CSPM 开始运行安全检查并生成控制结果，以帮助您检测环境中的错误配置。 AWS

要接收控制结果，必须启用和配置 S AWS Config ecurity Hub CSPM。有关更多信息，请参阅 启用和配置 AWS Config 适用于 Security Hub CSPM。

启用 Security Hub CSPM 后，你还可以利用 Security Hub CSPM 与其他 AWS 服务 和第三方解决方案之间的集成，在 Security Hub CSPM 中查看他们的发现。Security Hub CSPM 聚合了来自不同来源的调查发现，并以一致的格式提取它们。有关更多信息，请参阅 了解 Security Hub CSPM 中的集成。

启用和配置 AWS Config 适用于 Security Hub CSPM

AWS Security Hub CSPM 使用 AWS Config 规则来运行安全检查并生成大多数控件的调查结果。AWS Config 提供了中 AWS 资源配置的详细视图 AWS 账户。它使用规则为您的资源建立基准配置，并使用配置记录器来检测特定资源是否违反了规则的条件。

有些规则（称为托 AWS Config 管规则）是由预定义和开发的 AWS Config。其他规则是 Security Hub CSPM 开发的自定义 AWS Config 规则。 AWS Config Security Hub CSPM 用于控制的规则称为服务相关规则。 Service-linked AWS 服务 诸如 Security Hub CSPM 之类的规则允许在你的 AWS Config 账户中创建规则。

如果您同时启用了 S AWS ecurity Hub CSPM 和 Security Hub，Security Hub CSPM 会自动创建与服务相关的配置记录器来评估您的安全控制措施。您无需手动启用或配置 AWS Config。有关更多信息，请参阅 使用与服务相关的配置记录器。

如果您在未启用 Security Hub 的情况下启用了 Security Hub CSPM，则必须手动启用 AWS Config 并打开资源记录。有关更多信息，请参阅 手动配置 AWS Config。

主题

- 使用与服务相关的配置记录器
- 手动配置 AWS Config
- 了解 Config.1 控件
- 生成服务相关规则

使用与服务相关的配置记录器

当你同时启用 S AWS ecurity Hub CSPM 和 Security Hub 时，Security Hub CSPM 会自动在你的账户和区域中创建和管理与服务相关的配置记录器。您无需手动启用或配置 AWS Config。

此配置记录器的名称是`AWSConfigurationRecorderForSecurityHubCSPM`。Security Hub CSPM 为同时启用 Security Hub CSPM 和 Security Hub 的每个账户和区域创建相应的服务相关配置记

录器。当你为新版本启用 Security Hub CSPM 时， AWS 账户 AWS 区域 Security Hub CSPM 会自动创建与服务相关的配置记录器。

Security Hub CSPM 管理与服务相关的配置记录器的资源配置，确保为与 Security Hub 支持的控件相关的所有资源启用录制。有关所需资源的列表，请参阅必填 AWS Config 控制结果的资源。

当 Security Hub CSPM 创建此与服务相关的配置记录器时，Security Hub 不会在中使用客户管理的配置记录器。 AWS Config

有关配置记录器的更多信息，请参阅《AWS Config 开发人员指南》中的使用配置记录器。

手动配置 AWS Config

当您在未启用 Security Hub 的情况下启用 Security Hub CSPM 时，以下步骤适用。在这种情况下，您必须 AWS Config 为您的账户启用资源记录，并针对已启用的控件评估的资源类型开启资源记录。完成此操作后，Security Hub CSPM 会创建相应的 AWS Config 规则并开始运行安全检查以生成调查结果。

启用和配置前的注意事项 AWS Config

要在 Security Hub CSPM 中接收控制结果， AWS Config 必须在每个启用 Security Hub CSPM AWS 区域 的地方为你的账户启用控制结果。如果您将 Security Hub CSPM 用于多账户环境，则必须在每个区域中为管理员账户和所有成员账户启用 AWS Config 。

我们强烈建议您在启用任何 Security Hub CSPM 标准和控件 AWS Config 之前，先开启资源记录功能。这有助于确保您的控件调查发现准确无误。

要开启资源记录功能 AWS Config，您必须具有足够的权限才能记录附加到配置记录器的 AWS Identity and Access Management (IAM) 角色中的资源。此外，请确保任何 IAM 策略或 AWS Organizations 策略都不会 AWS Config 阻止您获得记录资源的权限。Security Hub CSPM 控件直接评估资源配置，不考虑 AWS Organizations 策略。有关 AWS Config 记录的更多信息，请参阅《AWS Config 开发人员指南》中的使用配置记录器。

如果您在 Security Hub CSPM 中启用了标准但尚未启用 AWS Config，则 Security Hub CSPM 会尝试按照以下计划创建与服务相关的 AWS Config 规则：

- 启用标准当天。
- 启用标准后的第二天。
- 启用标准后的 3 天。
- 启用标准后的 7 天，此后连续每 7 天一次。

如果您使用集中配置，则每次将启用一个或多个标准的配置策略与账户、组织单位 (OU) 或根关联时，Security Hub CSPM 还会尝试创建与服务相关的 AWS Config 规则。

在中录制资源 AWS Config

启用后 AWS Config，必须指定要 AWS Config 配置记录器记录哪些 AWS 资源。通过服务相关规则，配置记录器允许 Security Hub CSPM 检测对您的资源配置所做的更改。

要使 Security Hub CSPM 生成准确的控件调查发现，您必须在 AWS Config 中为与已启用的控件对应的资源类型启用记录。它主要启用具有变更已触发计划类型的控件，这些控件需要资源记录。某些具有定期计划类型的控件也需要资源记录。有关这些控件及其对应资源的列表，请参阅必填 AWS Config 控制结果的资源。

> **Warning**
>
> 如果您没有为 Security Hub CSPM 控件正确配置 AWS Config 录制，则可能会导致控制结果不准确，尤其是在以下情况下：
>
> - 您从未为给定控件记录资源，或者在创建该类型资源之前禁用了资源的记录。在这些情况下，即使您在禁用记录后创建了该控件范围内的资源，您也会收到有关该控件的 `WARNING` 调查发现。此 `WARNING` 调查发现为默认调查发现，实际上并不评估资源的配置状态。
> - 您可以对特定控件评估的资源禁用记录。在这种情况下，即使控件未评估新的或更新的资源，Security Hub CSPM 也会保留在您禁用记录之前生成的控件调查发现。Security Hub CSPM 还将调查发现的合规状态更改为 `WARNING`。这些保留的调查发现可能无法准确反映资源的当前配置状态。

默认情况下，会 AWS Config 记录它在运行时发现的所有支持的区域资源。 AWS 区域 要接收所有 Security Hub CSPM 控制结果，还必须配置 AWS Config 为记录全局资源。为了节省成本，我们建议仅在一个区域内记录全局资源。如果您使用中心配置或跨区域聚合，则此区域应是您的主区域。

在中 AWS Config，您可以在连续记录和每日记录资源状态变化之间进行选择。如果您选择每日记录，则如果资源状态发生变化，则会在每 24 小时结束时 AWS Config 提供资源配置数据。如果没有任何更改，则不会传送任何数据。这可能会延迟变更触发的控件的 Security Hub CSPM 调查发现的生成，直到 24 小时期限结束。

有关 AWS Config 录制的更多信息，请参阅《AWS Config 开发者指南》中的录制 AWS 资源。

启用和配置的方法 AWS Config

您可以通过以下任一方式启用 AWS Config 和开启资源记录：

- AWS Config 控制台-您可以使用控制 AWS Config 台 AWS Config 为帐户启用。有关说明，请参阅《AWS Config 开发者指南》中的 AWS Config 使用控制台进行设置。
- AWS CLI 或 SDK — 您可以使用 AWS Command Line Interface (AWS CLI) AWS Config 为账户启用。有关说明，请参阅《AWS Config 开发者指南》 AWS CLI中的 AWS Config 使用进行设置。AWS 软件开发套件 (SDK) 也适用于多种编程语言。
- CloudFormation 模板-要 AWS Config 为许多账户启用，我们建议使用名为 “启用” 的 AWS CloudFormation 模板 AWS Config。要访问此模板，请参阅《AWS CloudFormation 用户指南》中的AWS CloudFormation StackSet 示例模板。

  默认情况下，此模板会排除 IAM 全局资源的记录。为了节省记录成本，请确保仅在一个 AWS 区域中启用 IAM 全局资源的记录。如果启用了跨区域聚合，则此区域应为您的 Security Hub CSPM 主区域。否则，它可以是任何支持 IAM 全局资源记录且 Security Hub CSPM 可用的区域。我们建议运行一个 StackSet 来记录主区域或其他选定区域中的所有资源，包括 IAM 全球资源。然后，运行一秒钟 StackSet 以记录除其他区域的 IAM 全球资源之外的所有资源。
- GitHub 脚本 — S ecurity Hub CSPM 提供了一个GitHub脚本，该脚本可以启用 Security Hub CSPM 以及跨区域 AWS Config 的多个账户。如果您尚未与组织集成 AWS Organizations，或者您的某些成员帐户不是组织的一部分，则此脚本非常有用。

有关更多信息，请参阅AWS 安全博客上的以下博客文章：针对 Security Hub CSPM AWS Config 进行 AWS 优化，以有效管理您的云安全状况。

成本注意事项

Security Hub CSPM 可以通过更新 AWS Config 配置项目来影响您的`AWS::Config::ResourceCompliance`配置记录器成本。每当与 AWS Config 规则关联的 Security Hub CSPM 控件更改合规状态、启用或禁用或更新参数时，都会进行更新。如果您仅将 AWS Config 配置记录器用于 Security Hub CSPM，并且不将此配置项目用于其他用途，我们建议您在中关闭其录制功能。 AWS Config这可以降低您的 AWS Config 成本。您无需为安全检查记录 `AWS::Config::ResourceCompliance` 即可在 Security Hub CSPM 中工作。

有关与资源记录关联的成本的信息，请参阅 AWS Security Hub CSPM 定价和 AWS Config 定价。

了解 Config.1 控件

> **Note**
>
> 当同时启用 Sec AWS urity Hub CSPM 和 Security Hub 时， Config.1 控件的状态始终为。PASSEDSecurity Hub CSPM 可以通过与服务相关的配置记录器直接访问配置项目。有关更多信息，请参阅 使用与服务相关的配置记录器。

在 Security Hub CSPM 中，如果 AWS Config 禁用，该Config.1控件会在你的账户中生成FAILED调查结果。如果 AWS Config 启用了资源记录但未开启资源记录，它还会在您的账户中生成FAILED调查结果。

如果已启用 AWS Config 且资源记录已开启，但未为已启用的控件所检查的资源类型开启资源记录，则 Security Hub CSPM 会为控件生成FAILED查找结果。 Config.1 除了此 FAILED 调查发现外，Security Hub CSPM 还会针对已启用控件以及该控件检查的资源类型生成 WARNING 调查发现。例如，如果您启用KMS.5控件但未为其开启资源记录 AWS KMS keys，则 Security Hub CSPM 会为该 Config.1 控件生成FAILED查找结果。Security Hub CSPM 还会生成 KMS.5控件和您的 KMS 密钥的WARNING调查结果。

要接收 Config.1 控件的PASSED调查结果，请为所有与已启用控件对应的资源类型启用资源记录。同时禁用您的组织不需要的控件。这有助于确保您的安全控件检查中没有配置漏洞。它还有助于确保您收到有关错误配置的资源的准确调查发现。

如果您是某个组织的 Security Hub CSPM 委派管理员，则必须为您的账户和成员账户正确配置 AWS Config 记录。如果您使用跨区域聚合，则必须在主区域和所有关联区域中正确配置 AWS Config 录制。关联区域中无需记录全局资源。

生成服务相关规则

对于每个使用服务相关 AWS Config 规则的控件，Security Hub CSPM 都会在您的环境中创建所需规则的实例。 AWS

这些服务相关规则特定于 Security Hub CSPM。即使已存在相同规则的其他实例，Security Hub CSPM 也会创建这些服务相关规则。服务相关规则在原始规则名称前添加 `securityhub`，并在规则名称后添加唯一标识符。例如，对于 AWS Config 托管规则`vpc-flow-logs-enabled`，服务相关规则的名称可能是。`securityhub-vpc-flow-logs-enabled-12345`

可用于评估控件的 AWS Config 托管规则数量有配额。 AWS Config Security Hub CSPM 创建的规则不计入这些配额。即使您的账户中已达到托管规则的 AWS Config 配额，也可以启用安全标准。要了解

有关 AWS Config 规则配额的更多信息，请参阅《AWS Config 开发人员指南》 AWS Config中的服务限制。

> **Note**
>
> 如果您使用的是 Security Hub CSPM 和 Security Hub，则可以在中看到与服务相关的规则，AWS Config 但您将无法看到与该规则关联的合规或不合规资源。合规和不合规的资源只能在 Security Hub CSPM 和 Security Hub 中可见。

了解 Security Hub CSPM 中的本地配置

本地配置是在 Security Hub CSPM 中配置 AWS 组织的默认方式。如果您不选择启用中心配置，则组织会默认使用本地配置。

在本地配置下，Security Hub CSPM 委派管理员账户对配置设置的控制有限。委派管理员可以强制实施的唯一设置是在新的组织账户中自动启用 Security Hub CSPM 和默认安全标准。这些设置仅适用于您在其中指定了委派管理员账户的区域。默认安全标准是 AWS 基础安全最佳实践 (FSBP) 和互联网安全中心 (CIS) AWS 基金会基准 v1.2.0。本地配置设置不适用于现有组织账户，也不适用于在其中指定了委派管理员账户的区域以外的区域。

除了在单个区域的新组织账户中启用 Security Hub CSPM 和默认标准外，您还必须在每个区域和账户中单独配置其他 Security Hub CSPM 设置，包括标准和控件。由于这可能是一个重复的过程，因此，如果以下一项或多项适用于您，我们建议您在多账户环境中使用中心配置：

- 您需要为组织的不同部分使用不同的配置设置（例如，为不同的团队启用不同的标准或控件）。
- 您在多个区域开展业务，并希望减少在这些区域配置服务的时间和复杂性。
- 您希望新账户在加入组织时使用特定的配置设置。
- 您希望组织账户从父账户或根账户继承特定配置设置。

有关中心配置的信息，请参阅了解 Security Hub CSPM 中的中心配置。

了解 Security Hub CSPM 中的中心配置

中央配置是 S AWS ecurity Hub CSPM 的一项功能，可帮助您跨多个和设置和管理 Security Hub CSPM。 AWS 账户 AWS 区域要使用集中配置，必须先集成 Security Hub CSPM 和。 AWS Organizations您可以通过创建组织并为该组织指定 Security Hub CSPM 委派管理员账户来集成服务。

通过委派的 Security Hub CSPM 管理员帐户，您可以跨区域为组织的账户和组织单位 () OUs 启用 Security Hub CSPM。您还可以为账户和 OUs 跨区域启用、配置和禁用个人安全标准和安全控制。只需几个步骤即可从一个主要区域（称为主区域）配置这些设置。

使用集中配置时，授权的管理员可以选择 OUs 要配置的帐户。如果委派管理员将成员账户或 OU 指定为自行管理，则该成员可以在每个区域中单独配置自己的设置。如果委派管理员将成员账户或 OU 指定为集中管理，则只有委派管理员才能跨区域配置成员账户或 OU。您可以将组织 OUs 中的所有账户指定为集中管理、全部自我管理或两者兼而有之。

要配置集中管理账户，委派管理员使用 Security Hub CSPM 配置策略。配置策略允许委派管理员指定是启用还是禁用 Security Hub CSPM，以及启用或禁用哪些标准控件。它们还可以用来自定义某些控件的参数。

配置策略在主区域和所有关联区域生效。委派管理员在开始使用中心配置之前指定组织的主区域和关联区域。指定关联区域是可选的。授权的管理员可以为整个组织创建单个配置策略，也可以创建多个配置策略来为不同的账户和配置变量设置OUs。

> **Tip**
>
> 如果您不使用中心配置，则必须主要在每个账户和区域中单独配置 Security Hub CSPM。这称为本地配置。在本地配置下，委派管理员可以在当前区域的新组织账户中自动启用 Security Hub CSPM 和一组有限的安全标准。本地配置不适用于现有组织账户或当前区域以外的其他区域。本地配置也不支持使用配置策略。

本部分提供中心配置概述。

使用中心配置的优势

中心配置的优势包括以下内容：

简化 Security Hub CSPM 服务和功能的配置

当您使用中心配置时，Security Hub CSPM 会引导您完成为组织配置安全最佳实践的过程。它还会 OUs 自动将生成的配置策略部署到指定的账户。如果您已有 Security Hub CSPM 设置，例如自动启用新的安全控件，则可以将其用作配置策略的起点。此外，Securit y Hub CSPM 控制台上的 “配置” 页面会显示您的配置策略以及哪些账户和 OUs 使用每个策略的实时摘要。

跨账户和区域进行配置

您可以使用中心配置跨多个账户和区域配置 Security Hub CSPM。这有助于确保组织的每个部分都保持一致的配置和足够的安全覆盖。

在不同的账户中适应不同的配置 OUs

通过集中配置，您可以选择以不同的 OUs 方式配置组织的帐户。例如，您的测试账户和生产账户可能需要不同的配置。您还可以创建配置策略，以在新账户加入组织后涵盖这些新账户。

防止配置偏差

当用户对与委派管理员的选择冲突的服务或功能进行更改时，会发生配置偏差。中心配置可防止这种偏差。当您将账户或 OU 指定为集中管理时，只能由该组织的委派管理员对其进行配置。如果您希望特定账户或 OU 自行配置设置，则可以将其指定为自行管理。

何时使用中心配置？

对于包含多个 Security Hub CSPM 帐户的 AWS 环境，集中配置最有利。它旨在帮助您集中管理多个账户的 Security Hub CSPM。

您可以使用中心配置来配置 Security Hub CSPM 服务、安全标准和安全控件。您也可以使用它来自定义某些控件的参数。有关安全标准的更多信息，请参阅 了解 Security Hub CSPM 中的安全标准。有关安全控件的更多信息，请参阅了解 Security Hub CSPM 中的安全控件。

中心配置术语和概念

了解以下关键术语和概念可以帮助您使用 Security Hub CSPM 中心配置。

中心配置

Security Hub CSPM 的一项功能，可帮助组织的 Security Hub CSPM 委派管理员账户跨多个账户和区域配置 Security Hub CSPM 服务、安全标准和安全控件。要配置这些设置，委派管理员为其组织中的集中管理账户创建并管理 Security Hub CSPM 配置策略。自行管理账户可以在每个区域单独配置自己的设置。要使用集中配置，必须集成 Security Hub CSPM 和。 AWS Organizations

主区域

委托管理员通过创建和管理配置策略 AWS 区域 从中集中配置 Security Hub CSPM。配置策略在主区域和所有关联区域生效。

主区域还充当 Security Hub CSPM 聚合区域，接收来自关联区域的发现、见解和其他数据。

在 2019 年 3 月 20 日当天或之后 AWS 推出的区域被称为选择加入区域。选择加入区域不能是主区域，但可以是关联区域。有关选择加入区域的列表，请参阅《AWS 账户管理参考指南》中的启用和禁用区域之前的注意事项。

关联区域

AWS 区域 可以从家乡区域进行配置。配置策略由主区域的委派管理员创建。这些策略在主区域和所有关联的区域生效。指定关联区域是可选的。

关联区域还会将调查发现、见解和其他数据发送到主区域。

在 2019 年 3 月 20 日当天或之后 AWS 推出的区域被称为选择加入区域。必须先为账户启用这样的区域，然后才能对其应用配置策略。组织管理账户可以为成员账户启用选择加入区域。有关更多信息，请参阅《账户管理参考指南》中的指定 AWS 区域 您的AWS 账户可以使用哪个账户。

目标

AWS 账户、组织单位 (OU) 或组织根目录。

Security Hub CSPM 配置策略

一组 Security Hub CSPM 设置，委派管理员可以为集中管理目标配置这些设置。这包括：

- 是启用还是禁用 Security Hub CSPM。
- 是否启用一个或多个安全标准。
- 在已启用的标准中启用哪些安全控件。委派管理员可以通过提供应启用的特定控件列表来实现此目的，Security Hub CSPM 会禁用所有其他控件（包括在新控件发布时直接禁用）。或者，委派管理员可以提供应禁用的特定控件列表，并且 Security Hub CSPM 会启用所有其他控件（包括在新控件发布时直接启用）。
- （可选）在已启用的标准中为选定的已启用控件自定义参数。

配置策略在与至少一个账户、组织单元（OU）或根关联后，将在主区域和所有关联区域中生效。

在 Security Hub CSPM 控制台上，委派管理员可以选择 Security Hub CSPM 推荐的配置策略或创建自定义配置策略。使用 Security Hub CSPM API 和 AWS CLI，委托的管理员只能创建自定义配置策略。委派管理员最多可以创建 20 个自定义配置策略。

在推荐的配置策略中，Security Hub CSPM、 AWS 基础安全最佳实践（FSBP）标准以及所有现有和新的 FSBP 控件均已启用。接受参数的控件使用默认值。推荐的配置策略适用于整个组织。

要对组织应用不同的设置，或者将不同的配置策略应用于不同的账户 OUs，然后创建自定义配置策略。

本地配置

在集成 Security Hub CSPM 和之后，组织的默认配置类型。 AWS Organizations通过本地配置，委派管理员可以选择在当前区域的新组织账户中自动启用 Security Hub CSPM 和默认安全标准。如果委派管理员自动启用默认标准，则属于这些标准的所有控件也会自动启用，附带新组织账户的默认参数。这些设置不适用于现有账户，因此账户加入组织后可能会出现配置偏差。必须分别在每个账户和区域中禁用属于默认标准的特定控件以及配置其他标准和控件。

本地配置不支持使用配置策略。要使用配置策略，必须切换到中心配置。

手动账户管理

如果您未将 Security Hub CSPM 与 Security Hub CSPM 集成， AWS Organizations 或者您拥有独立账户，则必须在每个区域中分别为每个账户指定设置。手动账户管理不支持使用配置策略。

中心配置 APIs

Security Hub CSPM 操作，只有 Security Hub CSPM 委派的 Security Hub CSPM 管理员才能在主区域中使用，以管理集中管理账户的配置策略。操作包括：

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

特定于账户 APIs

Security Hub CSPM 操作，可用于在基础上启用或禁用 Security Hub CSPM、标准和控件。account-by-account这些操作用于每个单独的区域。

自行管理账户可以使用特定于账户的操作来配置自己的设置。集中管理的账户不能在主区域和关联区域使用以下特定于账户的操作。在这些区域中，只有委派管理员才能通过中心配置操作和配置策略对集中管理的账户进行配置。

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

要查看账户状态，集中管理账户的所有者可以使用 Security Hub CSPM API 的任何 `Get` 或 `Describe` 操作。

如果您使用本地配置或手动账户管理，而不是中心配置，则可以使用这些特定于账户的操作。

自行管理账户也可以使用 `*Invitations` 和 `*Members` 操作。但是，我们不建议自行管理账户使用这些操作。如果成员账户的成员与委派管理员属于不同的组织，则策略关联可能会失败。

组织部门（OU）

在 and S AWS Organizations ecurity Hub CSPM 中，一个可容纳一群人的容器。 AWS 账户组织单位 (OU) 也可以包含其他组织 OUs，从而使您能够创建类似于倒置树的层次结构，父组织单位位于顶部，其分支向下延伸，结尾是树叶的帐户。 OUs 一个 OU 有且仅有一个父级，账户可能是且仅是一个 OU 的成员。

你可以在 AWS Organizations 或 OUs 中进行管理 AWS Control Tower。有关更多信息，请参阅《AWS Organizations 用户指南》中的管理组织单元 或《AWS Control Tower 用户指南》中的使用 AWS Control Tower管理组织和账户。

授权的管理员可以将配置策略与特定账户或 OUs根账户相关联，以涵盖组织 OUs 中的所有账户。

集中管理

只有委派管理员才能使用配置策略跨区域配置的目标。

委派管理员账户指定是否集中管理目标。委派管理员还可以将目标的状态从集中管理更改为自行管理，或者从自行管理更改为集中管理。

自行管理

管理自己的 Security Hub CSPM 设置的目标。自行管理目标使用特定于账户的操作在每个区域中为自己单独配置 Security Hub CSPM。这与集中管理目标形成鲜明对比，后者只能由委派管理员通过配置策略跨区域进行配置。

委派管理员账户指定目标是否为自行管理目标。委派管理员可以对目标应用自行管理行为。或者，账户或 OU 可以继承父代的自行管理行为。

委派管理员账户本身可以是自行管理账户。委派管理员账户可以将目标的状态从自行管理更改为集中管理，或者反过来。

配置策略关联

配置策略与账户、组织单元（OU）或根之间的链接。当存在策略关联时，账户、OU 或根将使用配置策略定义的设置。在以下任一情况下都存在关联：

- 当委派管理员直接将配置策略应用于账户、OU 或根时
- 当账户或 OU 从父 OU 或根继承配置策略时

在应用或继承不同的配置之前，关联一直存在。

应用的配置策略

一种配置策略关联，在这种关联中，委派的管理员将配置策略直接应用于目标账户或根账户。 OUs 目标按照配置策略定义的方式进行配置，只有委派管理员才能更改其配置。如果应用于 root 用户，则该配置策略会影响组织 OUs 中所有不通过应用程序或从最亲近的父级继承使用不同配置的账户和组织。

委派的管理员还可以将自我管理的配置应用于特定账户或根账户。 OUs

继承的配置策略

一种配置策略关联，在这种关联中，账户或 OU 采用最近的父 OU 或根的配置。如果配置策略未直接应用于账户或 OU，则它会继承最近的父级的配置。策略的所有元素都是继承的。换句话说，账户或 OU 不能选择仅继承策略中自己选择的一部分内容。如果最近的父级是自行管理的，则子账户或 OU 将继承父级的自行管理行为。

继承不能覆盖已应用的配置。也就是说，如果将配置策略或自行管理配置直接应用于账户或 OU，则它将使用该配置，并且不会继承父级的配置。

根

在 AWS Organizations 和 Security Hub CSPM 中，组织中的顶级父节点。如果授权的管理员将配置策略应用于 root，则该策略将与组织 OUs 中的所有账户相关联，除非这些账户通过应用程序或继承使用不同的策略，或者被指定为自我管理。如果管理员将 root 指定为自我管理，则组织 OUs 中的所有账户和账户都是自我管理的，除非他们通过应用程序或继承使用配置策略。如果根是自行管理的，并且当前不存在任何配置策略，则组织中的所有新账户都将保留其当前设置。

加入组织的新账户在被分配到特定 OU 之前一直处于根之下。如果未将新账户分配给 OU，则该账户将继承根配置，除非委派管理员将其指定为自行管理账户。

在 Security Hub CSPM 中启用中心配置

委派的 Sec AWS urity Hub CSPM 管理员帐户可以使用中央配置为多个账户和组织单位 () 配置 Security Hub CSPM、标准和控制。OUs AWS 区域

有关中心配置的好处及其工作原理的背景信息，请参阅了解 Security Hub CSPM 中的中心配置。

本节介绍中心配置的先决条件以及如何开始使用。

中心配置的先决条件

在开始使用中央配置之前，必须将 Security Hub CSPM 与主区域集成， AWS Organizations 并指定主区域。如果您使用 Security Hub CSPM 控制台，则这些先决条件包含在中心配置的选择加入工作流中。

与 Organizations 集成

您必须集成 Security Hub CSPM 和 Organizations 才能使用中心配置。

要集成这些服务，首先要在 Organizations 中创建一个组织。在 Organizations 管理账户中，指定一个 Security Hub CSPM 委派管理员账户。有关说明，请参阅将 Security Hub CSPM 与 AWS Organizations。

确保您在预期主区域指定您的委派管理员。当您开始使用中心配置时，还会在所有关联区域中自动设置相同的委派管理员。组织管理账户不能设置为委派管理员账户。

> **Important**
>
> 当你使用集中配置时，你无法使用 Security Hub CSPM 控制台或 Security Hub CSPM APIs 来更改或删除委派的管理员帐户。如果 Organizations 管理帐户使用 AWS Organizations APIs 更改或删除 Security Hub CSPM 授权的管理员，则 Security Hub CSPM 会自动停止中央配置。您的配置策略也将被取消关联和删除。成员账户保留其在更改或删除委派管理员之前的配置。

指定主区域

您必须指定主区域才能使用中心配置。主区域是委派管理员从中配置组织的区域。

> **Note**
>
> 主区域不能是 AWS 已指定为可选区域的区域。默认情况下，选择加入区域处于禁用状态。有关选择加入区域的列表，请参阅《AWS 账户管理参考指南》中的启用和禁用区域之前的注意事项。

或者，您可以指定一个或多个可从主区域进行配置的关联区域。

委派管理员只能从主区域创建和管理配置策略。配置策略在主区域和所有关联区域生效。您无法创建仅适用于某些区域而不适用于其他区域的配置策略。唯一的例外是涉及全球资源的控制。如果您使用中心配置，Security Hub CSPM 会自动禁用涉及除主区域之外的所有区域中全局资源的控件。有关更多信息，请参阅 使用全局资源的控件。

主区域也是您的 Security Hub CSPM 聚合区域，用于接收来自关联区域的调查发现、见解和其他数据。

如果您已经为跨区域聚合设置了聚合区域，那么这就是中心配置的默认主区域。在开始使用中心配置之前，您可以通过删除当前的调查发现聚合器并在所需的主区域中创建一个新的聚合器来更改主区域。调查发现聚合器是一种 Security Hub CSPM 资源，用于指定主区域和关联区域。

要指定主区域，请参阅设置聚合区域的步骤。如果您已经有主区域，则可以调用 GetFindingAggregator API 来查看有关它的详细信息，包括当前与其关联的区域。

启用中心配置的说明

选择您的首选方法，然后按照步骤为组织启用中心配置。

Security Hub CSPM console

启用中心配置（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置和配置。然后，选择启用中心配置。

   如果要加入 Security Hub CSPM，请选择前往 Security Hub CSPM。
3. 在指定委派管理员页面上，选择您的委派管理员账户或输入其账户 ID。如果适用，我们建议选择您为其他 AWS 安全与合规服务设置的相同委派管理员。选择设置委派管理员。

4. 在集中组织页面的区域部分，选择您的主区域。您必须登录到主区域才能继续。如果您已经为跨区域聚合设置了聚合区域，则该聚合区域将显示为主区域。要更改主区域，请选择编辑区域设置。然后，您可以选择首选的主区域并返回到此工作流程。
5. 至少选择一个区域以链接到主区域。或者选择是否要自动将未来受支持的区域链接到主区域。您在此处选择的区域可由委派管理员从主区域进行配置。配置策略将在主区域和所有关联区域生效。
6. 选择确认并继续。
7. 现在可以使用中心配置了。继续按照控制台提示创建您的第一个配置策略。如果您尚未准备好创建配置策略，请选择我还没准备好配置。您可以稍后通过在导航窗格中选择设置和配置来创建策略。有关创建配置策略的说明，请参阅创建和关联配置策略。

Security Hub CSPM API

启用中心配置（API）

1. 使用委派管理员账户的凭证，从主区域调用 UpdateOrganizationConfiguration API。
2. 将 `AutoEnable` 字段设置为 `false`。
3. 将 `OrganizationConfiguration` 对象中的 `ConfigurationType` 字段设置为 `CENTRAL`。此操作会产生以下影响：
   - 在所有关联区域中将调用账户指定为 Security Hub CSPM 委派管理员。
   - 在所有关联区域的委派管理员账户中启用 Security Hub CSPM。
   - 将调用账户指定为使用 Security Hub CSPM 且属于该组织的新账户和现有账户的 Security Hub CSPM 委派管理员。在主区域和所有关联区域均如此。只有当新组织账户与启用了 Security Hub CSPM 的配置策略关联时，才会将调用账户设置为该新账户的委派管理员。只有当现有组织账户已启用 Security Hub CSPM 时，才会将调用账户设置为该现有账户的委派管理员。
   - 在所有关联区域中将 AutoEnable 设置为 `false`，并在主区域和所有关联区域中将 AutoEnableStandards 设置为 `NONE`。如果您使用中心配置，则这些参数在主区域和关联区域中无关，但您可以通过使用配置策略在组织账户中自动启用 Security Hub CSPM 和默认安全标准。
4. 现在可以使用中心配置了。委派管理员可以通过创建配置策略来在您的组织中配置 Security Hub CSPM。有关创建配置策略的说明，请参阅创建和关联配置策略。

API 请求示例：

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

启用中心配置（AWS CLI）

1. 使用委派管理员账户的凭证，从主区域运行 update-organization-configuration 命令。
2. 包含 `no-auto-enable` 参数。
3. 将 `organization-configuration` 对象中的 `ConfigurationType` 字段设置为 `CENTRAL`。此操作会产生以下影响：
   - 在所有关联区域中将调用账户指定为 Security Hub CSPM 委派管理员。
   - 在所有关联区域的委派管理员账户中启用 Security Hub CSPM。
   - 将调用账户指定为使用 Security Hub CSPM 且属于该组织的新账户和现有账户的 Security Hub CSPM 委派管理员。在主区域和所有关联区域均如此。只有当新组织账户与启用了 Security Hub 的配置策略关联时，才会将调用账户设置为该新账户的委派管理员。只有当现有组织账户已启用 Security Hub CSPM 时，才会将调用账户设置为该现有账户的委派管理员。
   - 在所有关联区域中将自动启用选项设置为 no-auto-enable，并在主区域和所有关联区域中将 auto-enable-standards 设置为 `NONE`。如果您使用中心配置，则这些参数在主区域和关联区域中无关，但您可以通过使用配置策略在组织账户中自动启用 Security Hub CSPM 和默认安全标准。
4. 现在可以使用中心配置了。委派管理员可以通过创建配置策略来在您的组织中配置 Security Hub CSPM。有关创建配置策略的说明，请参阅创建和关联配置策略。

命令示例：

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

集中管理目标和自行管理目标

启用中央配置后，委派的 Sec AWS urity Hub CSPM 管理员可以将每个组织帐户、组织单位 (OU) 和根目录指定为集中管理或自我管理。目标的管理类型决定了如何指定其 Security Hub CSPM 设置。

有关中心配置的好处及其工作原理的背景信息，请参阅了解 Security Hub CSPM 中的中心配置。

本节说明了集中管理和自行管理的指定之间的区别，以及如何选择账户、OU 或根的管理类型。

自行管理

自我管理账户的所有者、OU 或 root 用户必须在每个 AWS 区域账户中分别配置其设置。委派管理员无法为自行管理目标创建配置策略。

集中管理

只有授权的 Security Hub CSPM 管理员才能为集中管理的账户配置设置 OUs，或者为主区域和关联区域的根账户配置设置。配置策略可以与集中管理的账户相关联，以及 OUs。

委派管理员可以在自行管理和集中管理之间切换目标的状态。默认情况下，当您通过 Security Hub CSPM API 启动中心配置时，所有账户和 OU 都是自行管理的。在控制台中，管理类型取决于您的第一个配置策略。您与 OUs 第一份保单关联的账户将进行集中管理。默认情况下，其他账户和账户 OUs 是自行管理的。

如果您将配置策略与以前自行管理的账户相关联，则策略设置将覆盖自行管理指定。账户将变成集中管理，并采用配置策略中反映的设置。

如果您将集中管理账户更改为自行管理账户，则之前通过配置策略应用于账户的设置将保持不变。例如，集中管理的账户最初可能与启用 Security Hub CSPM、启用 AWS 基础安全最佳实践和禁用 .1 的策略相关联。 CloudTrail如果您随后将账户指定为自行管理，则所有设置均保持不变。但是，账户所有者可以独立更改账户的设置。

子账号， OUs 可以继承自我管理的家长的自我管理行为，就像子女账户一样， OUs 可以继承集中管理的家长的配置策略。有关更多信息，请参阅 通过应用和继承进行策略关联。

自行管理账户或 OU 不能从父节点或根继承配置策略。例如，如果您希望组织 OUs 中的所有账户都从根目录继承配置策略，则必须将自我管理节点的管理类型更改为集中管理。

配置自行管理账户中的设置的选项

自行管理账户必须在每个区域单独配置自己的设置。

自行管理账户的所有者可以在每个区域调用以下 Security Hub CSPM API 操作，以配置其设置：

- `EnableSecurityHub` 和 `DisableSecurityHub`，以启用或禁用 Security Hub CSPM 服务（如果自行管理账户具有 Security Hub CSPM 委派管理员，则该管理员必须先解除关联账户，然后账户所有者才能禁用 Security Hub CSPM）。
- `BatchEnableStandards` 和 `BatchDisableStandards`，启用或禁用标准
- `BatchUpdateStandardsControlAssociations` 或 `UpdateStandardsControl`，启用或禁用控件

自行管理账户也可以使用 `*Invitations` 和 `*Members` 操作。但是，我们不建议自行管理账户使用这些操作。如果成员账户的成员与委派管理员属于不同的组织，则策略关联可能会失败。

有关 Security Hub CSPM API 操作的说明，请参阅 AWS Security Hub CSPM API 参考。

自行管理的账户也可以使用 Security Hub CSPM 控制台或在 AWS CLI 每个区域配置其设置。

自管理账户无法调用任何 APIs 与 Security Hub CSPM 配置策略和策略关联相关的账户。只有授权的管理员才能调用中央配置 APIs 并使用配置策略来配置集中管理的帐户。

选择目标的管理类型

选择您的首选方法，然后按照步骤在 Sec AWS urity Hub CSPM 中将账户或 OU 指定为集中管理或自行管理。

Security Hub CSPM console

要选择账户和 OU 的管理类型

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 选择配置。
3. 在组织选项卡上，选择目标账户或 OU。选择编辑。
4. 在定义配置页面上，对于管理类型，如果您希望委派管理员配置目标账户或 OU，请选择集中管理。然后，如果要将现有配置策略与目标关联，请选择应用特定策略。如果希望目标继承最接近父级的配置，请选择从我的组织继承。如果希望账户或 OU 配置自己的设置，请选择自行管理。
5. 选择下一步。检查更改，然后选择保存。

Security Hub CSPM API

要选择账户和 OU 的管理类型

1. 从主区域的 Security Hub CSPM 委派管理员账户调用 StartConfigurationPolicyAssociation API。
2. 对于 ConfigurationPolicyIdentifier 字段，如果希望账户或 OU 控制其自己的设置，请提供 SELF_MANAGED_SECURITY_HUB。如果希望委派管理员控制账户或 OU 的设置，请提供相关配置策略的 Amazon 资源名称（ARN）或 ID。
3. 在该Target字段中，提供要更改其管理类型的目标的 ID、OU ID 或根 ID。 AWS 账户 这会将自行管理行为或指定的配置策略与目标关联。目标的子账户可继承自行管理行为或配置策略。

指定自行管理账户的 API 请求示例：

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

要选择账户和 OU 的管理类型

1. 从主区域的 Security Hub CSPM 委派管理员账户运行 start-configuration-policy-association 命令。
2. 对于 configuration-policy-identifier 字段，如果希望账户或 OU 控制其自己的设置，请提供 SELF_MANAGED_SECURITY_HUB。如果希望委派管理员控制账户或 OU 的设置，请提供相关配置策略的 Amazon 资源名称（ARN）或 ID。
3. 在该target字段中，提供要更改其管理类型的目标的 ID、OU ID 或根 ID。 AWS 账户 这会将自行管理行为或指定的配置策略与目标关联。目标的子账户可继承自行管理行为或配置策略。

指定自行管理账户的命令示例：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Security Hub CSPM 中配置策略的工作原理

授权的 S AWS ecurity Hub CSPM 管理员可以创建配置策略来为组织配置 Security Hub CSPM、安全标准和安全控制。创建配置策略后，授权的管理员可以将其与特定账户、组织单位 (OUs) 或根相关联。然后，该策略在指定的账户或根账户中生效。 OUs

有关中心配置的好处及其工作原理的背景信息，请参阅了解 Security Hub CSPM 中的中心配置。

本节详细概述了配置策略。

策略注意事项

在 Security Hub CSPM 中创建配置策略之前，请注意以下事项。

- 必须关联配置策略才能生效 — 创建配置策略后，可以将其与一个或多个账户、组织单位 (OUs) 或根相关联。配置策略可以与账户关联，也可以 OUs 通过直接应用程序关联，也可以通过从父 OU 继承来关联。
- 一个账户或 OU 只能与一个配置策略相关联 – 为防止设置冲突，一个账户或 OU 在任何给定时间只能与一个配置策略相关联。或者，也可以对账户或 OU 进行自行管理。
- 配置策略已完成 — 配置策略提供了完整的设置规范。例如，子账户不能接受一个策略中的某些控件的设置和另一个策略中其他控件的设置。当您将策略与子账户关联时，请确保该策略指定了您希望该子账户使用的所有设置。
- 配置策略无法恢复 — 在将配置策略与账户关联后，无法选择恢复配置策略或 OUs。例如，如果您将禁用 CloudWatch 控件的配置策略与特定账户关联，然后取消该策略的关联，则该账户中的 CloudWatch 控件将继续处于禁用状态。要再次启用 CloudWatch 控件，您可以将该账户与启用控件的新策略相关联。或者，您可以将帐户更改为自我管理并启用帐户中的每个 CloudWatch 控件。
- 配置策略在您的主区域和所有关联区域生效 — 配置策略会影响主区域中的所有关联账户以及所有关联区域。您无法创建仅在其中某些区域生效而不在其他区域生效的配置策略。唯一的例外是使用全球资源的控件。Security Hub CSPM 会自动禁用涉及除主区域之外的所有区域中全局资源的控件。

  在 2019 年 3 月 20 日当天或之后 AWS 推出的区域被称为选择加入区域。必须先为账户启用这样的区域，然后配置策略才会在该区域生效。组织管理账户可以为成员账户启用选择加入区域。有关启用可选区域的说明，请参阅《账户管理参考指南》中的指定 AWS 区域 您的AWS 账户可以使用哪个区域。

  如果您的策略配置的控件在主区域或一个或多个关联区域中不可用，则 Security Hub CSPM 会跳过不可用区域中的控件配置，但会在控件可用的区域中应用该配置。您无法覆盖在主区域或任何关联区域中不可用的控件。

- 配置策略即资源 — 作为资源，配置策略有 Amazon 资源名称（ARN）和通用唯一标识符（UUID）。ARN 使用以下格式：`arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID`。自行管理配置没有 ARN 或 UUID。自行管理配置的标识符为 `SELF_MANAGED_SECURITY_HUB`。

配置策略的类型

每个配置策略指定以下设置：

- 启用或禁用 Security Hub CSPM。
- 启用一项或多项安全标准。
- 指明在已启用的标准中启用了哪些安全控件。您可以通过提供应启用的特定控件列表来实现这一点，而 Security Hub CSPM 会禁用所有其他控件（包括新发布的控件）。或者，您可以提供应禁用的特定控件列表，Security Hub CSPM 将启用所有其他控件（包括新发布的控件）。
- （可选）在已启用的标准中为选定的已启用控件自定义参数。

中央配置策略不包括 AWS Config 录制器设置。为了让 Secur AWS Config ity Hub CSPM 生成控制结果，必须单独启用和开启所需资源的记录。有关更多信息，请参阅 启用和配置前的注意事项 AWS Config。

如果您使用中心配置，Security Hub CSPM 会自动禁用涉及除主区域之外的所有区域中全局资源的控件。您选择通过配置策略启用的其他控件已在所有提供这些控件的区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。

如果涉及全局资源的已启用控件在主区域不受支持，则 Security Hub CSPM 会尝试在支持该控件的关联区域中启用该控件。使用中心配置，您无法覆盖在主区域或任何关联区域中不可用的控件。

有关涉及全球资源的控件列表，请参阅使用全局资源的控件。

建议的配置策略

首次在 Security Hub CSPM 控制台中创建配置策略时，您可以选择 Security Hub CSPM 推荐的策略。

推荐的策略启用 Security Hub CSPM、 AWS 基础安全最佳实践 (FSBP) 标准以及所有现有和新的 FSBP 控件。接受参数的控件使用默认值。推荐的策略适用于 root（所有账户 OUs，包括新账户和现有账户）。为您的组织创建推荐的策略后，您可以通过委派管理员账户对其进行修改。例如，您可以启用其他标准或控件或禁用特定的 FSBP 控件。有关修改配置策略的说明，请参阅更新配置策略。

自定义配置策略

委派管理员最多可以创建 20 个自定义配置策略，而不是推荐的策略。您可以将单个自定义策略与整个组织相关联，也可以将不同的自定义策略与不同的账户相关联，以及 OUs。对于自定义配置策略，您可以指定所需的设置。例如，您可以创建自定义策略，启用 FSBP、 Center for Internet Security（CIS）AWS 基金会基准 v1.4.0 以及这些标准中除了 Amazon Redshift 控件之外的所有控件。您在自定义配置策略中使用的粒度级别取决于整个组织的预期安全覆盖范围。

> **Note**
>
> 您无法将禁用 Security Hub CSPM 的配置策略与委派管理员账户相关联。这样的策略可以与其他账户关联，但会跳过与委派管理员的关联。委派管理员账户保留其当前配置。

创建自定义配置策略后，您可以更新配置策略，切换到推荐的配置策略，从而反映推荐的配置。但是，在创建第一个策略后，您无法在 Security Hub CSPM 控制台中看到创建推荐配置策略的选项。

通过应用和继承进行策略关联

当你第一次选择使用中心配置时，你的组织没有任何关联关系，其行为方式与选择加入之前相同。然后，授权的管理员可以在配置策略或自我管理的行为和帐户（或根帐户）之间建立关联。 OUs可以通过应用或继承来建立关联。

通过委派管理员账户，您可以直接将配置策略应用于账户、OU 或根。或者，委派管理员可以对账户、OU 或根直接应用自行管理指定。

在没有直接应用的情况下，账户或 OU 会继承具有配置策略或自行管理行为的最近父级的设置。如果最近的父级与配置策略相关联，则子级将继承该策略，并且只能由来自主区域的委派管理员进行配置。如果最亲近的父母是自我管理的，则孩子将继承自我管理的行为，并且能够在每个行为中指定自己的设置。 AWS 区域

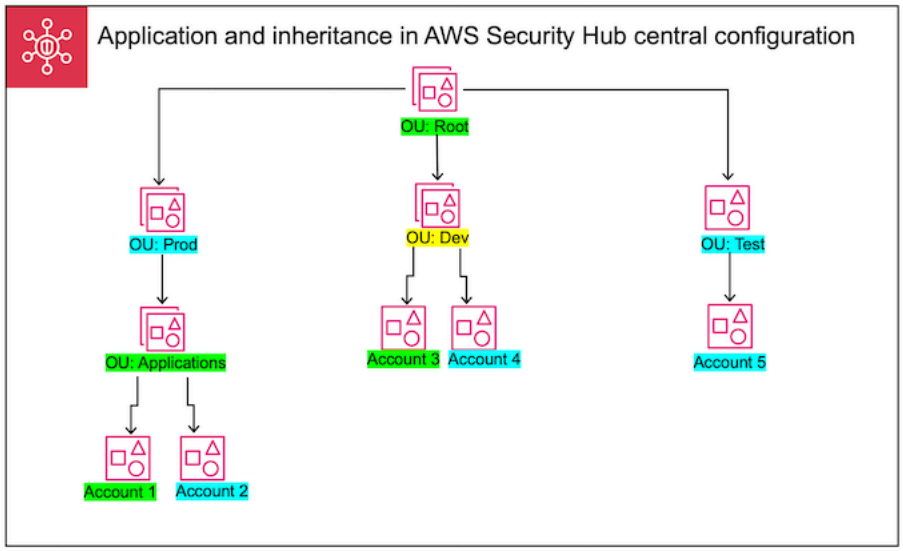
应用优先于继承。换句话说，继承不能覆盖委派管理员直接应用于账户或 OU 的配置策略或自行管理指定。

如果您对自行管理的账户直接应用配置策略，则该策略将覆盖自行管理指定。账户将变成集中管理，并采用配置策略中反映的设置。

我们建议对根直接应用配置策略。如果您对根应用策略，则加入组织的新账户将自动继承根策略，除非您将这些账户与其他策略关联或将其指定为自行管理。

在给定时间，只能通过应用或继承将配置策略与账户或 OU 关联。这旨在防止设置冲突。

下图说明了策略应用和继承在中心配置中的工作原理。



在此示例中，以绿色突出显示的节点具有已应用于该节点的配置策略。以蓝色突出显示的节点不具有已应用于该节点的配置策略。以黄色突出显示的节点已被指定为自行管理。每个账户和 OU 都使用以下配置：

- OU:Root（绿色）— 此 OU 使用已应用于它的配置策略。
- OU:Prod（蓝色）— 此 OU 继承了 OU:Root 的配置策略。
- OU:Applications（绿色）— 此 OU 使用已应用于它的配置策略。
- 账户 1（绿色）— 此账户使用已应用于它的配置策略。
- 账户 2（蓝色）：此账户继承了 OU:Applications 的配置策略。
- OU:Dev（黄色）— 此 OU 是自行管理的。
- 账户 3（绿色）— 此账户使用已应用于它的配置策略。
- 账户 4（蓝色）— 此账户继承了 OU:Dev 的自行管理行为。
- OU:Test（蓝色）— 此 OU 继承了 OU:Root 的配置策略。
- 账户 5（蓝色）— 此账户继承了 OU:Root 的配置策略，因为其直系父级 OU:Test 未与配置策略关联。

测试配置策略

为确保您了解配置策略的工作原理，我们建议您创建一个策略并将其与测试账户或 OU 关联。

要测试配置策略

1. 创建自定义配置策略，并验证 Security Hub CSPM 启用、标准和控件的指定设置是否正确。有关说明，请参阅创建和关联配置策略。
2. 将配置策略应用于没有任何子账号的测试账号或 OU 或 OUs。
3. 验证测试账户或 OU 在您的主区域和所有关联区域中是否按预期方式使用配置策略。您还可以验证组织 OUs 内的所有其他账户是否保持自我管理状态，并且可以在每个区域中更改自己的设置。

在单个账户或 OU 中测试配置策略后，您可以将其与其他账户关联和 OUs。

创建和关联配置策略

委派的 S AWS ecurity Hub CSPM 管理员帐户可以创建配置策略，指定如何在指定账户和组织单位中配置 Security Hub CSPM、标准和控制（ ）。OUs只有在授权的管理员将配置策略与至少一个账户或组织单位 (OUs) 或 root 关联后，该配置策略才会生效。委派的管理员还可以将自我管理的配置与账户 OUs、或 root 关联起来。

如果您是首次创建配置策略，我们建议您先查看 Security Hub CSPM 中配置策略的工作原理。

选择您的首选访问方法，然后按照步骤创建和关联配置策略或自行管理配置。使用 Security Hub CSPM 控制台时，您可以将一个配置与多个账户关联或 OUs 同时关联。使用 Security Hub CSPM API 或时 AWS CLI，您只能在每个请求中将配置与一个账户或 OU 相关联。

> **Note**
>
> 如果您使用中心配置，Security Hub CSPM 会自动禁用涉及除主区域之外的所有区域中全局资源的控件。您选择通过配置策略启用的其他控件已在所有提供这些控件的区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。
>
> 如果涉及全局资源的已启用控件在主区域不受支持，则 Security Hub CSPM 会尝试在支持该控件的关联区域中启用该控件。使用中心配置，您无法覆盖在主区域或任何关联区域中不可用的控件。
>
> 有关涉及全球资源的控件列表，请参阅使用全局资源的控件。

Security Hub CSPM console

要创建和关联配置策略

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择配置和策略选项卡。然后选择创建策略。
3. 如果这是您第一次创建配置策略，则在配置组织页面上，可以在配置类型下看到三个选项。如果您已经创建了至少一个配置策略，则只能看到自定义策略选项。

   - 选择 “在整个组织中使用 AWS 推荐的 Security Hub CSPM 配置” 以使用我们推荐的策略。推荐的策略在所有组织帐户中启用 Security Hub CSPM，启用 AWS 基础安全最佳实践 (FSBP) 标准，并启用所有新的和现有的 FSBP 控件。控件使用默认参数值。
   - 选择我还没准备好配置，以稍后创建配置策略。
   - 选择自定义策略，以创建自定义配置策略。指定是启用还是禁用 Security Hub CSPM、要启用哪些标准以及要在这些标准中启用哪些控件。（可选）为一个或多个支持自定义参数的已启用控件指定自定义参数值。
4. 在 “帐户” 部分，选择要将配置策略应用于哪些目标账户或根账户。 OUs

   - 如果要将配置策略应用于根，请选择所有账户。这包括组织 OUs 中所有未应用或继承其他政策的账户。
   - 如果要将配置策略应用于特定账户，请选择特定账户，或者 OUs。输入账户 IDs，或者 OUs 从组织结构中选择账户。创建策略时，您最多可以将策略应用于 15 个目标（账户或根）。OUs要指定更多目标，请在创建策略后进行编辑，然后将其应用于其他目标。
   - 选择仅限委派管理员，将配置策略应用于当前的委派管理员账户。
5. 选择下一步。
6. 在查看和应用页面上，查看您的配置策略详细信息。然后选择创建并应用策略。在您的主区域和关联区域中，此操作将覆盖与此配置策略关联的账户的现有配置设置。账户可以通过应用与配置策略相关联，也可以从父节点继承。子帐户和应用 OUs 的目标帐户将自动继承此配置策略，除非它们被特别排除、自行管理或使用不同的配置策略。

Security Hub CSPM API

要创建和关联配置策略

1. 从主区域的 Security Hub CSPM 委派管理员账户调用 CreateConfigurationPolicy API。
2. 对于 Name，输入配置策略的唯一名称。（可选）对于 Description，为配置策略提供描述。
3. 在 ServiceEnabled 字段中，指定要在此配置策略中启用还是禁用 Security Hub CSPM。
4. 在 EnabledStandardIdentifiers 字段中，指定要在此配置策略中启用哪些 Security Hub CSPM 标准。
5. 对于 SecurityControlsConfiguration 对象，请在此配置策略中指定要启用或禁用的控件。选择 EnabledSecurityControlIdentifiers 意味着指定的控件已启用。已启用标准中的其他控件（包括新发布的控件）将被禁用。选择 DisabledSecurityControlIdentifiers 意味着指定的控件被禁用。属于已启用标准的其他控件（包括新发布的控件）将被启用。
6. 或者，在 SecurityControlCustomParameters 字段中，指定要为其自定义参数的已启用控件。为 ValueType 字段提供 CUSTOM，为 Value 字段提供自定义参数值。该值必须是正确的数据类型，并且必须在 Security Hub CSPM 指定的有效范围内。只有精选控件支持自定义参数值。有关更多信息，请参阅 了解 Security Hub CSPM 中的控件参数。
7. 要将您的配置策略应用于账户或 OUs，请从所在区域的 Security Hub CSPM 委托管理员账户中调用 StartConfigurationPolicyAssociationAPI。
8. 请为 ConfigurationPolicyIdentifier 字段提供策略的 Amazon 资源名称（ARN）或用唯一标识符（UUID）。此 ARN 和 UUID 由 CreateConfigurationPolicy API 返回。对于自行管理配置，ConfigurationPolicyIdentifier 字段等于 SELF_MANAGED_SECURITY_HUB。
9. 在 Target 字段中，提供您希望此配置策略应用的 OU、账户或根 ID。您只能在每个 API 请求中提供一个目标。子帐户和选定目标 OUs 的子帐户将自动继承此配置策略，除非它们是自行管理的或使用不同的配置策略。

用于创建配置策略的 API 请求示例：

```
{
    "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
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

用于关联配置策略的 API 请求示例：

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

要创建和关联配置策略

1. 从主区域的 Security Hub CSPM 委派管理员账户运行 create-configuration-policy 命令。
2. 对于 name，输入配置策略的唯一名称。（可选）对于 description，为配置策略提供描述。
3. 在 ServiceEnabled 字段中，指定要在此配置策略中启用还是禁用 Security Hub CSPM。
4. 在 EnabledStandardIdentifiers 字段中，指定要在此配置策略中启用哪些 Security Hub CSPM 标准。
5. 在 SecurityControlsConfiguration 字段中，请在此配置策略中指定要启用或禁用的控件。选择 EnabledSecurityControlIdentifiers 意味着指定的控件已启用。已启用标准中的其他控件（包括新发布的控件）将被禁用。选择 DisabledSecurityControlIdentifiers 意味着指定的控件被禁用。适用于您已启用标准的其他控件（包括新发布的控件）已启用。
6. 或者，在 SecurityControlCustomParameters 字段中，指定要为其自定义参数的已启用控件。为 ValueType 字段提供 CUSTOM，为 Value 字段提供自定义参数值。该值必须是正确的数据类型，并且必须在 Security Hub CSPM 指定的有效范围内。只有精选控件支持自定义参数值。有关更多信息，请参阅 了解 Security Hub CSPM 中的控件参数。
7. 要将您的配置策略应用于账户或 OUs，请从所在区域的 Security Hub CSPM 委托管理员账户运行start-configuration-policy-association命令。
8. 请为 configuration-policy-identifier 字段提供配置策略的 Amazon 资源名称（ARN）或 ID。此 ARN 和 ID 由 create-configuration-policy 命令返回。
9. 在 target 字段中，提供您希望此配置策略应用的 OU、账户或根 ID。您只能在每次运行命令时提供一个目标。所选目标的子账户将自动继承此配置策略，除非它们是自行管理的或使用不同的配置策略。

用于创建配置策略的命令示例：

```
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}}}}]}}'
```

用于关联配置策略的命令示例：

```
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"}'
```

StartConfigurationPolicyAssociation API 返回一个名为 AssociationStatus 的字段。此字段会告诉您策略关联是待处理还是处于成功或失败状态。状态从 PENDING 变为 SUCCESS 或 FAILURE 可能需要长达 24 小时的时间。有关关联状态的更多信息，请参阅查看配置策略的关联状态。

查看配置策略的状态和详细信息

授权的 S AWS ecurity Hub CSPM 管理员可以查看组织的配置策略及其详细信息。这包括策略与哪些账户和组织单位 (OUs) 相关联。

有关中心配置的好处及其工作原理的背景信息，请参阅了解 Security Hub CSPM 中的中心配置。

选择首选方法，然后按照步骤查看配置策略。

Security Hub CSPM console

查看配置策略（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡以查看配置策略概述。
4. 选择一个配置策略，然后选择 View det ails 以查看有关该策略的其他详细信息，包括与哪些账户及其 OUs 关联的账户。

Security Hub CSPM API

要查看所有配置策略的摘要列表，请使用 Security Hub CSPM API 的 ListConfigurationPolicies 操作。如果您使用 AWS CLI，请运行该list-configuration-policies命令。Security Hub CSPM 委派管理员账户应在主区域调用该操作。

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

要查看有关特定配置策略的详细信息，请使用 GetConfigurationPolicy 操作。如果您使用 AWS CLI，请运行get-configuration-policy。委派管理员应在主区域调用此操作。提供要查看其详细信息的配置策略的 Amazon 资源名称（ARN）或 ID。

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

要查看所有配置策略及其账户关联情况的摘要列表，请使用 ListConfigurationPolicyAssociations 操作。如果您使用 AWS CLI，请运行该list-configuration-policy-associations命令。委派管理员应在主区域调用此操作。或者，您可以提供分页参数，或者按特定策略 ID、关联类型或关联状态筛选结果。

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

要查看特定账户的关联情况，请使用 GetConfigurationPolicyAssociation 操作。如果您使用 AWS CLI，请运行该get-configuration-policy-association命令。委派管理员应在主区域调用此操作。对于 `target`，请提供账户、OU ID 或根 ID。

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

查看配置策略的关联状态

以下中心配置 API 操作将返回一个名为 `AssociationStatus` 的字段：

- `BatchGetConfigurationPolicyAssociations`

- GetConfigurationPolicyAssociation
- ListConfigurationPolicyAssociations
- StartConfigurationPolicyAssociation

当基础配置为配置策略，并且是自行管理行为时，都将返回此字段。

AssociationStatus 的值指明特定账户的策略关联是处于待定状态还是成功或失败状态。状态从 PENDING 变为 SUCCESS 或 FAILED 可能需要长达 24 小时的时间。状态 SUCCESS 表示配置策略中指定的所有设置都与账户相关联。状态 FAILED 表示配置策略中指定的一个或多个设置未能与账户关联。尽管处于 FAILED 状态，但可以根据策略对账户进行部分配置。例如，您可以尝试将账户与启用 Security Hub CSPM、启用 AWS 基础安全最佳实践和禁用 .1 的配置策略相关联。 CloudTrail最初的两个设置可能会成功，但是 CloudTrail .1 设置可能会失败。在此示例中，即使某些设置配置正确，关联状态仍为 FAILED。

父 OU 或根的关联状态取决于其子级的状态。如果所有子级的关联状态均为 SUCCESS，则父级的关联状态为 SUCCESS。如果一个或多个子级的关联状态均为 FAILED，则父级的关联状态为 FAILED。

值 AssociationStatus 取决于所有相关区域中该策略的关联状态。如果关联在主区域和所有关联区域成功，则 AssociationStatus 的值为 SUCCESS。如果关联在一个或多个区域失败，则 AssociationStatus 的值为 FAILED。

以下行为也会影响 AssociationStatus 的值：

- 如果目标是父 OU 或根，则只有当所有子级的状态为 SUCCESS 或 FAILED 时，AssociationStatus 才具有 SUCCESS 或 FAILED 状态。在首次将父级与配置关联后，如果子账户或 OU 的关联状态变更（例如，添加或删除了关联区域时），则除非再次调用 StartConfigurationPolicyAssociation API，否则变更不会使父级的关联状态更新。
- 如果目标是账户，则只有当主区域和所有关联区域的关联结果为 SUCCESS 或 FAILED 时，AssociationStatus 才具有 SUCCESS 或 FAILED 状态。在首次将目标账户与配置关联后，如果目标账户的关联状态变更（例如，添加或删除了关联区域时），则配置的关联状态也会随之更新。但除非再次调用 StartConfigurationPolicyAssociation API，否则变更不会使父级的关联状态更新。

如果您添加新的关联区域，Security Hub CSPM 会复制新区域中处于 PENDING、SUCCESS 或 FAILED 状态的现有关联。

即使关联状态为 SUCCESS，作为策略一部分的标准的启用状态也可能转变为未完成状态。在这种情况下，Security Hub CSPM 无法为标准的控件生成调查发现。有关更多信息，请参阅 检查标准的状态。

关联失败问题排查

在 S AWS ecurity Hub CSPM 中，配置策略关联可能由于以下常见原因而失败。

- 组织管理账户不是成员 — 如果要将配置策略与组织管理账户关联，则该账户必须已启用 Sec AWS urity Hub CSPM。这将使管理账户成为组织的成员账户。
- AWS Config 未启用或未正确配置-要在配置策略中启用标准， AWS Config 必须启用并配置为记录相关资源。
- 必须从委托管理员账户进行关联 — 只有在登录委派的 Security Hub CSPM 管理员账户 OUs 时，您才能将策略与目标账户相关联。
- 必须从本地区进行关联 — 您只能将保单与目标账户相关联，也只能在您登录所在地区 OUs 时进行关联。
- 未启用选择加入区域：如果关联区域是委派管理员尚未启用的选择加入区域，则该区域中的成员账户或 OU 的策略关联将会失败。您可以在从委派管理员账户启用区域后重试。
- 成员账户已暂停：如果尝试将策略与暂停的成员账户关联，则策略关联将失败。

更新配置策略

创建配置策略后，委托的 S AWS ecurity Hub CSPM 管理员帐户可以更新策略详细信息和策略关联。更新策略详细信息后，与配置策略关联的账户会自动开始使用更新后的策略。

有关中心配置的好处及其工作原理的背景信息，请参阅了解 Security Hub CSPM 中的中心配置。

委派管理员可以更新以下策略设置：

- 启用或禁用 Security Hub CSPM。
- 启用一项或多项安全标准。
- 指明在已启用的标准中启用了哪些安全控件。您可以通过提供应启用的特定控件列表来实现这一点，而 Security Hub CSPM 会禁用所有其他控件（包括新发布的控件）。或者，您可以提供应禁用的特定控件列表，Security Hub CSPM 将启用所有其他控件（包括新发布的控件）。
- （可选）在已启用的标准中为选定的已启用控件自定义参数。

选择首选方法，然后按照步骤更新配置策略。

> **Note**
>
> 如果您使用中心配置，Security Hub CSPM 会自动禁用涉及除主区域之外的所有区域中全局资源的控件。您选择通过配置策略启用的其他控件已在所有提供这些控件的区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。
>
> 如果涉及全局资源的已启用控件在主区域不受支持，则 Security Hub CSPM 会尝试在支持该控件的关联区域中启用该控件。使用中心配置，您无法覆盖在主区域或任何关联区域中不可用的控件。
>
> 有关涉及全球资源的控件列表，请参阅使用全局资源的控件。

Console

要更新配置策略

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。
4. 选择要编辑的配置策略，然后选择编辑。如果需要，请编辑策略设置。如果要保持策略设置不变，请保留此部分。
5. 选择下一步。如果需要，请编辑策略关联。如果要保持策略关联不变，请保留此部分。更新策略时，您可以将策略与最多 15 个目标（账户或 root）关联或取消关联。 OUs
6. 选择下一步。
7. 检查更改，然后选择保存并应用。在您的主区域和关联区域中，此操作将覆盖与此配置策略关联的账户的现有配置设置。账户可以通过应用与配置策略相关联，也可以从父节点继承。

API

要更新配置策略

1. 要更新配置策略中的设置，请从主区域的 Security Hub CSPM 委派管理员账户调用 UpdateConfigurationPolicy API。
2. 提供要更新的配置策略的 Amazon 资源名称（ARN）或 ID。

3. 为 ConfigurationPolicy 下方的字段提供更新后的值。（可选）您还可以提供更新原因。
4. 要为此配置策略添加新的关联，请从主区域的 Security Hub CSPM 委派管理员账户调用 StartConfigurationPolicyAssociation API。要删除一个或多个当前关联，请从主区域的 Security Hub CSPM 委派管理员账户调用 StartConfigurationPolicyDisassociation API。
5. 对于 ConfigurationPolicyIdentifier 字段，提供要更新其关联的配置策略的 ARN 或 ID。
6. 在该Target字段中，提供您想要关联或取消关联的账户 OUs、或根 ID。此操作将覆盖指定 OUs 或账户之前的策略关联。

> **Note**
>
> 调用 UpdateConfigurationPolicy API 时，Security Hub CSPM 会对 EnabledStandardIdentifiers、EnabledSecurityControlIdentifiers、DisabledSec 和 SecurityControlCustomParameters 字段执行完整列表替换。每次调用此 API 时，请提供要启用的标准的完整列表，以及要为其启用或禁用和自定义参数的控件的完整列表。

更新配置策略的 API 请求示例：

```
{
    "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

要更新配置策略

1. 要更新配置策略中的设置，请从主区域的 Security Hub CSPM 委派管理员账户运行 update-configuration-policy 命令。
2. 提供要更新的配置策略的 Amazon 资源名称（ARN）或 ID。
3. 为 `configuration-policy` 下方的字段提供更新后的值。（可选）您还可以提供更新原因。
4. 要为此配置策略添加新的关联，请从主区域的 Security Hub CSPM 委派管理员账户运行 start-configuration-policy-association 命令。要移除一个或多个当前关联，请从主区域的 Security Hub CSPM 委派管理员账户运行 start-configuration-policy-disassociation 命令。
5. 对于 `configuration-policy-identifier` 字段，提供要更新其关联的配置策略的 ARN 或 ID。
6. 在该`target`字段中，提供您想要关联或取消关联的账户 OUs、或根 ID。此操作将覆盖指定 OUs 或账户之前的策略关联。

> **Note**
>
> 运行 update-configuration-policy 命令时，Security Hub CSPM 会对 EnabledStandardIdentifiers、EnabledSecurityControlIdentifiers、DisabledSec 和 SecurityControlCustomParameters 字段执行完整列表替换。每次运行此命令时，请提供要启用的标准的完整列表，以及要为其启用或禁用和自定义参数的控件的完整列表。

更新配置策略的命令示例：

```
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}}}}]}}}'
```

StartConfigurationPolicyAssociation API 返回一个名为 AssociationStatus 的字段。此字段会告诉您策略关联是待处理还是处于成功或失败状态。状态从 PENDING 变为 SUCCESS 或 FAILURE 可能需要长达 24 小时的时间。有关关联状态的更多信息，请参阅查看配置策略的关联状态。

删除配置策略

创建配置策略后，委托的 S AWS ecurity Hub CSPM 管理员可以将其删除。或者，授权的管理员可以保留该策略，但将其与特定账户或组织单位 (OUs) 或根解除关联。有关取消关联策略的说明，请参阅取消配置与其目标的关联。

有关中心配置的好处及其工作原理的背景信息，请参阅了解 Security Hub CSPM 中的中心配置。

本节介绍如何删除配置策略。

删除配置策略后，该策略将不再存在于组织中。目标账户 OUs和组织根用户不能再使用配置策略。与已删除的配置策略关联的目标将继承最接近父级的配置策略，或者如果最接近父级是自行管理的，则会变为自行管理。如果希望目标使用其他配置，可以将该目标与新的配置策略相关联。有关更多信息，请参阅 创建和关联配置策略。

我们建议至少创建一个配置策略，并将其与组织关联，以提供足够的安全覆盖。

在删除配置策略之前，必须取消该策略与当前应用该策略的任何账户或根账户的关联。 OUs

选择首选方法，然后按照步骤删除配置策略。

Console

要删除配置策略

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。选择要删除的配置策略，然后选择删除。如果配置策略仍与任何账户相关联或 OUs，则系统会提示您先取消策略与这些目标的关联，然后才能将其删除。
4. 查看确认消息。输入 **`confirm`**，然后选择删除。

API

要删除配置策略

从主区域的 Security Hub CSPM 委派管理员账户调用 DeleteConfigurationPolicy API。

提供要删除的配置策略的 Amazon 资源名称（ARN）或 ID。如果您收到`ConflictException`错误，则配置策略仍适用于账户或 OUs 您的组织。要解决此错误，请取消配置策略与这些账户的关联，或者 OUs 在尝试删除配置策略之前。

删除配置策略的 API 请求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

要删除配置策略

从主区域的 Security Hub CSPM 委派管理员账户运行 delete-configuration-policy 命令。

提供要删除的配置策略的 Amazon 资源名称（ARN）或 ID。如果您收到ConflictException错误，则配置策略仍适用于账户或 OUs 您的组织。要解决此错误，请取消配置策略与这些账户的关联，或者 OUs 在尝试删除配置策略之前。

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

取消配置与其目标的关联

通过委派的 S AWS ecurity Hub CSPM 管理员帐户，您可以取消配置策略或自管理配置与账户、组织单位或根的关联。取消关联会保留策略以备将来使用，但会删除特定账户或 root 的现有关联。您只能取消关联直接应用的配置，而不能取消继承的配置。 OUs要更改继承的配置，可以将配置策略或自行管理行为应用于受影响的账户或 OU。您还可以将新的配置策略（包括所需的修改）应用于最接近的父级。

取消关联不会删除配置策略。该策略保留在您的账户中，因此您可以将其与组织中的其他目标关联。有关删除配置策略的说明，请参阅删除配置策略。解除关联完成后，受影响的目标将继承最接近的父级的配置策略或自行管理行为。如果没有可继承的配置，目标会保留解除关联之前的设置，但变为自行管理。

选择首选方法，然后按照步骤解除账户、OU 或根与其当前配置的关联。

Console

要解除账户或 OU 与其当前配置的关联

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。

3. 在组织选项卡上，选择要解除与其当前配置关联的账户、OU 或根。选择编辑。
4. 在定义配置页面上，对于管理，如果您希望委派管理员能够将策略直接应用于目标，请选择应用的策略。如果希望目标继承最接近父级的配置，请选择继承。在这两种情况下，委派管理员都将控制目标的设置。如果希望账户或 OU 控制自己的设置，请选择自行管理。
5. 查看更改后，选择下一步和应用。如果任何账户的现有配置或范围内的配置与您当前 OUs 的选择相冲突，则此操作将覆盖这些配置。

API

要解除账户或 OU 与其当前配置的关联

1. 从主区域的 Security Hub CSPM 委派管理员账户调用 StartConfigurationPolicyDisassociation API。
2. 对于 `ConfigurationPolicyIdentifier`，提供要解除关联的配置策略的 Amazon 资源名称（ARN）或 ID。对于该字段，提供 `SELF_MANAGED_SECURITY_HUB` 以解除自行管理行为的关联。
3. 对于`Target`，请提供您要与该配置策略解除关联的账户或根目录。 OUs

解除配置策略关联的 API 请求示例：

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

要解除账户或 OU 与其当前配置的关联

1. 从主区域的 Security Hub CSPM 委派管理员账户运行 start-configuration-policy-disassociation 命令。
2. 对于 `configuration-policy-identifier`，提供要解除关联的配置策略的 Amazon 资源名称（ARN）或 ID。对于该字段，提供 `SELF_MANAGED_SECURITY_HUB` 以解除自行管理行为的关联。
3. 对于`target`，请提供您要与该配置策略解除关联的账户或根目录。 OUs

解除配置策略关联的命令示例：

```
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"}'
```

在上下文中配置标准或控件

在 Sec AWS urity Hub CSPM 中使用集中配置时，委派的 Security Hub CSPM 管理员可以创建配置策略，指定如何为组织配置 Security Hub CSPM、安全标准和安全控制。委派管理员可以将策略与特定账户和组织单元（OU）相关联。这些策略会在您的主区域和所有关联区域中生效。委派管理员可以根据需要更新配置策略。

在 Security Hub CSPM 控制台上，委派管理员可以通过两种方式更新配置策略：从配置页面更新或者在现有工作流的上下文中更新。第二种方法可能很有益，因为在查看安全调查发现时，您还可以发现哪些标准和控件与环境最相关，同时对其进行配置。

上下文配置仅在 Security Hub CSPM 控制台上可用。委派管理员必须以编程方式调用 Security Hub CSPM API 的 UpdateConfigurationPolicy 操作，才能更改组织中特定标准或控件的配置方式。

请按照以下步骤在上下文中配置 Security Hub CSPM 标准或控件。

在上下文中配置标准或控件（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择以下选项之一：

   - 要配置标准，请选择安全标准，然后选择特定标准。
   - 要配置控件，请选择控件，然后选择特定控件。
3. 控制台会列出您现有的 Security Hub CSPM 配置策略以及每个策略中选定的标准或控件的状态。在每个现有配置策略中选择启用或禁用标准或控件的选项。对于控件，您还可以选择自定义控件参数。在上下文中进行配置的过程中，您无法创建新策略。要创建新策略，必须前往配置页面，选择策略选项卡，然后选择创建策略。
4. 更改后，选择下一步。

5. 查看更改，然后选择应用。这些更新会影响所有与 OUs 已更改的配置策略关联的账户。更新同时在主区域和所有关联区域中生效。

在 Security Hub CSPM 中禁用中心配置

在 Sec AWS urity Hub CSPM 中禁用中央配置后，委派的管理员将无法在多个组织单位 () OUs 和之间配置 Security Hub CSPM AWS 账户、安全标准和安全控制。 AWS 区域相反，您必须为每个区域中的每个账户单独配置大部分设置。

> **Important**
>
> 在禁用中央配置之前，必须先解除账户及其 OUs当前配置的关联，无论是配置策略还是自我管理行为。
> 在禁用中心配置之前，还必须删除现有配置策略。

禁用中心配置后，将发生以下变化：

- 委派管理员无法再为组织创建配置策略。
- 已应用或继承配置策略的账户将保留其当前设置，但会变为自行管理。
- 组织切换到本地配置。在本地配置下，大多数 Security Hub CSPM 设置必须在每个组织账户和区域中单独配置。委派管理员可以选择自动启用 Security Hub CSPM、默认安全标准以及属于新组织账户默认标准的所有控件。默认标准是 AWS 基础安全最佳实践 (FSBP) 和互联网安全中心 (CIS) AWS 基金会基准 v1.2.0。这些设置仅在当前区域生效，并且仅影响新的组织账户。委派管理员无法更改默认标准。本地配置不支持在 OU 级别使用配置策略或配置。

停止使用中心配置后，委派管理员账户的身份将保持不变。主区域和关联区域也保持不变（主区域现在称为聚合区域，可用于查找聚合）。

选择首选方法，然后按照步骤停止使用中心配置并切换到本地配置。

Security Hub CSPM console

禁用中心配置（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。

2. 在导航窗格中，选择设置和配置。
3. 在概述部分，选择编辑。
4. 在编辑组织配置框中，选择本地配置。如果未这样做，系统会提示您解除关联并删除当前的配置策略，然后才能停止中心配置。必须取消账户或 OUs 指定为自我管理的账户与其自我管理配置的关联。您可以在控制台中执行此操作，方法是将每个自行管理账户或 OU 的管理类型更改为集中管理和从我的组织继承。
5. （可选）为新组织账户选择本地配置默认设置。
6. 选择确认。

Security Hub CSPM API

禁用中心配置（API）

1. 调用 UpdateOrganizationConfiguration API。
2. 将 `OrganizationConfiguration` 对象中的 `ConfigurationType` 字段设置为 `LOCAL`。如果您有现有的配置策略或策略关联，API 会返回错误。要解除配置策略的关联，请调用 `StartConfigurationPolicyDisassociation` API。要删除配置策略，请调用 `DeleteConfigurationPolicy` API。
3. 如果要在新组织账户中自动启用 Security Hub CSPM，请将 `AutoEnable` 字段设置为 `true`。默认情况下，此字段的值为 `false`，并且 Security Hub CSPM 不会在新组织账户中自动启用。（可选）如果要在新组织账户中自动启用默认安全标准，请将 `AutoEnableStandards` 字段设置为 `DEFAULT`。这是默认值。如果不想在新组织账户中自动启用默认安全标准，请将 `AutoEnableStandards` 字段设置为 `NONE`。

API 请求示例：

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

禁用中心配置（AWS CLI）

1. 运行 update-organization-configuration 命令。
2. 将 organization-configuration 对象中的 ConfigurationType 字段设置为 LOCAL。如果您有现有的配置策略或策略关联，命令会返回错误。要解除配置策略关联，请运行 start-configuration-policy-disassociation 命令。要删除配置策略，请运行 delete-configuration-policy 命令。
3. 如果要在新组织账户中自动启用 Security Hub CSPM，请包含 auto-enable 参数。默认情况下，此参数的值为 no-auto-enable，并且 Security Hub CSPM 不会在新组织账户中自动启用。（可选）如果要在新组织账户中自动启用默认安全标准，请将 auto-enable-standards 字段设置为 DEFAULT。这是默认值。如果不想在新组织账户中自动启用默认安全标准，请将 auto-enable-standards 字段设置为 NONE。

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

管理 Security Hub CSPM 中的管理员账户和成员账户

如果您的 AWS 环境有多个帐户，则可以将使用 Sec AWS urity Hub CSPM 的帐户视为成员帐户，并将它们与单个管理员帐户关联。管理员可以监控您的整体安全状况，对成员账户执行允许的操作。管理员还可以大规模执行各种账户管理任务，例如监控预计使用成本和评测账户配额。

您可以通过两种方式将成员帐户与管理员关联：将 Security Hub CSPM 与 Security Hub CSPM 集成，AWS Organizations 或者在 Security Hub CSPM 中手动发送和接受会员邀请。

使用管理账户 AWS Organizations

AWS Organizations 是一项全球账户管理服务，允许 AWS 管理员整合和管理多个账户 AWS 账户。它提供账户管理和整合账单功能，这些功能旨在满足预算、安全性和合规性需求。它不收取额外费用，并且可以与多个 AWS 服务集成，包括Sec AWS urity Hub CSPM、Amazon Macie和亚马逊。GuardDuty有关更多信息，请参阅 AWS Organizations 《用户指南》。

当你集成 Security Hub CSPM 和时 AWS Organizations，Organizations 管理账户会指定 Security Hub CSPM 授权的管理员。Security Hub CSPM 将在指定的委托管理员账户 AWS 区域 中自动启用。

指定委派管理员后，我们建议使用中心配置在 Security Hub CSPM 中管理账户。这是自定义 Security Hub CSPM 并确保为组织提供足够的安全覆盖的有效方法。

中央配置允许授权管理员跨多个组织账户和区域自定义 Security Hub CSPM，而不必进行配置。Region-by-Region您可以为整个组织创建配置策略，也可以为不同的账户和创建不同的配置策略 OUs。这些策略指定了在关联账户中启用还是禁用 Security Hub CSPM，以及启用哪些安全标准和控件。

委派管理员可将账户指定为集中管理或自行管理。集中管理的账户只能由委派管理员配置。自行管理账户可以自行指定设置。

如果您不选择使用中心配置，则委派管理员配置 Security Hub CSPM 的能力将更为有限（称为本地配置）。在本地配置下，委派管理员可以在当前区域的新组织账户中自动启用 Security Hub CSPM 和默认安全标准。但现有账户不使用这些设置，因此账户加入组织后可能会出现配置偏差。

除了这些新账户设置外，本地配置是针对特定账户和特定区域的。每个组织账户必须在每个区域单独配置 Security Hub CSPM 服务、标准和控件。本地配置也不支持使用配置策略。

通过邀请手动管理账户

如果您拥有独立账户或未与 Organizations 集成，则必须在 Security Hub CSPM 中通过邀请手动管理成员账户。独立账户不能与 Organizations 集成，因此需要手动管理。如果您将来添加其他帐户，我们建议您与中央配置集成 AWS Organizations 并使用中央配置。

使用手动账户管理时，要将一个账户指定为 Security Hub CSPM 管理员。管理员账户可以查看成员账户中的数据，对成员账户的调查发现执行某些操作。Security Hub CSPM 管理员邀请其他账户成为成员账户，当潜在成员账户接受邀请后，管理员与成员关系即建立。

手动账户管理不支持使用配置策略。如果没有配置策略，管理员就无法通过为不同的账户配置变量设置来集中自定义 Security Hub CSPM。相反，每个组织账户必须在每个区域中单独为自己启用和配置 Security Hub CSPM。这可能会增加确保在使用 Security Hub CSPM 的所有账户和区域中实现充分安全覆盖的难度和时间。这还可能导致配置偏差，因为成员账户可以指定自己的设置，而无需管理员输入。

要通过邀请管理账户，请参阅在 Security Hub CSPM 中通过邀请管理账户。

在 Security Hub CSPM 中管理多个账户的建议

以下部分总结了在 Sec AWS urity Hub CSPM 中管理成员帐户时需要注意的一些限制和建议。

成员账户的最大数量

如果您使用与的集成 AWS Organizations，Security Hub CSPM 在每个委托管理员账户中最多支持 10,000 个成员账户。 AWS 区域如果手动启用和管理 Security Hub CSPM，Security Hub CSPM 支持每个区域每个管理员账户最多 1,000 个成员账户邀请。

创建管理员与成员关系

> **Note**
>
> 如果您将 Security Hub CSPM 与 AWS Organizations Security Hub CSPM 集成，并且尚未手动邀请任何成员帐户，则此部分不适用于您。

账户不能既是管理员账户又是成员账户。

一个成员账户只能与一个管理员账户关联。如果组织账户由 Security Hub CSPM 管理员账户启用，则该账户将无法接受来自其他账户的邀请。如果某账户已经接受邀请，则该账户无法通过组织的 Security Hub CSPM 管理员账户启用。它也无法接收来自其他账户的邀请。

对于手动邀请流程，接受成员资格邀请是可选的。

通过以下方式获得会 AWS Organizations

如果您将 Security Hub CSPM 与集成 AWS Organizations，则组织管理帐户可以为 Security Hub CSPM 指定委托管理员 (DA) 帐户。不能将组织管理账户设置为组织的 DA。虽然 Security Hub CSPM 允许这样做，但我们建议不要将 Organizations 管理账户设为 DA。

我们建议在所有区域选择同一个 DA 账户。如果使用中心配置，则 Security Hub CSPM 会在您为组织配置 Security Hub CSPM 的所有区域中设置相同的 DA 账户。

我们还建议您在 AWS 安全与合规服务中选择相同的 DA 帐户，以帮助您在单一管理平台中管理与安全相关的问题。

通过邀请的成员资格

对于通过邀请创建的成员账户，管理员与成员账户的关联仅在发出邀请的地区创建。管理员账户必须在要使用的每个区域中启用 Security Hub CSPM。然后，管理员账户会邀请每个账户成为该区域的成员账户。

> **Note**
>
> 我们建议使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的会员账户。

跨服务协调管理员账户

Security Hub CSPM 汇总了来自亚马逊、亚马逊 Insp GuardDuty ector 和 Amazon Macie 等各种 AWS 服务的调查结果。Security Hub CSPM 还允许用户从调查 GuardDuty 结果转向在 Amazon Detective 中开始调查。

但是，您在这些其他服务中设置的管理员与成员关系不会自动应用于 Security Hub CSPM。Security Hub CSPM 建议所有这些服务使用与管理员账户相同的账户。此管理员账户应该是负责安全工具的账户。同一个账户也应该是 AWS Config的聚合器账户。

例如， GuardDuty 管理员账户 A 中的用户可以在 GuardDuty 控制台上查看 GuardDuty成员账户 B 和 C 的调查结果。如果账户 A 随后启用 Security Hub CSPM，则账户 A 的用户不会自动在 Security Hub CSPM 中看到账户 B 和 C 的搜索 GuardDuty结果。这些账户还需要建立 Security Hub CSPM 管理员与成员关系。

为此，请将账户 A 设为 Security Hub CSPM 管理员账户，并使账户 B 和 C 成为 Security Hub CSPM 成员账户。

使用管理多个账户的 Security Hub CSPM AWS Organizations

你可以将 S AWS ecurity Hub CSPM 与组织中的账户集成 AWS Organizations，然后为组织中的账户管理 Security Hub CSPM。

要将 Security Hub CSPM 与 Security Hub CSPM 集成 AWS Organizations，你需要在中创建一个组织。 AWS Organizations Organizations 管理账户会将一个账户指定为该组织的 Security Hub CSPM 委派管理员。然后，委派管理员可以为组织中的其他账户启用 Security Hub CSPM，将这些账户添加为 Security Hub CSPM 成员账户，并对成员账户采取允许的操作。Security Hub CSPM 委派管理员可以为多达 1 万个成员账户启用和管理 Security Hub CSPM。

委派管理员的配置能力范围取决于您是否使用中心配置。启用中心配置后，您无需在每个成员账户和 AWS 区域中单独配置 Security Hub CSPM。授权的管理员可以在各区域的指定成员账户和组织单位 (OUs) 中强制执行特定的 Security Hub CSPM 设置。

Security Hub CSPM 委派管理员账户可以对成员账户执行以下操作：

- 如果使用集中配置，请为成员账户集中配置 Security Hub CSPM，并 OUs 通过创建 Security Hub CSPM 配置策略进行配置。配置策略可用于启用和禁用 Security Hub CSPM、启用和禁用标准以及启用和禁用控件。
- 在将新账户加入组织时，自动将其视为 Security Hub CSPM 成员账户。如果您使用中心配置，则与 OU 关联的配置策略包括属于 OU 的现有账户和新账户。
- 将现有组织账户视为 Security Hub CSPM 成员账户。如果您使用中心配置，这种情况会自动出现。
- 取消关联属于该组织的成员账户。如果您使用中心配置，则只有在将成员账户指定为自行管理之后，才能取消其关联。或者，您可以将禁用 Security Hub CSPM 的配置策略与特定的集中管理的成员账户相关联。

如果您不选择中心配置，则组织会使用称为本地配置的默认配置类型。在本地配置下，委派管理员在成员账户中强制设置的能力将更为有限。有关更多信息，请参阅 了解 Security Hub CSPM 中的本地配置。

有关委派管理员可以对成员账户执行的操作的完整列表，请参阅Security Hub CSPM 中管理员和成员账户可以执行的操作。

本节中的主题说明了如何将 Security Hub CSPM 与组织中的账户集成， AWS Organizations 以及如何为组织中的账户管理 Security Hub CSPM。在相关时，每个部分都确定了中心配置用户在管理方面的好处和差异。

主题

- 将 Security Hub CSPM 与 AWS Organizations
- 在新组织账户中自动启用 Security Hub CSPM。
- 在新组织账户中手动启用 Security Hub CSPM
- 解除 Security Hub CSPM 成员账户与组织的关联

将 Security Hub CSPM 与 AWS Organizations

要集成 S AWS ecurity Hub CSPM 和 AWS Organizations，您需要在 “组织” 中创建组织，然后使用组织管理帐户指定委托的 Security Hub CSPM 管理员帐户。这使 Security Hub CSPM 成为组织中的可信

服务。它还为委派管理员账户启用当前 AWS 区域 中的 Security Hub CSPM，并允许委派管理员为成员账户启用 Security Hub CSPM，查看成员账户中的数据，并对成员账户执行其他允许的操作。

如果您使用中心配置，则委派管理员还可以创建 Security Hub CSPM 配置策略，指定应如何在组织账户中配置 Security Hub CSPM 服务、标准和控件。

创建企业

组织是您为整合组织而创建的实体， AWS 账户 以便您可以将其作为一个单位进行管理。

您可以使用 AWS Organizations 控制台创建组织，也可以使用来自 AWS CLI 或其中一个 SDK 的命令来创建组织 APIs。有关详细说明，请参阅《AWS Organizations 用户指南》中的创建组织。

您可以使用集中 AWS Organizations 查看和管理组织内的所有帐户。一个组织有一个管理账户以及零个或多个成员账户。您可以将帐户组织成树状的分层结构，根目录位于顶部，组织单位 (OUs) 嵌套在根目录下。每个账户可以直接位于根目录下，也可以放在层次结构 OUs 中的一个账户中。OU 是特定账户的容器。例如，您可以创建一个财务 OU，其中包括与财务操作相关的所有账户。

选择委派的 Security Hub CSPM 管理员的建议

如果您在手动邀请流程中拥有管理员帐户，并且正在过渡到账户管理，我们建议将该帐户指定为委派的 Security Hub CSPM 管理员。 AWS Organizations

尽管 Security Hub CSPM APIs 和控制台允许组织管理帐户成为委托的 Security Hub CSPM 管理员，但我们建议选择两个不同的帐户。这是因为有权访问组织管理账户来管理账单的用户可能与需要访问 Security Hub CSPM 进行安全管理的用户不同。

我们建议您在所有区域使用同一个委派管理员。如果您选择使用中心配置，Security Hub CSPM 会自动在您的主区域和任何关联区域中指定相同的委派管理员。

验证配置委派管理员的权限

要指定和删除委派的 Security Hub CSPM 管理员账户，组织管理账户必须具有在 Security Hub CSPM 中执行 `EnableOrganizationAdminAccount` 和 `DisableOrganizationAdminAccount` 操作的权限。Organizations 管理账户还必须拥有 Organizations 的管理权限。

要授予所有必需的权限，请将以下 Security Hub CSPM 托管策略附加到组织管理账户的 IAM 主体：

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

指定委派管理员

要指定委派的 Security Hub CSPM 管理员账户，您可以使用 Security Hub CSPM 控制台、Security Hub CSPM API 或 AWS CLI。Security Hub CSPM AWS 区域 仅在当前区域设置委托管理员，您必须在其他区域重复该操作。如果您开始使用中心配置，则 Security Hub CSPM 会自动在主区域和关联区域中设置相同的委派管理员。

组织管理账户不必启用 Security Hub CSPM 即可指定委派的 Security Hub CSPM 管理员账户。

我们不建议将组织管理账户作为委派的 Security Hub CSPM 管理员账户。但是，如果您选择了组织管理账户作为 Security Hub CSPM 委派管理员，则该管理账户必须启用 Security Hub CSPM。如果管理账户未启用 Security Hub CSPM，则必须手动为其启用 Security Hub CSPM。无法为组织管理账户自动启用 Security Hub CSPM。

必须使用以下方法之一指定委派的 Security Hub CSPM 管理员。在 Organizations 中指定委派的 Security Hub CSPM 管理员并 APIs 不能反映在 Security Hub CSPM 中。

选择您喜欢的方法，然后按照步骤指定委派的 Security Hub CSPM 管理员账户。

Security Hub CSPM console

在引导阶段指定委托 Security Hub 管理员

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 选择转到 Security Hub CSPM。系统会提示您登录到组织管理账户。
3. 在指定委派管理员页面的委派管理员账户部分，指定委派管理员账户。我们建议选择您为其他 AWS 安全与合规服务设置的相同委派管理员。
4. 选择设置委派管理员。系统会提示您登录委派管理员账户（如果您尚未登录），以便继续使用中心配置进行登录。如果您不想启用中心配置，请选择取消。您的委派管理员已设置完毕，但您尚未使用中心配置。

从设置页面指定委托 Security Hub 管理员

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在 Security Hub CSPM 导航窗格中，选择设置。然后，选择常规。
3. 如果当前分配了 Security Hub CSPM 管理员账户，则必须先删除当前账户，然后才能指定新账户。

在委派管理员下，要删除当前账户，请选择删除。

4. 输入您要指定为 Security Hub CSPM 委派管理员账户的账户 ID。

   您必须在所有区域指定同一个 Security Hub CSPM 管理员账户。如果您指定的账户与其他区域指定的账户不同，控制台会返回错误。

5. 选择 Delegate（委派）。

Security Hub CSPM API, AWS CLI

在组织管理账户中，使用 Security Hub CSPM API 的 EnableOrganizationAdminAccount 操作。如果您使用的是 AWS CLI，请运行 enable-organization-admin-account 命令。提供委派的 Security Hub CSPM 管理员的 AWS 账户 ID。

以下示例将指定委派的 Security Hub CSPM 管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

移除或更改委派管理员

仅组织管理账户可以删除委派的 Security Hub CSPM 管理员账户。

要更改委派的 Security Hub CSPM 管理员，必须先删除当前委派管理员账户并指定新账户。

> **Warning**
>
> 当你使用集中配置时，你无法使用 Security Hub CSPM 控制台或 Security Hub CSPM APIs 来更改或删除委派的管理员帐户。如果组织管理帐户使用 AWS Organizations 控制台或更改或 AWS Organizations APIs 删除委派的 Security Hub CSPM 管理员，Security Hub CSPM 会自动停止中央配置，并删除您的配置策略和策略关联。成员账户保留其在更改或删除委派管理员之前的配置。

如果您使用 Security Hub CSPM 控制台删除一个区域的委派管理员，该管理员将在所有区域中被自动删除。

Security Hub CSPM API 仅从发出 API 调用或命令的区域中删除委派的 Security Hub CSPM 管理员账户。您必须在其他区域重复执行此操作。

如果您使用 Organizations API 删除委派的 Security Hub CSPM 管理员账户，则该账户将在所有区域中被自动删除。

移除委托管理员（Organizations API， AWS CLI）

您可以使用 Organizations 删除所有区域中委派的 Security Hub CSPM 管理员。

如果您使用中心配置来管理账户，则移除委派管理员账户会导致您的配置策略和策略关联被删除。成员账户保留其在更改或删除委派管理员之前的配置。但是，这些账户无法再由已删除的委派管理员账户进行管理。它们成为自行管理账户，必须在每个区域单独配置。

选择您的首选方法，然后按照说明删除委托的 Security Hub CSPM 管理员帐户。 AWS Organizations

Organizations API, AWS CLI

删除委派的 Security Hub CSPM 管理员

在组织管理账户中，使用 Organizations API 的 DeregisterDelegatedAdministrator 操作。如果您使用的是 AWS CLI，请运行 deregister-delegated-administrator 命令。提供委派管理员账户的账户 ID 以及 Security Hub CSPM 的服务主体，即 `securityhub.amazonaws.com`。

以下示例将删除委派的 Security Hub CSPM 管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

删除委派管理员（Security Hub CSPM 控制台）

您可以使用 Security Hub CSPM 控制台删除所有区域中委派的 Security Hub CSPM 管理员。

删除委派的 Security Hub CSPM 管理员账户后，成员账户将与已删除的委派的 Security Hub CSPM 管理员账户解除关联。

成员账户仍会启用 Security Hub CSPM。它们将变为独立账户，直至新的 Security Hub CSPM 管理员将它们启用为成员账户。

如果组织管理账户不是 Security Hub CSPM 中已启用的账户，请使用欢迎使用 Security Hub CSPM 页面上的选项。

从欢迎使用 Security Hub CSPM 页面中删除委派的 Security Hub CSPM 管理员账户

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 选择转到 Security Hub。
3. 在委派管理员下，选择删除。

如果组织管理账户是 Security Hub 中已启用的账户，请使用设置页面的常规选项卡上的选项。

从设置页面删除委派的 Security Hub CSPM 管理员账户

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在 Security Hub CSPM 导航窗格中，选择设置。然后，选择常规。
3. 在委派管理员下，选择删除。

移除委派的管理员（Security Hub CSPM API，）AWS CLI

您可以使用 Security Hub CSPM API 或 Security Hub CSPM 操作 AWS CLI 来移除委派的 Security Hub CSPM 管理员。当您使用其中一种方法删除委派管理员时，只有在发出 API 调用或命令的区域中的委派管理员才会被删除。Security Hub CSPM 不会更新其他区域，也不会删除中的委托管理员帐户。 AWS Organizations

选择您喜欢的方法，然后按照这些步骤用 Security Hub CSPM 删除委派的 Security Hub CSPM 管理员账户。

Security Hub CSPM API, AWS CLI

删除委派的 Security Hub CSPM 管理员

在组织管理账户中，使用 Security Hub CSPM API 的 DisableOrganizationAdminAccount 操作。如果您使用的是 AWS CLI，请运行该disable-organization-admin-account命令。提供委派的 Security Hub CSPM 管理员的账户 ID。

以下示例将删除委派的 Security Hub CSPM 管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

禁用 Security Hub CSPM 与的集成 AWS Organizations

AWS Organizations 组织与 Sec AWS urity Hub CSPM 集成后，组织管理帐户随后可以禁用集成。作为 Organizations 管理账户的用户，您可以通过在 AWS Organizations中禁用对 Security Hub CSPM 的可信访问来实现。

当您禁用 Security Hub CSPM 的可信访问权限时，会出现以下情况：

- Security Hub CSPM 失去了其作为受信任服务的地位。 AWS Organizations
- Security Hub CSPM 委派管理员账户将无法访问 AWS 区域中所有 Security Hub CSPM 成员账户的 Security Hub CSPM 设置、数据和资源。
- 如果您使用的是中心配置，Security Hub CSPM 会自动停止在您的组织中使用它。您的配置策略和策略关联会被删除。账户保留在您禁用可信访问之前的配置。
- 所有 Security Hub CSPM 成员账户都将成为独立账户，并保留其当前设置。如果在一个或多个区域为成员账户启用 Security Hub CSPM，则这些区域的账户将继续启用 Security Hub CSPM。启用的标准和控件也保持不变。您可以在每个账户和地区中分别更改这些设置。但是，该账户不再与任何地区的委派管理员账户关联。

有关禁用可信服务访问的结果的更多信息，请参阅《AWS Organizations 用户指南》 AWS 服务中的“AWS Organizations 与其他人一起使用”。

要禁用可信访问，您可以使用 AWS Organizations 控制台、Organizations API 或 AWS CLI。只有 Organizations 管理账户的用户可以禁用 Security Hub CSPM 的可信服务访问权限。有关所需权限的详细信息，请参阅《AWS Organizations 用户指南》中的禁用可信访问所需的权限。

在禁用可信访问权限之前，可以选择与组织的委派管理员合作，禁用成员账户的 Security Hub CSPM，并清理这些账户的 Security Hub CSPM 资源。

选择您喜欢的方法，然后按照以下步骤禁用 Security Hub CSPM 的受信任访问。

Organizations console

禁用 Security Hub CSPM 的受信任访问

1. AWS 管理控制台 使用 AWS Organizations 管理账户的凭据登录。
2. 打开 “组织” 控制台，网址为https://console.aws.amazon.com/organizations/。
3. 在导航窗格中，选择服务。
4. 在集成服务下，选择 AWS Security Hub CSPM。

5. 选择 Disable trusted access（禁用信任访问权限）。
6. 确认您要禁用可信访问权限。

Organizations API

禁用 Security Hub CSPM 的受信任访问

调用 AWS Organizations API 的 “禁用AWSService访问权限” 操作。对于 `ServicePrincipal` 参数，指定 Security Hub CSPM 服务主体（`securityhub.amazonaws.com`）。

AWS CLI

禁用 Security Hub CSPM 的受信任访问

运行 AWS Organizations API 的disable-aws-service-access命令。对于 `service-principal` 参数，指定 Security Hub CSPM 服务主体（`securityhub.amazonaws.com`）。

示例：

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

在新组织账户中自动启用 Security Hub CSPM。

当新帐户加入您的组织时，它们将被添加到 Sec AWS urity Hub CSPM 控制台的 “帐户” 页面上的列表中。对于组织账户，类型为按组织。默认情况下，新账户在加入组织时不会成为 Security Hub CSPM 成员。他们的身份是非成员。当委派管理员账户加入组织后，可以自动添加新账户作为成员，并在这些账户中启用 Security Hub CSPM。

> **Note**
>
> 尽管默认情况下，您的许多区域 AWS 区域 处于活动状态 AWS 账户，但您必须手动激活某些区域。在本文档中，这些区域被称为选择加入区域。要在选择加入区域的新账户中自动启用 Security Hub CSPM，则账户必须先激活该区域。只有账户所有者才能激活选择加入区域。有关选择加入区域的更多信息，请参阅指定 AWS 区域 您的账户可以使用的区域。

根据您使用的是中心配置（推荐）还是本地配置，此过程会有所不同。

自动启用新组织账户（中心配置）

如果您使用中心配置，则可以通过创建启用 Security Hub CSPM 的配置策略，在新的和现有组织账户中自动启用 Security Hub CSPM。然后，您可以将该策略与组织根目录或特定的组织单位相关联 (OUs)。

如果您将启用了 Security Hub CSPM 的配置策略与特定 OU 相关联，则会自动在属于该 OU 的所有账户（现有账户和新账户）中启用 Security Hub CSPM。不属于 OU 的新账户是自行管理的，并且不会自动启用 Security Hub CSPM。如果您将启用了 Security Hub CSPM 的配置策略与根相关联，则会自动在加入组织的所有账户（现有账户和新账户）中启用 Security Hub CSPM。如果一个账户通过应用或继承使用不同的策略，或者是自行管理的，则为例外情况。

在配置策略中，您还可以定义应在 OU 中启用哪些安全标准和控件。要生成针对已启用标准的控制结果，OU 中的账户必须已 AWS Config 启用并配置为记录所需资源。有关 AWS Config 录制的更多信息，请参阅启用和配置 AWS Config。

有关创建配置策略的说明，请参阅创建和关联配置策略。

自动启用新组织账户（本地配置）

当您使用本地配置并开启自动启用默认标准时，Security Hub CSPM 会将新组织账户添加为成员，并在当前区域的这些账户中启用 Security Hub CSPM。其他地区均不受影响。此外，开启自动启用不会在现有组织账户中启用 Security Hub CSPM，除非这些账户已添加为成员账户。

开启自动启用后，如果当前区域有新成员账户加入组织，也会为其启用默认安全标准。默认标准是 AWS 基础安全最佳实践 (FSBP) 和互联网安全中心 (CIS) AWS 基金会基准 v1.2.0。您不能更改默认标准。如果您想在整个组织中启用其他标准，或者要为特定账户启用标准 OUs，我们建议您使用集中配置。

要生成默认标准（和其他启用的标准）的控制结果，您组织中的账户必须已 AWS Config 启用并配置为记录所需资源。有关 AWS Config 录制的更多信息，请参阅启用和配置 AWS Config。

选择您喜欢的方法，然后按照步骤在新组织账户中自动启用 Security Hub CSPM。这些说明仅在您使用本地配置时适用。

Security Hub CSPM console

将新组织账户自动启用为 Security Hub CSPM 成员

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

使用委派管理员账户凭证登录。

2. 在 Security Hub CSPM 导航窗格中的设置下，选择配置。
3. 在账户部分，打开自动启用账户。

Security Hub CSPM API

将新组织账户自动启用为 Security Hub CSPM 成员

从委派管理员账户调用 UpdateOrganizationConfiguration API。将 AutoEnable 字段设置为 true，以便在新组织账户中自动启用 Security Hub CSPM。

AWS CLI

将新组织账户自动启用为 Security Hub CSPM 成员

从委派管理员账户运行 update-organization-configuration 命令。添加 auto-enable 参数以在新组织账户中自动启用 Security Hub CSPM。

```
aws securityhub update-organization-configuration --auto-enable
```

在新组织账户中手动启用 Security Hub CSPM

如果您在新组织账户加入组织时没有自动启用 Security Hub CSPM，则可以将这些账户添加为成员，并在这些账户加入组织后在其中手动启用 Security Hub CSPM。您还必须手动启用 Security Hub CSPM AWS 账户 ，因为您之前已取消与组织的关联。

> **Note**
>
> 如果您使用中心配置，则本节不适用于您。如果您使用集中配置，则可以创建配置策略，在指定的成员账户和组织单位中启用 Security Hub CSPM（ ）OUs。您还可以在这些帐户中启用特定的标准和控制，以及 OUs.

如果账户已经是其他组织中的成员账户，则无法在账户中启用 Security Hub CSPM。

您也无法在当前已暂停的账户中启用 Security Hub CSPM。如果您尝试在已暂停的账户中启用服务，则账户状态会更改为账户已暂停。

- 如果该账户未启用 Security Hub CSPM，则会在该账户中启用 Security Hub CSPM。除非您关闭默认安全标准，否则账户中还会启用 AWS AWS 基础安全最佳实践 (FSBP) 标准和 CIS Foundations Benchmark v1.2.0。

  组织管理账户除外。无法在 Organizations 管理账户中自动启用 Security Hub CSPM。您必须在 Organizations 管理账户中手动启用 Security Hub CSPM，然后才能将其作为成员账户添加。
- 如果该账户已经启用了 Security Hub CSPM，则 Security Hub CSPM 不会对该账户进行任何其他更改。它仅启用成员资格。

为了让 Security Hub CSPM 生成控制结果，必须 AWS Config 启用并配置成员账户以记录所需的资源。有关更多信息，请参阅启用和配置 AWS Config。

选择您喜欢的方法，然后按照步骤将组织账户启用为 Security Hub CSPM 成员账户。

Security Hub CSPM console

手动将组织账户启用为 Security Hub CSPM 成员

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用委派管理员账户凭证登录。
2. 在 Security Hub CSPM 导航窗格中的设置下，选择配置。
3. 在账户列表中，选中要启用的每个组织账户。
4. 选择操作，然后选择添加成员。

Security Hub CSPM API

手动将组织账户启用为 Security Hub CSPM 成员

从委派管理员账户调用 `CreateMembers` API。对于要启用的每个账户，请提供账户 ID。

与手动邀请流程不同，当您调用 `CreateMembers` 启用组织账户时，无需发送邀请。

AWS CLI

手动将组织账户启用为 Security Hub CSPM 成员

从委派管理员账户运行 `create-members` 命令。对于要启用的每个账户，请提供账户 ID。

与手动邀请流程不同，当您运行 `create-members` 启用组织账户时，无需发送邀请。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

示例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

解除 Security Hub CSPM 成员账户与组织的关联

要停止接收和查看 Sec AWS urity Hub CSPM 成员账户的调查结果，您可以取消该成员账户与您的组织的关联。

> **Note**
>
> 如果您使用中心配置，则取消关联的工作原理会有所不同。您可以创建一个配置策略，在一个或多个集中管理的成员账户中禁用 Security Hub CSPM。之后，这些账户仍然是组织的一部分，但不会生成 Security Hub CSPM 调查发现。如果您使用中心配置，但也有手动邀请的成员账户，则可以取消关联一个或多个手动邀请的账户。

使用管理的成员账户 AWS Organizations 无法取消其账户与管理员账户的关联。只有管理员账户可以取消成员账户的关联。

取消关联成员账户不会删除该账户。相反，它会从组织中删除该成员账户。已取消关联的成员账户变为独立账户 AWS 账户 ，不再由 Security Hub CSPM 与的集成管理。 AWS Organizations

选择您的首选方法，然后按照步骤取消成员账户与组织的关联。

Security Hub CSPM console

要取消成员账户与组织之间的关联

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用委派管理员账户凭证登录。
2. 在导航窗格中的设置下，选择配置。

3. 在账户部分，选中要取消关联的账户。如果您使用中心配置，则可以选择一个手动邀请的账户来取消与 Invitation accounts 选项卡的关联。仅当您使用中心配置时，才可以看到此选项卡。
4. 选择操作，然后选择取消账户关联。

Security Hub CSPM API

要取消成员账户与组织的关联

从委派管理员账户调用 DisassociateMembers API。您必须 AWS 账户 IDs 提供成员账户才能解除关联。要查看成员账户列表，请调用 ListMembers API。

AWS CLI

要取消成员账户与组织的关联

从委派管理员账户运行 >disassociate-members 命令。您必须 AWS 账户 IDs 提供成员账户才能解除关联。要查看成员账户列表，请运行 >list-members 命令。

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

示例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

您也可以使用 AWS Organizations 控制台 AWS CLI、或 AWS SDKs 取消成员账户与您的组织的关联。有关更多信息，请参阅 AWS Organizations 用户指南中的从组织中删除成员账户。

在 Security Hub CSPM 中通过邀请管理账户

您可以通过两种方式集中管理多个 Sec AWS urity Hub CSPM 账户，即将 Security Hub CSPM 与 Security Hub CSPM 集成， AWS Organizations 或者手动发送和接受会员邀请。如果您拥有独立账户或未与之集成，则必须使用手动流程 AWS Organizations。在手动账户管理中，Security Hub CSPM 管理员邀请账户成为成员。当潜在成员接受邀请时，管理员与成员的关系即已建立。一个 Security Hub CSPM 管理员账户可以管理多达 1,000 个基于邀请的成员账户的 Security Hub CSPM。

> **Note**
>
> 如果您在 Security Hub CSPM 中创建基于邀请的组织，则随后可以转换到使用 AWS Organizations。如果您有多个会员账户，我们建议您使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的成员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

对于您通过手动邀请流程邀请的账户，可以跨区域聚合调查发现和其他数据。但是，管理员必须邀请来自聚合区域和所有关联区域的成员账户，才能使跨区域聚合生效。此外，成员账户必须在聚合区域和所有关联区域中启用 Security Hub CSPM，这样管理员才能查看成员账户中的调查发现。

手动邀请的成员账户不支持配置策略。相反，您必须在每个成员账户中以及使用手动邀请流程 AWS 区域 时分别配置 Security Hub CSPM 设置。

对于不属于您组织的账户，您还必须使用基于手动邀请的流程。例如，您的组织中可能不包含测试账号。或者，您可能想将来自多个组织的账户整合到一个 Security Hub CSPM 管理员账户下。Security Hub CSPM 管理员账户必须向属于其他组织的账户发送邀请。

在 Security Hub CSPM 控制台的配置页面上，通过邀请添加的账户列在邀请账户选项卡中。如果您使用中心配置，但同时邀请了组织外的账户，则可以在此选项卡中查看基于邀请的账户的调查发现。但是，Security Hub CSPM 管理员无法通过使用配置策略跨区域配置基于邀请的账户。

此部分介绍如何通过邀请管理成员账户。

主题

- 在 Security Hub CSPM 中添加和邀请成员账户
- 响应成为 Security Hub CSPM 成员账户的邀请
- 在 Security Hub CSPM 中解除关联成员账户
- 在 Security Hub CSPM 中删除成员账户
- 解除关联 Security Hub CSPM 管理员账户
- 过渡到 Organizations 以管理 Security Hub CSPM 中的账户

在 Security Hub CSPM 中添加和邀请成员账户

> **Note**
>
> 我们建议使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的会员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

对于接受你邀请成为 Sec AWS urity Hub CSPM 成员账户的账户，你的账户将成为 Security Hub CSPM 管理员。

当您接受另一个账户的邀请时，您的账户成为成员账户，那个账户成为您的管理员。

如果您的账户是管理员账户，则您无法接受成为成员账户的邀请。

添加成员账户包括以下步骤：

1. 管理员账户将成员账户添加到他们的成员账户列表中。
2. 管理员账户向成员账户发送邀请。
3. 成员账户接受邀请。

添加成员账户

通过 Security Hub CSPM 控制台，您可以将账户添加到成员账户列表中。在 Security Hub CSPM 控制台中，您可以单独选择账户，也可以上传包含账户信息的 `.csv` 文件。

对于每个账户，您必须提供账户 ID 和一个电子邮件地址。电子邮件地址应该是就账户中的安全问题进行联系的电子邮件地址。它不用于验证账户。

选择您的首选方法，然后按照以下步骤添加成员账户。

Security Hub CSPM console

要将账户添加到您的成员账户列表中

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用管理员账户的凭证登录。
2. 在左侧窗格中，选择设置。

3. 在设置页面上，选择账户，然后选择添加账户。然后，您可以单独添加账户，也可以上传包含账户列表的 .csv 文件。
4. 要选择账户，请执行以下操作之一：

   - 要单独添加账户，在输入账户中，输入要添加的账户的账户 ID 和电子邮件地址，然后选择添加。

     为每个账户重复这一过程。
   - 要使用逗号分隔值（.csv）文件添加多个账户，请先创建该文件。该文件必须包含要添加的每个账户的账户 ID 和电子邮件地址。

     在 .csv 列表中，账户必须一行一个。.csv 文件的第一行必须包含标题。在标题中，第一列是 **Account ID**，第二列是 **Email**。

     后面的每一行必须包含要添加的账户的有效账户 ID 和电子邮件地址。

     以下是在文本编辑器中查看 .csv 文件时的示例。

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     在电子表格程序中，这些字段显示在单独的列中。基础格式仍以逗号分隔。您必须将账户格式化 IDs 为非十进制数字。例如，账户 ID 444455556666 的格式不能为 444455556666.0。另外，请确保数字格式不会从账户 ID 中删除任何前导零。

     要选择文件，请在控制台上选择上传列表（.csv）。然后选择浏览。

     选择该文件后，选择添加账户。
5. 添加完账户后，在要添加的账户下，选择下一步。

Security Hub CSPM API

要将账户添加到您的成员账户列表中

从管理员账户调用 `CreateMembers` API。对于要添加的每个成员账户，您都必须提供 AWS 账户 ID。

AWS CLI

要将账户添加到您的成员账户列表中

从管理员账户运行 `create-members` 命令。对于要添加的每个成员账户，您都必须提供 AWS 账户 ID。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

示例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

邀请成员账户

添加成员账户之后，您会向成员账户发送邀请。您也可以向已和管理员取消关联的账户重新发送邀请。

Security Hub CSPM console

要邀请潜在成员账户

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用管理员账户的凭证登录。
2. 在导航窗格中，选择设置，然后选择账户。
3. 要邀请的账户，请在状态列中选择邀请。
4. 当系统提示确认时，请选择邀请。

> **Note**
>
> 要向已取消关联的账户重新发送邀请，请在账户页面上选择每个已取消关联的账户。从操作中选择重新发送邀请。

Security Hub CSPM API

要邀请潜在成员账户

从管理员账户调用 `InviteMembers` API。对于要邀请的每个账户，您都必须提供 AWS 账户 ID。

AWS CLI

要邀请潜在成员账户

从管理员账户运行 `invite-members` 命令。对于要邀请的每个账户，您都必须提供 AWS 账户 ID。

```
aws securityhub invite-members --account-ids <accountIDs>
```

示例

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

响应成为 Security Hub CSPM 成员账户的邀请

> **Note**
>
> 我们建议使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的会员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

您可以接受或拒绝成为 Sec AWS urity Hub CSPM 成员账户的邀请。

如果您接受邀请，您的账户将成为 Security Hub CSPM 成员账户。发送邀请的账户将成为您的 Security Hub CSPM 管理员账户。管理员账户用户可以在 Security Hub CSPM 中查看您的成员账户的调查发现。

如果您拒绝邀请，则在管理员账户的成员账户列表中，您的账户将被标记为已放弃。

您只能接受一次成为会员账户的邀请。

在接受或拒绝邀请之前，您必须启用 Security Hub CSPM。

请记住，所有 Security Hub CSPM 账户都必须已 AWS Config 启用并配置为记录所有资源。有关要求的详细信息 AWS Config，请参阅启用和配置 AWS Config。

接受邀请

您可以通过管理员账户发送成为 Security Hub CSPM 成员账户的邀请。然后，您可以在登录成员账户后接受邀请。

选择您的首选方法，然后按照以下步骤接受邀请成为成员账户。

Security Hub CSPM console

要接受成员邀请

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置，然后选择账户。
3. 在管理员账户部分，开启接受，然后选择接受邀请。

Security Hub CSPM API

要接受成员邀请

调用 AcceptAdministratorInvitation API。您必须提供邀请标识符和管理员账户的 AWS 账户 ID。要检索有关邀请的详细信息，请使用 ListInvitations 操作。

AWS CLI

要接受成员邀请

运行 accept-administrator-invitation 命令。您必须提供邀请标识符和管理员账户的 AWS 账户 ID。要检索有关邀请的详细信息，运行 list-invitations 命令。

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

示例

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Security Hub CSPM 控制台继续使用 AcceptInvitation。它最终会改为使用 AcceptAdministratorInvitation。任何专门控制此功能访问权限的 IAM policy 都必须继续使用 AcceptInvitation。您还应在策略

中添加 `AcceptAdministratorInvitation`，以确保在控制台开始使用 `AcceptAdministratorInvitation` 后正确的权限已到位。

拒绝邀请

您可以拒绝成为 Security Hub CSPM 成员账户的邀请。当您在 Security Hub CSPM 控制台中拒绝邀请时，您的账户将在管理员账户的成员账户列表中会标记为已放弃。仅当您使用管理员账户登录 Security Hub CSPM 控制台时，才会显示已放弃状态。但是，在您登录管理员账户并删除成为成员账户的邀请之前，该邀请在控制台中保持不变。

要拒绝邀请，您必须登录收到邀请的成员账户。

选择您的首选方法，然后按照以下步骤拒绝邀请成为成员账户。

Security Hub CSPM console

要拒绝成员邀请

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置，然后选择账户。
3. 在管理员账户部分，选择拒绝邀请。

Security Hub CSPM API

要拒绝成员邀请

调用 `DeclineInvitations` API。您必须提供发出邀请的管理员账户的 AWS 账户 ID。要查看有关您的邀请的信息，请使用 `ListInvitations` 操作。

AWS CLI

要拒绝成员邀请

运行 `decline-invitations` 命令。您必须提供发出邀请的管理员账户的 AWS 账户 ID。要查看有关您的邀请的信息，请运行 `list-invitations` 命令。

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

示例

```
aws securityhub decline-invitations --account-ids "123456789012"
```

在 Security Hub CSPM 中解除关联成员账户

> **Note**
>
> 我们建议使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的会员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

Sec AWS urity Hub CSPM 管理员帐户可以取消关联成员帐户，以停止接收和查看来自该账户的调查结果。您必须首先取消关联成员账户，然后才能将其删除。

取消关联成员账户后，该账户仍将保留在您的成员账户列表中，其状态为已移除（已取消关联）。您的账户已从该成员账户的管理员账户信息中删除。

要恢复接收该账户的调查发现，您可以重新发送邀请。要完全移除成员账户，您可以删除该成员账户。

选择您的首选方法，然后按照步骤取消手动邀请的成员账户与管理员账户的关联。

Security Hub CSPM console

要取消手动邀请的成员账户的关联

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用管理员账户的凭证登录。
2. 在导航窗格中的设置下，选择配置。
3. 在账户部分，选中要取消关联的账户。
4. 选择操作，然后选择取消账户关联。

Security Hub CSPM API

要取消手动邀请的成员账户的关联

从管理员账户调用 DisassociateMembers API。您必须提供要取消关联的成员账户。 AWS 账户 IDs 要查看成员账户列表，请使用 ListMembers 操作。

AWS CLI

要取消手动邀请的成员账户的关联

从管理员账户运行 disassociate-members 命令。您必须提供要取消关联的成员账户。 AWS 账户 IDs 要查看成员账户列表，请运行 list-members 命令。

```
aws securityhub disassociate-members --account-ids <accountIds>
```

示例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

在 Security Hub CSPM 中删除成员账户

> **Note**
>
> 我们建议使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的会员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

作为 S AWS ecurity Hub CSPM 管理员帐户，您可以删除通过邀请添加的成员帐户。在您可以删除已启用的账户之前，您必须先取消其关联。

当您删除成员账户时，该账户将从列表中完全移除。要恢复该账户的成员资格，您必须将其添加并向其发送邀请，就像它是一个全新的成员账户一样。

您无法删除属于某个组织且使用与集成进行管理的帐户 AWS Organizations。

选择您的首选方法，然后按照以下步骤删除手动邀请的成员账户。

Security Hub CSPM console

要删除手动邀请的成员账户

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

使用管理员账户登录。

2. 在导航窗格中，选择设置，然后选择配置。
3. 选择邀请账户选项卡。然后，选择要删除的账户。
4. 选择操作，然后选择删除。此选项仅在您取消关联账户后可用。您必须先取消关联成员账户，然后才能将其删除。

Security Hub CSPM API

要删除手动邀请的成员账户

从管理员账户调用 DeleteMembers API。您必须提供要删除的成员帐户。 AWS 账户 IDs 要检索成员账户列表，请调用 ListMembers API。

AWS CLI

要删除手动邀请的成员账户

从管理员账户运行 delete-members 命令。您必须提供要删除的成员帐户。 AWS 账户 IDs 要检索成员账户列表，运行 list-members 命令。

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

示例

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

解除关联 Security Hub CSPM 管理员账户

> **Note**
>
> 我们建议使用 AWS Organizations 代替 Security Hub CSPM 邀请来管理您的会员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

如果您的账户是通过邀请添加为 S AWS ecurity Hub CSPM 成员账户的，则可以取消该成员账户与管理员账户的关联。解除关联成员账户后，Security Hub CSPM 不会将该账户的调查发现发送到管理员账户。

使用与的集成进行管理的成员账户 AWS Organizations 无法取消其账户与管理员账户的关联。只有 Security Hub CSPM 委派管理员可以解除与 Organizations 管理的成员帐户的关联。

当您取消与管理员账户的关联后，您的账户将保留在管理员账户的成员列表中，状态为已放弃。但是，管理员账户不会收到有关您账户的任何调查发现。

在您取消与管理员账户的关联后，成为成员的邀请仍然有效。将来你可以再次接受邀请。

Security Hub CSPM console

要从管理员账户取消关联

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置，然后选择账户。
3. 在管理员账户部分，关闭接受，然后选择更新。

Security Hub CSPM API

要从管理员账户取消关联

调用 DisassociateFromAdministratorAccount API。

AWS CLI

要从管理员账户取消关联

运行 disassociate-from-administrator-account 命令。

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Security Hub CSPM 控制台继续使用 DisassociateFromMasterAccount。它最终会改为使用 DisassociateFromAdministratorAccount。任何专门控制此功能访问权限的 IAM policy 都必须继续使用 DisassociateFromMasterAccount。您还应在策略中添加 DisassociateFromAdministratorAccount，以确保在控制台开始使用 DisassociateFromAdministratorAccount 后正确的权限已到位。

过渡到 Organizations 以管理 Security Hub CSPM 中的账户

在 Sec AWS urity Hub CSPM 中手动管理账户时，必须邀请潜在成员账户，并在每个账户中分别配置每个成员账户。 AWS 区域

通过集成 Security Hub CSPM 和 AWS Organizations，您无需发送邀请，并可以更好地控制组织中如何配置和自定义 Security Hub CSPM。为此，建议使用 AWS Organizations 代替 Security Hub CSPM 邀请管理成员账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。

您可以使用组合方法，即使用 AWS Organizations 集成，也可以手动邀请组织外部的帐户。但我们建议仅使用 Organizations 集成。中心配置是一项功能，可帮助您跨多个账户和区域管理 Security Hub CSPM，仅当您与 Organizations 集成时才可用。

本节将介绍如何从基于邀请的手动账户管理转换到使用 AWS Organizations管理账户。

将 Security Hub CSPM 与 AWS Organizations

首先，你必须集成 Security Hub CSPM 和。 AWS Organizations

您可以完成以下步骤，来集成这些服务：

- 在 AWS Organizations中创建组织。有关说明，请参阅《AWS Organizations 用户指南》中的创建组织。
- 在 Organizations 管理账户中，指定一个 Security Hub CSPM 委派管理员账户。

> **Note**
>
> 不能将组织管理账户设置为 DA 账户。

有关详细说明，请参阅将 Security Hub CSPM 与 AWS Organizations。

完成上述步骤后，您就可以在中授予对 Security Hub CSPM 的可信访问权限。 AWS Organizations这还会 AWS 区域 为委派的管理员帐户启用当前的 Security Hub CSPM。

委派管理员可以在 Security Hub CSPM 中管理组织，主要方法是添加组织账户作为 Security Hub CSPM 成员账户。管理员还可以访问这些账户的某些 Security Hub CSPM 设置、数据和资源。

在转换到使用 Organizations 进行账户管理后，基于邀请的账户不会自动成为 Security Hub CSPM 成员。只有您添加到新组织的账户才能成为 Security Hub CSPM 成员。

激活集成后，您可以使用组织管理账户。有关信息，请参阅使用管理多个账户的 Security Hub CSPM AWS Organizations。账户管理因组织的配置类型而异。

Security Hub CSPM 中管理员和成员账户可以执行的操作

管理员和成员账户可以访问下表中提到的 Sec AWS urity Hub CSPM 操作。表中的值具有以下含义：

- Any：该账户可为同一管理员下的任何成员账户执行操作。
- Current：该账户只能为其本身执行操作（当前登录的账户）。
- Dash：表示该账户无法执行操作。

如表中所述，允许的操作会根据您是否集成 AWS Organizations 以及您的组织使用的配置类型而有所不同。有关集中配置和本地配置之间的差异的信息，请参阅使用管理账户 AWS Organizations。

Security Hub CSPM 不会将成员账户的调查发现复制到管理员账户。在 Security Hub CSPM 中，所有调查发现都会被提取到特定账户的特定区域。在每个区域，管理员账户均可以查看和管理其在该区域的成员账户的调查发现。

如果设置了聚合区域，管理员账户可以查看和管理复制到聚合区域的关联区域的成员账户调查发现。有关跨区域聚合的更多信息，请参阅跨区域聚合。

下表指定了管理员账户和成员账户的默认权限。您可以使用自定义 IAM 策略进一步限制对 Security Hub CSPM 特性和功能的访问。有关指导和示例，请参阅博客文章 Sec AWS urity Hub CSPM 的 IAM 策略与 Security Hub CSPM 的用户角色保持一致。

与 Organizations 集成并使用中心配置时允许执行的操作

与 Organizations 集成并使用中心配置时，管理员账户和成员账户可以按如下方式访问 Security Hub CSPM 操作。

Action	Security Hub CSPM 委派管理员账户	集中管理的成员账户	自行管理的成员账户
创建和管理 Security Hub CSPM 配置策略	对于自我管理和集中管理的账户	–	–
查看组织账户	任何	–	–
取消成员账户的关联	任何	–	–

Action	Security Hub CSPM 委派管理员账户	集中管理的成员账户	自行管理的成员账户
删除成员账户	任何非组织账户	–	–
禁用 Security Hub CSPM	对于当前账户和集中管理的账户	–	当前（必须与管理员账户取消关联）
查看调查发现和调查发现历史	任何	Current	Current
更新调查发现	任何	Current	Current
查看见解结果	任何	Current	Current
查看控件详细信息	任何	Current	Current
开启或关闭整合控件调查发现	任何	–	–
启用和禁用标准	对于当前账户和集中管理的账户	–	Current
启用和禁用控件	对于当前账户和集中管理的账户	–	Current
启用和禁用集成	Current	Current	Current
配置跨区域聚合	任何	–	–
选择主区域和关联区域	Any（必须停止并重新启动中心配置才能更改主区域）	–	–
配置自定义操作	Current	Current	Current
配置自动化规则	任何	–	–
配置自定义见解	Current	Current	Current

与 Organizations 集成并使用本地配置时允许执行的操作

与 Organizations 集成并使用本地配置时，管理员账户和成员账户可以按如下方式访问 Security Hub CSPM 操作。

Action	Security Hub CSPM 委派管理员账户	成员帐户
创建和管理 Security Hub CSPM 配置策略	–	–
查看组织账户	任何	–
取消成员账户的关联	任何	–
删除成员账户	–	–
禁用 Security Hub CSPM	–	Current（如果账户与委派管理员解除关联）
查看调查发现和调查发现历史	任何	Current
更新调查发现	任何	Current
查看见解结果	任何	Current
查看控件详细信息	任何	Current
开启或关闭整合控件调查发现	任何	–
启用和禁用标准	Current	Current
在新组织账户中自动启用 Security Hub CSPM 和默认标准	对于当前账户和新组织账户	–
启用和禁用控件	Current	Current
启用和禁用集成	Current	Current
配置跨区域聚合	任何	–

Action	Security Hub CSPM 委派管理员账户	成员帐户
配置自定义操作	Current	Current
配置自动化规则	任何	–
配置自定义见解	Current	Current

允许对基于邀请的账户执行的操作

如果您使用基于邀请的方法手动管理帐户，而不是与集成，则管理员和成员帐户可以按如下方式访问 Security Hub CSPM 操作。 AWS Organizations

Action	Security Hub CSPM 管理员账户	成员帐户
创建和管理 Security Hub CSPM 配置策略	–	–
查看组织账户	任何	–
取消成员账户的关联	任何	Current
删除成员账户	任何	–
禁用 Security Hub CSPM	Current（如果没有启用的成员账户）	Current（如果账户与管理员账户解除关联）
查看调查发现和调查发现历史	任何	Current
更新调查发现	任何	Current
查看见解结果	任何	Current
查看控件详细信息	任何	Current
开启或关闭整合控件调查发现	任何	–
启用和禁用标准	Current	Current

Action	Security Hub CSPM 管理员账户	成员帐户
在新组织账户中自动启用 Security Hub CSPM 和默认标准	–	–
启用和禁用控件	Current	Current
启用和禁用集成	Current	Current
配置跨区域聚合	任何	–
配置自定义操作	Current	Current
配置自动化规则	任何	–
配置自定义见解	Current	Current

账户操作对 Security Hub CSPM 数据的影响

这些账户操作会对 Sec AWS urity Hub CSPM 数据产生以下影响。

Security Hub CSPM 已禁用

如果您使用集中配置，则委托管理员 (DA) 可以创建 Security Hub CSPM 配置策略，在特定账户和组织单位中禁用 Sec AWS urity Hub CSPM（ ）。OUs在这种情况下，Security Hub CSPM 将在指定账户、您的家乡地区和任何关联区域 OUs 中被禁用。如果不使用中心配置，则必须在启用了 Security Hub CSPM 的每个账户和区域中单独禁用。如果在 DA 账户中禁用了 Security Hub CSPM，则无法使用中心配置。

如果在管理员账户中禁用了 Security Hub CSPM，则不会为管理员账户生成或更新调查发现。现有存档的调查发现将在 30 天后删除。现有活跃调查发现将在 90 天后删除。

与他人的集成 AWS 服务 已删除。

已启用的安全标准和控件将被禁用。

其他 Security Hub CSPM 数据和设置（包括自定义操作、见解和第三方产品订阅）将会保留 90 天。

会员账号与管理员账号解除关联

当成员账户与管理员账户解除关联时，管理员账户将失去查看成员账户中的调查发现的权限。但是，这两个账户仍会启用 Security Hub CSPM。

如果使用中心配置，则 DA 无法为与 DA 账户解除关联的成员账户配置 Security Hub CSPM。

为管理员账户定义的自定义设置或集成不会应用于前成员账户的调查发现。例如，取消关联账户后，您可能会在管理员账户中使用自定义操作作为 Amazon EventBridge 规则中的事件模式。但是，此自定义操作不能在成员账户中使用。

在 Security Hub CSPM 管理员账户的账户列表中，已删除账户的状态为已解除关联。

成员账户从组织中移除

从组织中删除成员账户后，Security Hub CSPM 管理员账户将失去在成员账户中查看调查发现的权限。但两个账户仍启用了 Security Hub CSPM，其设置与删除之前的设置相同。

如果使用中心配置，则在将成员账户从委派管理员所属的组织中删除后，就将无法为其配置 Security Hub CSPM。但除非您手动更改，否则该账户将保留删除之前的设置。

在 Security Hub CSPM 管理员账户的账户列表中，已删除账户的状态为已删除。

账户已暂停

被暂停后，该账户将失去在 Security Hub CSPM 中查看其发现结果的权限。 AWS 账户 没有为该账户生成或更新任何调查发现。已暂停账户的管理员账户可以查看账户的现有调查发现。

对于组织账户，成员账户状态也可以更改为账户已暂停。如果在管理员账户尝试启用账户的同时该账户被暂停，则会发生这种情况。已暂停账户的管理员账户无法查看该账户的调查发现。否则，暂停状态不会影响成员账户状态。

如果使用中心配置，则当委派管理员尝试将配置策略与已暂停的账户关联时，策略关联将会失败。

90 天后，该账户将被停用或重新激活。重新激活账户后，将恢复其 Security Hub CSPM 权限。如果成员账户状态为账户已暂停，则管理员账户必须手动启用该账户。

账户已关闭

关闭后， AWS 账户 Security Hub CSPM 会按如下方式对关闭做出响应。

如果该账户是 Security Hub CSPM 管理员账户，则会以管理员账户身份删除该账户，并删除所有成员账户。如果该账户是成员账户，则会解除关联并将其作为成员从 Security Hub CSPM 管理员账户中删除。

Security Hub CSPM 会将现有已存档的调查发现在账户中保留 30 天。对于控件调查发现，30 天的计算基于该调查发现的 `UpdatedAt` 字段的值。对于另一种类型的调查发现，则根据调查发现的 `UpdatedAt` 或 `ProcessedAt` 字段的值（以较晚者为准）进行计算。30 天期限结束后，Security Hub CSPM 会永久删除账户中的调查发现。

Security Hub CSPM 会将现有活跃调查发现在账户中保留 90 天。对于控件调查发现，90 天的计算基于该调查发现的 `UpdatedAt` 字段的值。对于另一种类型的调查发现，则根据调查发现的 `UpdatedAt` 或 `ProcessedAt` 字段的值（以较晚者为准）进行计算。90 天期限结束后，Security Hub CSPM 会永久删除账户中的调查发现。

为了长期保留现有调查发现，您可以将调查发现导出到 S3 存储桶。您可以通过使用带有 Amazon EventBridge 规则的自定义操作来实现此目的。有关更多信息，请参阅 EventBridge 用于自动响应和补救。

> **Important**
>
> 对于中的客户 AWS GovCloud (US) Regions，请在关闭账户之前备份并删除您的保单数据和其他账户资源。关闭账户后，您将无法访问这些资源和数据。

有关更多信息，请参阅《AWS 账户管理 参考指南》中的 Close an AWS 账户。

了解 Security Hub CSPM 中的跨区域聚合

> **Note**
>
> 聚合区域现在称为主区域。某些 Security Hub CSPM API 操作仍使用旧术语“聚合区域”。

通过在 Sec AWS urity Hub CSPM 中使用跨区域聚合，您可以将多个主区域的发现、查找更新、见解、控制合规状态和安全评分汇总 AWS 区域 到单个主区域。然后，您可以管理主区域中的所有这些数据。

假设您将美国东部（弗吉尼亚州北部）设置为主区域，将美国西部（俄勒冈州）和美国西部（北加利福尼亚）设置为关联区域。在美国东部（弗吉尼亚州北部）查看调查发现页面时，您会看到所有三个地区的调查发现。这些调查发现的最新情况也反映在所有三个区域。

> **Note**
>
> 在中 AWS GovCloud (US)，跨区域聚合仅支持对调查结果、发现更新和洞察进行跨 AWS GovCloud (US)区域聚合。具体而言，您只能汇总 AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）之间的调查结果、最新发现和见解。在中国区域，跨区域聚合仅支持对中国区域的调查发现、调查发现更新和见解进行跨区域聚合。具体而言，您只能聚合中国（北京）和中国（宁夏）之间的调查发现、调查发现更新和见解。

如果在关联区域中启用了控件，但在主区域中禁用了控件，则可以从主区域查看该控件的合规性状态，但不能在主区域启用或禁用该控件。例外情况是您使用中心配置。如果您使用中心配置，则 Security Hub CSPM 委派管理员可以在主区域和主区域的关联区域中配置控件。

如果您设置了主区域，则安全评分会将所有关联区域中的控件状态考虑在内。要查看跨区域安全分数和合规性状态，请向使用 Security Hub CSPM 的 IAM 角色添加以下权限：

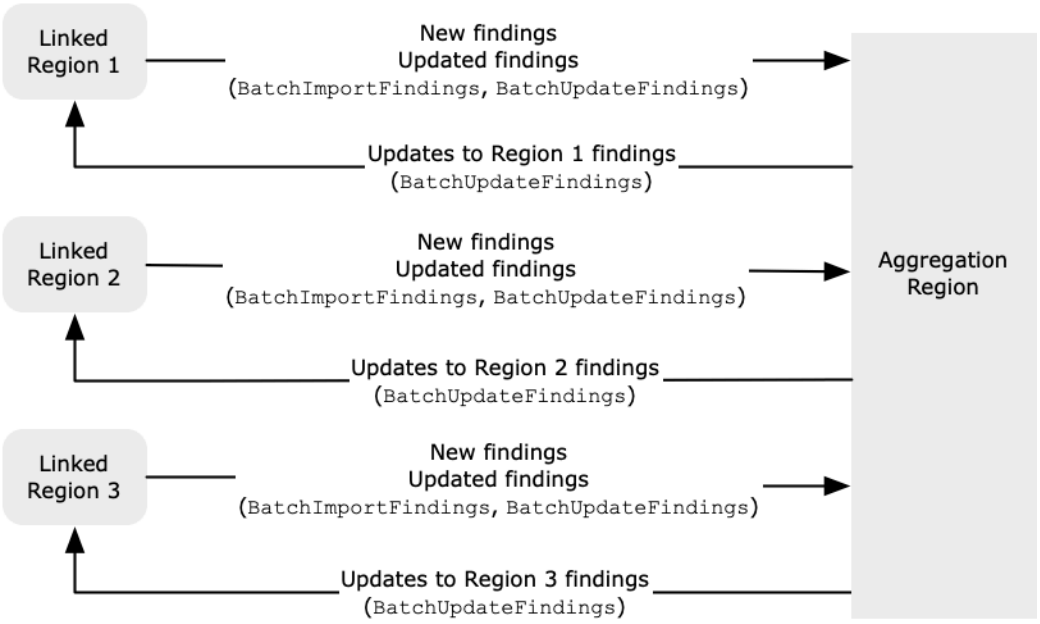
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

聚合的数据类型

在一个或多个关联区域中启用跨区域聚合后，Security Hub CSPM 会将以下数据从关联区域复制到主区域。每个启用了跨区域聚合的账户都会发生这种情况。

- 结果
- 见解
- 控制合规性状态
- 安全分数

除了先前列表中的新数据之外，Security Hub CSPM 还会在关联区域和主区域之间复制对这些数据的更新。关联区域中进行的更新会被复制到主区域。主区域中进行的更新会被复制回关联区域。如果主区域和关联区域中的更新相互冲突，则使用最新的更新。



跨区域聚合不会增加 Security Hub CSPM 的费用。Security Hub CSPM 复制新数据或更新时，您无需付费。

在主区域中，摘要页面提供了您在关联区域中活动调查发现的视图。有关信息，请参阅按严重性查看跨区域调查发现摘要。其他用于分析调查发现的摘要页面面板还会显示来自关联区域的信息。

您在主区域中的安全评分是通过比较所有关联区域中已通过的控件数量和已启用的控件数量来计算的。此外，如果在至少一个关联区域中启用了控件，则该控件将在主区域的安全标准详细信息页面上可见。标准详情页面上控件的合规状态反映了关联区域的调查发现。如果与控件关联的安全检查在一个或多个关联区域中失败，则该控件的合规性状态将在主区域的标准详细信息页面上显示为失败。安全检查的数量包括来自所有关联区域的调查发现。

Security Hub CSPM 仅聚合账户启用了 Security Hub CSPM 的区域的数据。根据跨区域聚合配置，不会自动为账户启用 Security Hub CSPM。

可以在不选择任何关联区域的情况下启用跨区域聚合。在这种情况下，不会进行数据复制。

聚合管理员账户和成员账户

独立账户、成员账户和管理员账户可以配置跨区域聚合。如果由管理员配置，则管理员账户的存在对于跨区域聚合在托管账户中发挥作用至关重要。如果管理员账户被移除或与成员账户取消关联，则成员账户的跨区域聚合将停止。即使该账户在管理员与成员的关系开始之前就已启用跨区域聚合，也是如此。

管理员账户启用跨区域聚合后，Security Hub CSPM 会将管理员账户在所有关联区域中生成的数据复制到主区域。此外，Security Hub CSPM 会识别与该管理员关联的成员账户，并且每个成员账户都会

继承管理员的跨区域聚合设置。Security Hub CSPM 会将成员账户在所有关联区域生成的数据复制到主区域。

管理员可以访问和管理托管区域内所有成员账户的安全调查发现。但是，作为 Security Hub CSPM 管理员，您必须登录到主区域才能查看所有成员账户和关联区域的聚合数据。

作为 Security Hub CSPM 成员账户，您必须登录到主区域才能查看您的账户和所有关联区域的聚合数据。成员账户无权查看其他成员账户的数据。

管理员账户可以手动邀请成员账户，也可以作为与之集成的组织的委托管理员 AWS Organizations。对于手动邀请的成员账户，管理员必须从主区域和所有关联区域邀请该账户，才能使跨区域聚合发挥作用。此外，成员账户必须在主区域和所有关联区域中启用 Security Hub CSPM，这样管理员才能查看成员账户中的调查发现。如果您不将主区域用于其他用途，则可以在该区域中禁用 Security Hub CSPM 标准和集成以防止产生费用。

如果您计划使用跨区域聚合，并且拥有多个管理员账户，则我们推荐以下最佳实践：

- 每个管理员账户都有不同的成员账户。
- 每个管理员账户在不同地区都有相同的成员账户。
- 每个管理员账户使用不同的主区域。

> **Note**
>
> 要了解跨区域聚合如何影响中心配置，请参阅中心配置对跨区域聚合的影响。

中心配置对跨区域聚合的影响

中央配置是 Sec AWS urity Hub CSPM 中的一项可选功能，如果您与之集成，则可以使用该功能。AWS Organizations如果您使用中心配置，则委派管理员账户可以为组织中的账户和组织单元（OU）配置 Security Hub CSPM 服务、标准和控件。要配置账户和 OUs，授权的管理员会创建 Security Hub CSPM 配置策略。配置策略可用于定义是启用还是禁用 Security Hub CSPM，以及启用哪些标准和控件。授权的管理员将配置策略与特定账户或根账户（整个组织）关联起来。 OUs

委派管理员只能从主区域为组织创建和管理配置策略。此外，配置策略会在主区域和所有关联区域中生效。您无法创建仅适用于某些关联区域而不适用于其他区域的配置策略。有关跨区域聚合的信息，请参阅跨区域聚合。

要使用中心配置，必须指定主区域。（可选）您可以选择一个或多个区域作为关联区域。您也可以选择指定没有任何关联区域的主区域。

更改跨区域聚合设置可能会影响您的配置策略。当您添加关联区域时，您的配置策略将在该区域生效。如果该区域是选择加入的区域，则必须启用该区域才能使您的配置策略在该区域生效。相反，当您移除关联区域后，配置策略在该区域不再生效。在该区域中，账户将保留移除关联区域时的区域设置。您可以更改这些设置，但必须在分别每个账户和区域中进行更改。

如果您移除或更改主区域，则您的配置策略和策略关联将被删除。您将不能再在任何区域使用中心配置或创建配置策略。账户将保留更改或移除主区域之前的设置。您可以随时更改这些设置，但由于您不再使用中心配置，因此必须分别在每个账户和区域中修改设置。如果您指定了新的主区域，则可以使用中心配置并再次创建配置策略。

有关中心配置的更多信息，请参阅了解 Security Hub CSPM 中的中心配置。

启用跨区域聚合

> **Note**
>
> 聚合区域现在称为主区域。某些 Security Hub CSPM API 操作仍使用旧术语“聚合区域”。

您必须从要指定为主区域 AWS 区域 的中启用跨区域聚合。

要启用跨区域聚合，您需要创建一项名为调查发现聚合器的 Security Hub CSPM 资源。调查发现聚合器资源指定主区域和关联区域（如果有）。

您不能使用默认禁用的区域作为您的主区域。 AWS 区域 有关默认禁用的区域列表，请参阅 AWS 一般参考 中的启用区域。

启用跨区域聚合时，如果需要，您可以选择指定一个或多个关联区域。您还可以选择在 Security Hub CSPM 开始支持新区域并且您已选择加入新区域时是否自动关联这些区域。

Security Hub CSPM console

要启用跨区域聚合

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 使用 AWS 区域 选择器登录要用作聚合区域的区域。

3. 在 Security Hub CSPM 导航菜单中，选择设置，然后选择区域。
4. 对于调查发现聚合，选择配置调查发现聚合。

   默认情况下，主区域设置为无聚合区域。
5. 在聚合区域下，选择将当前区域指定为主区域的选项。
6. （可选）对于关联区域，选择要从中聚合数据的区域。
7. 当 Security Hub CSPM 支持分区中的新区域并且您选择加入这些区域时，要自动聚合这些区域的数据，请选择关联未来区域。
8. 选择保存。

Security Hub CSPM API

在您要用作主区域的区域中，使用 Security Hub CSPM API 的 `CreateFindingAggregator` 操作。如果您使用 AWS CLI，请运行该create-finding-aggregator命令。

对于`RegionLinkingMode`，请选择下列选项之一：

- `ALL_REGIONS` – Security Hub CSPM 聚合所有区域的数据。当新区域受支持并且您选择加入这些区域时，Security Hub CSPM 还会聚合这些区域的数据。
- `ALL_REGIONS_EXCEPT_SPECIFIED` – Security Hub CSPM 聚合除要排除的区域之外的所有区域的数据。当新区域受支持并且您选择加入这些区域时，Security Hub CSPM 还会聚合这些区域的数据。用 `Regions` 提供要从聚合中排除的区域列表。
- `SPECIFIED_REGIONS` – Security Hub CSPM 聚合选定区域列表的数据。Security Hub CSPM 不会自动聚合新区域的数据。使用 `Regions` 用于提供要聚合的区域列表。
- `NO_REGIONS` – Security Hub CSPM 不会聚合数据，因为您没有选择任何关联区域。

以下示例会配置跨区域聚合。主区域为美国东部（弗吉尼亚州北部）。关联区域是美国西部（北加利福尼亚）和美国西部（俄勒冈州）。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

查看跨区域聚合设置

> **Note**
>
> 聚合区域现在称为主区域。某些 Security Hub CSPM API 操作仍使用旧术语“聚合区域”。

您可以从任何位置在 Sec AWS urity Hub CSPM 中查看当前的跨区域聚合配置。 AWS 区域配置包括主区域、关联区域（如果有），以及是否自动关联 CSPM 支持的新区域。

成员账户可以查看管理员账户配置的跨区域聚合设置。

选择您的首选方法，然后按照以下步骤查看当前的跨区域聚合设置。

Security Hub CSPM console

查看跨区域聚合设置（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置，然后选择区域选项卡。

如果未启用跨区域聚合，则区域选项卡将显示启用跨区域聚合的选项。只有管理员账户和独立账户才能启用跨区域聚合。

如果启用了跨区域聚合，则区域选项卡将显示以下信息：

- 主区域
- 是否自动聚合 Security Hub CSPM 支持且您选择加入的新区域的调查发现、见解、控件状态和安全分数
- 关联区域列表（如果选择了任何区域）

Security Hub CSPM API

查看跨区域聚合设置（Security Hub CSPM API）

使用 Security Hub CSPM API 的 `GetFindingAggregator` 操作。如果您使用 AWS CLI，请运行该get-finding-aggregator命令。

发出请求时，请提供调查发现聚合器 ARN。要获取调查发现聚合器 ARN，请使用 `ListFindingAggregators` 操作或 list-finding-aggregators 命令。

以下示例显示了指定的调查发现聚合器 ARN 的跨区域聚合设置。此示例针对 Linux、macOS 或 Unix 进行了格式化，它使用反斜杠 (\ ) 续行字符以提高可读性

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

更新跨区域聚合设置

> **Note**
>
> 聚合区域现在称为主区域。某些 Security Hub CSPM API 操作仍使用旧术语“聚合区域”。

您可以通过更改链接的区域或当前的主区域来更新 Sec AWS urity Hub CSPM 中当前的跨区域聚合设置。您还可以更改是否自动聚合支持 Security Hub CSPM 的新增 AWS 区域 数据。

只有在 AWS 账户中启用选择加入的区域后，才会对该区域实施跨区域聚合的更改。在 2019 年 3 月 20 日当天或之后 AWS 推出的区域为可选区域。

当您停止聚合来自关联区域的数据时，Sec AWS urity Hub CSPM 不会从该区域中删除可在原区域访问的任何现有聚合数据。

您不能使用本节中的更新过程来更改主区域。要更改主区域，您必须执行以下操作：

1. 停止跨区域聚合。有关说明，请参阅the section called “停止聚合”。
2. 更改为要作为新的主区域的区域。
3. 启用跨区域聚合。有关说明，请参阅the section called “启用聚合”。

您必须从当前主区域更新跨区域聚合配置。

Security Hub CSPM console

更改关联区域

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   登录到当前聚合区域。
2. 在 Security Hub CSPM 导航菜单中，选择设置，然后选择区域。
3. 对于调查发现聚合，选择编辑。
4. 对于关联区域，更新所选的关联区域。
5. 如有必要，更改是否选择关联未来区域。此设置决定当 Security Hub 支持新区域并且您选择加入这些区域时 Security Hub CSPM 是否自动关联这些区域。
6. 选择保存。

Security Hub CSPM API

使用 `UpdateFindingAggregator` 操作。如果您使用 AWS CLI，请运行该update-finding-aggregator命令。要识别调查发现聚合器，必须提供调查发现聚合器 ARN。要获取查找聚合器 ARN，请使用操作list-finding-aggregators或`ListFindingAggregators`命令...

如果关联模式为 `ALL_REGIONS_EXCEPT_SPECIFIED` 或 `SPECIFIED_REGIONS`，则可以更改已排除或已包含区域的列表。如果您要将区域关联模式更改为 `NO_REGIONS`，则不应提供区域列表。

更改排除或已包含区域的列表时，必须提供包含更新的完整列表。例如，假设您当前美国东部（俄亥俄州）的调查发现，同时还要聚合美国西部（俄勒冈州）的调查发现。您必须提供同时包含美国东部（俄亥俄州）和美国西部（俄勒冈州）的 `Regions` 列表。

以下示例会更新所选区域的跨区域聚合。从当前主区域 [即美国东部（弗吉尼亚州北部）] 运行命令。关联区域是美国西部（北加利福尼亚）和美国西部（俄勒冈州）。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
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
```

停止跨区域聚合

> **Note**
>
> 聚合区域现在称为主区域。某些 Security Hub CSPM API 操作仍使用旧术语“聚合区域”。

如果您不希望 S AWS ecurity Hub CSPM 聚合数据，则可以删除您的查找聚合器。或者，您可以通过将现有聚合器更新为链接模式 AWS 区域 来保留查找聚合器，但不能将任何聚合器`NO_REGIONS`链接到主区域。

要更改主区域，您必须删除当前的调查发现聚合器并创建新的聚合器。

删除调查发现聚合器后，Security Hub CSPM 会停止聚合数据。它不会从主区域中移除任何现有的聚合数据。

删除调查发现聚合器（控制台）

您只能从当前的主区域中删除调查发现聚合器。

在主区域以外的区域中，Security Hub CSPM 控制台上的调查发现聚合面板会显示一条消息，提示您必须在主区域中编辑配置。选择此消息可显示切换到主区域的链接。

Security Hub CSPM console

停止跨区域聚合（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 确保您已登录到当前主区域。
3. 在 Security Hub CSPM 导航菜单中，选择设置，然后选择区域。
4. 在调查发现聚合下，选择编辑。
5. 在聚合区域下，选择无聚合区域。
6. 选择保存。
7. 在确认对话框的确认字段中，键入 **`Confirm`**。
8. 选择确认。

Security Hub CSPM API

使用 Security Hub CSPM API 的 DeleteFindingAggregator 操作。如果您使用的是 AWS CLI，请运行delete-finding-aggregator命令。

要识别要删除的调查发现聚合器，请提供调查发现聚合器 ARN。要获取调查发现聚合器 ARN，请使用 ListFindingAggregators 操作或 list-finding-aggregators 命令。

以下示例会删除调查发现聚合器。从当前主区域 [即美国东部（弗吉尼亚州北部）] 运行命令。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-
east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --
region us-east-1
```

了解 Security Hub CSPM 中的安全标准

在 Sec AWS urity Hub CSPM 中，安全标准是一组基于监管框架、行业最佳实践或公司政策的要求。有关 Security Hub CSPM 当前支持的标准（包括适用于每个标准的安全控件）的详细信息，请参阅Security Hub CSPM 标准参考。

启用标准时，Security Hub CSPM 会自动启用适用于该标准的所有控件。然后，Security Hub CSPM 会对控件运行安全检查，从而生成 Security Hub CSPM 调查发现。您可以根据需要禁用和稍后重新启用单个控件。您也可以完全禁用某个标准。如果禁用某个标准，Security Hub CSPM 将停止对适用于该标准的控件运行安全检查。不再为控件生成调查发现。

除了调查发现外，Security Hub CSPM 还会为您启用的每个标准生成安全分数。该分数基于适用于该标准的控件的状态。如果设置聚合区域，则标准的安全分数将反映所有关联区域中控件的状态。如果您是某个组织的 Security Hub CSPM 管理员，则该分数反映了您组织中所有账户的控件状态。有关更多信息，请参阅 计算安全分数。

要审查和管理标准，您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。在控制台上，安全标准页面显示了 Security Hub CSPM 当前支持的所有安全标准。这包括每个标准的描述以及标准的当前状态。如果您启用某个标准，则还可以使用此页面访问该标准的更多详细信息。例如，您可以查看：

- 标准的当前安全分数。
- 适用于标准的控件的聚合统计数据。
- 适用于标准且当前已启用的控件列表，包括每个控件的合规性状态。

- 适用于标准但当前已禁用的控件列表。

要进行更深入的分析，您可以对数据进行筛选和排序，然后深入查看适用于标准的各个控件的详细信息。

您可以为单个账户单独启用标准，以及 AWS 区域。但是，为了节省时间并减少多账户和多区域环境中的配置偏差，建议使用中心配置来启用和管理标准。通过中心配置，委派的 Security Hub CSPM 管理员可以创建策略来指定如何跨多个账户和区域配置标准。

主题

- Security Hub CSPM 标准参考
- 启用安全标准
- 查看安全标准的详细信息
- 关闭自动启用的安全标准
- 禁用安全标准

Security Hub CSPM 标准参考

在 Sec AWS urity Hub CSPM 中，安全标准是一组基于监管框架、行业最佳实践或公司政策的要求。Security Hub CSPM 将这些要求映射到控件，并对控件运行安全检查，以评测是否符合标准的要求。每个标准都包含多个控件。

Security Hub CSPM 当前支持以下标准：

- AWS 基础安全最佳实践 — 该标准由 AWS 行业专业人士制定，汇编了适用于任何行业或规模的组织的安全最佳实践。它提供了一组控件，用于检测您的 AWS 账户 和资源何时偏离了安全最佳实践。它提供了有关如何改进和维护安全状况的规范性指导。
- AWS 资源标记 — 该标准由 Security Hub CSPM 开发，可以帮助您确定您的 AWS 资源是否有标签。标签是用作资源元数据的键值对。 AWS 标签可以帮助您识别、分类、管理和搜索 AWS 资源。例如，您可以使用标签按用途、所有者或环境对资源进行分类。
- CIS AWS 基金会基准 — 该标准由互联网安全中心 (CIS) 开发，提供了以下方面的安全配置指南 AWS。它为一部分和资源指定了一套安全配置指南 AWS 服务 和最佳实践，重点是基础设置、可测试设置和架构不可知设置。指南包括清晰的分步实施和评测过程。
- NIST SP 800-53 修订版 5 – 此标准符合美国国家标准与技术研究院（NIST）关于保护信息系统和关键资源的机密性、完整性和可用性的要求。相关框架通常适用于 U.S。联邦机构或与 U.S联邦机构或信息系统合作的组织。但是，私人组织也可以将这些要求用作指导框架。

- NIST SP 800-171 修订版 2 — 该标准符合 NIST 的安全建议和要求，以保护不属于联邦政府的系统和组织中受控非机密信息 (CUI) 的机密性。 U.SCUI 是不符合政府分类标准但被视为敏感的信息，由联邦政府或其他实体代表联邦政府创建或拥有 U.S。 U.S
- PCI DSS：此标准符合支付卡行业数据安全标准（PCI DSS）合规框架，该框架由 PCI 安全标准委员会（SSC）定义。该框架提供了一套安全处理信用卡和借记卡信息的规则和指南。该框架通常适用于存储、处理或传输持卡人数据的组织。
- Service-managed 标准， AWS Control Tower— 此标准可帮助您配置 Security Hub CSPM 提供的侦探控件。 AWS Control Tower AWS Control Tower 遵循规范性最佳实践，提供了一种设置和管理 AWS 多账户环境的简单方法。

Security Hub CSPM 的标准和控件并不能保证遵守任何监管框架或审计。相反，它们提供了一种评估和监控您的 AWS 账户 账户和资源状态的方法。建议您启用与您的业务需求、行业或使用案例相关的各项标准。

单个控件可以适用于多个标准。如果启用多个标准，则建议您同时启用整合的控件调查发现。如果这样做，Security Hub CSPM 会为每个控件生成一个调查发现，即使该控件适用于多个标准也是如此。如果不启用整合的控件调查发现，Security Hub CSPM 会为控件适用于的每个已启用标准生成单独的调查发现。例如，如果启用了两个标准，并且一个控件适用于这两个标准，则您会收到两个针对该控件的单独调查发现，每个标准一个。如果启用整合的控件调查发现，则只会收到控件的一个调查发现。有关更多信息，请参阅 整合的控件调查发现。

标准的详细参考

- AWS Security Hub CSPM 中的基础安全最佳实践标准
- AWS Security Hub CSPM 中的资源标记标准
- CIS AWS Security Hub CSPM 中的基础基准
- Security Hub CSPM 中的 NIST SP 800-53 修订版 5
- Security Hub CSPM 中的 NIST SP 800-171 修订版 2
- Security Hub CSPM 中的 PCI DSS
- Service-managed Security Hub CSPM 中的标准

AWS Security Hub CSPM 中的基础安全最佳实践标准

AWS 基础安全最佳实践 (FSBP) 标准由 AWS 行业专业人士制定，汇编了组织的最佳安全实践，无论组织部门或规模如何。它提供了一组控制措施，用于检测何时 AWS 账户 出现资源偏离安全最佳实践。它还提供了有关如何改进和维护组织的安全状况的规范性指导。

在 S AWS ecurity Hub CSPM 中， AWS 基础安全最佳实践标准包括持续评估您的 AWS 账户 和工作负载的控件，并帮助您识别偏离安全最佳实践的领域。这些控件包括多个 AWS 服务资源的安全最佳实践。为每个控件分配一个类别以反映控件应用于的安全功能。有关类别列表和其他详细信息，请参阅控件类别。

适用于标准的控件

以下列表指定了哪些 Sec AWS urity Hub CSPM 控件适用于 AWS 基础安全最佳实践标准 (v1.0.0)。要查看控件的详细信息，请选择该控件。

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

[ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度

[APIGateway.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录

[APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证

[APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 跟踪

[APIGateway.4] API Gateway 应与 WAF Web ACL 关联

[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密

[APIGateway.8] API Gateway 路由应指定授权类型

[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

[APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接

[APIGateway.11] API Gateway 域名应使用推荐的安全策略

[AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密

[AppSync.2] AWS AppSync 应该启用字段级日志记录

[AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证

[AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密

[Athena.4] Athena 工作组应启用日志记录

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

[AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域

[AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)

[Autoscaling.5] 使用 Auto Scaling 组启动配置启动的 EC2 亚马逊实例不应具有公有 IP 地址

[AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型

[AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板

[Backup.1] AWS Backup 恢复点应在静态状态下进行加密

[BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式

[BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权

[BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式

[BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制

[CloudFormation.3] CloudFormation 堆栈应启用终止保护

[CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色

[CloudFront.1] CloudFront 发行版应配置默认根对象

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

[CloudFront.4] CloudFront 发行版应配置源站故障转移

[CloudFront.5] CloudFront 发行版应启用日志记录

[CloudFront.6] CloudFront 发行版应启用 WAF

[CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

[CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

[CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

[CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

[CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

[CloudFront.13] CloudFront 发行版应使用源站访问控制

[CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略

[CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制

[CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

[CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

[CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密

[Cognito.2] Cognito 身份池不应允许未经身份验证的身份

[Cognito.3] Cognito 用户池的密码策略应具有可靠的配置

[Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证

[Cognito.5] 应为 Cognito 用户池启用 MFA

[Cognito.6] Cognito 用户池应启用删除保护

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

[Connect.2] Connect 客户实例应启用 CloudWatch 日志记录

[DataFirehose.1] Firehose 传输流应在静态状态下进行加密

[DataSync.1] DataSync 任务应启用日志记录

[DMS.1] Database Migration Service 复制实例不应公开

[DMS.6] DMS 复制实例应启用自动次要版本升级

[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录

[DMS.8] 源数据库的 DMS 复制任务应启用日志记录

[DMS.9] DMS 端点应使用 SSL

[DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权

[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

[DMS.12] Redis OSS 的 DMS 端点应启用 TLS

[DMS.13] DMS 复制实例应配置为使用多个可用区

[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密

[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期

[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护

[DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密

[DynamoDB.1] DynamoDB 表应根据需求自动扩展容量

[DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time

[DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密

[DynamodB.6] DynamoDB 表应启用删除保护

[DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密

[EC2.1] 不应将 Amazon EBS 快照配置为可公开还原

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.3] 附加的 Amazon EBS 卷应在静态状态下进行加密

[EC2.4] 应在指定时间段后移除已停止的 EC2 实例

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

[EC2.7] 应启用 EBS 默认加密

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)

[EC2.9] 亚马逊 EC2 实例不应有公有 IPv4 地址

[EC2.10] 应将 Amazon EC2 配置为使用为亚马逊 EC2 服务创建的 VPC 终端节点

[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址

[EC2.16] 应删除未使用的网络访问控制列表

[EC2.17] Amazon EC2 实例不应使用多个 ENI

[EC2.18] 安全组应只允许授权端口不受限制的传入流量

[EC2.19] 安全组不应允许不受限制地访问高风险端口

[EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启

[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389

[EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求

[EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

[EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录

[EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点

[EC2.56] 应为 VPC 配置 Docker Registry 的接口端点

[EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点

[EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点

[EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC

[EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)

[EC2.171] EC2 VPN 连接应启用日志记录

[EC2.172] EC2 VPC 阻止公共访问设置应阻止互联网网关流量

[EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密

[EC2.180] EC2 网络接口应启用 source/destination 检查功能

[EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密

[EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置

[EC2.183] EC2 VPN 连接应使用 IKEv2 协议

[ECR.1] ECR 私有存储库应配置图像扫描

[ECR.2] ECR 私有存储库应配置标签不可变性

[ECR.3] ECR 存储库应至少配置一个生命周期策略

[ECS.2] ECS 服务不应自动分配公有 IP 地址

[ECS.3] ECS 任务定义不应共享主机的进程命名空间

[ECS.4] ECS 容器应以非特权身份运行

[ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限

[ECS.8] 密钥不应作为容器环境变量传递

[ECS.9] ECS 任务定义应具有日志配置

[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行

[ECS.12] ECS 集群应使用容器见解

[ECS.16] ECS 任务集不应自动分配公有 IP 地址

[ECS.18] ECS 任务定义应对 EFS 卷使用传输中加密

[ECS.19] ECS 容量提供商应启用托管终止保护

[ECS.20] ECS 任务定义应在 Linux 容器定义中配置非 root 用户

[ECS.21] ECS 任务定义应在 Windows 容器定义中配置非管理员用户

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

[EFS.2] Amazon EFS 卷应包含在备份计划中

[EFS.3] EFS 接入点应强制使用根目录

[EFS.4] EFS 接入点应强制使用用户身份

[EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联

[EFS.7] EFS 文件系统应启用自动备份

[EFS.8] 应对 EFS 文件系统进行静态加密

[EKS.1] EKS 集群终端节点不应公开访问

[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行

[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

[EKS.8] EKS 集群应启用审核日志

[EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行

[ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份

[ElastiCache.2] ElastiCache 集群应启用自动次要版本升级

[ElastiCache.3] ElastiCache 复制组应启用自动故障切换

[ElastiCache.4] ElastiCache 复制组应进行静态加密

[ElastiCache.5] ElastiCache 复制组在传输过程中应加密

[ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证

[ElastiCache.7] ElastiCache 群集不应使用默认子网组

[ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

[ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新

[ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

[ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager

[ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止

[ELB.4] 应将应用程序负载均衡器配置为丢弃无效的 http 标头

[ELB.5] 应启用应用程序和经典负载均衡器日志记录

[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护

[ELB.7] 经典负载均衡器应启用连接耗尽功能

[ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

[ELB.9] 经典负载均衡器应启用跨区域负载均衡器

[ELB.10] 经典负载均衡器应跨越多个可用区

[ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

[ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略

[ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密

[ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议

[ELB.22] ELB 目标组应使用加密的传输协议

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置

[EMR.3] Amazon EMR 安全配置应静态加密

[EMR.4] Amazon EMR 安全配置应在传输过程中加密

[ES.1] Elasticsearch 域应启用静态加密

[ES.2] Elasticsearch 域名不应公开访问

[ES.3] Elasticsearch 域应加密节点之间发送的数据

[ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志

[ES.5] Elasticsearch 域应启用审核日志

[ES.6] Elasticsearch 域名应至少有三个数据节点

[ES.7] 应将 Elasticsearch 域配置为至少三个专用主节点

[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密

[EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

[FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷

[FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份

[FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署

[FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署

[FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统

[Glue.3] AWS Glue 机器学习转换应在静态时加密

[Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue

[GuardDuty.1] GuardDuty 应该启用

[GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控

[GuardDuty.6] 应启用 Lamb GuardDuty da 保护

[GuardDuty.7] 应启用 GuardDuty EKS 运行时监控

[GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护

[GuardDuty.9] 应启用 GuardDuty RDS 保护

[GuardDuty.10] 应启用 GuardDuty S3 保护

[GuardDuty.11] 应启用 “ GuardDuty 运行时监控”

[GuardDuty.12] 应启用 GuardDuty ECS 运行时监控

[GuardDuty.13] 应启用 GuardDuty EC2 运行时监控

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.7] IAM 用户的密码策略应具有可靠的配置

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作

[Inspector.1] 应启用 Amazon Inspector EC2 扫描

[Inspector.2] 应启用 Amazon Inspector ECR 扫描

[Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描

[Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描

[Kinesis.1] Kinesis 直播应在静态状态下进行加密

[Kinesis.3] Kinesis 流应有足够的数据留存期

[KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作

[KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

AWS KMS keys 不应无意中删除 [KMS.3]

[KMS.5] KMS 密钥不应可公开访问

[Lambda.1] Lambda 函数策略应禁止公众访问

[Lambda.2] Lambda 函数应使用支持的运行时

[Lambda.5] VPC Lambda 函数应在多个可用区中运行

[Macie.1] 应启用 Amazon Macie

[Macie.2] 应启用 Macie 敏感数据自动发现

[MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch

[MSK.1] MSK 集群应在代理节点之间传输时进行加密

[MSK.3] MSK Connect 连接器应在传输过程中进行加密

[MSK.4] MSK 集群应禁用公开访问

[MSK.5] MSK 连接器应启用日志记录

[MSK.6] MSK 集群应禁用未经身份验证的访问

[Neptune.1] 应对 Neptune 数据库集群进行静态加密

[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

[Neptune.3] Neptune 数据库集群快照不应公开

[Neptune.4] Neptune 数据库集群应启用删除保护

[Neptune.5] Neptune 数据库集群应启用自动备份

[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密

[Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证

[Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照

[NetworkFirewall.2] 应启用 Network Firewall 日志记录

[NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

[NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包

[NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

[NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

[NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护

[Opensearch.1] OpenSearch 域名应启用静态加密

[Opensearch.2] OpenSearch 域名不应向公众开放

[Opensearch.3] OpenSearch 域应加密节点之间发送的数据

[Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

[Opensearch.5] OpenSearch 域应启用审核日志

[Opensearch.6] OpenSearch 域名应至少有三个数据节点

[Opensearch.7] OpenSearch 域名应启用精细的访问控制

[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密

[Opensearch.10] OpenSearch 域名应安装最新的软件更新

[PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构

[Route53.2] Route 53 公有托管区域应记录 DNS 查询

[RDS.1] RDS 快照应该是私有的

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

[RDS.3] RDS 数据库实例应启用静态加密

[RDS.4] RDS 集群快照和数据库快照应在静态时加密

[RDS.5] RDS 数据库实例应配置多个可用区

[RDS.6] 应为 RDS 数据库实例配置增强监控

[RDS.7] RDS 集群应启用删除保护

[RDS.8] RDS 数据库实例应启用删除保护

[RDS.9] RDS 数据库实例应将日志发布到 CloudWatch 日志

[RDS.10] 应为 RDS 实例配置 IAM 身份验证

[RDS.11] RDS 实例应启用自动备份

[RDS.12] 应为 RDS 集群配置 IAM 身份验证

[RDS.13] 应启用 RDS 自动次要版本升级

[RDS.14] 亚马逊 Aurora 集群应启用回溯功能

[RDS.15] 应为多个可用区配置 RDS 数据库集群

[RDS.16] 应将 Aurora 数据库集群配置为将标签复制到数据库快照

[RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照

[RDS.19] 应为关键群集事件配置现有 RDS 事件通知订阅

[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

[RDS.22] 应为关键的数据库安全组事件配置 RDS 事件通知订阅

[RDS.23] RDS 实例不应使用数据库引擎的默认端口

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

[RDS.27] RDS 数据库集群应进行静态加密

[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志

[RDS.35] RDS 数据库集群应启用自动次要版本升级

[RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch

[RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch

[RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志

[RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密

[RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch

[RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密

[RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密

[RDS.45] Aurora MySQL 数据库集群应启用审计日志

[RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中

[RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照

[RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照

[RDS.50] RDS 数据库集群应设置足够的备份保留期

[RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行

[Redshift.1] Amazon Redshift 集群应禁止公共访问

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

[Redshift.3] Amazon Redshift 集群应启用自动快照

[Redshift.4] Amazon Redshift 集群应启用审核日志记录

[Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能

[Redshift.7] Redshift 集群应使用增强型 VPC 路由

[Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名

[Redshift.10] Redshift 集群应在静态状态下进行加密

[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口

[Redshift.18] Redshift 集群应启用多可用区部署

[RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由

[RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组

[RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问

[RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名

[RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

[S3.2] S3 通用存储桶应阻止公共读取访问权限

[S3.3] S3 通用存储桶应阻止公共写入访问权限

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户

[S3.8] S3 通用存储桶应屏蔽公共访问权限

[S3.9] S3 通用存储桶应启用服务器访问日志记录

ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限

[S3.13] S3 通用存储桶应具有生命周期配置

[S3.19] S3 接入点已启用屏蔽公共访问权限设置

[S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置

[S3.25] S3 目录存储桶应具有生命周期配置

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限

[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

[SageMaker.5] SageMaker 模型应启用网络隔离

[SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行

[SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密

[SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密

[SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离

[SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离

[SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密

[SageMaker.14] SageMaker 监控计划应启用网络隔离

[SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密

[SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表

[SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键

[SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

[SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换

[SecretsManager.3] 移除未使用的 Secrets Manager 密钥

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享

[SES.3] SES 配置集应启用 TLS 以发送电子邮件

[SNS.4] SNS 主题访问策略不应允许公共访问

[SQS.1] 应对 Amazon SQS 队列进行静态加密

[SQS.3] SQS 队列访问策略不应允许公开访问

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

[SSM.4] SSM 文档不应公开

[SSM.6] SSM 自动化应启用日志记录 CloudWatch

[SSM.7] SSM 文档应启用“阻止公开共享”设置

[StepFunctions.1] Step Functions 状态机应该开启日志功能

[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

[Transfer.3] Transfer Family 连接器应启用日志记录

[WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录

[WAF.2] AWS WAF 经典区域规则应至少有一个条件

[WAF.3] AWS WAF 经典区域规则组应至少有一条规则

[WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组

[WAF.6] AWS WAF 经典全局规则应至少有一个条件

[WAF.7] AWS WAF 经典全局规则组应至少有一条规则

[WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

[WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组

[WAF.12] AWS WAF 规则应启用指标 CloudWatch

[WorkSpaces.1] WorkSpaces 用户卷应在静态时加密

[WorkSpaces.2] WorkSpaces 根卷应在静态时加密

AWS Security Hub CSPM 中的资源标记标准

由 Sec AWS urity Hub CSPM 开发的 AWS 资源标记标准可帮助您确定您的 AWS 资源是否缺少标签。标签是键值对，用作组织 AWS 资源的元数据。大多数 AWS 资源都允许您在创建资源时或创建资

源后向资源添加标签。资源示例包括亚马逊 CloudFront 分配、亚马逊弹性计算云 (Amazon EC2) 实例和中的密钥。 AWS Secrets Manager标签可以帮助您管理、识别、组织、搜索和筛选 AWS 资源。

每个 标签具有两个部分：

- 标签键，例如 `CostCenter`、`Environment` 或 `Project`。标签键区分大小写。
- 标签值，例如 `111122223333` 或 `Production`。与标签键一样，标签值区分大小写。

您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。有关为 AWS 资源添加标签的信息，请参阅《标记 AWS 资源和标签编辑器用户指南》。

对于适用于 Security Hub CSPM 中 AWS 资源标记标准的每个控件，您可以选择使用支持的参数来指定要控件检查的标签密钥。如果未指定任何标签键，则该控件仅检查是否存在至少一个标签键，如果资源没有任何标签键，则该控件将失败。

在启用 AWS 资源标记标准之前，请务必在中 AWS Config启用和配置资源记录。配置资源记录时，还要确保为所有类型的 AWS 资源启用该功能，这些资源由适用于标准的控件进行检查。否则，Security Hub CSPM 可能无法评估适当的资源，也无法针对适用于标准的控件生成准确的调查发现。有关更多信息，包括要记录的资源类型列表，请参阅 控制结果所需的 AWS Config 资源。

启用 AWS 资源标记标准后，您将开始收到适用于该标准的控件的调查结果。请注意，对于使用与适用于其他已启用标准的控件相同的 AWS Config 服务关联规则的控件，Security Hub CSPM 最多可能需要 18 小时才能生成结果。有关更多信息，请参阅 有关运行安全检查的计划。

AWS 资源标签标准具有以下 Amazon 资源名称 (ARN)`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`：，*`region`*其中是适用的区域代码。 AWS 区域您还可以使用 Security Hub CSPM API 的GetEnabledStandards操作来检索当前启用的标准的 ARN。

> **Note**
>
> AWS 资源标注标准不适用于亚太地区（新西兰）和亚太地区（台北）区域。

适用于标准的控件

以下列表指定了哪些 Sec AWS urity Hub CSPM 控件适用于 AWS 资源标记标准 (v1.0.0)。要查看控件的详细信息，请选择该控件。

- [ACM.3] 应标记 ACM 证书

- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.4] 应标记 AWS AppSync Gr APIs aphQL
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Backup.2] AWS Backup 应标记恢复点
- [Backup.3] AWS Backup 应给保管库加标签
- [Backup.4] AWS Backup 报告计划应加标签
- [Backup.5] AWS Backup 应标记备份计划
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudTrail.9] CloudTrail 路径应加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图

- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DynamoDB.5] 应标记 DynamoDB 表
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关
- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL
- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应标记 Amazon VPC
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.52] 应标记 EC2 传输网关
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标

- [ECR.4] 应标记 ECR 公有存储库
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [EFS.5] 应标记 EFS 接入点
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.3] GuardDuty IPSets 应该被标记
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.23] 应标记 IAM Access Analyzer 分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型

- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.2] 应标记 Kinesis 流
- [Lambda.6] 应标记 Lambda 函数
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [Redshift.11] 应标记 Redshift 集群

- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Redshift.17] 应标记 Redshift 集群参数组
- [Route53.1] 应标记 Route53 运行状况检查
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SNS.3] 应标记 SNS 主题
- [SQS.2] 应标记 SQS 队列
- [SSM.5] 应标记 SSM 文档
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件

CIS AWS Security Hub CSPM 中的基础基准

互联网安全中心 (CIS) AWS 基金会基准测试是一组安全配置最佳实践 AWS。这些行业公认的最佳实践为您提供了清晰、分步的实施和评估程序。从操作系统到云服务和网络设备，此基准测试中的控件可帮助您保护组织使用的特定系统。

AWS Security Hub CSPM 支持 CIS AWS 基金会基准测试版本 5.0.0、3.0.0、1.4.0 和 1.2.0。本页列出了每个版本支持的安全控件。它还提供了版本的比较。

CIS AWS 基础基准测试版本 5.0.0

Security Hub CSPM 支持 CIS 基金会基准测试的 5.0.0 版 (v5.0.0)。 AWS Security Hub CSPM 已满足 CIS 安全软件认证的要求，并已根据以下 CIS 基准获得 CIS 安全软件认证：

- CIS AWS 基金会基准测试基准，v5.0.0，第 1 级
- CIS AWS 基金会基准测试基准，v5.0.0，第 2 级

适用于 CIS 的控制措施 AWS 基础基准测试版本 5.0.0

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

[EC2.7] 应启用 EBS 默认加密

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)

[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389

[EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口

[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

[EFS.8] 应对 EFS 文件系统进行静态加密

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.9] 应为根用户启用 MFA

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.18] 确保已创建支持角色来管理事件 AWS 支持

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

[IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书

[IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess

[IAM.28] 应启用 IAM Access Analyzer 外部访问分析器

[KMS.4] 应启用 AWS KMS 密钥轮换

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

[RDS.3] RDS 数据库实例应启用静态加密

[RDS.5] RDS 数据库实例应配置多个可用区

[RDS.13] 应启用 RDS 自动次要版本升级

[RDS.15] 应为多个可用区配置 RDS 数据库集群

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

[S3.8] S3 通用存储桶应屏蔽公共访问权限

[S3.20] S3 通用存储桶应启用 MFA 删除

[S3.22] S3 通用存储桶应记录对象级写入事件

[S3.23] S3 通用存储桶应记录对象级读取事件

CIS AWS 基础基准测试版本 3.0.0

Security Hub CSPM 支持 CIS 基金会基准测试的 3.0.0 版 (v3.0.0)。 AWS Security Hub CSPM 已满足 CIS 安全软件认证的要求，并已根据以下 CIS 基准获得 CIS 安全软件认证：

- CIS AWS 基金会基准测试基准，v3.0.0，第 1 级
- CIS AWS 基金会基准测试基准，v3.0.0，第 2 级

适用于 CIS 的控制措施 AWS 基础基准测试版本 3.0.0

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

[EC2.7] 应启用 EBS 默认加密

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)

[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389

[EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口

[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.9] 应为根用户启用 MFA

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.18] 确保已创建支持角色来管理事件 AWS 支持

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

[IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书

[IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess

[IAM.28] 应启用 IAM Access Analyzer 外部访问分析器

[KMS.4] 应启用 AWS KMS 密钥轮换

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

[RDS.3] RDS 数据库实例应启用静态加密

[RDS.13] 应启用 RDS 自动次要版本升级

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

[S3.8] S3 通用存储桶应屏蔽公共访问权限

[S3.20] S3 通用存储桶应启用 MFA 删除

[S3.22] S3 通用存储桶应记录对象级写入事件

[S3.23] S3 通用存储桶应记录对象级读取事件

CIS AWS 基础基准测试版本 1.4.0

Security Hub CSPM 支持 CIS 基金会基准测试的 1.4.0 版 (v1.4.0)。 AWS

适用于 CIS 的控制措施 AWS 基础基准测试版本 1.4.0

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

[CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报

[CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报

[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报

[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

[CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报

[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报

[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报

[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报

[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

[EC2.7] 应启用 EBS 默认加密

[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.9] 应为根用户启用 MFA

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.18] 确保已创建支持角色来管理事件 AWS 支持

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

[KMS.4] 应启用 AWS KMS 密钥轮换

[RDS.3] RDS 数据库实例应启用静态加密

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

[S3.8] S3 通用存储桶应屏蔽公共访问权限

[S3.20] S3 通用存储桶应启用 MFA 删除

CIS AWS 基础基准测试版本 1.2.0

Security Hub CSPM 支持 CIS 基金会基准测试的 1.2.0 版 (v1.2.0)。 AWS Security Hub CSPM 已满足 CIS 安全软件认证的要求，并已根据以下 CIS 基准获得 CIS 安全软件认证：

- CIS AWS 基金会基准测试基准，v1.2.0，第 1 级
- CIS AWS 基金会基准测试基准，v1.2.0，第 2 级

适用于 CIS 的控制措施 AWS 基础基准测试版本 1.2.0

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报

[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报

[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

[CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报

[CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报

[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报

[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

[CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报

[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报

[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报

[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报

[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22

[EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.9] 应为根用户启用 MFA

[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母

[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母

[IAM.13] 确保 IAM 密码策略要求包含至少一个符号

[IAM.14] 确保 IAM 密码策略要求包含至少一个数字

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效

[IAM.18] 确保已创建支持角色来管理事件 AWS 支持

[KMS.4] 应启用 AWS KMS 密钥轮换

CIS 的版本比较 AWS 基金会基准

本节总结了互联网安全中心 (CIS) AWS 基金会基准测试的特定版本之间的区别 — v5.0.0、v3.0.0、v1.4.0 和 v1.2.0。 AWS Security Hub CSPM 支持 CIS AWS 基金会基准测试的每个

版本。但是，建议使用 v5.0.0 以了解最新的安全最佳实践。您可以同时启用多个版本的 CIS AWS 基金会基准标准。有关启用标准的信息，请参阅启用安全标准。如果要升级到 v5.0.0，请先启用新版本，然后再禁用旧版本。这可以防止您的安全检查出现漏洞。如果您使用与 Security Hub CSPM 集成，AWS Organizations 并希望在多个账户中批量启用 v5.0.0，我们建议使用集中配置。

将控件映射到每个版本中的 CIS 要求

了解每个版本的 CIS AWS 基金会基准测试支持的控件。

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[Account.1] 应为以下人员提供安全联系信息 AWS 账户	1.2	1.2	1.2	1.18
[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	3.1	3.1	3.1	2.1
[CloudTrail.2] CloudTrail 应该启用静态加密	3.5	3.5	3.7	2.7
[CloudTrail.4] 应启用 CloudTrail 日志文件验证	3.2	3.2	3.2	2.2
[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	3.4	2.4
[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	3.3	2.3
[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录	3.4	3.4	3.6	2.6
[CloudWatch.1] “root” 用户应有日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.3	3.3

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	不支持 – 手动检查	3.1
[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	不支持 – 手动检查	3.2
[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.4	3.4
[CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.5	3.5
[CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.6	3.6
[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.7	3.7
[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.8	3.8
[CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.9	3.9
[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.10	3.10

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.11	3.11
[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.12	3.12
[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.13	3.13
[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报	不支持 – 手动检查	不支持 – 手动检查	4.14	3.14
[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录	3.3	3.3	3.5	2.5
[EC2.2] VPC 默认安全组不应允许入站或出站流量	5.5	5.4	5.3	4.3
[EC2.6] 应在所有 VPC 中启用 VPC 流量记录	3.7	3.7	3.9	2.9
[EC2.7] 应启用 EBS 默认加密	5.1.1	2.2.1	2.2.1	不支持
[EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)	5.7	5.6	不支持	不支持
[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22	不支持 – 替换为要求 5.3 和 5.4	不支持 – 替换为要求 5.2 和 5.3	不支持 – 替换为要求 5.2 和 5.3	4.1

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389	不支持 – 替换为要求 5.3 和 5.4	不支持 – 替换为要求 5.2 和 5.3	不支持 – 替换为要求 5.2 和 5.3	4.2
[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389	5.2	5.1	5.1	不支持
[EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口	5.3	5.2	不支持	不支持
[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口	5.4	5.3	不支持	不支持
[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS	2.3.1	2.4.1	不支持	不支持
[EFS.8] 应对 EFS 文件系统进行静态加密	2.3.1	不支持	不支持	不支持
[IAM.1] IAM policy 不应允许完整的“*”管理权限	不支持	不支持	1.16	1.22
[IAM.2] IAM 用户不应附加 IAM policy	1.14	1.15	不支持	1.16
[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次	1.13	1.14	1.14	1.4
[IAM.4] 不应存在 IAM 根用户访问密钥	1.3	1.4	1.4	1.12

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA	1.9	1.10	1.10	1.2
[IAM.6] 应该为根用户启用硬件 MFA	1.5	1.6	1.6	1.14
[IAM.8] 应移除未使用的 IAM 用户凭证	不支持 – 改为参阅 [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证	不支持 – 改为参阅 [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证	不支持 – 改为参阅 [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证	1.3
[IAM.9] 应为根用户启用 MFA	1.4	1.5	1.5	1.13
[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	1.5
[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	1.6
[IAM.13] 确保 IAM 密码策略要求包含至少一个符号	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	1.7
[IAM.14] 确保 IAM 密码策略要求包含至少一个数字	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	1.8
[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14	1.7	1.8	1.8	1.9
[IAM.16] 确保 IAM 密码策略阻止重复使用密码	1.8	1.9	1.9	1.10
[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	1.11

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[IAM.18] 确保已创建支持角色来管理事件 AWS 支持	1.16	1.17	1.17	1.2
[IAM.20] 避免使用根用户	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	不支持 – CIS 删除了此要求	1.1
[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证	1.11	1.12	1.12	不支持 – CIS 在更高版本中添加了此要求
[IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书	1.18	1.19	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess	1.21	1.22	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[IAM.28] 应启用 IAM Access Analyzer 外部访问分析器	1.19	1.20	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[KMS.4] 应启用 AWS KMS 密钥轮换	3.6	3.6	3.8	2.8
[Macie.1] 应启用 Amazon Macie	不支持 – 手动检查	不支持 – 手动检查	不支持 – 手动检查	不支持 – 手动检查
[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置	2.2.3	2.3.3	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[RDS.3] RDS 数据库实例应启用静态加密	2.2.1	2.3.1	2.3.1	不支持 – CIS 在更高版本中添加了此要求

控件 ID 和标题	CIS v5.0.0 要求	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[RDS.5] RDS 数据库实例应配置多个可用区	2.2.4	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[RDS.13] 应启用 RDS 自动次要版本升级	2.2.2	2.3.2	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[RDS.15] 应为多个可用区配置 RDS 数据库集群	2.2.4	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求	不支持 – CIS 在更高版本中添加了此要求
[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置	2.1.4	2.1.4	2.1.5	不支持 – CIS 在更高版本中添加了此要求
[S3.5] S3 通用存储桶应需要请求才能使用 SSL	2.1.1	2.1.1	2.1.2	不支持 – CIS 在更高版本中添加了此要求
[S3.8] S3 通用存储桶应屏蔽公共访问权限	2.1.4	2.1.4	2.1.5	不支持 – CIS 在更高版本中添加了此要求
[S3.20] S3 通用存储桶应启用 MFA 删除	2.1.2	2.1.2	2.1.3	不支持 – CIS 在更高版本中添加了此要求

CIS 的 ARN AWS 基金会基准

启用一个或多个版本的 CIS AWS 基金会基准测试后，您将开始收到 AWS 安全调查结果格式 (ASFF) 中的调查结果。在 ASFF 中，每个版本都使用以下 Amazon 资源名称（ARN）：

CIS AWS 基金会基准测试 v5.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/5.0.0
```

CIS AWS 基金会基准测试 v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

CIS AWS 基金会基准测试 v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

CIS AWS 基金会基准测试 v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

您可以使用 Security Hub CSPM API 的 GetEnabledStandards 操作找出已启用标准的 ARN。

前面的值与 StandardsArn 对应。但是，StandardsSubscriptionArn 是指在您通过在某个区域中调用 BatchEnableStandards 订阅标准时 Security Hub CSPM 创建的标准订阅资源。

> **Note**
>
> 启用 CIS AWS 基金会基准测试版本时，Security Hub CSPM 最多可能需要 18 小时才能为使用与其他已启用标准中的已启用控件相同的 AWS Config 服务关联规则的控件生成调查结果。有关生成控件调查发现的时间表的更多信息，请参阅有关运行安全检查的计划。

如果您启用了整合的控件调查发现，则调查发现字段会有所不同。有关这些区别的信息，请参阅 合并对 ASFF 字段和值的影响。有关控件调查发现样本，请参阅控件调查发现示例。

Security Hub CSPM 不支持的 CIS 要求

如上表所述，Security Hub CSPM并不支持每个版本的CIS AWS 基金会基准测试中的所有CIS要求。许多不受支持的要求只能通过查看 AWS 资源的状态手动评估。

Security Hub CSPM 中的 NIST SP 800-53 修订版 5

NIST 特别出版物 800-53 修订版 5（NIST SP 800-53 Rev. 5）是由美国国家标准与技术研究所（NIST）制定的网络安全与合规框架，该机构是该机构的一部分。 U.S商务部。该合规框架提供了一

系列安全和隐私要求，用于保护信息系统和关键资源的机密性、完整性和可用性。 U.S。联邦政府机构和承包商必须遵守这些要求以保护其系统和组织。私营机构也可以自愿将这些要求作为降低网络安全风险的指导框架。有关该框架及其要求的更多信息，请参阅 NIST 计算机安全资源中心中的 NIST SP 800-53 Rev. 5。

AWS Security Hub CSPM 提供的安全控制措施支持 NIST SP 800-53 修订版 5 要求的子集。这些控件会对某些 AWS 服务 资源执行自动安全检查。要启用和管理这些控件，您可以将 NIST SP 800-53 修订版 5 框架作为 Security Hub CSPM 中的标准启用。请注意，控件不支持需要手动检查的 NIST SP 800-53 修订版 5 要求。

与其他框架不同，NIST SP 800-53 修订版 5 框架没有规定如何评估其要求。相反，该框架提供了指南。在 Security Hub CSPM 中，NIST SP 800-53 修订版 5 标准和控件代表了该服务对这些指南的理解。

主题

- 为适用于标准的控件配置资源记录
- 确定哪些控件适用于标准

为适用于标准的控件配置资源记录

为了优化覆盖范围和结果的准确性，在 Sec AWS urity Hub CSPM 中启用 NIST SP 800-53 修订版 5 标准 AWS Config 之前，在中启用和配置资源记录非常重要。配置资源记录时，还要确保为所有类型的 AWS 资源启用该功能，这些资源由适用于标准的控件进行检查。这主要适用于具有变更已触发计划类型的控件。但是，某些具有定期计划类型的控件也需要资源记录。如果未正确启用或配置资源记录，Security Hub CSPM 可能无法评估适当的资源，也无法针对适用于标准的控件生成准确的调查发现。

有关 Security Hub CSPM 如何在中使用资源记录的信息 AWS Config，请参阅。启用和配置 AWS Config 适用于 Security Hub CSPM有关在中配置资源记录的信息 AWS Config，请参阅《AWS Config 开发人员指南》中的使用配置记录器。

下表指定了适用于 Security Hub CSPM 中的 NIST SP 800-53 修订版 5 标准的控件要记录的资源类型。

AWS 服务	资源类型
Amazon API Gateway	`AWS::ApiGateway::Stage` ，`AWS::ApiGatewayV2::Stage`

AWS 服务	资源类型
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
亚马逊 CloudFront	AWS::CloudFront::Distribution
亚马逊 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

AWS 服务	资源类型
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`
亚马逊 ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
亚马逊 EventBridge	`AWS::Events::Endpoint` ，`AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (IAM)	`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`

AWS 服务	资源类型
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`
亚马逊 OpenSearch 服务	`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`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

AWS 服务	资源类型
亚马逊 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`

确定哪些控件适用于标准

以下列表列出了支持 NIST SP 800-53 修订版 5 要求并适用于 Security Hub CSPM 中的 NIST SP 800-53 修订版 5 标准的控件。 AWS 有关控件支持的特定要求的详细信息，请选择该控件。然后参阅控件详细信息中的相关要求字段。此字段指定控件支持的每个 NIST 要求。如果该字段未指定特定 NIST 要求，则控件不支持该要求。

- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [APIGateway.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 跟踪
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.5] API Gateway REST API 缓存数据应进行静态加密
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [Autoscaling.5] 使用 Auto Scaling 组启动配置启动的 EC2 亚马逊实例不应具有公有 IP 地址
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
- [CloudTrail.2] CloudTrail 应该启用静态加密
- [CloudTrail.4] 应启用 CloudTrail 日志文件验证
- [CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.1] DynamoDB 表应根据需求自动扩展容量
- [DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.1] 不应将 Amazon EBS 快照配置为可公开还原
- [EC2.2] VPC 默认安全组不应允许入站或出站流量
- [EC2.3] 附加的 Amazon EBS 卷应在静态状态下进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.6] 应在所有 VPC 中启用 VPC 流量记录
- [EC2.7] 应启用 EBS 默认加密
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)

- [EC2.9] 亚马逊 EC2 实例不应有公有 IPv4 地址
- [EC2.10] 应将 Amazon EC2 配置为使用为亚马逊 EC2 服务创建的 VPC 终端节点
- [EC2.12] 应移除未使用的 Amazon EC2 EIP
- [EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.19] 安全组不应允许不受限制地访问高风险端口
- [EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.2] ECS 服务不应自动分配公有 IP 地址
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限

- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EKS.1] EKS 集群终端节点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.8] EKS 集群应启用审核日志
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.4] 应将应用程序负载均衡器配置为丢弃无效的 http 标头
- [ELB.5] 应启用应用程序和经典负载均衡器日志记录
- [ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护

- [ELB.7] 经典负载均衡器应启用连接耗尽功能
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.9] 经典负载均衡器应启用跨区域负载均衡器
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不应公开访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [ES.5] Elasticsearch 域应启用审核日志
- [ES.6] Elasticsearch 域名应至少有三个数据节点
- [ES.7] 应将 Elasticsearch 域配置为至少三个专用主节点
- [ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.1] GuardDuty 应该启用
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- AWS KMS keys 不应无意中删除 [KMS.3]
- [KMS.4] 应启用 AWS KMS 密钥轮换
- [Lambda.1] Lambda 函数策略应禁止公众访问
- [Lambda.2] Lambda 函数应使用支持的运行时
- [Lambda.3] Lambda 函数应位于 VPC 中
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份

- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [RDS.1] RDS 快照应该是私有的
- [RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置
- [RDS.3] RDS 数据库实例应启用静态加密
- [RDS.4] RDS 集群快照和数据库快照应在静态时加密
- [RDS.5] RDS 数据库实例应配置多个可用区
- [RDS.6] 应为 RDS 数据库实例配置增强监控
- [RDS.7] RDS 集群应启用删除保护

- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.9] RDS 数据库实例应将日志发布到 CloudWatch 日志
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.11] RDS 实例应启用自动备份
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 Aurora 数据库集群配置为将标签复制到数据库快照
- [RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照
- [RDS.19] 应为关键群集事件配置现有 RDS 事件通知订阅
- [RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅
- [RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅
- [RDS.22] 应为关键的数据库安全组事件配置 RDS 事件通知订阅
- [RDS.23] RDS 实例不应使用数据库引擎的默认端口
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.4] Amazon Redshift 集群应启用审核日志记录
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由

- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置
- [S3.2] S3 通用存储桶应阻止公共读取访问权限
- [S3.3] S3 通用存储桶应阻止公共写入访问权限
- [S3.5] S3 通用存储桶应需要请求才能使用 SSL
- [S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.8] S3 通用存储桶应屏蔽公共访问权限
- [S3.9] S3 通用存储桶应启用服务器访问日志记录
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.14] S3 通用存储桶应启用版本控制
- [S3.15] S3 通用存储桶应启用对象锁定
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SecretsManager.1] Secrets Manager 密钥应启用自动轮换
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥

- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch

Security Hub CSPM 中的 NIST SP 800-171 修订版 2

NIST 特别出版物 800-171 修订版 2（NIST SP 800-171 Rev. 2）是由美国国家标准与技术研究所（NIST）制定的网络安全与合规框架，该机构是该机构的一部分。 U.S商务部。该合规框架提供了建议的安全要求，用于保护不属于联邦政府的系统和组织中受控非机密信息的机密性 U.S。受控非机密信息（也称为 CUI）是不符合政府保密标准但必须受到保护的敏感信息。这些信息被认为是敏感的，由联邦政府 U.S或其他实体代表联邦政府创建或持有 U.S。

NIST SP 800-171 Rev. 2 提供了针对以下情况下保护 CUI 机密性的建议安全要求：

- 该信息存在于非联邦系统和组织中，

- 非联邦组织未代表联邦机构收集或维护信息，也未代表联邦机构使用或运营系统，并且
- 对于 CUI Registry 中列出的 CUI 类别，授权法律、法规或政府范围内的政策没有规定保护 CUI 机密性的具体保障要求。

这些要求适用于处理、存储或传输 CUI 或者为组件提供安全保护的非联邦系统和组织的所有组件。有关更多信息，请参阅 NIST 计算机安全资源中心中的 NIST SP 800-171 Rev. 2。

AWS Security Hub CSPM 提供的安全控制措施支持 NIST SP 800-171 修订版 2 要求的子集。这些控件会对某些 AWS 服务 资源执行自动安全检查。要启用和管理这些控件，您可以将 NIST SP 800-171 修订版 2 框架作为 Security Hub CSPM 中的标准启用。请注意，控件不支持需要手动检查的 NIST SP 800-171 修订版 2 要求。

主题

- 为适用于标准的控件配置资源记录
- 确定哪些控件适用于标准

为适用于标准的控件配置资源记录

为了优化覆盖范围和结果的准确性，在 Sec AWS urity Hub CSPM 中启用 NIST SP 800-171 修订版 2 标准 AWS Config 之前，在中启用和配置资源记录非常重要。配置资源记录时，还要确保为所有类型的 AWS 资源启用该功能，这些资源由适用于标准的控件进行检查。否则，Security Hub CSPM 可能无法评估适当的资源，也无法针对适用于标准的控件生成准确的调查发现。

有关 Security Hub CSPM 如何在中使用资源记录的信息 AWS Config，请参阅。启用和配置 AWS Config 适用于 Security Hub CSPM有关在中配置资源记录的信息 AWS Config，请参阅《AWS Config 开发人员指南》中的使用配置记录器。

下表指定了适用于 Security Hub CSPM 中的 NIST SP 800-171 修订版 2 标准的控件要记录的资源类型。

AWS 服务	资源类型
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
亚马逊 CloudFront	`AWS::CloudFront::Distribution`

AWS 服务	资源类型
亚马逊 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`
AWS Identity and Access Management (IAM)	`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`

确定哪些控件适用于标准

以下列表列出了支持 NIST SP 800-171 修订版 2 要求并适用于 Security Hub CSPM 中的 NIST SP 800-171 修订版 2 标准的控件。 AWS 有关控件支持的特定要求的详细信息，请选择该控件。然后参阅控件详细信息中的相关要求字段。此字段指定控件支持的每个 NIST 要求。如果该字段未指定特定 NIST 要求，则控件不支持该要求。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudTrail.2] CloudTrail 应该启用静态加密
- [CloudTrail.3] 应至少启用一条 CloudTrail 跟踪
- [CloudTrail.4] 应启用 CloudTrail 日志文件验证
- [CloudWatch.1] “root” 用户应有日志指标筛选器和警报
- [CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报
- [CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报
- [CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报
- [CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报
- [CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
- [CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报
- [CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报
- [CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
- [CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
- [CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
- [CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
- [CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [EC2.6] 应在所有 VPC 中启用 VPC 流量记录
- [EC2.10] 应将 Amazon EC2 配置为使用为亚马逊 EC2 服务创建的 VPC 终端节点
- [EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.19] 安全组不应允许不受限制地访问高风险端口
- [EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

- [GuardDuty.1] GuardDuty 应该启用
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [S3.5] S3 通用存储桶应需要请求才能使用 SSL
- [S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户
- [S3.9] S3 通用存储桶应启用服务器访问日志记录
- [S3.11] S3 通用存储桶应启用事件通知
- [S3.14] S3 通用存储桶应启用版本控制
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch

Security Hub CSPM 中的 PCI DSS

支付卡行业数据安全标准（PCI DSS）是一个第三方合规框架，它提供了一套安全处理信用卡和借记卡信息的规则和指南。PCI 安全标准委员会（SSC）负责创建并更新此框架。

AWS Security Hub CSPM 提供了 PCI DSS 标准，可以帮助您保持对该第三方框架的合规性。您可以使用此标准来发现处理持卡人数据的 AWS 资源中的安全漏洞。建议在有资源存储、处理或传输持卡人数据或敏感的身份验证数据的 AWS 账户 中启用此标准。PCI SSC 的评测验证此标准。

Security Hub CSPM 同时支持 PCI DSS v3.2.1 和 PCI DSS v4.0.1。建议使用 v4.0.1 以了解最新的安全最佳实践。您可以同时启用两个版本的标准。有关启用标准的信息，请参阅启用安全标准。如果您当前使用的是 v3.2.1 版本，但只想使用 v4.0.1 版本，请先启用较新的版本，然后再禁用较旧的版本。这可以防止您的安全检查出现漏洞。如果您将 Security Hub CSPM 与集成一起使用， AWS Organizations 并希望在多个账户中批量启用 v4.0.1，我们建议您使用集中配置来实现此目的。

以下部分指定了哪些控件适用于 PCI DSS v3.2.1 和 PCI DSS v4.0.1。

适用于 PCI DSS v3.2.1 的控件

以下列表指定了哪些 Security Hub CSPM 控件适用于 PCI DSS v3.2.1。要查看控件的详细信息，请选择该控件。

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

[CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

[DMS.1] Database Migration Service 复制实例不应公开

[EC2.1] 不应将 Amazon EBS 快照配置为可公开还原

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

[EC2.12] 应移除未使用的 Amazon EC2 EIP

[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

[ES.1] Elasticsearch 域应启用静态加密

[ES.2] Elasticsearch 域名不应公开访问

[GuardDuty.1] GuardDuty 应该启用

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.9] 应为根用户启用 MFA

[IAM.10] IAM 用户的密码策略应具有很强的配置

[IAM.19] 应为所有 IAM 用户启用 MFA

[KMS.4] 应启用 AWS KMS 密钥轮换

[Lambda.1] Lambda 函数策略应禁止公众访问

[Lambda.3] Lambda 函数应位于 VPC 中

[Opensearch.1] OpenSearch 域名应启用静态加密

[Opensearch.2] OpenSearch 域名不应向公众开放

[RDS.1] RDS 快照应该是私有的

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

[Redshift.1] Amazon Redshift 集群应禁止公共访问

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

[S3.2] S3 通用存储桶应阻止公共读取访问权限

[S3.3] S3 通用存储桶应阻止公共写入访问权限

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

[S3.7] S3 通用存储桶应使用跨区域复制

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

适用于 PCI DSS v4.0.1 的控件

以下列表指定了哪些 Security Hub CSPM 控件适用于 PCI DSS v4.0.1。要查看控件的详细信息，请选择该控件。

[ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度

[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

[AppSync.2] AWS AppSync 应该启用字段级日志记录

[AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)

[Autoscaling.5] 使用 Auto Scaling 组启动配置启动的 EC2 亚马逊实例不应具有公有 IP 地址

[CloudFront.1] CloudFront 发行版应配置默认根对象

[CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

[CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

[CloudFront.5] CloudFront 发行版应启用日志记录

[CloudFront.6] CloudFront 发行版应启用 WAF

[CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

[DMS.1] Database Migration Service 复制实例不应公开

[DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权

[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

[DMS.12] Redis OSS 的 DMS 端点应启用 TLS

[DMS.6] DMS 复制实例应启用自动次要版本升级

[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录

[DMS.8] 源数据库的 DMS 复制任务应启用日志记录

[DMS.9] DMS 端点应使用 SSL

[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期

[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

[DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密

[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22

[EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389

[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址

[EC2.16] 应删除未使用的网络访问控制列表

[EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)

[EC2.171] EC2 VPN 连接应启用日志记录

[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389

[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

[EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录

[EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口

[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)

[ECR.1] ECR 私有存储库应配置图像扫描

[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行

[ECS.16] ECS 任务集不应自动分配公有 IP 地址

[ECS.2] ECS 服务不应自动分配公有 IP 地址

[ECS.8] 密钥不应作为容器环境变量传递

[EFS.4] EFS 接入点应强制使用用户身份

[EKS.1] EKS 集群终端节点不应公开访问

[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行

[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

[EKS.8] EKS 集群应启用审核日志

[ElastiCache.2] ElastiCache 集群应启用自动次要版本升级

[ElastiCache.5] ElastiCache 复制组在传输过程中应加密

[ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证

[ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新

[ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch

[ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止

[ELB.4] 应将应用程序负载均衡器配置为丢弃无效的 http 标头

[ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置

[ES.2] Elasticsearch 域名不应公开访问

[ES.3] Elasticsearch 域应加密节点之间发送的数据

[ES.5] Elasticsearch 域应启用审核日志

[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密

[EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

[GuardDuty.1] GuardDuty 应该启用

[GuardDuty.10] 应启用 GuardDuty S3 保护

[GuardDuty.6] 应启用 Lamb GuardDuty da 保护

[GuardDuty.7] 应启用 GuardDuty EKS 运行时监控

[GuardDuty.9] 应启用 GuardDuty RDS 保护

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.7] IAM 用户的密码策略应具有可靠的配置

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.9] 应为根用户启用 MFA

[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母

[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母

[IAM.14] 确保 IAM 密码策略要求包含至少一个数字

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效

[IAM.18] 确保已创建支持角色来管理事件 AWS 支持

[IAM.19] 应为所有 IAM 用户启用 MFA

[Inspector.1] 应启用 Amazon Inspector EC2 扫描

[Inspector.2] 应启用 Amazon Inspector ECR 扫描

[Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描

[Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描

[KMS.4] 应启用 AWS KMS 密钥轮换

[Lambda.1] Lambda 函数策略应禁止公众访问

[Lambda.2] Lambda 函数应使用支持的运行时

[MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch

[MSK.1] MSK 集群应在代理节点之间传输时进行加密

[MSK.3] MSK Connect 连接器应在传输过程中进行加密

[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

[Neptune.3] Neptune 数据库集群快照不应公开

[Opensearch.10] OpenSearch 域名应安装最新的软件更新

[Opensearch.5] OpenSearch 域应启用审核日志

[RDS.13] 应启用 RDS 自动次要版本升级

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

[RDS.22] 应为关键的数据库安全组事件配置 RDS 事件通知订阅

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志

[RDS.35] RDS 数据库集群应启用自动次要版本升级

[RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch

[RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch

[RDS.9] RDS 数据库实例应将日志发布到 CloudWatch 日志

[Redshift.1] Amazon Redshift 集群应禁止公共访问

[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

[Redshift.4] Amazon Redshift 集群应启用审核日志记录

[Route53.2] Route 53 公有托管区域应记录 DNS 查询

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

[S3.15] S3 通用存储桶应启用对象锁定

[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys

[S3.19] S3 接入点已启用屏蔽公共访问权限设置

[S3.22] S3 通用存储桶应记录对象级写入事件

[S3.23] S3 通用存储桶应记录对象级读取事件

[S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

[S3.8] S3 通用存储桶应屏蔽公共访问权限

[S3.9] S3 通用存储桶应启用服务器访问日志记录

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

[SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

[StepFunctions.1] Step Functions 状态机应该开启日志功能

[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

[WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录

[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

Service-managed Security Hub CSPM 中的标准

服务管理标准是其他人管理的安全标准，但您可以在 AWS 服务 Security Hub CSPM 中查看该标准。例如，Service-Managed 标准： AWS Control Tower是一种管理的服务 AWS Control Tower 管理标准。服务托管标准与 AWS Security Hub CSPM 托管的安全标准在以下方面有所不同：

- 标准创建和删除——您可以使用托管服务的控制台或 API 或使用 AWS CLI创建和删除服务托管标准。在您通过其中一种方式在管理服务中创建标准之前，该标准不会出现在 Security Hub CSPM 控制台中，也无法通过 Security Hub CSPM API 或 AWS CLI进行访问。
- 不自动启用控件 – 创建服务托管标准时，Security Hub CSPM 和管理服务不会自动启用适用于该标准的控件。此外，当 Security Hub CSPM 发布标准的新控件时，新控件不会自动启用。这与 Security Hub CSPM 管理的标准有所不同。有关在 Security Hub CSPM 中配置控件的常用方法的更多信息，请参阅了解 Security Hub CSPM 中的安全控件。
- 启用和禁用控件——我们建议在托管服务中启用和禁用控件，以避免出现偏差。
- 控件的可用性——托管服务选择哪些控件可作为服务托管标准的一部分。可用控件可能包括所有或部分现有的 Security Hub CSPM 控件。

管理服务创建服务托管标准并为其提供控件后，您可以在 Security Hub CSPM 控制台、Security Hub CSPM API 或 AWS CLI中访问控件调查发现、控件状态和标准安全分数。在托管服务中也可能提供部分或全部信息。

从以下列表中选择服务托管标准可查看有关它的更多详细信息。

Service-managed 标准

- Service-Managed 标准： AWS Control Tower

Service-Managed 标准： AWS Control Tower

本节提供有关 Service-Managed 标准的信息: AWS Control Tower.

什么是 Service-Managed 标准： AWS Control Tower?

Service-Managed 标准： AWS Control Tower 是一种服务托管标准， AWS Control Tower 用于管理支持 Security Hub 控件的子集。该标准专为 Sec AWS urity Hub CSPM 和. AWS Control Tower它允许你通过服务配置 Security Hub CSPM 的侦探控件。 AWS Control Tower

侦探控件可检测您 AWS 账户内部的资源不合规（例如，错误配置）。

> **Tip**
>
> Service-managed 标准与 Sec AWS urity Hub CSPM 管理的标准不同。例如，您必须在托管服务中创建和删除服务托管标准。有关更多信息，请参阅 Service-managed Security Hub CSPM 中的标准。

当你通过启用 Security Hub CSPM 控件时 AWS Control Tower，Control Tower 还会在这些特定账户和区域中为你启用 Security Hub CSPM（如果尚未启用）。在 Security Hub CSPM 控制台和 API 中，在启用 Service-Managed 标准后，您可以查看 “标准： AWS Control Tower 以及其他 Security Hub CSPM 标准”。 AWS Control Tower

有关此标准的更多信息，请参阅《AWS Control Tower 用户指南》中的 Security Hub CSPM 控件。

创建标准

只有从中启用 Security Hub CSPM 控件时，此标准才在 Security Hub CSPM 中可用。 AWS Control Tower AWS Control Tower 使用以下方法之一首次启用适用的控件时创建标准：

- AWS Control Tower 控制台
- AWS Control Tower API（调用 `EnableControl`API）
- AWS CLI （运行`enable-control`命令）

当你通过启用 Security Hub CSPM 控件时 AWS Control Tower，如果你尚未启用 Security Hub CSPM，还可以在这些特定的账户和区域中为你启用 S AWS Control Tower ecurity Hub CSPM。

要通过控制目录中的控件 ID 识别 Security Hub CSPM 控件，可以使用中的字段`Implementation.Identifier`。 AWS Control Tower此字段映射到 Security Hub CSPM 控件 ID，可用于筛选特定的控件 ID。要检索中特定 Security Hub CSPM 控件（比如 CodeBuild.1 “”）的控件元数据 AWS Control Tower，可以使用 API：`ListControls`

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

您无法在 Security Hub CSPM 控制台、Security Hub CSPM API 中查看或访问此标准，也 AWS CLI 无法 AWS Control Tower 使用上述方法之一先设置和启用 S AWS Control Tower ecurity Hub CSPM 控件。

该标准仅在可用AWS 区域 的地方可 AWS Control Tower 用。

在标准中启用和禁用控件

通过启用 Security Hub CSPM 控件 AWS Control Tower 并创建 Service-Managed 标准： AWS Control Tower 标准后，您可以在 Security Hub CSPM 中查看该标准及其可用控件。

当 Security Hub CSPM 在 “ Service-Managed 标准： AWS Control Tower 标准” 中添加新控件时，启用标准的客户不会自动启用这些控件。您应使用以下方法之一启用和禁用标准控件： AWS Control Tower

- AWS Control Tower 控制台
- AWS Control Tower API（调用EnableControl和 DisableControlAPI）
- AWS CLI （运行enable-control和disable-control命令）

当您在中更改控件的启用状态时 AWS Control Tower，更改也会反映在 Security Hub CSPM 中。

但是，在 Security Hub CSPM 中禁用已启用的控件会 AWS Control Tower 导致控制偏差。中的控件状态 AWS Control Tower 显示为Drifted。您可以使用 ResetEnabledControlAPI 重置处于偏移状态的控件，或者在控制 AWS Control Tower 台中选择 Re-register OU，或者 AWS Control Tower 使用上述方法之一禁用并重新启用控件，从而解决这种偏差。

在中完成启用和禁用操作 AWS Control Tower 可帮助您避免控制偏差。

当您在中启用或禁用控件时 AWS Control Tower，该操作将应用于受控制的账户和区域 AWS Control Tower。如果您在 Security Hub CSPM 中启用和禁用控件（不建议在本标准中使用），则该操作仅适用于当前账户和区域。

> **Note**
>
> 无法使用@@ 中央配置来管理 Service-Managed 标准: AWS Control Tower。在本标准中，您只能使用该 AWS Control Tower 服务来启用和禁用控件。

查看启用状态和控件状态

您可以使用以下方法之一查看控件的启用状态：

- Security Hub CSPM 控制台、Security Hub CSPM API 或 AWS CLI

- AWS Control Tower 控制台
- AWS Control Tower 用于查看已启用控件列表的 API（调用 ListEnabledControlsAPI）
- AWS CLI 查看已启用的控件列表（运行list-enabled-controls命令）

除非您在 Security Hub CSPM 中 AWS Control Tower 明确启用该控件，否则您在Disabled中禁用的控件在 Security Hub CSPM 中的启用状态为。

Security Hub CSPM 根据控件调查发现的工作流状态和合规性状态来计算控件状态。有关启用状态和控件状态的更多信息，请参阅 查看 Security Hub CSPM 中的控件的详细信息。

根据控制状态，Security Hub CSPM 计算标准版的安全分数：。 Service-Managed AWS Control Tower此分数仅在 Security Hub CSPM 中可用。此外，您只能在 Security Hub CSPM 中查看控件调查发现。中没有标准安全评分和控制结果 AWS Control Tower。

> **Note**
>
> 启用 Service-Managed 标准:控件后 AWS Control Tower，Security Hub CSPM 最多可能需要 18 小时才能为使用现有 AWS Config 服务关联规则的控件生成调查结果。如果您在 Security Hub CSPM 中启用了其他标准和控件，则可能已有服务相关规则。有关更多信息，请参阅 有关运行安全检查的计划。

删除标准

您可以使用以下方法之一禁用所有适用的控件， AWS Control Tower 从而在中删除此服务托管标准：

- AWS Control Tower 控制台
- AWS Control Tower API（调用 DisableControlAPI）
- AWS CLI （运行disable-control命令）

禁用所有控件会删除 AWS Control Tower中所有托管账户和受管辖区域中的标准。 AWS Control Tower 删除中的标准会将其从 Security Hub CSPM 控制台的 “标准” 页面中删除，并且您将无法再使用 Security Hub CSPM API 或访问该标准。 AWS CLI

> **Note**
>
> 在 Security Hub CSPM 中禁用标准中的所有控件并不能禁用或删除该标准。

禁用 Security Hub CSPM 服务会移除 Service-Managed Stand AWS Control Tower ard: 以及您已启用的任何其他标准。

Service-Managed 标准版的查找字段格式： AWS Control Tower

当你创建 Service-Managed Standar AWS Control Tower d: 并为其启用控件时，你将开始在 Security Hub CSPM 中收到控制结果。Security Hub CSPM 以 AWS 安全调查结果格式 (ASFF) 报告控件调查发现。以下是本标准的 Amazon 资源名称（ARN）的 ASFF 值，以及 `GeneratorId`：

- 标准 ARN——*`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`*

有关 Service-Managed 标准:的调查结果示例 AWS Control Tower，请参阅控件调查发现示例。

适用于 Service-Managed 标准版的控件： AWS Control Tower

Service-Managed 标准： AWS Control Tower 支持 AWS 基础安全最佳实践 (FSBP) 标准中的一部分控件。选择一个控件以查看有关该控件的信息，包括失败的调查发现的补救步骤。

要查看支持哪些 Security Hub CSPM 控件 AWS Control Tower，您可以使用以下方法之一：

- AWS 控制目录控制台，您可以在其中进行筛选 “`Control owner = AWS Security Hub`”
- AWS 控制目录 API（调用 `ListControls`API），其中包含`Implementations`要检查`Types`的过滤器 `AWS::SecurityHub::SecurityControl`
- AWS CLI（运行`list-controls`命令），并使用过滤器`Implementations`。示例 CLI 命令：

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

通过 Control Tower 标准启用时，对 Security Hub CSPM 控件的区域限制可能与底层控件的区域限制不一致。

在 Security Hub CSPM 中，如果在您的账户中关闭了合并控制结果，则生成的调查结果中的`ProductFields.ControlId`字段将使用基于标准的控制 ID。基于标准的对照 ID 的格式为 CT。***`ControlId`***（例如，CT.CodeBuild.1）。

有关此标准的更多信息，请参阅《AWS Control Tower 用户指南》中的 Security Hub CSPM 控件。

启用安全标准

当你在 Security Hub CSPM 中启用 AWS 安全标准时，Security Hub CSPM 会自动创建并启用适用于该标准的所有控件。Security Hub CSPM 还会开始运行安全检查，并生成控件的调查发现。

要优化覆盖范围和结果的准确性，请在启用标准 AWS Config 之前在中启用和配置资源记录。在配置资源记录时，还要确保为适用于标准的控件检查的所有 资源类型启用它。否则，Security Hub CSPM 可能无法评估适当的资源，也无法针对适用于标准的控件生成准确的调查发现。有关更多信息，请参阅启用和配置 AWS Config 适用于 Security Hub CSPM。

启用某个标准后，您可以禁用或稍后重新启用适用于该标准的各个控件。如果禁用某个标准的控件，Security Hub CSPM 将停止为该控件生成调查发现。此外，Security Hub CSPM 在计算标准的安全分数时会忽略该控件。安全分数是指通过评估的控件占适用于标准、已启用且具有评估数据的控件总数的百分比。

启用某个标准后，Security Hub CSPM 会在您首次访问 Security Hub CSPM 控制台上的摘要或安全标准页面后 30 分钟内生成该标准的初步安全分数。仅针对您访问控制台上的这些页面时启用的标准生成安全分数。此外，必须在中 AWS Config 配置资源记录才能显示分数。在中国地区 AWS GovCloud (US) Regions和，Security Hub CSPM 最多可能需要 24 小时才能生成标准的初步安全评分。在 Security Hub CSPM 生成初步分数后，每 24 小时更新一次分数。要确定安全分数上次更新的时间，您可以参考 Security Hub CSPM 提供的分数时间戳。有关更多信息，请参阅 计算安全分数。

如何启用标准取决于您是否使用中心配置来管理多个账户和 AWS 区域的 Security Hub CSPM。如果要在多账户、多区域环境中启用标准，我们建议使用中心配置。如果您将 Security Hub CSPM 与集成，则可以使用中央配置。 AWS Organizations如果不使用中心配置，则必须在每个帐户和每个区域中分别启用每个标准。

主题

- 在多个账户中启用标准和 AWS 区域
- 在单个账户中启用标准版和 AWS 区域
- 检查标准的状态

在多个账户中启用标准和 AWS 区域

要跨多个账户启用和配置安全标准 AWS 区域，请使用集中配置。通过中心配置，受委派的 Security Hub CSPM 管理员可以创建 Security Hub CSPM 配置策略，以启用一个或多个标准。然后，管理员可以将配置策略与单个帐户、组织单元（OU）或根帐户关联起来。配置策略会影响主区域（也称为聚合区域）以及所有关联区域。

配置策略提供自定义选项。例如，您可以选择仅为一个 OU 启用 AWS 基础安全最佳实践 (FSBP) 标准。对于另一个 OU，您可以选择同时启用 FSBP 标准和互联网安全中心 (CIS) AWS 基金会基准 v1.4.0 标准。有关如何创建启用您指定的特定标准的配置策略的信息，请参阅创建和关联配置策略。

如果您使用中心配置，Security Hub CSPM 不会在新账户或现有账户中自动启用任何标准。相反，Security Hub CSPM 管理员在为其组织创建 Security Hub CSPM 配置策略时，会指定要在不同的账户中启用哪些标准。Security Hub CSPM 提供了一种推荐的配置策略，其中仅启用 FSBP 标准。有关更多信息，请参阅 配置策略的类型。

> **Note**
>
> Security Hub CSPM 管理员可以使用配置策略启用除 AWS Control Tower 服务托管标准之外的任何标准。要启用此标准，管理员必须 AWS Control Tower 直接使用。他们还必须使用 AWS Control Tower 此标准为集中管理的账户启用或禁用个人控件。

如果您希望某些账户为自己的账户启用和配置标准，Security Hub CSPM 管理员可以将这些账户指定为自我管理的帐户。 Self-managed 账户必须在每个地区分别启用和配置标准。

在单个账户中启用标准版和 AWS 区域

如果不使用中心配置或您有自行管理账户，则无法使用配置策略在多个账户或 AWS 区域中集中启用安全标准。但是，您可以在单个账户和区域中启用标准。您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API 执行此操作。

Security Hub CSPM console

按照以下步骤使用 Security Hub CSPM 控制台在一个账户和区域中启用标准。

要在一个账户和区域中启用标准

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 使用页面右上角的选择 AWS 区域 器，选择要启用该标准的区域。
3. 在导航窗格中，选择安全标准。安全标准页面列出了 Security Hub CSPM 目前支持的所有标准。如果您已经启用了某个标准，则该标准的部分将包含当前安全分数和该标准的更多详细信息。
4. 在要启用的标准的部分中，选择启用标准。

要在其他区域启用该标准，请在每个其他区域中重复上述步骤。

Security Hub CSPM API

要在单个账户和区域中以编程方式启用标准，请使用 BatchEnableStandards 操作。或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该batch-enable-standards命令。

在您的请求中，使用 `StandardsArn` 参数指定要启用的标准的 Amazon 资源名称（ARN）。此外，请指定您的请求适用的区域。例如，以下命令启用 AWS 基础安全最佳实践 (FSBP) 标准：

```
$ 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
```

美国东部（弗吉尼亚北部）地区的 FSBP 标准的 ARN 在哪里*arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0*，*us-east-1*也是启用该标准的区域。

要获取标准的 ARN，请使用DescribeStandards操作，或者，如果您使用的是 AWS CLI，则运行命令。describe-standards

要查看您的账户中当前已启用的标准列表，可以使用 GetEnabledStandards 操作。如果您使用的是 AWS CLI，则可以运行 get-enabled-standards 命令来检索此列表。

启用某个标准后，Security Hub CSPM 将开始执行任务以在账户和指定的区域中启用该标准。这包括创建适用于该标准的所有控件。要监控这些任务的状态，您可以检查账户和区域中该标准的状态。

检查标准的状态

当您为某个账户启用安全标准时，Security Hub CSPM 会开始在账户中创建适用于该标准的所有控件。Security Hub CSPM 还会执行其他任务来为账户启用该标准，例如为该标准生成初步安全分数。当 Security Hub CSPM 执行这些任务时，该账户的标准的状态为 Pending。该标准的状态随后会经历其他状态，您可以监控和检查这些状态。

> **Note**
>
> 对标准的各个控件的更改不会影响标准的总体状态。例如，如果启用以前禁用的控件，则您的更改不会影响标准的状态。同样，如果更改已启用控件的参数值，则更改不会影响标准的状态。

要使用 Security Hub CSPM 控制台检查标准的状态，请在导航窗格中选择安全标准。安全标准页面列出了 Security Hub CSPM 目前支持的所有标准。如果 Security Hub CSPM 当前正在执行启用该标准的任务，则该标准的部分会指示 Security Hub CSPM 仍在为该标准生成安全分数。如果启用了某个标准，则该标准的部分将包括当前分数。选择查看结果以查看其他详细信息，包括适用于标准的各个控件的状态。有关更多信息，请参阅 有关运行安全检查的计划。

要使用 Security Hub CSPM API 以编程方式检查标准的状态，请使用 GetEnabledStandards 操作。在请求中，可以选择使用 `StandardsSubscriptionArns` 参数来指定要检查状态的标准的 Amazon 资源名称（ARN）。如果你使用的是 AWS Command Line Interface (AWS CLI)，你可以运行 get-enabled-standards 命令来检查标准的状态。要指定要检查的标准 ARN，请使用 `standards-subscription-arns` 参数。要确定要指定哪个 ARN，您可以使用DescribeStandards操作，或者为 AWS CLI运行命令。describe-standards

如果您的请求成功，Security Hub CSPM 将返回一个 `StandardsSubscription` 对象数组。标准订阅是 Security Hub CSPM 在为账户启用标准时在账户中创建的一种 AWS 资源。每个 `StandardsSubscription` 对象都提供有关为账户当前已启用、正在启用或禁用的标准的详细信息。在每个对象中，`StandardsStatus` 字段指定账户的标准的当前状态。

标准的状态（`StandardsStatus`）可以是以下之一。

PENDING

Security Hub CSPM 当前正在执行为该账户启用标准的任务。这包括创建适用于该标准的控件以及为该标准生成初步安全分数。Security Hub CSPM 完成所有任务可能需要几分钟时间。如果已经为账户启用了某个标准，并且 Security Hub CSPM 目前正在向该标准添加新控件，则该标准也可能具有此状态。

如果某个标准具有这种状态，您可能无法检索适用于该标准的各个控件的详细信息。此外，您可能无法为标准配置或禁用单个控件。例如，如果您尝试使用 UpdateStandardsControl 操作禁用控件，则会发生错误。

要确定是否可以配置或以其他方式管理标准的各个控件，请参考 `StandardsControlsUpdatable` 字段的值。如果此字段的值为 `READY_FOR_UPDATES`，则可以开始管理该标准的各个控件。否则，请等待 Security Hub CSPM 完成其他处理任务以启用该标准。

READY

目前已为账户启用该标准。Security Hub CSPM 可以运行安全检查，并针对适用于该标准且当前已启用的所有控件生成调查发现。Security Hub CSPM 还可以计算标准的安全分数。

如果某个标准具有这种状态，则可以检索适用于该标准的各个控件的详细信息。此外，您还可以配置、禁用或重新启用这些控件。您也可以禁用标准。

INCOMPLETE

Security Hub CSPM 无法为账户完全启用标准。Security Hub CSPM 无法运行安全检查并针对适用于该标准且当前已启用的所有控件生成调查发现。此外，Security Hub CSPM 无法计算标准的安全分数。

要确定为什么标准没有完全启用，请参考 `StandardsStatusReason` 数组中的信息。此数组指定了导致 Security Hub CSPM 无法启用标准的问题。如果发生内部错误，请尝试再次为账户启用标准。对于其他类型的问题，请检查您的 AWS Config 设置。您还可以禁用不需要检查的单个控件，也可以完全禁用标准。

DELETING

Security Hub CSPM 当前正在处理对账户禁用标准的请求。这包括禁用适用于标准的控件以及移除关联的安全分数。Security Hub CSPM 处理请求可能需要几分钟时间。

如果某个标准具有这种状态，则您无法为账户重新启用标准或再次尝试禁用它。Security Hub CSPM 必须首先完成对当前请求的处理。此外，您无法检索适用于标准的各个控件的详细信息，也无法管理这些控件。

FAILED

Security Hub CSPM 无法为账户禁用标准。Security Hub CSPM 尝试禁用标准时发生了一个或多个错误。此外，Security Hub CSPM 无法计算标准的安全分数。

要确定为什么标准没有完全禁用，请参考 `StandardsStatusReason` 数组中的信息。此数组指定了导致 Security Hub CSPM 无法禁用标准的问题。

如果某个标准具有这种状态，则无法检索适用于该标准的各个控件的详细信息，也无法管理这些控件。但是，您可以为账户重新启用标准。如果解决了导致 Security Hub CSPM 无法禁用标准的问题，则也可以再次尝试禁用标准。

如果某标准的状态为 `READY`，则 Security Hub CSPM 会运行安全检查，并针对适用于该标准且当前已启用的所有控件生成调查发现。对于其他状态，Security Hub CSPM 可能会对某些（但不是全部）已启用的控件运行检查并生成调查发现。生成或更新控件调查发现可能需要长达 24 小时。有关更多信息，请参阅 有关运行安全检查的计划。

查看安全标准的详细信息

在 Security Hub CSPM 中启用 AWS 安全标准后，您可以使用控制台查看该标准的详细信息。在 控制台上，标准的详细信息页面包含以下信息：

- 标准的当前安全分数。
- 适用于标准的控件表。
- 适用于标准的控件的聚合统计数据。
- 适用于标准的控件的状态的视觉摘要。
- 已启用并适用于标准的控件的安全检查的可视化摘要。如果您与集成 AWS Organizations，则在至少一个组织账户中启用的控件将被视为已启用。

要查看这些详细信息，请在控制台的导航窗格中选择安全标准。然后，在标准的部分中，选择查看结果。要进行更深入的分析，您可以对数据进行筛选和排序，然后深入查看适用于标准的各个控件的详细信息。

主题

- 了解标准安全分数
- 查看标准的控件

了解标准安全分数

在 Sec AWS urity Hub CSPM 控制台上，标准的详细信息页面显示该标准的安全分数。分数是指通过评估的控件占适用于标准、已启用且具有评估数据的控件总数的百分比。分数下方是一个图表，汇总了针对标准启用的控件的安全检查。这包括通过和未通过的安全检查数。对于管理员账户，标准分数和图表是在跨管理员账户和所有成员账户之间汇总的。要查看具有特定严重性的控件的未通过安全检查，请选择严重性。

启用某个标准后，Security Hub CSPM 会在您首次访问 Security Hub CSPM 控制台上的摘要页面或安全标准页面后 30 分钟内生成该标准的初步安全分数。仅针对您访问这些页面时启用的标准生成分数。此外，必须配置 AWS Config 资源记录才能显示分数。在中国地区 AWS GovCloud (US) Regions 和，Security Hub CSPM 最多可能需要 24 小时才能得出初步分数。Security Hub CSPM 生成标准的初步分数后，每 24 小时更新一次分数。有关更多信息，请参阅 计算安全分数。

AWS 区域 除非您设置聚合区域，否则安全标准详情页面上的所有数据均特定于当前数据。如果您设置了聚合区域，则安全分数适用于各个区域，并包括所有关联区域的调查发现。此外，控件的合规状态反映了关联区域的调查发现，安全检查的数量包括关联区域的调查发现。

查看标准的控件

当您使用 Sec AWS urity Hub CSPM 控制台查看已启用的标准的详细信息时，可以查看适用于该标准的安全控制表。对于每个控件，该表包含以下信息：

- 控件 ID 和标题。
- 控件的状态。有关更多信息，请参阅 评估合规性状态和控件状态。
- 分配给控件的严重性。
- 未通过检查数和检查总数。如果适用，未通过的检查字段还会指定状态为未知的调查发现数量。
- 控件是否支持自定义参数。有关更多信息，请参阅 了解 Security Hub CSPM 中的控件参数。

Security Hub CSPM 每 24 小时更新一次控件状态和安全检查计数。页面顶部的时间戳显示了 Security Hub CSPM 最近一次更新此数据的时间。

对于管理员账户，控件状态和安全检查数量按管理员账户和所有成员账户进行聚合。已启用控件计数包括在管理员账户或至少一个成员账户中为标准启用的控件。已禁用控件计数包括在管理员账户和所有成员账户中为标准禁用的控件。

您可以筛选适用于标准的控件表。使用表旁边的筛选依据选项，您可以选择仅查看已为标准启用或禁用的控件。如果仅显示已启用的控件，则可以按控件状态进一步筛选表。然后，您可以专注于具有特定控件状态的控件。除了筛选依据选项外，您还可以在筛选条件控件框中输入筛选条件。例如，您可以按控件 ID 或标题进行筛选。

选择首选访问方法。然后，按照步骤查看适用于已启用标准的控件。

Security Hub CSPM console

查看已启用标准的控件

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中选择安全标准。
3. 然后，在标准的部分中，选择查看结果。

页面底部的表格列出了适用于该标准的所有控件。您可以对表格进行筛选和排序。您还可以将表格的当前页面下载为 CSV 文件。为此，请选择表格上方的下载。如果对表格进行筛选，下载的文件将仅包含与当前筛选条件设置匹配的控件。

Security Hub CSPM API

查看已启用标准的控件

1. 使用 Security Hub CSPM API 的 ListSecurityControlDefinitions 操作。如果你使用的是 AWS CLI，请运行 list-security-control-definitions 命令。

   指定要查看其控件的标准的 Amazon 资源名称（ARN）。要获取标准的 ARN，请使用DescribeStandards操作或运行 desc ribe-standards 命令。如果未指定标准的 ARN，则 Security Hub CSPM 将返回所有安全控件 ID。

2. 使用 Security Hub CSPM API 的 ListStandardsControlAssociations 操作或运行 list-standards-control-associations 命令。此操作会告诉您在哪些标准中启用了控件。

   通过提供安全控件 ID 或 ARN 识别控件。分页参数是可选的。

以下示例告诉您该 Config.1 控件是在哪些标准中启用的。

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

关闭自动启用的安全标准

如果您的组织不使用中心配置，则会使用称为本地配置的配置类型。通过本地配置， AWS Security Hub CSPM 可以在新成员账户加入您的组织时自动启用默认安全标准。适用于这些默认标准的所有控件也会自动启用。

目前，默认安全标准是 AWS 基础安全最佳实践标准和互联网安全中心 (CIS) AWS 基金会基准 v1.2.0 标准。有关这些标准的信息，请参阅Security Hub CSPM 标准参考。

如果您希望手动为新成员账户启用安全标准，则可以关闭默认标准的自动启用。只有与本地配置集成 AWS Organizations 并使用本地配置时，才能执行此操作。如果使用中心配置，则可以创建启用默认标准的配置策略并将该策略与根相关联。然后，您的所有组织账户和 OU 都将继承此配置策略，除非它们与其他策略关联或是自行管理账户。如果您未与集成 AWS Organizations，则可以在最初启用 Security Hub CSPM 或更高版本时禁用默认标准。要了解如何操作，请参阅禁用标准。

要为新的成员账户关闭默认标准自动启用，可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。

Security Hub CSPM console

请按照以下步骤使用 Security Hub CSPM 控制台关闭默认标准自动启用。

关闭默认标准的自动启用

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用管理员账户的凭证登录。
2. 在导航窗格中的设置下，选择配置。
3. 在概述部分，选择编辑。
4. 在新账户设置下，清除启用默认安全标准复选框。
5. 选择确认。

Security Hub CSPM API

要以编程方式从 Security Hub CSPM 管理员账户关闭默认标准的自动启用，请使用 Security Hub CSPM API 的 UpdateOrganizationConfiguration 操作。在您的请求中，为 `AutoEnableStandards` 参数指定 `NONE`。

如果您使用的是 AWS CLI，请运行update-organization-configuration命令以关闭默认标准的自动启用。对于 `auto-enable-standards` 参数，请指定 `NONE`。例如，以下命令会自动为新成员账户启用 Security Hub CSPM，并关闭账户默认标准的自动启用。

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

禁用安全标准

在 Security Hub CSPM 中禁用 AWS 安全标准时，会出现以下情况：

- 除非与当前已启用的其他标准相关联，否则适用于该标准的所有控件均已禁用。
- 不再对已禁用控件执行安全检查，并且不会为已禁用控件生成其他调查发现。
- 已禁用控件的现有调查发现将在大约 3-5 天后自动存档。
- AWS Config Security Hub CSPM 为禁用的控件创建的规则将被删除。

通常会在禁用标准后的几分钟内删除相应的 AWS Config 规则。但是，这可能需要更长时间。如果删除规则的第一个请求失败，则 Security Hub CSPM 每 12 小时重试一次。但是，如果您禁用了 Security Hub CSPM 或没有启用任何其他标准，则 Security Hub CSPM 无法再次尝试，这意味着它无法删除规则。如果发生这种情况并且您需要删除规则，请联系 AWS 支持。

主题

- 在多个账户中禁用标准和 AWS 区域
- 在单个账户中禁用标准版和 AWS 区域

在多个账户中禁用标准和 AWS 区域

要在多个账户中禁用安全标准 AWS 区域，请使用集中配置。通过中心配置，受委派的 Security Hub CSPM 管理员可以创建 Security Hub CSPM 配置策略，以禁用一个或多个标准。然后，管理员可以将配置策略与单个帐户、组织单元（OU）或根帐户关联起来。配置策略会影响主区域（也称为聚合区域）以及所有关联区域。

配置策略提供自定义选项。例如，您可以选择在一个 OU 中禁用支付卡行业数据安全标准（PCI DSS）。对于另一个 OU，您可以选择禁用 PCI DSS 和美国国家标准与技术研究院（NIST）SP 800-53 Rev. 5 标准。有关如何创建启用或禁用您指定的各个标准的配置策略的信息，请参阅创建和关联配置策略。

> **Note**
>
> Security Hub CSPM 管理员可以使用配置策略禁用除 AWS Control Tower 服务托管标准之外的任何标准。要禁用此标准，管理员必须 AWS Control Tower 直接使用。他们还必须使用 AWS Control Tower 此标准为集中管理的账户禁用或启用个人控件。

如果您希望某些帐户为自己的帐户配置或禁用标准，Security Hub CSPM 管理员可以将这些帐户指定为自我管理的帐户。 Self-managed 账户必须在每个地区单独禁用标准。

在单个账户中禁用标准版和 AWS 区域

如果不使用中心配置或您有自行管理账户，则无法使用配置策略在多个账户或 AWS 区域中集中禁用安全标准。但是，您可以在单个账户和区域中禁用标准。您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API 执行此操作。

Security Hub CSPM console

按照以下步骤使用 Security Hub CSPM 控制台在一个账户和区域中禁用标准。

在一个账户和区域中禁用标准

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 使用页面右上角的选择 AWS 区域 器，选择要禁用标准的区域。
3. 在导航窗格中，选择安全标准。
4. 在要禁用的标准的部分中，选择禁用标准。

要在其他区域禁用标准，请在每个其他区域重复上述步骤。

Security Hub CSPM API

要在单个账户和区域中以编程方式禁用标准，请使用 BatchDisableStandards 操作。或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该batch-disable-standards命令。

在您的请求中，使用 `StandardsSubscriptionArns` 参数指定要禁用的标准的 Amazon 资源名称（ARN）。如果您使用的是 AWS CLI，请使用`standards-subscription-arns`参数指定 ARN。此外，请指定您的请求适用的区域。例如，以下命令禁用账户 () AWS 的基础安全最佳实践 (FSBP) 标准：*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
```

美国东部（弗吉尼亚北部）地区账户的 FSBP 标准的 ARN 在哪里*arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0*，*us-east-1*是要禁用该标准的区域。

要获取标准的 ARN，您可以使用 GetEnabledStandards 操作。此操作会检索有关您账户中当前已启用的标准的信息。如果您使用的是 AWS CLI，则可以运行 get-enabled-standards 命令来检索此信息。

禁用某个标准后，Security Hub CSPM 将开始执行任务以在账户和指定的区域中禁用该标准。这包括禁用适用于该标准的所有控件。要监控这些任务的状态，您可以检查账户和区域中该标准的状态。

了解 Security Hub CSPM 中的安全控件

在 Sec AWS urity Hub CSPM 中，安全控制（也称为控制）是安全标准中的一种保护措施，可帮助组织保护其信息的机密性、完整性和可用性。在 Security Hub CSPM 中，控件与特定 AWS 资源相关。

当您在一个或多个标准中启用控件时，Security Hub CSPM 会开始对其运行安全检查。安全检查会生成 Security Hub CSPM 调查发现。当您禁用控件时，Security Hub CSPM 会停止对其运行安全检查，并且不会再生成调查发现。

您可以为单个帐户单独启用或禁用控件，以及 AWS 区域. 为了节省时间并减少多账户环境中的配置偏差，我们建议使用中心配置启用或禁用控件。通过中心配置，Security Hub CSPM 委派管理员可以创建策略来指定如何跨多个账户和区域配置控件。有关启用和禁用控件的更多信息，请参阅在 Security Hub CSPM 中启用控件。

整合控件视图

S ec urity Hub CSPM 控制台的 “控件” 页面显示当前版本中所有可用的控件 AWS 区域 （您可以通过访问 “安全标准” 页面并选择启用的标准来查看标准环境中的控件）。Security Hub CSPM 为控件分配了各项标准一致的安全控件 ID、标题和描述。控件 IDs 包括相关的 AWS 服务 和唯一的数字（例如，CodeBuild.3）。

Security Hub CSPM 控制台的控件页面上提供了以下信息：

- 总体安全评分基于已通过的控件占已启用控件总数与包含数据的控件总数的比例
- 所有支持的 Security Hub CSPM 控件的控件状态细分
- 通过和未通过的安全检查总数。
- 针对不同严重程度的控件未通过的安全检查次数，以及查看有关这些未通过检查的更多详细信息的链接。
- Security Hub CSPM 控件列表，其中包含用于查看特定控件子集的筛选条件。

在控件页面中，您可以选择一个控件来查看其详细信息并对该控件生成的调查发现采取行动。在此页面上，您还可以在当前 AWS 账户 和中启用或禁用安全控件 AWS 区域。控件页面中的启用和禁用操作适用于所有标准。有关更多信息，请参阅 在 Security Hub CSPM 中启用控件。

对于管理员账户，控件页面反映了成员账户中的控件状态。如果至少一个成员账户中的控件检查失败，则控件状态为失败。如果您设置了聚合区域，则控件页面将反映所有关联区域中控件的状态。如果至少一个关联区域中的控件检查失败，则控件状态为失败。

合并控件视图会导致对 AWS 安全调查结果格式 (ASFF) 中的控制查找字段进行更改，这可能会影响工作流程。有关更多信息，请参阅 整合的控件视图——ASFF 变更。

控件的总体安全评分

控件页面显示的总体安全评分介于 0-100% 之间。总体安全评分是根据通过的控件与启用的控件（包含各标准的数据）总数的比例来计算的。

> **Note**
>
> 要查看控件的总体安全分数，您必须将调用 **`BatchGetControlEvaluations`** 的权限添加到您用于访问 Security Hub CSPM 的 IAM 角色中。查看特定标准的安全评分不需要此权限。

启用 Security Hub CSPM 后，Security Hub CSPM 会在您首次访问 Security Hub CSPM 控制台上的摘要页面或安全标准页面后 30 分钟内计算出初始安全分数。在中国地区和 AWS GovCloud (US) Regions生成首次获得安全评分最多需要 24 小时。

除了总体安全分数之外，Security Hub CSPM 还会在您首次访问摘要页面或安全标准页面后 30 分钟内计算每个已启用标准的标准安全分数。要查看当前启用的标准列表，请使用 `GetEnabledStandards` API 操作。

AWS Config 必须启用资源记录功能才能显示分数。有关 Security Hub CSPM 如何计算安全分数的信息，请参阅计算安全分数。

首次生成分数后，Security Hub CSPM 每 24 小时更新一次安全分数。Security Hub CSPM 显示时间戳以指示安全分数上次更新的时间。

如果您设置了聚合区域，则总体安全分数将反映关联区域的控件调查发现。

Security Hub CSPM 控件参考

此控件参考提供了可用的 Sec AWS urity Hub CSPM 控件表，其中包含指向有关每个控件的更多信息的链接。在该表中，控件按控件 ID 的字母顺序排列。此处仅包含 Security Hub CSPM 正在使用的控件。已停用的控件不包含在表中。

该表提供了每个控件的以下信息：

- 安全控制 ID — 此 ID 适用于所有标准，并表示该控件所涉及的 AWS 服务 和资源。无论账户中开启还是关闭了整合的控件调查发现，Security Hub CSPM 控制台都会显示安全控件 ID。但是，只有在

账户中启用了整合的控件调查发现时，Security Hub CSPM 调查发现才会引用安全控件 ID。如果在账户中关闭了整合的控件调查发现，则控件调查发现中的某些控件 ID 可能会因标准而异。有关特定于标准的控件 ID 与安全控件 ID 的映射，请参阅 整合如何影响控件 ID 和标题。

如果您想为安全控件设置自动化，我们建议您根据控件 ID 而不是标题或描述进行筛选。尽管 Security Hub CSPM 偶尔会更新控件标题或描述，但控件 ID 保持不变。

控件 ID 可能会跳过数字。这些是未来控件的占位符。

- 安全控件标题——此标题适用于各类标准。无论账户中开启还是关闭了整合的控件调查发现，Security Hub CSPM 控制台都会显示安全控件标题。但是，只有在账户中开启了整合的控件调查发现时，Security Hub CSPM 调查发现才会引用安全控件标题。如果在账户中关闭了整合的控件调查发现，则控件调查发现中的某些控件标题可能会因标准而异。有关特定于标准的控件 ID 与安全控件 ID 的映射，请参阅 整合如何影响控件 ID 和标题。
- 适用标准——指明控件适用于哪些标准。请选择一个控件以查看第三方合规性框架的具体要求。
- 严重性——从安全角度来看，控制的严重性确定了其重要性。有关 Security Hub CSPM 如何确定控件严重性的信息，请参阅控件调查发现的严重性级别。
- 支持自定义参数-指示控件是否支持一个或多个参数的自定义值。请选择一个控件以查看参数详细信息。有关更多信息，请参阅 了解 Security Hub CSPM 中的控件参数。
- 计划类型——指明何时评估控件。有关更多信息，请参阅 有关运行安全检查的计划。

请选择一个控件以查看更多详细信息。控件按安全控件 ID 的字母顺序排列。

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Account.1	应为以下人员提供安全联系信息 AWS 账户	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、AWS 基础安全最佳实践 v1.0.0、NIST SP 800-53 修订版 5	MEDIUM	⊗没有	定期
Account.2	AWS 账户 应该是 AWS Organizations 组织的一部分	NIST SP 800-53 Rev. 5	HIGH（高）	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ACM.1	导入并应在指定时间段后续订 ACM-issued 证书	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	MEDIUM	✓ 是	变更已触发且定期进行
ACM.2	由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度	AWS 基础安全最佳实践 v1.0.0，PCI DSS v4.0.1	HIGH	✗ 没有	变更已触发
ACM.3	应标记 ACM 证书	AWS 资源标签标准	LOW	✓ 是	变更已触发
Amplify.1	应标记 Amplify 应用	AWS 资源标签标准	LOW	✓ 是	变更已触发
Amplify.2	应标记 Amplify 分支	AWS 资源标签标准	LOW	✓ 是	变更已触发
APIGateway.1	应启用 API Gateway REST 和 WebSocket API 执行日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	变更已触发
APIGateway.2	API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	✗ 没有	变更已触发
APIGateway.3	API Gateway REST API 阶段应启用 AWS X-Ray 跟踪	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
APIGateway.4	API Gateway 应与 WAF Web ACL 关联	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
APIGateway.5	API Gateway REST API 缓存数据应静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
APIGateway.8	API Gateway 路由应指定授权类型	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	定期
APIGateway.9	应为 API Gateway V2 阶段配置访问日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
APIGateway.10	API Gateway V2 集成应使用 HTTPS 进行私有连接	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
APIGateway.11	API Gateway 域名应使用推荐的安全策略	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
AppConfig.1	AWS AppConfig 应用程序应该被标记	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppConfig.2	AWS AppConfig 应标记配置文件	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppConfig.3	AWS AppConfig 应该给环境加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppConfig.4	AWS AppConfig 应标记扩展关联	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
AppFlow.1	应标记 Amazon AppFlow 流程	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppRunner.1	应标记 App Runer 服务	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppRunner.2	应标记 App Runner VPC 连接器	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppSync.2	AWS AppSync 应该启用字段级日志记录	AWS 基础安全最佳实践 v1.0.0，PCI DSS v4.0.1	MEDIUM	✓ 是	变更已触发
AppSync.4	AWS AppSync 应标记 GraphQL API	AWS 资源标签标准	LOW	✓ 是	变更已触发
AppSync.5	AWS AppSync 不应使用 API 密钥对 GraphQL API 进行身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	✗ 没有	变更已触发
Athena.2	应标记 Athena 数据目录	AWS 资源标签标准	LOW	✓ 是	变更已触发
Athena.3	应标记 Athena 工作组	AWS 资源标签标准	LOW	✓ 是	变更已触发
Athena.4	Athena 工作组应启用日志记录	AWS 基础安全最佳实践	MEDIUM	✗ 没有	变更已触发
AutoScaling.1	与负载均衡器关联的自动扩缩组应使用 ELB 运行状况检查	AWS 基础安全最佳实践，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	LOW	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
AutoScaling.2	Amazon EC2 Auto Scaling 组应覆盖多个可用区	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	变更已触发
AutoScaling.3	自动扩缩组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2（IMDSv2）	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	✗ 没有	变更已触发
Autoscaling.5	使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	✗ 没有	变更已触发
AutoScaling.6	自动扩缩组组应在多个可用区中使用多种实例类型	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
AutoScaling.9	EC2 自动扩缩组应使用 EC2 启动模板	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
AutoScaling.10	应标记 EC2 自动扩缩组	AWS 资源标签标准	LOW	✓ 是	变更已触发
Backup.1	AWS Backup 恢复点应在静态状态下进行加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
Backup.2	AWS Backup 应标记恢复点	AWS 资源标签标准	LOW	✓ 是	变更已触发
Backup.3	AWS Backup 应给保管库加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Backup.4	AWS Backup 报告计划应加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
Backup.5	AWS Backup 应标记备份计划	AWS 资源标签标准	LOW	✓ 是	变更已触发
Batch.1	应标记批处理作业队列	AWS 资源标签标准	LOW	✓ 是	变更已触发
Batch.2	应标记批处理计划策略	AWS 资源标签标准	LOW	✓ 是	变更已触发
Batch.3	应标记批处理计算环境	AWS 资源标签标准	LOW	✓ 是	变更已触发
Batch.4	应标记托管批处理计算环境中的计算资源属性	AWS 资源标签标准	LOW	✓ 是	变更已触发
BedrockAgentCore.1	基岩 AgentCore 运行时应配置为 VPC 网络模式	AWS 基础安全最佳实践	HIGH	✗ 没有	变更已触发
BedrockAgentCore.2	基岩 AgentCore 网关应要求对入站请求进行授权	AWS 基础安全最佳实践	HIGH	✗ 没有	变更已触发
BedrockAgentCore.3	Bedrock AgentCore Memory 应使用客户管理 AWS KMS 的密钥进行加密	NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
BedrockAgentCore.4	Bedrock AgentCore Gateway 应使用客户管理 AWS KMS 的密钥进行加密	NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
BedrockAgentCore.5	Bedrock AgentCore 自定义浏览器不应使用公共网络模式	AWS 基础安全最佳实践	HIGH	⊗没有	变更已触发
BedrockAgentCore.6	Bedrock AgentCore 自定义浏览器应启用会话录制	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
CloudFormation.2	CloudFormation 堆栈应该被标记	AWS 资源标签标准	LOW	✓ 是	变更已触发
CloudFormation.3	CloudFormation 堆栈应启用终止保护	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
CloudFormation.4	CloudFormation 堆栈应该有相关的服务角色	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
CloudFront.1	CloudFront 发行版应该配置一个默认的根对象	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
CloudFront.3	CloudFront 发行版在传输过程中应要求加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
CloudFront.4	CloudFront 发行版应配置源站故障转移	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
CloudFront.5	CloudFront 发行版应该启用日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudFront.6	CloudFront 发行版应启用 WAF	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
CloudFront.7	CloudFront 发行版应使用自定义 SSL/TLS 证书	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	LOW	⊗没有	变更已触发
CloudFront.8	CloudFront 发行版应使用 SNI 来处理 HTTPS 请求	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
CloudFront.9	CloudFront 发行版应加密发往自定义来源的流量	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
CloudFront.10	CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
CloudFront.12	CloudFront 发行版不应指向不存在的 S3 来源	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	定期
CloudFront.13	CloudFront 发行版应使用源站访问控制	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudFront.14	CloudFront 应该给发行版加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
CloudFront.15	CloudFront 发行版应使用推荐的 TLS 安全策略	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
CloudFront.16	CloudFront 分发应该对 Lambda 函数 URL 来源使用源访问控制	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
CloudFront.17	CloudFront 发行版应为签名 URL 和 Cookie 使用可信密钥组	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
CloudTrail.1	CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、CIS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践 AWS 、N AWS IST SP 800-53 修订版 5	HIGH	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudTrail.2	CloudTrail 应该启用静态加密	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1. AWS 4.0 基础安全最佳实践 v1.0.0、N AWS IST SP 800-53 修订版 5、NIST SP 800-171 修订版 2、PCI DSS v3.2.1、PCI DSS v4.0.1	MEDIUM	⊗没有	定期
CloudTrail.3	至少应启用一条 CloudTrail 跟踪	NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、PCI DSS v3.2.1	HIGH	⊗没有	定期
CloudTrail.4	CloudTrail 应启用日志文件验证	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践 v1.0.0、N AWS IST SP 800-53 修订版 5 AWS 、NIST SP 800-171 修订版 2、PCI DSS v4.0.1、PCI DSS v3.2.1	LOW	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudTrail.5	CloudTrail 跟踪应与 Amazon CloudWatch 日志集成	CIS AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1.4.0、AWS 基础安全最佳实践 v1.0.0、NIST SP 800-53 修订版 5、PCI DSS v3.2.1、PCI DSS v3.2.1、PCI DSS v4.0.1	MEDIUM	⊗没有	定期
CloudTrail.6	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	CIS AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1.4.0、PCI DSS v4.0.1	关键	⊗没有	变更已触发且定期进行
CloudTrail.7	确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v3.0.0、PCI DSS v4.0.1 AWS	LOW	⊗没有	定期
CloudTrail.9	CloudTrail 应标记步道	AWS 资源标签标准	LOW	⊙ 是	变更已触发
CloudTrail.10	CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudWatch.1	应具有有关“根”用户使用的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2、PCI DSS v3.2.1 v3.2.1	LOW	⊗没有	定期
CloudWatch.2	确保存在关于未经授权的 API 调用的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.2.0，NIST SP 800-171 Rev. 2	LOW	⊗没有	定期
CloudWatch.3	确保存在关于无 MFA 的管理控制台登录的日志指标筛选条件和警报	CIS AWS 基金会基准测试 v1.2.0	LOW	⊗没有	定期
CloudWatch.4	确保存在关于 IAM 策略更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.5	确保存在 CloudTrail 配置更改的日志指标筛选器和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.6	确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudWatch.7	确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.8	确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.9	确保存在 AWS Config 配置更改的日志指标筛选器和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.10	确保存在关于安全组更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.11	确保存在关于网络访问控制列表（NACL）更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.12	确保存在关于网络网关更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudWatch.13	确保存在关于路由表更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.14	确保存在关于 VPC 更改的日志指标筛选条件和警报	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2	LOW	⊗没有	定期
CloudWatch.15	CloudWatch 警报应配置指定的操作	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	HIGH	⊙ 是	变更已触发
CloudWatch.16	CloudWatch 日志组应在指定的时间段内保留	NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	定期
CloudWatch.17	CloudWatch 应启用警报操作	NIST SP 800-53 Rev. 5	HIGH（高）	⊗没有	变更已触发
CodeArtifact.1	CodeArtifact 存储库应该被标记	AWS 资源标签标准	LOW	⊙ 是	变更已触发
CodeBuild.1	CodeBuild Bitbucket 源存储库网址不应包含敏感凭据	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	关键	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CodeBuild.2	CodeBuild 项目环境变量不应包含明文凭证	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	关键	⊗没有	变更已触发
CodeBuild.3	CodeBuild 应对 S3 日志进行加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	LOW	⊗没有	变更已触发
CodeBuild.4	CodeBuild 项目环境应该有日志配置	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
CodeBuild.7	CodeBuild 报告组导出应进行静态加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
CodeGuruProfiler.1	CodeGuru 应标记 Profiler 分析组	AWS 资源标签标准	LOW	✓ 是	变更已触发
CodeGuruReviewer.1	CodeGuru 应标记 Reviewer 存储库关联	AWS 资源标签标准	LOW	✓ 是	变更已触发
Cognito.1	Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证	AWS 基础安全最佳实践	MEDIUM	✓ 是	变更已触发
Cognito.2	Cognito 身份池不应允许未经身份验证的身份	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
Cognito.3	Cognito 用户池的密码策略应具有可靠的配置	AWS 基础安全最佳实践	MEDIUM	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Cognito.4	Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
Cognito.5	应为 Cognito 用户池启用 MFA	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
Cognito.6	Cognito 用户池应启用删除保护	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
Config.1	AWS Config 应该启用并使用服务相关角色进行资源记录	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、CIS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践、NIST SP 800-53 修订版 5 AWS 、PCI DSS v3.2.1	关键	⊙ 是	定期
Connect.1	应标记 Connect 客户档案对象类型	AWS 资源标签标准	LOW	⊙ 是	变更已触发
Connect.2	Connect 客户实例应启用 CloudWatch 日志记录	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
DataFirehose.1	应静态加密 Firehose 传输流	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	定期
DataSync.1	DataSync 任务应该启用日志记录	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DataSync.2	DataSync 任务应该被标记	AWS 资源标签标准	LOW	✓ 是	变更已触发
Detective.1	应标记 Detective 行为图	AWS 资源标签标准	LOW	✓ 是	变更已触发
DMS.1	Database Migration Service 复制实例不应公开	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	关键	✗ 没有	定期
DMS.2	应标记 DMS 证书	AWS 资源标签标准	LOW	✓ 是	变更已触发
DMS.3	应标记 DMS 事件订阅	AWS 资源标签标准	LOW	✓ 是	变更已触发
DMS.4	应标记 DMS 复制实例	AWS 资源标签标准	LOW	✓ 是	变更已触发
DMS.5	应标记 DMS 复制子网组	AWS 资源标签标准	LOW	✓ 是	变更已触发
DMS.6	DMS 复制实例应启用自动次要版本升级	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
DMS.7	目标数据库的 DMS 复制任务应启用日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DMS.8	源数据库的 DMS 复制任务应启用日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
DMS.9	DMS 端点应使用 SSL	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
DMS.10	Neptune 数据库的 DMS 端点应启用 IAM 授权	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
DMS.11	MongoDB 的 DMS 端点应启用身份验证机制	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
DMS.12	Redis OSS 的 DMS 端点应启用 TLS	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
DMS.13	DMS 复制实例应配置为使用多个可用区	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
DocumentDB.1	Amazon DocumentDB 集群应进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DocumentDB.2	Amazon DocumentDB 集群应有足够的备份保留期	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✅ 是	变更已触发
DocumentDB.3	Amazon DocumentDB 手动集群快照不应公开	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	关键	❌没有	变更已触发
DocumentDB.4	Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	❌没有	变更已触发
DocumentDB.5	Amazon DocumentDB 集群应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	❌没有	变更已触发
DocumentDB.6	Amazon DocumentDB 集群应在传输过程中加密	AWS 基础安全最佳实践	MEDIUM	❌没有	定期
DynamoDB.1	DynamoDB 表应根据需求自动扩展容量	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✅ 是	定期
DynamoDB.2	DynamoDB 表应启用时间点故障恢复	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	❌没有	变更已触发
DynamoDB.3	DynamoDB Accelerator（DAX）集群应在静态状态下进行加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	❌没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DynamoDB.4	备份计划中应有 DynamoDB 表	NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	定期
DynamoDB.5	应标记 DynamoDB 表	AWS 资源标签标准	LOW	✓ 是	变更已触发
DynamoDB.6	DynamoDB 表应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
DynamoDB.7	应在传输过程中加密 DynamoDB Accelerator 集群	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	定期
EC2.1	不应公开还原 EBS 快照	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	关键	✗ 没有	定期
EC2.2	VPC 默认安全组不应允许入站或出站流量	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践 v1.0.0、PCI DSS v3.2.1 AWS 、CIS 基金会基准 v1.4.0、N AWS IST SP 800-53 修订版 5 AWS	HIGH	✗ 没有	变更已触发
EC2.3	挂载的 EBS 卷应进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.4	停止的 EC2 实例应在指定时间段后删除	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	定期
EC2.6	应在所有 VPC 中启用 VPC 流日志记录	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践 v1.0.0、PCI DSS v3.2.1 AWS 、AWS CIS 基金会基准 v1.4.0、NIST SP 800-53 修订版 5、NIS AWS T SP 800-171 修订版 2	MEDIUM	⊗没有	定期
EC2.7	EBS 默认加密应该为已启用。	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、基础 AWS 安全最佳实践 v1.0.0、CIS 基金会基准 v1.4.0、NIST SP 800-53 修订版 5 AWS	MEDIUM	⊗没有	定期
EC2.8	EC2 实例应使用实例元数据服务版本 2（IMDSv2）	CIS AWS 基金会基准 v5.0.0，CIS AWS 基金会基准 v3.0.0，AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.9	EC2 实例不应拥有公有 IPv4 地址	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
EC2.10	应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	定期
EC2.12	应删除未使用的 EC2 EIP	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
EC2.13	安全组不应允许从 0.0.0 开始的入口。0/0 或:: /0 到端口 22	CIS F AWS oundations 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	HIGH	⊗没有	变更已触发且定期进行
EC2.14	安全组不应允许从 0.0.0 开始的入口。0/0 或者:: /0 到端口 3389	CIS AWS 基金会基准测试 v1.2.0，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发且定期进行
EC2.15	EC2 子网不应自动分配公有 IP 地址	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.16	应删除未使用的网络访问控制列表	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1，	LOW	⊗没有	变更已触发
EC2.17	EC2 实例不应使用多个 ENI	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
EC2.18	安全组应仅允许授权端口不受限制的传入流量	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	HIGH	✓ 是	变更已触发
EC2.19	安全组不应允许无限制地访问高风险端口	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 Rev. 2	关键	⊗没有	变更已触发且定期进行
EC2.20	VPN 连接的两个 AWS Site-to-Site VPN 隧道都应处于开启状态	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.21	网络 ACL 不应允许从 0.0.0 开始的入口。0/0 到端口 22 或端口 3389	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、NIST SP 800-171 修订版 2、PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
EC2.22	应删除未使用的 EC2 安全组		MEDIUM	⊗没有	定期
EC2.23	EC2 中转网关不应自动接受 VPC 附件请求	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
EC2.24	不应使用 EC2 半虚拟化实例类型	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
EC2.25	EC2 启动模板不应将公共 IP 分配给网络接口	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
EC2.28	EBS 卷应包含在备份计划中	NIST SP 800-53 Rev. 5	低	⊘ 是	定期
EC2.33	应标记 EC2 中转网关连接	AWS 资源标签标准	LOW	⊘ 是	变更已触发
EC2.34	应标记 EC2 中转网关路由表	AWS 资源标签标准	LOW	⊘ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.35	应标记 EC2 网络接口	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.36	应标记 EC2 客户网关	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.37	应标记 EC2 弹性 IP 地址	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.38	应标记 EC2 实例	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.39	应标记 EC2 互联网网关	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.40	应标记 EC2 NAT 网关	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.41	应标记 EC2 网络 ACL	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.42	应标记 EC2 路由表	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.43	应标记 EC2 安全组	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.44	应标记 EC2 子网	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.45	应标记 EC2 卷	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.46	应标记 Amazon VPC	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.47	应标记 Amazon VPC 端点服务	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.48	应标记 Amazon VPC 流日志	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.49	应标记 Amazon VPC 对等连接	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.50	应标记 EC2 VPN 网关	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.51	EC2 Client VPN 端点应启用客户端连接日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	LOW	✗ 没有	变更已触发
EC2.52	应标记 EC2 中转网关	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.53	EC2 安全组不应允许从 0.0.0 开始的入口。0/0 到远程服务器管理端口	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、PCI DSS v4.0.1	HIGH	✗ 没有	定期
EC2.54	EC2 安全组不应允许从 ::/0 到远程服务器管理端口的入口流量	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、PCI DSS v4.0.1	HIGH	✗ 没有	定期
EC2.55	应为 VPC 配置用于 ECR API 的接口端点	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.56	应为 VPC 配置用于 Docker Registry 的接口端点	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	定期
EC2.57	应为 VPC 配置用于 Systems Manager 的接口端点	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	定期
EC2.58	应为 VPC 配置用于 Systems Manager Incident Manager Contacts 的接口端点	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	定期
EC2.60	应为 VPC 配置用于 Systems Manager Incident Manager 的接口端点	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	定期
EC2.170	EC2 启动模板应使用实例元数据服务版本 2（IMDSv2）	AWS 基础安全最佳实践，PCI DSS v4.0.1	LOW	✗ 没有	变更已触发
EC2.171	EC2 VPN 连接应启用日志记录	AWS 基础安全最佳实践，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
EC2.172	EC2 VPC 阻止公开访问设置应阻止互联网网关流量	AWS 基础安全最佳实践	MEDIUM	✓ 是	变更已触发
EC2.173	带有启动参数的 EC2 竞价型实例集请求应为连接的 EBS 卷启用加密	AWS 基础安全最佳实践	MEDIUM	✗ 没有	变更已触发
EC2.174	应标记 EC2 DHCP 选项集	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.175	应标记 EC2 启动模板	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.176	应标记 EC2 前缀列表	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.177	应标记 EC2 流量镜像会话	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.178	应标记 EC2 流量镜像筛选条件	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.179	应标记 EC2 流量镜像目标	AWS 资源标签标准	LOW	✓ 是	变更已触发
EC2.180	EC2 网络接口应启用 source/destination 检查功能	AWS 基础安全最佳实践 v1.0.0	MEDIUM	✗ 没有	变更已触发
EC2.181	EC2 启动模板应为附加的 EBS 卷启用加密	AWS 基础安全最佳实践 v1.0.0	MEDIUM	✗ 没有	变更已触发
EC2.182	EBS 快照不应公开访问	AWS 基础安全最佳实践	HIGH	✗ 没有	变更已触发
EC2.183	EC2 VPN 连接应使用 IKEv2 协议	AWS 基础安全最佳实践	MEDIUM	✗ 没有	变更已触发
ECR.1	ECR 私有存储库应配置图像扫描	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	✗ 没有	定期
ECR.2	ECR 私有存储库应配置标签不可变性	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ECR.3	ECR 存储库应至少配置一项生命周期策略	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ECR.4	应标记 ECR 公有存储库	AWS 资源标签标准	LOW	⊙ 是	变更已触发
ECR.5	ECR 存储库应使用客户管理型 AWS KMS keys进行加密	NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	变更已触发
ECS.2	ECS 服务不应自动分配公共 IP 地址	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
ECS.3	ECS 任务定义不应共享主机的进程命名空间	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
ECS.4	ECS 容器应以非特权身份运行	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
ECS.5	ECS 容器应限制为仅对根文件系统具有只读访问权限。	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
ECS.8	密钥不应作为容器环境变量传递	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
ECS.9	ECS 任务定义应具有日志配置	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ECS.10	ECS Fargate 服务应在最新的 Fargate 平台版本上运行	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
ECS.12	ECS 集群应该使用容器详情	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ECS.13	应标记 ECS 服务	AWS 资源标签标准	LOW	⊙ 是	变更已触发
ECS.14	应标记 ECS 集群	AWS 资源标签标准	LOW	⊙ 是	变更已触发
ECS.15	应标记 ECS 任务定义	AWS 资源标签标准	LOW	⊙ 是	变更已触发
ECS.16	ECS 任务集不应自动分配公有 IP 地址	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
ECS.17	ECS 任务定义不应使用主机网络模式	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ECS.18	ECS 任务定义应对 EFS 卷使用传输中加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
ECS.19	ECS 容量提供商应启用托管终止保护	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
ECS.20	ECS 任务定义应在 Linux 容器定义中配置非 root 用户	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ECS.21	ECS 任务定义应在 Windows 容器定义中配置非管理员用户	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
EFS.1	应将 Elastic 文件系统配置为使用以下方法对静态文件数据进行加密 AWS KMS	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、AWS 基础安全最佳实践 v1.0.0、NIST SP 800-53 修订版 5	MEDIUM	⊗没有	定期
EFS.2	Amazon EFS 卷应包含在备份计划中	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	定期
EFS.3	EFS 接入点应强制使用根目录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
EFS.4	EFS 接入点应强制使用用户身份	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
EFS.5	应标记 EFS 接入点	AWS 资源标签标准	LOW	✓ 是	变更已触发
EFS.6	EFS 挂载目标不应与启动时分配公有 IP 地址的子网关联	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
EFS.7	EFS 文件系统应启用自动备份	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EFS.8	应静态加密 EFS 文件系统	CIS AWS 基金会基准测试 v5.0.0， AWS 基础安全最佳实践	MEDIUM	✓ 是	变更已触发
EKS.1	EKS 集群端点不应公开访问	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	✗ 没有	定期
EKS.2	EKS 集群应在受支持的 Kubernetes 版本上运行	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	✗ 没有	变更已触发
EKS.3	EKS 集群应使用加密的 Kubernetes 密钥	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	定期
EKS.6	应标记 EKS 集群	AWS 资源标签标准	LOW	✓ 是	变更已触发
EKS.7	应标记 EKS 身份提供者配置	AWS 资源标签标准	LOW	✓ 是	变更已触发
EKS.8	EKS 集群应启用审核日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
EKS.9	EKS 节点组应在支持的 Kubernetes 版本上运行	AWS 基础安全最佳实践	HIGH	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ElastiCache.1	ElastiCache (Redis OSS) 集群应启用自动备份	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	✓ 是	定期
ElastiCache.2	ElastiCache 集群应启用自动次要版本升级	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	定期
ElastiCache.3	ElastiCache 复制组应启用自动故障切换	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	定期
ElastiCache.4	ElastiCache 应对复制组进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	定期
ElastiCache.5	ElastiCache 复制组应在传输过程中进行加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	定期
ElastiCache.6	ElastiCache（Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	定期
ElastiCache.7	ElastiCache 群集不应使用默认子网组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	定期
ElasticBeanstalk.1	Elastic Beanstalk 环境应启用增强型运行状况报告	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ElasticBeanstalk.2	应启用 Elastic Beanstalk 托管平台更新	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	✓ 是	变更已触发
ElasticBeanstalk.3	Elastic Beanstalk 应该将日志流式传输到 CloudWatch	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	✓ 是	变更已触发
ELB.1	应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	定期
ELB.2	带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	✗ 没有	变更已触发
ELB.3	应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
ELB.4	应将应用程序负载均衡器配置为删除 http 标头	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
ELB.5	应启用应用程序和经典负载均衡器日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ELB.6	应用程序、网关和网络负载均衡器应启用删除保护	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
ELB.7	经典负载均衡器应启用连接耗尽功能	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
ELB.8	具有 SSL 侦听器的经典负载均衡器应使用具有强大配置的预定义安全策略	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
ELB.9	经典负载均衡器应启用跨区域负载均衡器	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ELB.10	经典负载均衡器应跨越多个可用区	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	变更已触发
ELB.12	应用程序负载均衡器应配置为防御性或最严格的异步缓解模式	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
ELB.13	应用程序、网络和网关负载均衡器应跨越多个可用区	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	变更已触发
ELB.14	经典负载均衡器应配置为防御性或最严格的异步缓解模式	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ELB.16	应用程序负载均衡器应与 AWS WAF Web ACL 关联	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ELB.17	带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ELB.18	应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
ELB.21	应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
ELB.22	ELB 目标组应使用加密传输协议	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
EMR.1	Amazon EMR 集群主节点不应有公有 IP 地址	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	定期
EMR.2	应启用 Amazon EMR 屏蔽公共访问权限设置	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	关键	⊗没有	定期
EMR.3	Amazon EMR 安全配置应静态加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EMR.4	Amazon EMR 安全配置应在传输过程中加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
ES.1	Elasticsearch 域应启用静态加密	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	定期
ES.2	Elasticsearch 域名不可供公共访问	AWS 基础安全最佳实践，PCI DSS v3.2.1，PCI DSS v4.0.1，NIST SP 800-53 Rev. 5	关键	⊗没有	定期
ES.3	Elasticsearch 域应加密节点之间发送的数据	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
ES.4	应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ES.5	Elasticsearch 域名应该启用审核日志	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
ES.6	Elasticsearch 域应拥有至少三个数据节点	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
ES.7	Elasticsearch 域应配置至少三个专用主节点	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ES.8	与 Elasticsearch 域的连接应使用最新的 TLS 安全策略进行加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
ES.9	应标记 Elasticsearch 域	AWS 资源标签标准	LOW	⊙ 是	变更已触发
EventBridge.2	EventBridge 应标记活动总线	AWS 资源标签标准	LOW	⊙ 是	变更已触发
EventBridge.3	EventBridge 自定义事件总线应附加基于资源的策略	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	LOW	⊗没有	变更已触发
EventBridge.4	EventBridge 全局端点应启用事件复制	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
FraudDetector.1	应标记 Amazon Fraud Detector 实体类型	AWS 资源标签标准	LOW	⊙ 是	变更已触发
FraudDetector.2	应标记 Amazon Fraud Detector 标签	AWS 资源标签标准	LOW	⊙ 是	变更已触发
FraudDetector.3	应标记 Amazon Fraud Detector 结果	AWS 资源标签标准	LOW	⊙ 是	变更已触发
FraudDetector.4	应标记 Amazon Fraud Detector 变量	AWS 资源标签标准	LOW	⊙ 是	变更已触发
FSx.1	应将 FSx for OpenZFS 文件系统配置为将标签复制到备份和卷	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
FSx.2	应将适用于 Lustre 的 FSx 文件系统配置为将标签复制到备份	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	LOW	⊗没有	定期
FSx.3	应为部署配置适用于 OpenZFS 文件系统的 FSX Multi-AZ	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
FSx.4	应将 NetApp ONTAP 文件系统的 FSx 配置为用于部署 Multi-AZ	AWS 基础安全最佳实践	MEDIUM	⊙ 是	定期
FSx.5	应配置 Multi-AZ 适用于 Windows File Server 的 FSx 文件系统以进行部署	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
Glue.1	AWS Glue 应该给工作加标签	AWS 资源标签标准	LOW	⊙ 是	变更已触发
Glue.3	AWS Glue 机器学习转换应在静态状态下进行加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
Glue.4	AWS Glue Spark 作业应在支持的版本上运行 AWS Glue	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
GlobalAccelerator.1	应标记 Global Accelerator 加速器	AWS 资源标签标准	LOW	⊙ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
GuardDuty.1	GuardDuty 应该启用	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v3.2.1，PCI DSS v4.0.1	HIGH	⊗没有	定期
GuardDuty.2	GuardDuty 应该给过滤器加标签	AWS 资源标签标准	LOW	⊙ 是	变更已触发
GuardDuty.3	GuardDuty 应标记 IP 集	AWS 资源标签标准	LOW	⊙ 是	变更已触发
GuardDuty.4	GuardDuty 应给探测器加标签	AWS 资源标签标准	LOW	⊙ 是	变更已触发
GuardDuty.5	GuardDuty 应启用 EKS 审核日志监控	AWS 基础安全最佳实践	HIGH	⊗没有	定期
GuardDuty.6	GuardDuty 应启用 Lambda 保护	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
GuardDuty.7	GuardDuty 应启用 EKS 运行时监控	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
GuardDuty.8	GuardDuty 应启用 EC2 的恶意软件防护	AWS 基础安全最佳实践	HIGH	⊗没有	定期
GuardDuty.9	GuardDuty 应启用 RDS 保护	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
GuardDuty.10	GuardDuty 应启用 S3 保护	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
GuardDuty.11	GuardDuty 应启用 “运行时监控”	AWS 基础安全最佳实践	HIGH	⊗没有	定期
GuardDuty.12	GuardDuty 应启用 ECS 运行时监控	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
GuardDuty.13	GuardDuty 应启用 EC2 运行时监控	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
IAM.1	IAM policy 不应允许完全“*”管理权限	CIS AWS 基金会基准 v1.2.0、 AWS 基础安全最佳实践 v1.0.0、PCI DSS v3.2.1、CIS 基金会基准 v1.4.0、NIST SP 800-53 修订版 5、NIST SP 800-171 修订版 2、NIS AWS T SP 800-171 修订版 2	HIGH	⊗没有	变更已触发
IAM.2	IAM 用户不应附加 IAM policy	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CI S AWS 基金会基准 v1.2.0、基础安全最佳实践 v1.0.0、PCI DSS v3.2.1、N AWS IST SP 800-53 修订版 5 AWS 、NIST SP 800-171 修订版 2、NIST SP 800-171 修订版 2	LOW	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.3	IAM 用户访问密钥应每 90 天或更短时间轮换一次	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、CIS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、PCI DSS v4.0.1	MEDIUM	⊗没有	定期
IAM.4	不应存在 IAM 根用户访问密钥	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践 v1.0.0、PCI DSS v3.2.1 AWS 、N AWS IST SP 800-53 修订版 5	关键	⊗没有	定期
IAM.5	应为拥有控制台密码的所有 IAM 用户启用 MFA	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、CIS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、PCI DSS v4.0.1	MEDIUM	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.6	应该为根用户启用硬件 MFA	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、PCI DSS v3.2.1、PCI DSS v4.0.1	关键	⊗没有	定期
IAM.7	IAM 用户的密码策略应具有可靠的配置	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	MEDIUM	⊙ 是	定期
IAM.8	应移除未使用的 IAM 用户凭证	CIS AWS Foundations Benchmark v1.2.0， AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v3.2.1，PCI DSS v4.0.1	MEDIUM	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.9	应为根用户启用 MFA	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NAWS IST SP 800-53 修订版 5、PCI DSS v3.2.1、PCI DSS v4.0.1	关键	⊗没有	定期
IAM.10	IAM 用户的密码策略应具有可靠的配置	NIST SP 800-171 Rev. 2、PCI DSS v3.2.1	MEDIUM	⊗没有	定期
IAM.11	确保 IAM 密码策略要求包含至少一个大写字母	CIS F AWS oundations Benchmark v1.2.0，NIST SP 800-171 Rev. 2，PCI DSS v4.0.1	MEDIUM	⊗没有	定期
IAM.12	确保 IAM 密码策略要求包含至少一个小写字母	CIS F AWS oundations Benchmark v1.2.0，NIST SP 800-171 Rev. 2，PCI DSS v4.0.1	MEDIUM	⊗没有	定期
IAM.13	确保 IAM 密码策略要求包含至少一个符号	CIS AWS 基金会基准 v1.2.0，NIST SP 800-171 Rev. 2	MEDIUM	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.14	确保 IAM 密码策略要求包含至少一个数字	CIS F AWS oundation s Benchmark v1.2.0，NIST SP 800-171 Rev. 2，PCI DSS v4.0.1	MEDIUM	⊗没有	定期
IAM.15	确保 IAM 密码策略要求最短密码长度不低于 14	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NAWS IST SP 800-171 修订版 2	MEDIUM	⊗没有	定期
IAM.16	确保 IAM 密码策略阻止重复使用密码	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NAWS IST SP 800-171 修订版 2、PCI DSS v4.0.1	LOW	⊗没有	定期
IAM.17	确保 IAM 密码策略使密码在 90 天或更短时间内失效	CIS AWS 基金会基准测试 v1.2.0，PCI DSS v4.0.1	LOW	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.18	确保创建支持角色来管理涉及 AWS 支持的事务	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NIST SP 800-171 修订版 2、PCI DSS v4.0.1	LOW	⊗没有	定期
IAM.19	应该为所有 IAM 用户启用 MFA	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1	MEDIUM	⊗没有	定期
IAM.21	您创建的 IAM 客户管理型策略不应允许对服务执行通配符操作	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	LOW	⊗没有	变更已触发
IAM.22	应移除在 45 天内未使用的 IAM 用户凭证	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、NIST SP 800-171 修订版 2	MEDIUM	⊗没有	定期
IAM.23	应标记 IAM Access Analyzer 分析器	AWS 资源标签标准	LOW	✓ 是	变更已触发
IAM.24	应标记 IAM 角色	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.25	应标记 IAM 用户	AWS 资源标签标准	LOW	✓ 是	变更已触发
IAM.26	应移除 IAM 中管理的过期 SSL/TLS 证书	CIS AWS 基金会基准 v5.0.0，CIS AWS 基金会基准 v3.0.0	MEDIUM	⊗没有	定期
IAM.27	IAM 身份不应附加 AWSCloudShellFullAccess 策略	CIS AWS 基金会基准 v5.0.0，CIS AWS 基金会基准 v3.0.0	MEDIUM	⊗没有	变更已触发
IAM.28	应启用 IAM Access Analyzer 外部访问分析器	CIS AWS 基金会基准 v5.0.0，CIS AWS 基金会基准 v3.0.0	HIGH	⊗没有	定期
Inspector.1	应启用 Amazon Inspector EC2 扫描	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
Inspector.2	应启用 Amazon Inspector ECR 扫描	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
Inspector.3	应启用 Amazon Inspector Lambda 代码扫描	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
Inspector.4	应启用 Amazon Inspector Lambda 标准扫描	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期
IoT.1	AWS IoT Device Defender 应标记安全配置文件	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoT.2	AWS IoT Core 应标记缓解措施	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IoT.3	AWS IoT Core 应给尺寸加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoT.4	AWS IoT Core 应给授权者加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoT.5	AWS IoT Core 应标记角色别名	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoT.6	AWS IoT Core 策略应该被标记	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTEvents.1	AWS IoT Events 应标记输入	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTEvents.2	AWS IoT Events 应标记探测器型号	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTEvents.3	AWS IoT Events 应标记警报型号	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTSiteWise.1	AWS IoT SiteWise 应为资产模型加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTSiteWise.2	AWS IoT SiteWise 仪表板应该被标记	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTSiteWise.3	AWS IoT SiteWise 应该给网关加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTSiteWise.4	AWS IoT SiteWise 应该给门户加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTSiteWise.5	AWS IoT SiteWise 应该给项目加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IoTTwinMaker.1	AWS 应标记 IoT TwinMaker 同步作业	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTTwinMaker.2	AWS 应标 TwinMaker 记 IoT 工作空间	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTTwinMaker.3	AWS 应标记物联网 TwinMaker 场景	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTTwinMaker.4	AWS 应标记物联网 TwinMaker 实体	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTWireless.1	AWS 应标记 IoT Wireless 组播组	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTWireless.2	AWS 应标记 IoT Wireless 服务配置文件	AWS 资源标签标准	LOW	✓ 是	变更已触发
IoTWireless.3	AWS 应标记 IoT Wireless FUOTA 任务	AWS 资源标签标准	LOW	✓ 是	变更已触发
IVS.1	应标记 IVS 播放密钥对	AWS 资源标签标准	LOW	✓ 是	变更已触发
IVS.2	应标记 IVS 录制配置	AWS 资源标签标准	LOW	✓ 是	变更已触发
IVS.3	应标记 IVS 频道	AWS 资源标签标准	LOW	✓ 是	变更已触发
Keyspaces.1	应标记 Amazon Keyspaces 密钥空间	AWS 资源标签标准	LOW	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Kinesis.1	Kinesis 直播应在静态状态下进行加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Kinesis.2	应标记 Kinesis 流	AWS 资源标签标准	LOW	✓ 是	变更已触发
Kinesis.3	Kinesis 流应有足够的数据留存期	AWS 基础安全最佳实践	MEDIUM	✓ 是	变更已触发
KMS.1	IAM 客户管理型策略不应允许对所有 KMS 密钥执行解密操作	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
KMS.2	IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
KMS.3	AWS KMS keys 不应无意中删除	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	关键	⊗没有	变更已触发
KMS.4	AWS KMS key 应该启用旋转	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、NAWS IST SP 800-53 修订版 5、PCI DSS v3.2.1、PCI DSS v4.0.1	MEDIUM	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
KMS.5	KMS 密钥不应可公开访问	AWS 基础安全最佳实践	关键	⊗没有	变更已触发
Lambda.1	Lambda 函数策略应禁止公共访问	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	关键	⊗没有	变更已触发
Lambda.2	Lambda 函数应使用受支持的运行时系统	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
Lambda.3	Lambda 函数应位于 VPC 中	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
Lambda.5	VPC Lambda 函数应在多个可用区内运行	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	变更已触发
Lambda.6	应标记 Lambda 函数	AWS 资源标签标准	LOW	✓ 是	变更已触发
Lambda.7	Lambda 函数应启用 AWS X-Ray 主动跟踪	NIST SP 800-53 Rev. 5	低	⊗没有	变更已触发
Macie.1	应启用 Amazon Macie	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	定期
Macie.2	应启用 Macie 敏感数据自动发现	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
MSK.1	MSK 集群应在代理节点之间传输时进行加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
MSK.2	MSK 集群应配置增强监控	NIST SP 800-53 Rev. 5	低	⊗没有	变更已触发
MSK.3	应在传输过程中加密 MSK Connect 连接器	AWS 基础安全最佳实践，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
MSK.4	MSK 集群应禁用公开访问	AWS 基础安全最佳实践	关键	⊗没有	变更已触发
MSK.5	MSK 连接器应启用日志记录	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
MSK.6	MSK 集群应禁用未经身份验证的访问	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
MQ.2	ActiveMQ 代理应将审核日志流式传输到 CloudWatch	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
MQ.4	应标记 Amazon MQ 代理	AWS 资源标签标准	LOW	✓ 是	变更已触发
MQ.5	ActiveMQ 代理应该使用部署模式 active/standby	NIST SP 800-53 Rev. 5	低	⊗没有	变更已触发
MQ.6	RabbitMQ 代理应该使用集群部署模式	NIST SP 800-53 Rev. 5	低	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Neptune.1	应对 Neptune 数据库集群进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Neptune.2	Neptune 数据库集群应将审核日志发布到日志 CloudWatch	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
Neptune.3	Neptune 数据库集群快照不应公开	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	关键	⊗没有	变更已触发
Neptune.4	Neptune 数据库集群应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
Neptune.5	Neptune 数据库集群应启用自动备份	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	变更已触发
Neptune.6	应对 Neptune 数据库集群快照进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Neptune.7	Neptune 数据库集群应启用 IAM 数据库身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Neptune.8	应将 Neptune 数据库集群配置为将标签复制到快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Neptune.9	Neptune 数据库集群应部署在多个可用区中	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
NetworkFirewall.1	Network Firewall 防火墙应跨多个可用区部署	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
NetworkFirewall.2	应启用 Network Firewall 日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	定期
NetworkFirewall.3	Network Firewall 策略应至少关联一个规则组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	变更已触发
NetworkFirewall.4	Network Firewall 策略的默认无状态操作应为丢弃或转发完整数据包	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
NetworkFirewall.5	Network Firewall 策略的默认无状态操作应为丢弃或转发分段数据包	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
NetworkFirewall.6	无状态网络防火墙规则组不应为空	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	变更已触发
NetworkFirewall.7	应标记 Network Firewall 防火墙	AWS 资源标签标准	LOW	✓ 是	变更已触发
NetworkFirewall.8	应标记 Network Firewall 防火墙策略	AWS 资源标签标准	LOW	✓ 是	变更已触发
NetworkFirewall.9	Network Firewall 防火墙应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
NetworkFirewall.10	Network Firewall 防火墙应启用子网更改保护	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
Opensearch.1	OpenSearch 域应启用静态加密	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Opensearch.2	OpenSearch 域名不应公开访问	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	关键	⊗没有	变更已触发
Opensearch.3	OpenSearch 域应加密节点之间发送的数据	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Opensearch.4	OpenSearch 应该启用记录到 CloudWatch 日志的域错误	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Opensearch.5	OpenSearch 域应启用审核日志	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
Opensearch.6	OpenSearch 域应至少有三个数据节点	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Opensearch.7	OpenSearch 域名应启用细粒度访问控制	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
Opensearch.8	应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
Opensearch.9	OpenSearch 域名应该被标记	AWS 资源标签标准	LOW	✓ 是	变更已触发
Opensearch.10	OpenSearch 域名应安装最新的软件更新	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
Opensearch.11	OpenSearch 域应至少有三个专用的主节点	NIST SP 800-53 Rev. 5	低	⊗没有	定期
PCA.1	AWS 私有 CA 应禁用根证书颁发机构	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
PCA.2	AWS 应标记私有 CA 证书颁发机构	AWS 资源标签标准	LOW	✓ 是	变更已触发
RDS.1	RDS 快照应为私有快照	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	关键	✗ 没有	变更已触发
RDS.2	根据 PubliclyAccessible 配置，RDS 数据库实例应禁止公共访问	CIS AWS 基金会基准 v5.0.0，CIS AWS 基金会基准 v3.0.0，AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v3.2.1，PCI DSS v4.0.1	关键	✗ 没有	变更已触发
RDS.3	RDS 数据库实例应启用静态加密	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、CIS 基金会基准 v1.4.0、基础安全最佳实践 v1.0.0 AWS 、N AWS IST SP 800-53 修订版 5	MEDIUM	✗ 没有	变更已触发
RDS.4	RDS 集群快照和数据库快照应进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.5	RDS 数据库实例应配置多个可用区	CIS AWS Foundations Benchmark v5.0.0，AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
RDS.6	应为 RDS 数据库实例配置增强监控	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊙ 是	变更已触发
RDS.7	RDS 集群应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
RDS.8	RDS 数据库实例应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
RDS.9	RDS 数据库实例应将日志发布到 CloudWatch 日志	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
RDS.10	应为 RDS 实例配置 IAM 身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
RDS.11	RDS 实例应启用自动备份	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	变更已触发
RDS.12	应为 RDS 集群配置 IAM 身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.13	应启用 RDS 自动次要版本升级	CIS AWS 基金会基准 v5.0.0，CIS AWS 基金会基准 v3.0.0，AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
RDS.14	Amazon Aurora 集群应启用回溯功能	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	变更已触发
RDS.15	应为多个可用区配置 RDS 数据库集群	CIS AWS Foundations Benchmark v5.0.0， AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
RDS.16	应将 Aurora 数据库集群配置为将标签复制到数据库快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
RDS.17	应将 RDS 数据库实例配置为将标签复制到快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
RDS.19	应为关键集群事件配置现有 RDS 事件通知订阅	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
RDS.20	应为关键数据库实例事件配置现有 RDS 事件通知订阅	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	LOW	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.21	应为关键数据库参数组事件配置 RDS 事件通知订阅	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	LOW	⊗没有	变更已触发
RDS.22	应为关键数据库安全组事件配置 RDS 事件通知订阅	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	LOW	⊗没有	变更已触发
RDS.23	RDS 实例不应使用数据库引擎的默认端口	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
RDS.24	RDS 数据库集群应使用自定义管理员用户名	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
RDS.25	RDS 数据库实例应使用自定义管理员用户名	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
RDS.26	RDS 数据库实例应受备份计划保护	NIST SP 800-53 Rev. 5	MEDIUM	⊙ 是	定期
RDS.27	应对 RDS 数据库集群进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
RDS.28	应标记 RDS 数据库集群	AWS 资源标签标准	LOW	⊙ 是	变更已触发
RDS.29	应标记 RDS 数据库集群快照	AWS 资源标签标准	LOW	⊙ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.30	应标记 RDS 数据库实例	AWS 资源标签标准	LOW	✓ 是	变更已触发
RDS.31	应标记 RDS 数据库安全组	AWS 资源标签标准	LOW	✓ 是	变更已触发
RDS.32	应标记 RDS 数据库快照	AWS 资源标签标准	LOW	✓ 是	变更已触发
RDS.33	应标记 RDS 数据库子网组	AWS 资源标签标准	LOW	✓ 是	变更已触发
RDS.34	Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
RDS.35	RDS 数据库集群应启用自动次要版本升级	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
RDS.36	适用于 PostgreSQL 的 RDS 数据库实例应将日志发布到日志 CloudWatch	AWS 基础安全最佳实践，PCI DSS v4.0.1	MEDIUM	✓ 是	变更已触发
RDS.37	Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch	AWS 基础安全最佳实践，PCI DSS v4.0.1	MEDIUM	✗ 没有	变更已触发
RDS.38	RDS for PostgreSQL 数据库实例应在传输过程中加密	AWS 基础安全最佳实践	MEDIUM	✗ 没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.39	RDS for MySQL 数据库实例应在传输过程中加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
RDS.40	适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	变更已触发
RDS.41	RDS for SQL Server 数据库实例应在传输过程中加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
RDS.42	适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	✓ 是	定期
RDS.43	RDS 数据库代理应要求对连接进行 TLS 加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
RDS.44	RDS for MariaDB 数据库实例应在传输过程中加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
RDS.45	Aurora MySQL 数据库集群应启用审核日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	定期
RDS.46	RDS 数据库实例不应部署在具有通往互联网网关路由的公共子网中	AWS 基础安全最佳实践	HIGH	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.47	应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照	AWS 基础安全最佳实践	LOW	⊗没有	变更已触发
RDS.48	应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照	AWS 基础安全最佳实践	LOW	⊗没有	变更已触发
RDS.50	RDS 数据库集群应设置足够的备份保留期	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗ 是	变更已触发
RDS.51	RDS 全局集群应在支持的 Aurora MySQL 版本上运行	AWS 基础安全最佳实践	HIGH	⊗没有	变更已触发
Redshift.1	Amazon Redshift 集群应禁止公共访问	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	关键	⊗没有	变更已触发
Redshift.2	与 Amazon Redshift 集群的连接应在传输过程中加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
Redshift.3	Amazon Redshift 集群应启用自动快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Redshift.4	Amazon Redshift 集群应启用审核日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
Redshift.6	Amazon Redshift 应该启用自动升级到主要版本的功能	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Redshift.7	Redshift 集群应使用增强型 VPC 路由	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Redshift.8	Amazon Redshift 集群不应使用默认管理员用户名	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Redshift.10	Redshift 集群应静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Redshift.11	应标记 Redshift 集群	AWS 资源标签标准	LOW	✓ 是	变更已触发
Redshift.12	应标记 Redshift 事件通知订阅	AWS 资源标签标准	LOW	✓ 是	变更已触发
Redshift.13	应标记 Redshift 集群快照	AWS 资源标签标准	LOW	✓ 是	变更已触发
Redshift.14	应标记 Redshift 集群子网组	AWS 资源标签标准	LOW	✓ 是	变更已触发
Redshift.15	Redshift 安全组应仅允许从受限来源到集群端口的入口流量	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Redshift.16	Redshift 集群子网组应具有来自多个可用区的子网	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
Redshift.17	应标记 Redshift 集群参数组	AWS 资源标签标准	LOW	✓ 是	变更已触发
Redshift.18	Redshift 集群应启用部署 Multi-AZ	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
RedshiftServerless.1	Amazon Redshift Serverless 工作组应使用增强型 VPC 路由	AWS 基础安全最佳实践	HIGH	⊗没有	定期
RedshiftServerless.2	连接到 Redshift Serverless 工作组时应需要使用 SSL	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
RedshiftServerless.3	Redshift Serverless 工作组应禁止公开访问	AWS 基础安全最佳实践	HIGH	⊗没有	定期
RedshiftServerless.4	Redshift 无服务器命名空间应使用客户托管进行加密 AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIUM	✓ 是	定期
RedshiftServerless.5	Redshift Serverless 命名空间不应使用默认管理员用户名	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
RedshiftServerless.6	Redshift 无服务器命名空间应将日志导出到日志 CloudWatch	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Route53.1	应标记 Route53 运行状况检查	AWS 资源标签标准	LOW	✅ 是	变更已触发
Route53.2	Route 53 公共托管区域应记录 DNS 查询	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	❌没有	变更已触发
S3.1	S3 通用存储桶应启用屏蔽公共访问权限设置	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、PCI DSS v3.2.1、PCI DSS v3.2.1、PCI DSS v4.0.1	MEDIUM	❌没有	定期
S3.2	S3 通用存储桶应阻止公共读取访问权限	AWS 基础安全最佳实践，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	关键	❌没有	变更已触发且定期进行
S3.3	S3 通用存储桶应阻止公共写入访问权限	AWS 基础安全最佳实践，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	关键	❌没有	变更已触发且定期进行

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
S3.5	S3 通用存储桶应需要请求才能使用 SSL	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、NIST SP 800-171 修订版 2、PCI DSS v3.2.1、PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
S3.6	S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 Rev. 2	HIGH	⊗没有	变更已触发
S3.7	S3 通用存储桶应使用跨区域复制	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	LOW	⊗没有	变更已触发
S3.8	S3 通用存储桶应屏蔽公共访问权限	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、CIS 基金会基准 v1.4.0、基础安全最佳实践、NAWS IST SP 800-53 修订版 5 AWS 、PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
S3.9	S3 通用存储桶应启用服务器访问日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
S3.10	启用版本控制的 S3 通用存储桶应具有生命周期配置	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
S3.11	S3 存储桶应启用事件通知	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	MEDIUM	✓ 是	变更已触发
S3.12	不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
S3.13	S3 通用存储桶应具有生命周期配置	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	LOW	✓ 是	变更已触发
S3.14	S3 通用存储桶应启用版本控制	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	LOW	⊗没有	变更已触发
S3.15	S3 通用存储桶应启用对象锁定	NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	MEDIUM	✓ 是	变更已触发
S3.17	S3 通用存储桶应使用静态加密 AWS KMS keys	NIST SP 800-53 Rev. 5，NIST SP 800-171 Rev. 2，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
S3.19	S3 接入点应启用屏蔽公共访问权限设置	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	关键	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
S3.20	S3 通用存储桶应启用 MFA 删除功能	CIS AWS 基金会基准 v5.0.0、CIS 基金会基准 v3.0.0、CIS AWS 基金会基准 v1.4.0、NAWS IST SP 800-53 修订版 5	LOW	⊗没有	变更已触发
S3.22	S3 通用存储桶应记录对象级写入事件	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、PCI DSS v4.0.1	MEDIUM	⊗没有	定期
S3.23	S3 通用存储桶应记录对象级读取事件	CIS AWS 基金会基准 v5.0.0、CIS AWS 基金会基准 v3.0.0、PCI DSS v4.0.1	MEDIUM	⊗没有	定期
S3.24	S3 Multi-Region 接入点应启用屏蔽公共访问设置	AWS 基础安全最佳实践，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
S3.25	S3 目录存储桶应具有生命周期配置	AWS 基础安全最佳实践	LOW	⊘ 是	变更已触发
SageMaker.1	Amazon SageMaker 笔记本实例不应直接访问互联网	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	HIGH	⊗没有	定期
SageMaker.2	SageMaker 笔记本实例应在自定义 VPC 中启动	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SageMaker.3	用户不应拥有 SageMaker 笔记本实例的 root 访问权限	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH	⊗没有	变更已触发
SageMaker.4	SageMaker 端点生产变体的初始实例数应大于 1	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	定期
SageMaker.5	SageMaker 模型应启用网络隔离	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
SageMaker.6	SageMaker 应用映像配置应加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
SageMaker.7	SageMaker 应给图片加标签	AWS 资源标签标准	LOW	✓ 是	变更已触发
SageMaker.8	SageMaker 笔记本实例应在支持的平台上运行	AWS 基础安全最佳实践	MEDIUM	⊗没有	定期
SageMaker.9	SageMaker 数据质量任务定义应启用容器间流量加密	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
SageMaker.10	SageMaker 模型可解释性任务定义应启用容器间流量加密	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
SageMaker.11	SageMaker 数据质量作业定义应启用网络隔离	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
SageMaker.12	SageMaker 模型偏差任务定义应启用网络隔离	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SageMaker.13	SageMaker 模型质量任务定义应启用容器间流量加密	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
SageMaker.14	SageMaker 监控计划应启用网络隔离	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
SageMaker.15	SageMaker 模型偏差任务定义应启用容器间流量加密	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	变更已触发
SageMaker.16	SageMaker 模型应该在 VPC 中为主容器使用私有注册表	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
SageMaker.17	SageMaker 功能组离线存储应使用 AWS KMS 密钥进行加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
SageMaker.18	SageMaker 具有标准存储空间的功能组在线商店应使用 AWS KMS 密钥进行加密	NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
SageMaker.19	SageMaker 模型应在 VPC 中使用私有注册表进行多容器推理管道	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
SecretsManager.1	Secrets Manager 密钥应启用自动轮换	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✓ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SecretsManager.2	配置自动轮换的 Secrets Manager 密钥应成功轮换	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	变更已触发
SecretsManager.3	移除未使用 Secrets Manager 密钥	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊙ 是	定期
SecretsManager.4	Secrets Manager 密钥应在指定的天数内轮换	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊙ 是	定期
SecretsManager.5	应标记 Secrets Manager 密钥	AWS 资源标签标准	LOW	⊙ 是	变更已触发
ServiceCatalog.1	Service Catalog 产品组合只能在 AWS 组织内部共享	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	定期
SES.1	应标记 SES 联系人名单	AWS 资源标签标准	LOW	⊙ 是	变更已触发
SES.2	应标记 SES 配置集	AWS 资源标签标准	LOW	⊙ 是	变更已触发
SES.3	SES 配置集应启用 TLS 以发送电子邮件	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
SNS.1	SNS 主题应使用以下方法进行静态加密 AWS KMS	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	MEDIUM	⊗没有	变更已触发
SNS.3	应标记 SNS 主题	AWS 资源标签标准	LOW	⊙ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SNS.4	SNS 主题访问策略不应允许公共访问	AWS 基础安全最佳实践	关键	⊗没有	变更已触发
SQS.1	应对 Amazon SQS 队列进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
SQS.2	应标记 SQS 队列	AWS 资源标签标准	LOW	✓ 是	变更已触发
SQS.3	SQS 队列访问策略不应允许公开访问	AWS 基础安全最佳实践	关键	⊗没有	变更已触发
SSM.1	EC2 实例应由以下人员管理 AWS Systems Manager	AWS 基础安全最佳实践 v1.0.0，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
SSM.2	由 Systems Manager 管理的 EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2，PCI DSS v3.2.1，PCI DSS v4.0.1，PCI DSS v4.0.1	HIGH	⊗没有	变更已触发
SSM.3	由 Systems Manager 管理的 EC2 实例的关联合规性的状态应为 COMPLIANT	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，PCI DSS v3.2.1，PCI DSS v4.0.1	LOW	⊗没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SSM.4	SSM 文档不应公开	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	关键	⊗没有	定期
SSM.5	应标记 SSM 文档	AWS 资源标签标准	LOW	⊙ 是	变更已触发
SSM.6	SSM 自动化应该 CloudWatch 启用日志记录	AWS 基础安全最佳实践 v1.0.0	MEDIUM	⊗没有	定期
SSM.7	SSM 文档应启用“阻止公开共享”设置	AWS 基础安全最佳实践 v1.0.0	关键	⊗没有	定期
StepFunctions.1	Step Functions 状态机应该开启日志功能	AWS 基础安全最佳实践 v1.0.0，PCI DSS v4.0.1	MEDIUM	⊙ 是	变更已触发
StepFunctions.2	应标记 Step Functions 活动	AWS 资源标签标准	LOW	⊙ 是	变更已触发
Transfer.1	应标记 Transfer Family 工作流程	AWS 资源标签标准	LOW	⊙ 是	变更已触发
Transfer.2	Transfer Family 服务器不应使用 FTP 协议进行端点连接	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	⊗没有	定期
Transfer.3	Transfer Family 连接器应启用日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	MEDIUM	⊗没有	变更已触发
Transfer.4	应标记 Transfer Family 协议	AWS 资源标签标准	LOW	⊙ 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Transfer.5	应标记 Transfer Family 证书	AWS 资源标签标准	LOW	✓ 是	变更已触发
Transfer.6	应标记 Transfer Family 连接器	AWS 资源标签标准	LOW	✓ 是	变更已触发
Transfer.7	应标记 Transfer Family 配置文件	AWS 资源标签标准	LOW	✓ 是	变更已触发
WAF.1	AWS 应启用 WAF 经典版全球 Web ACL 日志记录	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5，PCI DSS v4.0.1	MEDIUM	✗ 没有	定期
WAF.2	AWS WAF 经典区域规则应至少有一个条件	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
WAF.3	AWS WAF 经典区域规则组应至少有一条规则	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
WAF.4	AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
WAF.6	AWS WAF Classic 全局规则应至少有一个条件	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发
WAF.7	AWS WAF Classic 全局规则组应至少有一条规则	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	✗ 没有	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
WAF.8	AWS WAF Classic 全球 Web ACL 应至少有一个规则或规则组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
WAF.10	AWS WAF Web ACL 应至少有一个规则或规则组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	MEDIUM	⊗没有	变更已触发
WAF.11	AWS 应启用 WAF 网络 ACL 日志记录	NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	LOW	⊗没有	定期
WAF.12	AWS WAF 规则应启用 CloudWatch 指标	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，NIST SP 800-171 修订版 2	MEDIUM	⊗没有	变更已触发
WorkSpaces.1	WorkSpaces 用户卷应在静态时加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发
WorkSpaces.2	WorkSpaces 根卷应在静态时加密	AWS 基础安全最佳实践	MEDIUM	⊗没有	变更已触发

Security Hub CSPM 控件的更改日志

以下更改日志跟踪现有 Sec AWS urity Hub CSPM 控件的重大更改，这些更改可能会导致控制的整体状态及其发现的合规性状态发生变化。有关 Security Hub CSPM 如何评估控件状态的信息，请参阅评估合规性状态和控件状态。在将更改输入此日志后，可能需要几天时间才能影响所有 AWS 区域 可用的控件。

此日志跟踪自 2023 年 4 月以来发生的更改。选择一个控件以查看其相关的更多详细信息。标题更改将在控件的详细描述中记录 90 天。

变更日期	控件 ID 和标题	更改的说明
2026年6月5日	[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥	Security Hub CSPM 通知说，该控件将在2026年8月10日之后停用并从所有适用的Security Hub CSPM标准中删除。从 Kubernetes 版本 1.28 开始，Amazon EKS 集群默认使用信封加密保护 Kubernetes 机密。
2026年6月5日	[IoTEvents.1] AWS 应标记 IoT Events 输入内容	Security Hub CSPM 通知说，该控件将在2026年7月7日之后停用并从所有适用的 Security Hub CSPM 标准中删除。 AWS 宣布从 2026 年 5 月 20 日起终止对 AWS IoT Events 服务的支持。
2026年6月5日	[IoTEvents.2] AWS 应标记 IoT Events 探测器模型	Security Hub CSPM 通知说，该控件将在2026年7月7日之后停用并从所有适用的 Security Hub CSPM 标准中删除。 AWS 宣布从 2026 年 5 月 20 日起终止对 AWS IoT Events 服务的支持。
2026年6月5日	[IoTEvents.3] AWS 应标记 IoT Events 警报模型	Security Hub CSPM 通知说，该控件将在2026年7月7日之后

变更日期	控件 ID 和标题	更改的说明
		停用并从所有适用的 Security Hub CSPM 标准中删除。 AWS 宣布从 2026 年 5 月 20 日起终止对 AWS IoT Events 服务的支持。
2026年6月5日	[ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义	Security Hub CSPM 取消了此控件，并将其从所有适用的标准中删除。此前，该控件会检查使用主机联网模式的有效 Amazon ECS 任务定义`privileged` 是否也有`user`容器定义。
2026年6月5日	[RDS.18] RDS 实例应部署在 VPC 中	Security Hub CSPM 取消了此控件，并将其从所有适用的标准中删除。由于亚马逊 EC2-Classic网络已停用，因此无法再在 VPC 外部部署亚马逊关系数据库服务 (Amazon RDS) 实例。之前，该控件会检查是否在上部署了 Amazon RDS 实例 EC2-VPC。

变更日期	控件 ID 和标题	更改的说明
2026 年 5 月 4 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持`ruby4.0`作为参数，不再包含此运行`nodejs20.x` 时 AWS Lambda 已弃用。
2026 年 4 月 27 日	[EC2.4] 应在指定时间段后移除已停止的 EC2 实例	为了简化评估逻辑，Security Hub CSPM 将此控件的支持规则从 ec2 停止实例更改为自定义 Security Hub CSPM 规则，即 ec2-stopped-instance-days-check。
2026 年 4 月 7 日	[EC2.1] 不应将 Amazon EBS 快照配置为可公开还原	Security Hub CSPM 更改了此控件的标题和描述。新的标题和描述更准确地反映了控件会检查 Amazon EBS 快照是否配置为可公开恢复。以前，此控件的标题是：Amazon EBS 快照不应公开恢复。

变更日期	控件 ID 和标题	更改的说明
2026 年 4 月 7 日	[EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置	Security Hub CSPM 更改了此控件的标题和描述。新的标题和描述更准确地反映了该控件检查是否为 Amazon EBS 快照启用了账户级别的封锁公开访问权限。以前，此控件的标题是：Amazon EBS 快照不应向公众开放。
2026年4月6日	[ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略	Security Hub CSPM 更新了此控件的参数值，以反映推荐的安全策略。
2026 年 4 月 3 日	[Cognito.3] Cognito 用户池的密码策略应具有可靠的配置	Security Hub CSPM 扩大了此控件`temporaryPasswordValidity` 参数的支持值范围。现在，您可以指定一个介于 1-365 天之间的值。以前，该区间为7-365天。

变更日期	控件 ID 和标题	更改的说明
2026 年 4 月 3 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件检查 Amazon EKS 集群是否在支持的 Kubernetes 版本上运行。Security Hub CSPM 将此控件的参数值从 `1.32` 更改为 `1.33`。亚马逊 EKS 对 Kubernetes 1.32 版本的标准支持已于 2026 年 3 月 23 日结束。
2026 年 4 月 3 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 支持的运行时的参数不再包含在内，因`ruby3.2`为 Lambda 已弃用此运行时。
2026年3月24日	[RDS.50] RDS 数据库集群应设置足够的备份保留期	Security Hub CSPM 更新了控件标题，以反映该控件会检查所有 RDS 数据库集群。
2026年3月24日	[ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限	Security Hub CSPM 更新了控件标题和描述，以反映该控件检查 ECS 任务定义的情况。Security Hub CSPM 还更新了控件，使其不为`runtimePlatform` 配置为指定`WINDOWS_SERVER` 操作系统系列的任务定义生成调查结果。

变更日期	控件 ID 和标题	更改的说明
2026年3月9日	[AppSync.1] AWS AppSync API 缓存应在静态状态下进行加密	Security Hub CSPM 停用了此控件，并将其从AWS 基础安全最佳实践 (FSB P) 标准中删除。 AWS AppSync 现在为所有当前和未来的 API 缓存提供默认加密。
2026年3月9日	[AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密	Security Hub CSPM 停用了此控件，并将其从AWS 基础安全最佳实践 (FSB P) 标准中删除。 AWS AppSync 现在为所有当前和未来的 API 缓存提供默认加密。
2026 年 3 月 4 日	[ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义	Security Hub CSPM 取消了此控件，并将其从AWS 基础安全最佳实践 (FSBP) 标准和 NIST SP 800-53 Rev. 5 标准中删除。
2026 年 2 月 5 日	[AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密	Security Hub CSPM 将于2026年3月9日取消该控制权，并从所有适用的Security Hub CSPM标准中删除。 AWS AppSync 正在为所有当前和未来的 API 缓存提供默认加密。

变更日期	控件 ID 和标题	更改的说明
2026 年 2 月 5 日	[AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密	Security Hub CSPM 将于2026年3月9日取消该控制权，并从所有适用的Security Hub CSPM标准中删除。AWS AppSync 正在为所有当前和未来的 API 缓存提供默认加密。
2026 年 1 月 16 日	[ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义	Security Hub CSPM 通知说，该控件将在2026年2月16日之后停用并从所有适用的Security Hub CSPM标准中删除。
2026 年 1 月 12 日	[Redshift.4] Amazon Redshift 集群应启用审核日志记录	Security Hub CSPM 更新了此控件以删除该参数。`loggingEnabled`

变更日期	控件 ID 和标题	更改的说明
2026 年 1 月 12 日	[MQ.3] Amazon MQ 代理应启用自动次要版本升级	Security Hub CSPM 停用了该控件，并将该控件从所有适用标准中删除。由于亚马逊 MQ 要求自动升级次要版本，Security Hub CSPM 取消了控制权。 以前，该控制适用于AWS 基础安全最佳实践 (FSBP) 标准、NIST SP 800-53 Rev. 5 标准和 PCI DSS v4.0.1 标准。
2026 年 1 月 12 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值相匹配。Security Hub CSPM 现在支持`dotnet10`作为此控件的参数值。 AWS Lambda 添加了对此运行时的支持。

变更日期	控件 ID 和标题	更改的说明
2025 年 12 月 15 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值相匹配。Security Hub CSPM 不再支持`python3.9` 作为此控件的参数值。AWS Lambda 不再支持此运行时。
2025 年 12 月 12 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件检查 Amazon EKS 集群是否在支持的 Kubernetes 版本上运行。Security Hub CSPM 将此控件的参数值从 `1.31` 更改为 `1.32`。亚马逊 EKS 对 Kubernetes 1.31 版本的标准支持已于 2025 年 11 月 26 日结束。
2025 年 11 月 21 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值相匹配。Security Hub CSPM 现在支持`nodejs24.x` 和`python3.14` 作为此控件的参数值。AWS Lambda 添加了对这些运行时的支持。

变更日期	控件 ID 和标题	更改的说明
2025 年 11 月 14 日	[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址	Security Hub CSPM 更新了此控件的描述和基本原理。以前，该控件仅使用该标志检查 Amazon VPC 子网中的 IPv4 公有 IP 自动分配。`MapPublicIpOnLaunch` 此控件现在会同时检查 IPv4 和 IPv6 公有 IP 的自动分配。该控件的描述和基本原理已更新，以反映这些变化。
2025 年 11 月 14 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值相匹配。Security Hub CSPM 现在支持将 `java25` 作为此控件的参数值。 AWS Lambda 添加了对此运行时的支持。
2025 年 11 月 13 日	[SNS.4] SNS 主题访问策略不应允许公共访问	Security Hub CSPM 将此控件的严重性从`HIGH`更改为。`CRITICAL`允许公众访问 Amazon SNS 主题会带来严重的安全风险。

变更日期	控件 ID 和标题	更改的说明
2025 年 11 月 13 日	[SQS.3] SQS 队列访问策略不应允许公开访问	Security Hub CSPM 将此控件的严重性从HIGH更改为。CRITICAL允许公众访问 Amazon SQS 队列会带来严重的安全风险。
2025 年 11 月 13 日	[GuardDuty.7] 应启用 GuardDuty EKS 运行时监控	Security Hub CSPM 将此控件的严重性从MEDIUM更改为。HIGH这种类型的运行时监控可增强对 Amazon EKS 资源的威胁检测。
2025 年 11 月 13 日	[MQ.3] Amazon MQ 代理应启用自动次要版本升级	Security Hub CSPM 将此控件的严重性从LOW更改为。MEDIUM次要版本升级包括维护 Amazon MQ 代理安全所需的安全补丁。
2025 年 11 月 13 日	[Opensearch.10] OpenSearch 域名应安装最新的软件更新	Security Hub CSPM 将此控件的严重性从LOW更改为。MEDIUM软件更新包括维护 OpenSearch 域安全所需的安全补丁。

变更日期	控件 ID 和标题	更改的说明
2025 年 11 月 13 日	[RDS.7] RDS 集群应启用删除保护	Security Hub CSPM 将此控件的严重性从LOW更改为。MEDIUM删除保护有助于防止未经授权的实体意外删除 Amazon RDS 数据库和删除 RDS 数据库。
2025 年 11 月 13 日	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成	Security Hub CSPM 将此控件的严重性从LOW更改为。MEDIUM AWS CloudTrail Amazon CloudWatch Logs 中的日志数据可用于审计活动、警报和其他重要的安全操作。
2025 年 11 月 13 日	[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享	Security Hub CSPM 将此控件的严重性从HIGH更改为。MEDIUM与特定账户共享 AWS Service Catalog 投资组合可能是故意的，并不一定表示投资组合可以公开访问。

变更日期	控件 ID 和标题	更改的说明
2025 年 11 月 13 日	[CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS	Security Hub CSPM 将此控件的严重性从MEDIUM更改为。LOWAmazon CloudFront 分配的默认cloudfront.net 域名是随机生成的，这降低了安全风险。
2025 年 11 月 13 日	[ELB.7] 经典负载均衡器应启用连接耗尽功能	Security Hub CSPM 将此控件的严重性从MEDIUM更改为。LOW在多实例部署中，其他运行状况良好的实例可以在实例终止时处理用户会话，而不会耗尽连接，从而降低运营影响和可用性风险。
2025 年 11 月 13 日	[RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名	Security Hub CSPM 更新了此控件以删除可选validAdminUserNames 参数。
2025 年 10 月 23 日	[ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份	Security Hub CSPM 于 2025 年 10 月 14 日恢复了对此控件的标题、描述和规则所做的更改。

变更日期	控件 ID 和标题	更改的说明
2025 年 10 月 22 日	[CloudFront.1] CloudFront 发行版应配置默认根对象	Security Hub CSPM 更新了此控件，使其不为使用自定义来源的亚马逊 CloudFront 发行版生成调查结果。
2025 年 10 月 16 日	[CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略	此控件会检查 Amazon CloudFront 分配是否配置为使用推荐的 TLS 安全策略。Security Hub CSPM 现在支持 `TLSv1.2_2025` 和 `TLSv1.3_2025` 作为此控件的参数值。

变更日期	控件 ID 和标题	更改的说明
2025 年 10 月 14 日	[ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份	Security Hub CSPM 更改了此控件的标题、描述和规则。之前，该控件使用 elasticache-redis-cluster-automatic-backup-check 规则检查 Redis OSS 集群和所有复制组。控件的标题是：ElastiCache（Redis OSS）集群应启用自动备份。 现在，除了 Redis OSS 集群和所有复制组之外，此控件还会使用 elasticache-automatic-backup-check-enabled 规则检查 Valkey 集群。新的标题和描述反映该控件检查两种类型的集群。

变更日期	控件 ID 和标题	更改的说明
2025 年 10 月 5 日	[Opensearch.10] OpenSearch 域名应安装最新的软件更新	此控件的规则已更新，还会生成一个PASSED结果，即某个 Amazon S OpenSearch ervice 域名是否没有可用的软件更新且更新状态不符合资格。以前，只有当 OpenSearch 域没有可用的软件更新且更新状态已完成时，此控件才会生成PASSED调查结果。
2025 年 9 月 24 日	[Redshift.9] Redshift 集群不应使用默认的数据库名称 [RedshiftServerless.7] Redshift Serverless 命名空间不应使用默认数据库名称	Security Hub CSPM 停用了这些控件，并将其从所有适用的标准中移除。Security Hub CSPM 停用了这些控件，这是因为 Amazon Redshift 固有的限制导致无法有效修复控件的 FAILED 调查发现。 以前，控件适用于 AWS 基础安全最佳实践（FSBP）标准和 NIST SP 800-53 Rev. 5 标准。该 Redshift. 9 控制也适用于AWS Control Tower 服务管理标准。

变更日期	控件 ID 和标题	更改的说明
2025 年 9 月 9 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值相匹配。Security Hub CSPM 不再支持`nodejs18.x` 作为此控件的参数值。AWS Lambda 不再支持 Node.js 18 个运行时。
2025 年 8 月 13 日	[SageMaker.5] SageMaker 模型应启用网络隔离	Security Hub CSPM 更改了此控件的标题和描述。新的标题和描述更准确地反映了控件会检查 Amazon A SageMaker I 托管模型的`EnableNetworkIsolation` 参数设置。以前，此控件的标题为：SageMaker models should block inbound traffic。

变更日期	控件 ID 和标题	更改的说明
2025 年 8 月 13 日	[EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联	Security Hub CSPM 更改了此控件的标题和描述。新的标题和描述更准确地反映了该控件所执行的检查的范围和性质。以前，此控件的标题为：EFS mount targets should not be associated with a public subnet。
2025 年 7 月 24 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件检查 Amazon EKS 集群是否在支持的 Kubernetes 版本上运行。Security Hub CSPM 将此控件的参数值从 `1.30` 更改为 `1.31`。Amazon EKS 对 Kubernetes 版本 1.30 的标准支持已于 2025 年 7 月 23 日结束。

变更日期	控件 ID 和标题	更改的说明
2025 年 7 月 23 日	[EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密	Security Hub CSPM 更改了此控件的标题。新标题更准确地反映了该控件仅检查指定了启动参数的 Amazon EC2 竞价型实例集请求。以前，此控件的标题为：EC2 Spot Fleet requests should enable encryption for attached EBS volumes。
2025 年 6 月 30 日	[IAM.13] 确保 IAM 密码策略要求包含至少一个符号	Security Hub CSPM 从 PCI DSS v4.0.1 标准中移除了此控件。PCI DSS v4.0.1 没有明确要求在密码中使用符号。
2025 年 6 月 30 日	[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效	Security Hub CSPM 从 NIST SP 800-171 修订版 2 标准中移除了此控件。NIST SP 800-171 修订版 2 没有明确要求密码过期时间为 90 天或更短。

变更日期	控件 ID 和标题	更改的说明
2025 年 6 月 30 日	[RDS.16] 应将 Aurora 数据库集群配置为将标签复制到数据库快照	Security Hub CSPM 更改了此控件的标题。新标题更准确地反映了该控件仅检查 Amazon Aurora DB 集群。以前，此控件的标题为：RDS DB clusters should be configured to copy tags to snapshots。
2025 年 6 月 30 日	[SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行	此控件根据为笔记本实例指定的平台标识符，检查 SageMaker Amazon AI 笔记本实例是否配置为在支持的平台上运行。Security Hub CSPM 不再支持 `notebook-al2-v1` 和 `notebook-al2-v2` 作为此控件的参数值。在这些平台上运行的笔记本实例已于 2025 年 6 月 30 日停止支持。

变更日期	控件 ID 和标题	更改的说明
2025 年 5 月 30 日	[IAM.10] IAM 用户的密码策略应具有很强的配置	Security Hub CSPM 从 PCI DSS v4.0.1 标准中移除了此控件。此控件检查 IAM 用户的账户密码策略是否满足最低要求，包括密码长度至少为 7 个字符。PCI DSS v4.0.1 现在要求密码至少包含 8 个字符。此控件继续适用于 PCI DSS v3.2.1 标准，该标准具有不同的密码要求。 要根据 PCI DSS v4.0.1 要求评估账户密码策略，您可以使用该控件。IAM.7 此控件要求密码至少包含 8 个字符。它还对密码长度和其他参数支持自定义值。该 IAM.7控件是 Security Hub CSPM 中 PCI DSS v4.0.1 标准的一部分。
2025 年 5 月 8 日	[RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中	Security Hub CSPM 全面撤销了 RDS.46 控件的发布。 AWS 区域以前，此控件支持 AWS 基础安全最佳实践 (FSBP) 标准。

变更日期	控件 ID 和标题	更改的说明
2025 年 4 月 7 日	[ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略	此控件检查应用程序负载均衡器的 HTTPS 侦听器或网络负载均衡器的 TLS 侦听器是否配置为使用推荐的安全策略对传输中数据进行加密。Security Hub CSPM 现在支持此控件的两个附加参数值：`ELBSecurityPolicy-TLS13-1-2-Res-2021-06` 和 `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04` 。
2025 年 3 月 27 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值匹配。Security Hub CSPM 现在支持`ruby3.4`作为此控件的参数值。 AWS Lambda 添加了对此运行时的支持。

变更日期	控件 ID 和标题	更改的说明
2025 年 3 月 26 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件可检查 Amazon Elastic Kubernetes Service（Amazon EKS）集群是否在支持的 Kubernetes 版本上运行。对于 `oldestVersionSupported` 参数，Security Hub CSPM 将其值从 `1.29` 更改为 `1.30`。目前支持的最旧 Kubernetes 版本是 `1.30`。
2025 年 3 月 10 日	[Lambda.2] Lambda 函数应使用支持的运行时	此控件检查 AWS Lambda 函数的运行时设置是否与每种语言支持的运行时的预期值匹配。Security Hub CSPM 不再支持`dotnet6`和`python3.8` 作为此控件的参数值。 AWS Lambda 不再支持这些运行时。

变更日期	控件 ID 和标题	更改的说明
2025 年 3 月 7 日	[RDS.18] RDS 实例应部署在 VPC 中	Security Hub CSPM 从 AWS 基础安全最佳实践标准中删除了此控件，并自动检查了 NIST SP 800-53 Rev. 5 的要求。由于亚马逊 EC2-Classic 网络已停用，因此无法再在 VPC 外部部署亚马逊关系数据库服务 (Amazon RDS) 实例。
2025 年 1 月 10 日	[Glue.2] AWS Glue 作业应启用日志记录	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。
2024 年 12 月 20 日	EC2.61 通过 EC2.169	Security Hub CSPM 撤销了 EC2.61 直通 EC2.169控件的发布。
2024 年 12 月 12 日	[RDS.23] RDS 实例不应使用数据库引擎的默认端口	RDS.23 检查 Amazon Relational Database Service (Amazon RDS) 集群或实例是否使用数据库引擎默认端口以外的端口。我们更新了控件，以便底层 AWS Config 规则返回属于集群`NOT_APPLICABLE` 的 RDS 实例的结果。

变更日期	控件 ID 和标题	更改的说明
2024 年 12 月 2 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `nodejs22.x` 作为参数。
2024 年 11 月 26 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件可检查 Amazon Elastic Kubernetes Service（Amazon EKS）集群是否在支持的 Kubernetes 版本上运行。目前支持的最旧版本是 `1.29`。

变更日期	控件 ID 和标题	更改的说明
2024 年 11 月 20 日	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录	Config.1 检查 AWS Config 是否已启用，使用服务相关角色，并记录已启用控件的资源。Security Hub CSPM 将此控件的严重性从 MEDIUM 提高到 CRITICAL。Security Hub CSPM 还为发现失败 Config.1 添加了新的状态代码和状态原因。这些变化反映了对 Securit Config.1 y Hub CSPM 控件操作的重要性。如果您禁用了 AWS Config 或禁用了资源记录，则可能会收到不准确的控制结果。 要接收PASSED调查结果 Config.1，请为与启用的 Security Hub CSPM 控件相对应的资源开启资源记录，并禁用组织中不需要的控件。有关配置 S AWS Config ecurity Hub CSPM 的说明，请参阅。启用和配置 AWS Config 适用于 Security Hub CSPM有关 Security Hub CSPM 控件及其

变更日期	控件 ID 和标题	更改的说明
		对应资源的列表，请参阅必填 AWS Config 控制结果的资源。
2024 年 11 月 12 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `python3.13` 作为参数。
2024 年 10 月 11 日	ElastiCache 控件	已更改 ElastiCache.3、 ElastiCache.4 ElastiCache.5、和的控件标题 ElastiCache.7。游戏不再提及 Redis OSS，因为这些控件也适用 ElastiCache 于 Valkey。
2024 年 9 月 27 日	[ELB.4] 应将应用程序负载均衡器配置为丢弃无效的 http 标头	将控件标题从应将应用程序负载均衡器配置为删除 http 标头更改为应将应用程序负载均衡器配置为删除无效的 http 标头。

变更日期	控件 ID 和标题	更改的说明
2024 年 8 月 19 日	标题更改为 DMS.12 和 ElastiCache 控件	更改了控件标题 DMS.12 以及全部 ElastiCache.1 控制标题 ElastiCache.7。我们更改了这些标题，以反映亚马逊 ElastiCache（Redis OSS）服务中的名称更改。
2024 年 8 月 15 日	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录	Config.1 检查 AWS Config 是否已启用，使用服务相关角色，并记录已启用控件的资源。Security Hub CSPM 添加了一个名为 `includeConfigServiceLinkedRoleCheck` 的自定义控件参数。通过将此参数设置为 `false`，您可以选择不检查 AWS Config 是否使用服务相关角色。
2024 年 7 月 31 日	[IoT.1] 应 AWS IoT Device Defender 标记安全配置文件	将控件标题从应该标记AWS IoT Core 安全配置文件更改为应该标记AWS IoT Device Defender 安全配置文件。

变更日期	控件 ID 和标题	更改的说明
2024 年 7 月 29 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 不再支持 `nodejs16.x` 作为参数。
2024 年 7 月 29 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件可检查 Amazon Elastic Kubernetes Service（Amazon EKS）集群是否在支持的 Kubernetes 版本上运行。目前支持的最旧版本是 `1.28`。
2024 年 6 月 25 日	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录	此控件检查 AWS Config 是否已启用，使用服务相关角色并记录已启用控件的资源。Security Hub CSPM 更新了控件标题以反映控件评估的内容。

变更日期	控件 ID 和标题	更改的说明
2024 年 6 月 14 日	[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志	此控件检查是否将 Amazon Aurora MySQL 数据库集群配置为向亚马逊日志发布审核 CloudWatch 日志。Security Hub CSPM 更新了控件，使其不会为 Aurora Serverless v1 数据库集群生成调查发现。
2024 年 6 月 11 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	此控件可检查 Amazon Elastic Kubernetes Service（Amazon EKS）集群是否在支持的 Kubernetes 版本上运行。目前支持的最旧版本是 1.27。

变更日期	控件 ID 和标题	更改的说明
2024 年 6 月 10 日	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录	此控件检查资源记录 AWS Config 是否已启用， AWS Config 资源记录是否已开启。以前，只有在为所有资源配置了记录时，控件才会生成 PASSED 调查发现。Security Hub CSPM 更新了控件，以便在为已启用控件所需的资源开启记录时生成 PASSED 调查发现。控件也已更新，以检查是否使用了 AWS Config 服务相关角色，该角色提供了记录必要资源的权限。

变更日期	控件 ID 和标题	更改的说明
2024 年 5 月 8 日	[S3.20] S3 通用存储桶应启用 MFA 删除	该控件检查受版本控制的 Amazon S3 通用存储桶是否启用了多重身份验证（MFA）删除。以前，该控件会为具有生命周期配置的存储桶生成 FAILED 调查发现。但是，无法在具有生命周期配置的存储桶上启用已启用版本控制的 MFA 删除。Security Hub CSPM 更新了控件，不会为具有生命周期配置的存储桶生成任何调查发现。控件描述已更新，以反映当前行为。
2024 年 5 月 2 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	Security Hub CSPM 更新了 Kubernetes 支持的最早版本，Amazon EKS 集群可以在该版本上运行，以得出通过的调查发现。目前支持的最旧版本是 Kubernetes 1.26。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 30 日	[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪	将控件标题从“CloudTrail 应启用”更改为“至少应启用一条 CloudTrail 跟踪”。如果启用 AWS 账户 了至少一条 CloudTrail 跟踪，则此控件当前会生成PASSED查找结果。标题和描述已更改，以准确反映当前行为。
2024 年 4 月 29 日	[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查	将控件标题从与经典负载均衡器关联的自动扩缩组应使用负载均衡器运行状况检查更改为与负载均衡器关联的自动扩缩组应使用 ELB 运行状况检查。此控件目前评估应用程序、网关、网络和经典负载均衡器。标题和描述已更改，以准确反映当前行为。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 19 日	[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	该控件检查 AWS CloudTrail 是否启用并配置了至少一个包含读写管理事件的多区域跟踪。以前，当账户 CloudTrail 启用并配置了至少一个多区域跟踪时，即使没有跟踪捕获读写管理事件，该控件也会错误地生成PASSED调查结果。现在，只有在启用并配置了至少一个捕获读写管理事件的多区域跟踪时 CloudTrail ，该控件才会生成PASSED查找结果。
2024 年 4 月 10 日	[Athena.1] Athena 工作组应进行静态加密	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。Athena 工作组将日志发送到 Amazon Simple Storage Service（Amazon S3）存储桶中。Amazon S3 现在在新存储桶和现有 S3 存储桶上使用 S3 托管密钥 (SS3-S3) 提供默认加密。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 10 日	[AutoScaling.4] Auto Scaling 组启动配置的元数据响应跳跃限制不应大于 1	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。Amazon Elastic Compute Cloud（Amazon EC2）实例的元数据响应跃点限制依赖于工作负载。
2024 年 4 月 10 日	[CloudFormation.1] CloudFormation 堆栈应与简单通知服务 (SNS) Semple Notification Service 集成	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。将 AWS CloudFormation 堆栈与 Amazon SNS 主题集成不再是一种安全最佳实践。尽管将重要的 CloudFormation 堆栈与 SNS 主题集成可能很有用，但并非所有堆栈都需要这样做。
2024 年 4 月 10 日	[CodeBuild.5] CodeBuild 项目环境不应启用特权模式	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。在 CodeBuild 项目中启用特权模式不会给客户环境带来额外的风险。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 10 日	[IAM.20] 避免使用 root 用户	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。此控件的目的由另一个控件 [CloudWatch.1] “root” 用户应有日志指标筛选器和警报 覆盖。
2024 年 4 月 10 日	[SNS.2] 应为发送到主题的通知消息启用传送状态记录	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。记录 SNS 主题的传输状态不再是安全最佳实践。尽管记录重要 SNS 主题的传输状态可能很有用，但并非所有主题都必须这样做。
2024 年 4 月 10 日	[S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置	Security Hub CSPM 从《 AWS 基础安全最佳实践和 Service-Managed 标准》中删除了此控件:. AWS Control Tower此控件的目的由另两个控件覆盖：[S3.13] S3 通用存储桶应具有生命周期配置 和 [S3.14] S3 通用存储桶应启用版本控制。此控件仍然是 NIST SP 800-53 Rev. 5 的一部分。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 10 日	[S3.11] S3 通用存储桶应启用事件通知	Security Hub CSPM 从《 AWS 基础安全最佳实践和 Service-Managed 标准》中删除了此控件:. AWS Control Tower尽管在某些情况下，S3 存储桶的事件通知很有用，但这不是通用的安全最佳实践。此控件仍然是 NIST SP 800-53 Rev. 5 的一部分。
2024 年 4 月 10 日	[SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS	Security Hub CSPM 从《 AWS 基础安全最佳实践和 Service-Managed 标准》中删除了此控件:. AWS Control Tower默认情况下，SNS 使用磁盘加密对静态主题进行加密。有关更多信息，请参阅数据加密。不再建议 AWS KMS 使用加密主题作为安全最佳实践。此控件仍然是 NIST SP 800-53 Rev. 5 的一部分。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 8 日	[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护	将控件标题从应启用应用程序负载均衡器删除保护更改为应用程序、网关和网络负载均衡器应启用删除保护。此控件目前评估应用程序、网关和网络负载均衡器。标题和描述已更改，以准确反映当前行为。
2024 年 3 月 22 日	[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密	将控制标题从应使用 TLS 1.2 加密到 OpenSearch 域的连接更改为应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密。以前，该控件仅检查与 OpenSearch 域的连接是否使用 TLS 1.2。现在，该控件会PASSED发现 OpenSearch 域名是否使用最新的 TLS 安全策略进行加密。控件标题和描述已更新，以反映当前行为。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 22 日	[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密	将控件标题从连接到 Elasticsearch 域时应使用 TLS 1.2 进行加密更改为连接到 Elasticsearch 域时应使用最新 TLS 安全策略进行加密。之前，该控件仅检查连接到 Elasticsearch 域时是否使用 TLS 1.2。现在，如果使用最新的 TLS 安全策略对 Elasticsearch 域进行加密，该控件会生成 PASSED 调查发现。控件标题和描述已更新，以反映当前行为。
2024 年 3 月 12 日	[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置	将标题从应启用 S3 阻止公共访问权限设置更改为 S3 通用存储桶应启用屏蔽公共访问权限设置。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.2] S3 通用存储桶应阻止公共读取访问权限	将标题从 S3 存储桶应禁止公共读取访问权限更改为 S3 通用存储桶应屏蔽公共读取访问权限。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.3] S3 通用存储桶应阻止公共写入访问权限	将标题从 S3 存储桶应禁止公共写入访问权限更改为 S3 通用存储桶应阻止公共写入访问权限。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.5] S3 通用存储桶应需要请求才能使用 SSL	将标题从 S3 存储桶应需要请求才能使用安全套接字层更改为 S3 通用存储桶应需要请求才能使用 SSL。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户	将标题从应限制授予存储桶策略中其他 AWS 账户 的 S3 权限更改为S3 通用存储桶策略应限制对其他 AWS 账户的访问。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.7] S3 通用存储桶应使用跨区域复制	将标题从 S3 存储桶应启用跨区域复制更改为 S3 通用存储桶应使用跨区域复制。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.7] S3 通用存储桶应使用跨区域复制	将标题从 S3 存储桶应启用跨区域复制更改为 S3 通用存储桶应使用跨区域复制。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.8] S3 通用存储桶应屏蔽公共访问权限	将标题从应在存储桶级启用 S3 阻止公共访问权限设置更改为 S3 通用存储桶应阻止公共访问权限。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.9] S3 通用存储桶应启用服务器访问日志记录	将标题从应启用 S3 存储桶服务器访问日志记录更改为应为S3 通用存储桶启用服务器访问日志记录。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置	将标题从启用版本控制的 S3 存储桶应配置生命周期策略更改为启用版本控制的 S3 通用存储桶应具有生命周期配置。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.11] S3 通用存储桶应启用事件通知	将标题从 S3 存储桶应启用事件通知更改为 S3 通用存储桶应启用事件通知。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限	将标题从 S3 访问控制列表（ACL）不应用于管理对存储桶的用户访问权限更改为不应使用 ACL 管理对 S3 通用存储桶的用户访问权限。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.13] S3 通用存储桶应具有生命周期配置	将标题从 S3 存储桶应配置生命周期策略更改为 S3 通用存储桶应具有生命周期配置。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.14] S3 通用存储桶应启用版本控制	将标题从 S3 存储桶应使用版本控制更改为 S3 通用存储桶应启用版本控制。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.15] S3 通用存储桶应启用对象锁定	将标题从应将 S3 存储桶配置为使用对象锁定更改为 S3 通用存储桶应启用对象锁定。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys	将标题从应使用 AWS KMS keys对 S3 存储桶进行静态加密更改为应使用 AWS KMS keys对 S3 通用存储桶进行静态加密。Security Hub CSPM 更改了账户的标题，以反映新的 S3 存储桶类型。
2024 年 3 月 7 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `nodejs20.x` 和 `ruby3.3` 作为参数。

变更日期	控件 ID 和标题	更改的说明
2024 年 2 月 22 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `dotnet8` 作为参数。
2024 年 2 月 5 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	Security Hub CSPM 更新了 Kubernetes 支持的最早版本，Amazon EKS 集群可以在该版本上运行，以得出通过的调查发现。目前支持的最旧版本是 Kubernetes `1.25`。

变更日期	控件 ID 和标题	更改的说明
2024 年 1 月 10 日	[CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证	已更改标题CodeBuild GitHub 或 Bitbucket 源存储库网址应使用 OAuth 到 CodeBuild Bitbucket 源存储库网址不应包含敏感凭据。Security Hub CSPM 移除了对 OAuth 的提及，因为其他连接方法也可以很安全。Security Hub CSPM 删除了提及，GitHub因为不再可能在 GitHub 源存储库 URL 中包含个人访问令牌或用户名和密码。
2024 年 1 月 8 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 不再支持 `go1.x` 和 `java8` 作为参数，因为这些运行时都已停用。

变更日期	控件 ID 和标题	更改的说明
2023 年 12 月 29 日	[RDS.8] RDS 数据库实例应启用删除保护	RDS.8 检查使用支持的数据库引擎之一的 Amazon RDS 数据库实例是否启用了删除保护。Security Hub CSPM 现在支持 `custom-oracle-ee`、`oracle-ee-cdb`、和 `oracle-se2-cdb` 作为数据库引擎。
2023 年 12 月 22 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `java21` 和 `python3.12` 作为参数。Security Hub CSPM 不再支持 `ruby2.7` 作为参数。
2023 年 12 月 15 日	[CloudFront.1] CloudFront 发行版应配置默认根对象	CloudFront.1 检查 Amazon CloudFront 分配是否配置了默认根对象。Security Hub CSPM 将此控件的严重性从“关键”降低到“高”，因为添加默认根对象是一个建议操作，具体取决于用户应用程序及特定需求。

变更日期	控件 ID 和标题	更改的说明
2023 年 12 月 5 日	[EC2.13] 安全组不应允许从 0.0.0 开始的入口。0/0 或:: /0 到端口 22	从安全组更改的控件标题不应允许从 0.0.0 开始进入。 0/0 到端口 22 到安全组不应允许从 0.0.0 进入。 0/0 或者:: /0 到端口 22。
2023 年 12 月 5 日	[EC2.14] 安全组不应允许从 0.0.0 开始的入口。0/0 或者:: /0 到端口 3389	将控件标题更改为 “确保没有安全组允许从 0.0.0 开始的入口”。 0/0 到端口 3389 到安全组不应允许从 0.0.0 进入。 0/0 或者:: /0 到端口 3389。
2023 年 12 月 5 日	[RDS.9] RDS 数据库实例应将日志发布到 CloudWatch 日志	应将控制标题从数据库日志记录更改为 RDS 数据库实例应将日志发布到 CloudWatch 日志。Security Hub CSPM 发现，此控件仅检查日志是否已发布到 Amazon CloudWatch Logs，而不检查是否已启用 RDS 日志。如果PASSED将 RDS 数据库实例配置为将日志发布到 CloudWatch 日志，则该控件会生成一个结果。控件标题已更新，以反映当前行为。

变更日期	控件 ID 和标题	更改的说明
2023 年 12 月 5 日	[EKS.8] EKS 集群应启用审核日志	此控件检查 Amazon EKS 集群是否启用了审计日志记录。Security Hub CSPM 用来评估此控件的 AWS Config 规则从`eks-cluster-logging-enabled` 更改为。`eks-cluster-log-enabled`
2023 年 11 月 17 日	[EC2.19] 安全组不应允许不受限制地访问高风险端口	EC2.19 检查被视为高风险的指定端口是否可以访问安全组不受限制的传入流量。Security Hub CSPM 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串 '0.0.0，则该控件会生成`FAILED`查找结果。 0/0' 或者 ':: /0'。
2023 年 11 月 16 日	[CloudWatch.15] CloudWatch 警报应配置指定操作	将控制标题从CloudWatch 警报更改为应为警报状态配置动作，而 CloudWatch 警报则应配置指定操作。

变更日期	控件 ID 和标题	更改的说明
2023 年 11 月 16 日	[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留	更改后的控制标题应从CloudWatch 日志组保留至少 1 年，而 CloudWatch 日志组应保留指定时间段。
2023 年 11 月 16 日	[Lambda.5] VPC Lambda 函数应在多个可用区中运行	将控件标题从 VPC Lambda 函数应在一个以上可用区中运行更改为 VPC Lambda 函数应在多个可用区中运行。
2023 年 11 月 16 日	[AppSync.2] AWS AppSync 应该启用字段级日志记录	将控件标题从 AWS AppSync 应开启请求级和字段级日志记录更改为 AWS AppSync 应启用字段级日志记录。
2023 年 11 月 16 日	[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址	控制标题从 Amazon Elastic MapReduce 集群主节点不应具有公有 IP 地址更改为 Amazon EMR 集群主节点不应具有公有 IP 地址。
2023 年 11 月 16 日	[Opensearch.2] OpenSearch 域名不应向公众开放	将控制标题从OpenSearch 域名应在 VPC 中更改为不应公开访问的OpenSearch域。

变更日期	控件 ID 和标题	更改的说明
2023 年 11 月 16 日	[ES.2] Elasticsearch 域名不应公开访问	将控件标题从 Elasticsearch 域名应位于 VPC 中更改为 Elasticsearch 域名不可供公共访问。
2023 年 10 月 31 日	[ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志	ES.4 检查 Elasticsearch 域是否配置为向亚马逊 CloudWatch 日志发送错误日志。该控件之前对一个 Elasticsearch 域生成了PASSED调查结果，该域将所有日志配置为发送到 CloudWatch 日志。Security Hub CSPM 更新了控件，使其仅针对配置为向日志发送错误日志的 Elasticsearch 域生成PASSED调查结果。 CloudWatch 该控件也进行了更新，将不支持错误日志的 Elasticsearch 版本排除在评估之外。

变更日期	控件 ID 和标题	更改的说明
2023 年 10 月 16 日	[EC2.13] 安全组不应允许从 0.0.0 开始的入口。0/0 或:: /0 到端口 22	EC2.13 检查安全组是否允许对端口 22 进行不受限制的入口访问。Security Hub CSPM 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串 '0.0.0，则该控件会生成FAILED查找结果。 0/0' 或者 ':: /0'。
2023 年 10 月 16 日	[EC2.14] 安全组不应允许从 0.0.0 开始的入口。0/0 或者:: /0 到端口 3389	EC2.14 检查安全组是否允许对端口 3389 进行不受限制的入口访问。Security Hub CSPM 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串 '0.0.0，则该控件会生成FAILED查找结果。 0/0' 或者 ':: /0'。

变更日期	控件 ID 和标题	更改的说明
2023 年 10 月 16 日	[EC2.18] 安全组应只允许授权端口不受限制的传入流量	EC2.18 检查正在使用的安全组是否允许不受限制的传入流量。Security Hub CSPM 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串 '0.0.0，则该控件会生成FAILED查找结果。 0/0' 或者 ':: /0'。
2023 年 10 月 16 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `python3.11` 作为参数。
2023 年 10 月 4 日	[S3.7] S3 通用存储桶应使用跨区域复制	Security Hub CSPM 添加了值为 `CROSS-REGION` 的参数 `ReplicationType`，以确保 S3 存储桶启用了跨区域复制，而非同区域复制。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 27 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	Security Hub CSPM 更新了 Kubernetes 支持的最早版本，Amazon EKS 集群可以在该版本上运行，以得出通过的调查发现。目前支持的最旧版本是 Kubernetes 1.24。
2023 年 9 月 20 日	[CloudFront.2] CloudFront 发行版应启用源站访问身份	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。请改为参阅[CloudFront.13] CloudFront 发行版应使用源站访问控制。“源访问标识”是当前的安全最佳实践。此控件将在 90 天后从文档中删除。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 20 日	[EC2.22] 应移除未使用的 Amazon EC2 安全组	Security Hub CSPM 从 AWS 基础安全最佳实践 (FSBP) 和美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5 中删除了此控件。它仍然是 Service-Managed 标准赛的一部分: AWS Control Tower. 如果安全组连接到 EC2 实例或弹性网络接口，此 控件会生成一个通过的调查发现。但是，对于某些用例，未附加的安全组不会构成安全风险。您可以使用其他 EC2 控件（例如 EC2.2、、 EC2.13 EC2.14 EC2.18、和 EC2.19）来监控您的安全组。
2023 年 9 月 20 日	[EC2.29] EC2 实例应在 VPC 中启动	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。Amazon EC2 已将 EC2-Classic 实例迁移到 VPC。此控件将在 90 天后从文档中删除。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 20 日	[S3.4] S3 存储桶应启用服务器端加密	Security Hub CSPM 停用了此控件，并将其从所有标准中移除。Amazon S3 现在在新存储桶和现有 S3 存储桶上使用 S3 托管密钥 (SS3-S3) 提供默认加密。使用服务器端加密 SS3-S3 或 SS3-KMS 服务器端加密的现有存储桶的加密设置保持不变。此控件将在 90 天后从文档中删除。
2023 年 9 月 14 日	[EC2.2] VPC 默认安全组不应允许入站或出站流量	已将控件标题从 VPC 默认安全组不应允许入站和出站流量更改为 VPC 默认安全组不应允许入站或出站流量。
2023 年 9 月 14 日	[IAM.9] 应为根用户启用 MFA	已将控件标题从应为根用户启用虚拟 MFA更改为应为根用户启用 MFA。
2023 年 9 月 14 日	[RDS.19] 应为关键群集事件配置现有 RDS 事件通知订阅	已将控件标题从应为关键集群事件配置 RDS 事件通知订阅更改为应为关键集群事件配置现有 RDS 事件通知订阅。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 14 日	[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅	已将控件标题从应为关键数据库实例事件配置 RDS 事件通知订阅更改为应为关键数据库实例事件配置现有 RDS 事件通知订阅。
2023 年 9 月 14 日	[WAF.2] AWS WAF 经典区域规则应至少有一个条件	已将控件标题从WAF Regional 规则应至少有一个条件更改为AWS WAF Classic Regional 规则应至少有一个条件。
2023 年 9 月 14 日	[WAF.3] AWS WAF 经典区域规则组应至少有一条规则	已将控件标题从 WAF Regional 规则组应至少包含一条规则更改为AWS WAF Classic Regional 规则组应至少包含一条规则。
2023 年 9 月 14 日	[WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组	已将控件标题从 WAF Regional web ACL 应至少有一个规则或规则组更改为AWS WAF Classic Regional Web ACL 应至少有一个规则或规则组。
2023 年 9 月 14 日	[WAF.6] AWS WAF 经典全局规则应至少有一个条件	已将控件标题从全局 WAF 规则应至少有一个条件更改为 Classic 全局AWS WAF 规则应至少有一个条件。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 14 日	[WAF.7] AWS WAF 经典全局规则组应至少有一条规则	已将控件标题从全局 WAF 规则组应至少包含一条规则更改为 Classic 全局AWS WAF 规则组应至少包含一条规则。
2023 年 9 月 14 日	[WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组	已将控件标题从 WAF 全局 Web ACL 应至少包含一个规则或规则组更改为AWS WAF Classic 全局 Web ACL 应至少有一个规则或规则组。
2023 年 9 月 14 日	[WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组	已将控件标题从 WAFv2 Web ACL 至少有一个规则或规则组更改为AWS WAF Web ACL 应至少有一个规则或规则组。
2023 年 9 月 14 日	[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录	已将控件标题从应激活AWS WAF v2 Web ACL 日志记录更改为应启用AWS WAF Web ACL 日志记录。

变更日期	控件 ID 和标题	更改的说明
2023 年 7 月 20 日	[S3.4] S3 存储桶应启用服务器端加密	S3.4 检查 Amazon S3 存储桶是否启用了服务器端加密，或者 S3 存储桶策略是否明确拒绝未经服务器端加密的`PutObject`请求。Security Hub CSPM 更新了此控件，加入了使用 KMS 密钥的双层服务器端加密 ()。DSSE-KMS 当使用、或对 S3 存储桶进行加密时 SSE-S3， SSE-KMS该控件会生成一个已通过的查找结果 DSSE-KMS。
2023 年 7 月 17 日	[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys	S3.17 检查 Amazon S3 存储桶是否使用加密 AWS KMS key。Security Hub CSPM 更新了此控件，加入了使用 KMS 密钥的双层服务器端加密 ()。DSSE-KMS 当使用 SSE-KMS 或对 S3 存储桶进行加密时，该控件会生成通过查找结果 DSSE-KMS。

变更日期	控件 ID 和标题	更改的说明
2023 年 6 月 9 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	EKS.2 检查 Amazon EKS 集群是否在受支持的 Kubernetes 版本上运行。现在是支持的最旧版本。`1.23`
2023 年 6 月 9 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `ruby3.2` 作为参数。
2023 年 6 月 5 日	[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密	APIGateway.5.checks Amazon API Gateway REST API 阶段中的所有方法是否都是静态加密的。Security Hub CSPM 更新了该控件，使其仅在为特定方法启用缓存时才评估该方法的加密。
2023 年 5 月 18 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `java17` 作为参数。

变更日期	控件 ID 和标题	更改的说明
2023 年 5 月 18 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 不再支持 `nodejs12.x` 作为参数。
2023 年 4 月 23 日	[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行	ECS.10 检查 Amazon ECS Fargate 服务是否运行最新的 Fargate 平台版本。客户可以直接通过 ECS 部署 Amazon ECS，也可以使用部署 CodeDeploy。Security Hub CSPM 更新了此控件，以便在使用部署 ECS Fargate CodeDeploy 服务时生成通过调查结果。
2023 年 4 月 20 日	[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户	S3.6 检查 Amazon Simple Storage Service (Amazon S3) 存储桶策略是否阻止 AWS 账户 其他人的委托人对 S3 存储桶中的资源执行被拒绝的操作。考虑存储桶策略中的条件，Security Hub CSPM 更新了该控件。

变更日期	控件 ID 和标题	更改的说明
2023 年 4 月 18 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 现在支持 `python3.10` 作为参数。
2023 年 4 月 18 日	[Lambda.2] Lambda 函数应使用支持的运行时	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub CSPM 不再支持 `dotnetcore3.1` 作为参数。
2023 年 4 月 17 日	[RDS.11] RDS 实例应启用自动备份	RDS.11 检查 Amazon RDS 实例是否启用了自动备份，其备份保留期大于或等于七天。Security Hub CSPM 更新了此控件，将只读副本排除在评估范围之外，因为并非所有引擎都支持对只读副本进行自动备份。此外，RDS 不提供在创建只读副本时指定备份保留期的选项。默认情况下，只读副本创建时的备份保留期为 `0`。

Security Hub CSPM 控件适用于 AWS 账户

这些 Security Hub CSPM 控件会进行评估。 AWS 账户

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

相关要求：CIS AWS 基金会基准 v5.0.0/1.2、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`security-account-information-provided`

计划类型：定期

参数：无

此控件可检查 Amazon Web Services（AWS）账户是否有安全联系信息。如果未提供账户的安全联系信息，则控制失败。

备用安全联系人 AWS 允许在您无法访问时就您的账户问题联系他人。有关与您的 AWS 账户 使用情况相关的安全相关主题的通知可以来自 支持其他 AWS 服务 团队。

修复

要将备用联系人作为安全联系人添加到您的 AWS 账户，请参阅《AWS 账户管理参考指南》 AWS 账户中的更新您的备用联系人。

[账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分

类别：保护 > 安全访问管理 > 访问控制

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`account-part-of-organizations`

计划类型：定期

参数：无

此控件检查是否 AWS 账户 是通过管理的组织的一部分 AWS Organizations。如果账户不属于组织，则控制失败。

随着工作负载的扩展，Organizations 可帮助你集中管理环境 AWS。您可以使用多个 AWS 账户 来隔离具有特定安全要求的工作负载，或者符合 HIPAA 或 PCI 等框架。通过创建组织，您可以将多个账户作为一个单位进行管理，并集中管理其对资源的访问权限 AWS 服务、资源和区域。

修复

要创建新组织并自动 AWS 账户 添加到该组织，请参阅AWS Organizations 用户指南中的创建组织。要向现有组织添加帐户，请参阅AWS Organizations 用户指南中的AWS 账户 邀请加入您的组织。

Security Hub CSPM 控件适用于 AWS Amplify

这些 Security Hub CSPM 控件用于评估 AWS Amplify 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Amplify.1] 应标记 Amplify 应用

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Amplify::App`

AWS Config 规则：amplify-app-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Amplify 应用程序是否具有`requiredKeyTags`参数指定的标签密钥。如果应用程序没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件将失败。如果没有为

requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果应用程序没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 AWS Amplify 应用程序添加标签的信息，请参阅《AWS Amplify 主机用户指南》中的资源标记支持。

[Amplify.2] 应标记 Amplify 分支

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Amplify::Branch

AWS Config 规则：amplify-branch-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Amplify 分支是否具有requiredKeyTags参数指定的标签密钥。如果分支没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件会失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果分支没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 AWS Amplify 分支添加标签的信息，请参阅《AWS Amplify 主机用户指南》中的资源标记支持。

适用于亚马逊 API Gateway 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon API Gateway 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[APIGateway.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录

相关要求： NIST.800-53.r5 AC-4(26)、、 NIST.800-53.r5 SC-7 (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 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：AWS::ApiGateway::Stage、AWS::ApiGatewayV2::Stage

AWS Config 规则：api-gw-execution-logging-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`loggingLevel`	Logging level（日志记录级别）	枚举	`ERROR`, `INFO`	`No default value`

此控件会检查 Amazon API Gateway REST 或 WebSocket API 的所有阶段是否都启用了日志记录。如果对于 API 的所有阶段 `loggingLevel` 不是 `ERROR` 或者 `INFO`，则控制失败。除非您提供自定义参数值来指示应启用特定的日志类型，否则如果日志级别为或`ERROR`，Security Hub CSPM 会生成一个通过的结果。`INFO`

API Gateway REST 或 WebSocket API 阶段应启用相关日志。API Gateway REST 和 WebSocket API 执行日志提供了向 API Gateway REST 和 WebSocket API 阶段发出的请求的详细记录。这些阶段包括 API 集成后端响应、Lambda 授权方响应和集成终端节点`requestId`。 AWS

修复

要启用 REST 和 WebSocket API 操作的日志记录，请参阅《AP CloudWatch I Gateway 开发者指南》中的使用 API Gateway 控制台设置 API 日志记录。

[APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证

相关要求： NIST.800-53.r5 AC-17 (2)、、(1) NIST.800-53.r5 AC-4、2 NIST.800-53.r5 IA-5 (3)、3、3 (3)、(3)、 NIST.800-53.r5 SC-1 (4)、 NIST.800-53.r5 SC-2 (1)、(NIST.800-53.r5 SC-12)、 NIST.800-53.r5 SC-7 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、nist.800-171.r2 3.13.15 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ApiGateway::Stage`

AWS Config 规则：api-gw-ssl-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon API Gateway REST API 阶段是否配置了 SSL 证书。后端系统使用这些证书来验证传入的请求是否来自 API Gateway。

API Gateway REST API 阶段应配置 SSL 证书，以允许后端系统对请求是否来自 API Gateway 进行身份验证。

修复

有关如何生成和配置 API Gateway REST API SSL 证书的详细说明，请参阅 API Gateway 开发人员指南中的生成和配置用于后端身份验证的 SSL 证书。

[APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 跟踪

相关要求： NIST.800-53.r5 CA-7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::ApiGateway::Stage`

AWS Config 规则：api-gw-xray-enabled

计划类型：已触发变更

参数：无

此控件检查您的 Amazon API Gateway REST API 阶段是否启用了 AWS X-Ray 主动跟踪。

X-Ray 主动跟踪可以更快速地响应底层基础设施的性能变化。性能变化可能会导致 API 的可用性不足。X-Ray 主动跟踪提供流经 API Gateway REST API 操作和关联服务的用户请求实时指标。

修复

有关如何为 API Gateway REST API 操作启用 X-REST 主动跟踪的详细说明，请参阅 AWS X-Ray 开发人员指南中的Amazon API Gateway 对 AWS X-Ray的主动跟踪支持。

[APIGateway.4] API Gateway 应与 WAF Web ACL 关联

相关要求： NIST.800-53.r5 AC-4(21)

类别：保护 > 防护服务

严重性：中

资源类型：`AWS::ApiGateway::Stage`

AWS Config 规则：api-gw-associated-with-waf

计划类型：已触发变更

参数：无

此控件检查 API Gateway 阶段是否使用 AWS WAF Web 访问控制列表 (ACL)。如果 AWS WAF Web ACL 未连接到 REST API Gateway 阶段，则此控件将失败。

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 APIs 免受攻击。它使您能够配置 ACL，这是一组规则，可根据您定义的可自定义 Web 安全规则和条件来允许、阻止或计数 Web 请求。确保您的 API Gateway 阶段与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。

修复

有关如何使用 API Gateway 控制台将 AWS WAF 区域 Web ACL 与现有 API Gateway API 阶段关联的信息，请参阅《API Gateway 开发者指南》 APIs中的使用 AWS WAF 来保护您。

[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::ApiGateway::Stage`

AWS Config 规则:`api-gw-cache-encrypted`（ 自定义 Security Hub CSPM 规则 ）

计划类型：已触发变更

参数：无

此控件检查 API Gateway REST API 阶段中启用缓存的所有方法是否都已加密。如果 API Gateway REST API 阶段中的任何方法配置为缓存并且缓存未加密，则控制将失败。只有在为特定方法启用缓存时，Security Hub CSPM 才会评估该方法的加密。

对静态数据进行加密可降低存储在磁盘上的数据被未经身份验证的用户访问的风险。 AWS它添加了另一组访问控制来限制未经授权的用户访问数据的能力。例如，需要 API 权限才能解密数据，然后才能读取数据。

API Gateway REST API 缓存应静态加密，以增加安全性。

修复

要为某个阶段配置 API 缓存，请参阅 API Gateway 开发人员指南中的启用 Amazon API Gateway 缓存。在缓存设置中，选择加密缓存数据。

[APIGateway.8] API Gateway 路由应指定授权类型

相关要求： NIST.800-53.r5 AC-3，nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::ApiGatewayV2::Route`

AWS Config 规则：api-gwv2-authorization-type-configured

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`authorizationType`	API 路由的授权类型	枚举	`AWS_IAM`, `CUSTOM`, `JWT`	无默认值

此控件检查 Amazon API Gateway 路由是否具有授权类型。如果 API 网关路由未指定任何授权类型，则控制失败。或者，如果您希望仅在路径使用 `authorizationType` 参数中指定的授权类型时才通过控件，则可以提供自定义参数值。

API Gateway 支持多种用于控制和管理对 API 的访问的机制：通过指定授权类型，您可以将对 API 的访问限制为仅授权用户或进程。

修复

要为 HTTP 设置授权类型 APIs，请参阅《API Gateway 开发者指南》中的 API Gateway 中控制和管理对 HTTP API 的访问权限。要为设置授权类型 WebSocket APIs，请参阅《API Gatew ay 开发者指南》中的 WebSocket API Gateway 中控制和管理对 API 的访问权限。

[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

相关要求： NIST.800-53.r5 AC-4(26)、、(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 SI-7 NIST.800-53.r5 SC-7 (8)、PCI DSS v4.0.1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ApiGatewayV2::Stage`

AWS Config 规则：api-gwv2-access-logs-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon API Gateway V2 阶段是否配置了访问日志记录。如果未定义访问日志设置，则控制失败。

API Gateway访问日志提供有关谁访问了您的 API 以及调用方访问 API 的方式的详细信息。这些日志对于安全和访问审核以及取证调查等应用程序非常有用。启用这些访问日志来分析流量模式并解决问题。

有关其他最佳实践，请参阅 API Gateway 开发者指南 APIs中的监控 REST。

修复

要设置访问日志，请参阅《 CloudWatch API Gateway 开发者指南》中的 “使用 API Gateway 控制台设置 API 日志”。

[APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ApiGatewayV2::Integration`

AWS Config 规则：apigatewayv2-integration-private-https-enabled

计划类型：已触发变更

参数：无

此控件检查 API Gateway V2 集成是否为私有连接启用了 HTTPS。如果私有连接未配置 TLS，则控制失败。

VPC 链接将 API Gateway 连接到私有资源。虽然 VPC 链路创建私有连接，但它们本质上并不加密数据。配置 TLS 可确保使用 HTTPS 进行从客户端通过 API Gateway 到后端的 end-to-end加密。如果没有 TLS，敏感的 API 流量会以未加密方式通过私有连接流动。HTTPS 加密可保护通过私有连接的流量免受数据拦截、 man-in-the-middle攻击和凭据泄露。

修复

要在 API Gateway v2 集成中为私有连接启用传输中的加密，请参阅 Amazon API Gateway 开发者指南中的更新私有集成。配置 TLS 配置，以便私有集成使用 HTTPS 协议。

[APIGateway.11] API Gateway 域名应使用推荐的安全策略

类别：保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ApiGateway::DomainName`

AWS Config 规则：apigateway-domain-name-tls-check

计划类型：已触发变更

参数：

- `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`（不可自定义）

此控件检查 API Gateway 域名是否配置为使用推荐的安全策略对传输中的数据进行加密。如果 API Gateway 域名未配置为使用推荐的安全策略，则控制失败。

安全策略 是 API Gateway 提供的最低 TLS 版本和密码套件的预定义组合。当您的客户端与您的 API 或自定义域名建立 TLS 握手时，安全策略会强制实施 API Gateway 接受的 TLS 版本和密码套件。安

全策略可保护您的域名 APIs 和自定义域名免受网络安全问题的影响，例如在客户端和服务器之间进行篡改和窃听。使用推荐的安全策略有助于确保 API Gateway 域名使用现代、安全 TLS 配置，以保护客户端和您的 API 之间传输的数据。

修复

要更新 API Gateway 域名的 TLS 安全策略，请参阅 Amazon API Gateway 开发者指南中的如何更改安全策略。

Security Hub CSPM 控件适用于 AWS AppConfig

这些 Security Hub CSPM 控件用于评估 AWS AppConfig 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AppConfig.1] 应为 AWS AppConfig 应用程序加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AppConfig::Application`

AWS Config 规则：`appconfig-application-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS AppConfig 应用程序是否具有参数中定义的特定键的标签`requiredKeyTags`。如果应用程序没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果应用程序未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS AppConfig 应用程序添加标签，请参阅 AWS AppConfig API 参考TagResource中的。

[AppConfig.2] 应标记 AWS AppConfig 配置文件

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AppConfig::ConfigurationProfile`

AWS Config 规则：`appconfig-configuration-profile-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS AppConfig 配置文件是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果配置文件没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果配置文件未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS AppConfig 配置文件添加标签，请参阅 AWS AppConfig API 参考TagResource中的。

[AppConfig.3] 应该对 AWS AppConfig 环境进行标记

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AppConfig::Environment`

AWS Config 规则：`appconfig-environment-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS AppConfig 环境是否具有参数中定义的特定密钥的标签requiredKeyTags。如果环境没有任何标签键或者未在 requiredKeyTags 参数中指定所有键，则此控件将失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果环境未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS AppConfig 环境添加标签，请参阅 AWS AppConfig API 参考TagResource中的。

[AppConfig.4] 应 AWS AppConfig 标记扩展关联

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::AppConfig::ExtensionAssociation

AWS Config 规则：`appconfig-extension-association-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS AppConfig 扩展关联是否具有参数中定义的特定键的标签`requiredKeyTags`。如果扩展关联没有任何标签键或者未在参数 `requiredKeyTags` 中指定所有键，则此控件会失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果扩展关联未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS AppConfig 扩展关联添加标签，请参阅 AWS AppConfig API 参考TagResource中的。

适用于亚马逊的 Security Hub CSPM 控件 AppFlow

这些 Security Hub CSPM 控件用于评估亚马逊的 AppFlow 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AppFlow.1] 应为亚马逊 AppFlow 流程加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AppFlow::Flow`

AWS Config 规则：`appflow-flow-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon AppFlow 流程是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果流没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果流未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向亚马逊 AppFlow 流程添加标签，请参阅亚马逊 AppFlow 用户指南中的 AppFlow在亚马逊中创建流程。

Security Hub CSPM 控件适用于 AWS App Runner

这些 AWS Security Hub CSPM 控制措施评估 AWS App Runner 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AppRunner.1] 应标记 App Runner 服务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AppRunner::Service`

AWS Config 规则：apprunner-service-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS App Runner 服务是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果 App Runner 服务没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失

败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果 App Runner 未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

有关向 AWS App Runner 服务添加标签的信息，请参阅 AWS App Runner API 参考TagResource中的。

[AppRunner.2] 应标记 App Runner VPC 连接器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AppRunner::VpcConnector`

AWS Config 规则：apprunner-vpc-connector-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS App Runner VPC 连接器是否具有参数中定义的特定密钥的标签requiredKeyTags。如果 VPC 连接器没有任何标签键或未在 requiredKeyTags 参数中指定所有键，则此控件将失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果 VPC 连接器未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

有关向 AWS App Runner VPC 连接器添加标签的信息，请参阅 AWS App Runner API 参考TagResource中的。

Security Hub CSPM 控件适用于 AWS AppSync

这些 Security Hub CSPM 控件用于评估 AWS AppSync 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密

> **Important**
>
> Security Hub CSPM 于 2026 年 3 月 9 日取消了该控制权。有关更多信息，请参阅Security Hub CSPM 控件的更改日志。 AWS AppSync 现在为所有当前和未来的 API 缓存提供默认加密。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::AppSync::GraphQLApi`

AWS Config 规则：appsync-cache-ct-encryption-at-rest

计划类型：已触发变更

参数：无

此控件检查 AWS AppSync API 缓存是否处于静态加密状态。如果未静态加密 API 缓存，则此控件会失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

为 AWS AppSync API 启用缓存后，您无法更改加密设置。您必须删除缓存，并在启用加密的情况下重新创建该缓存。有关更多信息，请参阅《AWS AppSync 开发人员指南》中的缓存加密。

[AppSync.2] AWS AppSync 应该启用字段级日志记录

相关要求：PCI DSS v4.0.1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::AppSync::GraphQLApi`

AWS Config 规则：appsync-logging-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
fieldLoggingLevel	字段日志记录级别	枚举	ERROR, ALL, INFO, DEBUG	No default value	

此控件检查 AWS AppSync API 是否开启了字段级日志记录。如果字段解析器日志级别设置为无，则控制失败。除非您提供自定义参数值来指示应启用特定的日志类型，否则如果字段解析器日志级别为或，Security Hub CSPM 会生成一个通过的结果。ERROR ALL

您可以使用日志记录和指标来识别、优化 GraphQL 查询和排除其问题。启用 AWS AppSync GraphQL 的日志记录功能可帮助您获取有关 API 请求和响应的详细信息、识别和响应问题以及遵守监管要求。

修复

要开启登录功能 AWS AppSync，请参阅《AWS AppSync 开发者指南》中的设置和配置。

[AppSync.4] 应标记 AWS AppSync Gr APIs aphQL

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::AppSync::GraphQLApi

AWS Config 规则:tagged-appsync-graphqlapi（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS AppSync GraphQL API 是否具有参数中定义的特定密钥的标签。requiredTagKeys如果 GraphQL API 没有任何标签键或未在参数 requiredTagKeys 中指定所有键，则此控件会失败。如果未提供参数 requiredTagKeys，则此控件仅会检查是否存在标签键，如果 GraphQL API 未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 AWS AppSync GraphQL API 添加标签，请参阅 AP AWS AppSync I 参考TagResource中的。

[AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证

相关要求： 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

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：高

资源类型：`AWS::AppSync::GraphQLApi`

AWS Config 规则：appsync-authorization-check

计划类型：已触发变更

参数：

- `AllowedAuthorizationTypes`： `AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS`（不可自定义）

此控件可检查您的应用程序是否使用 API 密钥与 AWS AppSync GraphQL API 进行交互。如果使用 API 密钥对 AWS AppSync GraphQL API 进行了身份验证，则控制失败。

API 密钥是应用程序中的硬编码值，在您创建未经身份验证的 GraphQL 端点时由 AWS AppSync 服务生成。如果此 API 密钥遭到泄露，您的端点很容易受到意外访问。除非您支持可公开访问的应用程序或网站，否则我们不建议使用 API 密钥进行身份验证。

修复

要为您的 AWS AppSync GraphQL API 设置授权选项，请参阅AWS AppSync 开发者指南中的授权和身份验证。

[AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密

> **Important**
>
> Security Hub CSPM 于 2026 年 3 月 9 日取消了该控制权。有关更多信息，请参阅Security Hub CSPM 控件的更改日志。 AWS AppSync 现在为所有当前和未来的 API 缓存提供默认加密。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::AppSync::ApiCache`

AWS Config 规则：appsync-cache-ct-encryption-in-transit

计划类型：已触发变更

参数：无

此控件检查 AWS AppSync API 缓存是否在传输过程中被加密。如果未在传输过程中加密 API 缓存，则此控件会失败。

传输中数据是指从一个位置移动到另一个位置的数据，例如在集群中的节点之间或在集群和应用程序之间。数据可能通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。

修复

为 AWS AppSync API 启用缓存后，您无法更改加密设置。您必须删除缓存，并在启用加密的情况下重新创建该缓存。有关更多信息，请参阅《AWS AppSync 开发人员指南》中的缓存加密。

适用于亚马逊 Athena 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Athena 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Athena.1] Athena 工作组应进行静态加密

> **Important**
>
> Security Hub CSPM 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub CSPM 控件的更改日志。

类别：保护 > 数据保护 > 静态数据加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

严重性：中

资源类型：`AWS::Athena::WorkGroup`

AWS Config 规则：athena-workgroup-encrypted-at-rest

计划类型：已触发变更

参数：无

此控件检查 Athena 工作组是否处于静态加密状态。如果 Athena 工作组未静态加密，则控制失败。

在 Athena 中，您可以创建工作组来运行团队、应用程序或不同工作负载的查询。每个工作组都有对所有查询启用加密的设置。您可以选择对亚马逊简单存储服务 (Amazon S3) 托管密钥使用服务器端加密、使用 () 密钥使用服务器端加密或使用客户托管的 KMS 密钥 AWS Key Management Service 进行 AWS KMS客户端加密。静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要为 Athena 工作组启用静态加密，请参阅 Amazon Athena 用户指南中的编辑工作组。在查询结果配置部分，选择加密查询结果。

[Athena.2] 应标记 Athena 数据目录

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Athena::DataCatalog`

AWS Config 规则:`tagged-athena-datacatalog`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件用于检查 Amazon Athena 数据目录是否具有带参数 `requiredTagKeys` 中定义的特定键的标签。如果数据目录没有任何标签键或未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供 `requiredTagKeys` 参数，则此控件仅会检查是否存在标签键，如果数据目录未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Athena 数据目录添加标签，请参阅《Amazon Athena 用户指南》中的标记 Athena 资源。

[Athena.3] 应标记 Athena 工作组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Athena::WorkGroup`

AWS Config 规则:`tagged-athena-workgroup`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件用于检查 Amazon Athena 工作组是否具有带参数 `requiredTagKeys` 中定义的特定键的标签。如果工作组没有任何标签键或未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果工作组未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Athena 工作组添加标签，请参阅《Amazon Athena 用户指南》中的在单个工作组中添加和删除标签。

[Athena.4] Athena 工作组应启用日志记录

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Athena::WorkGroup`

AWS Config 规则：athena-workgroup-logging-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon Athena 工作组是否启用了日志记录。如果工作组未启用日志记录，则此控件将失败。

审计日志跟踪和监控系统活动。它们提供了事件记录，可以帮助您检测安全漏洞、调查事件并遵守法规。审计日志还可以增强组织的整体问责制并提高组织透明度。

修复

有关为 Athena 工作组启用日志记录的信息，请参阅 Amazon Athena 用户指南中的在 Athena 中启用 CloudWatch 查询指标。

Security Hub CSPM 控件适用于 AWS Backup

这些 Security Hub CSPM 控件用于评估 AWS Backup 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Backup.1] AWS Backup 恢复点应在静态状态下进行加密

相关要求： NIST.800-53.r5 CP-9(8)， NIST.800-53.r5 SI-12

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::Backup::RecoveryPoint`

AWS Config 规则：`backup-recovery-point-encrypted`

计划类型：已触发变更

参数：无

此控件可检查 AWS Backup 恢复点是否处于静态加密状态。如果未对恢复点进行静态加密，则控制失败。

AWS Backup 恢复点是指在备份过程中创建的特定数据副本或快照。它代表备份数据的特定时刻，可作为恢复点，以防原始数据丢失、损坏或无法访问。对备份恢复点进行加密可增加额外的保护层来阻止未经授权的访问。加密是保护备份数据的机密性、完整性和安全性的最佳实践。

修复

要加密 AWS Backup 恢复点，请参阅《AWS Backup 开发人员指南》 AWS Backup中的备份加密。

[Backup.2] AWS Backup 应标记恢复点

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::RecoveryPoint`

AWS Config规则:`tagged-backup-recoverypoint`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Backup 恢复点是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果恢复点没有任何标签键或未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果恢复点未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要在创建备份时从源资源中复制标签，请参阅《AWS Backup 开发人员指南》中的将标签复制到备份。

在创建 parent/composite 恢复点时，不会复制标签。要在包括恢复点在内的 parent/composite 现有恢复点上添加标签，请参阅AWS Backup 开发人员指南中的在现有恢复点上添加或删除标签。

[Backup.3] AWS Backup 应给保管库加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::BackupVault`

AWS Config规则:`tagged-backup-backupvault`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Backup 文件库是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果恢复点没有任何标签键或未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果恢复点未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向... 添加标签 AWS Backup 文件库

1. 打开 AWS Backup 控制台，网址为https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 从列表中选择备份保管库。
4. 在备份保管库标签部分中，选择管理标签。
5. 输入标签的键和值。选择添加新标签以添加其他键值对。
6. 完成添加标签后，选择保存。

[Backup.4] AWS Backup 报告计划应加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::ReportPlan`

AWS Config规则:`tagged-backup-reportplan`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合AWS 要求的标签键。	无默认值

此控件检查 AWS Backup 报告计划是否包含参数中定义的特定键的标签`requiredTagKeys`。如果报告计划没有任何标签键或者未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果报告计划未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向... 添加标签 AWS Backup 报告计划

1. 打开 AWS Backup 控制台，网址为https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 从列表中选择备份保管库。
4. 在备份保管库标签部分中，选择管理标签。
5. 选择添加新标签。输入标签的键和值。针对其他键值对重复此操作。
6. 完成添加标签后，选择保存。

[Backup.5] AWS Backup 应标记备份计划

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::BackupPlan`

AWS Config规则:`tagged-backup-backupplan`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Backup 备份计划是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果备份计划没有任何标签键或者未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果备份计划未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向... 添加标签 AWS Backup 备份计划

1. 打开 AWS Backup 控制台，网址为https://console.aws.amazon.com/backup。

2. 在导航窗格中，选择备份保管库。
3. 从列表中选择备份保管库。
4. 在备份保管库标签部分中，选择管理标签。
5. 选择添加新标签。输入标签的键和值。针对其他键值对重复此操作。
6. 完成添加标签后，选择保存。

Security Hub CSPM 控件适用于 AWS Batch

这些 Security Hub CSPM 控件用于评估 AWS Batch 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Batch.1] 应标记批处理作业队列

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Batch::JobQueue`

AWS Config 规则：batch-job-queue-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Batch 作业队列是否具有参数中定义的特定键的标签`requiredKeyTags`。如果作业队列没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件会失败。如果未提供 `requiredKeyTags` 参数，则控件仅检查是否存在标签键，如果作业队列未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向批处理作业队列添加标签，请参阅《AWS Batch 用户指南》中的标记您的资源。

[Batch.2] 应标记批处理计划策略

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Batch::SchedulingPolicy`

AWS Config 规则：batch-scheduling-policy-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Batch 调度策略是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果计划策略没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件会失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果计划策略未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向批处理计划策略添加标签，请参阅《AWS Batch 用户指南》中的标记您的资源。

[Batch.3] 应标记批处理计算环境

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Batch::ComputeEnvironment`

AWS Config 规则：batch-compute-environment-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Batch 计算环境是否具有参数中定义的特定密钥的标签requiredKeyTags。如果计算环境没有任何标签键或者未在 requiredKeyTags 参数中指定所有键，则此控件会失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果计算1环境未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向批处理计算环境添加标签，请参阅《AWS Batch 用户指南》中的标记您的资源。

[Batch.4] 应标记托管批处理计算环境中的计算资源属性

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Batch::ComputeEnvironment

AWS Config 规则：batch-managed-compute-env-compute-resources-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查托管 AWS Batch 计算环境中的计算资源属性是否具有 `requiredKeyTags` 参数指定的标签键。如果计算资源属性没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件会失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果计算资源属性没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。此控件不评估非托管计算环境或使用 AWS Fargate 资源的托管环境。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关在托管 AWS Batch 计算环境中为计算资源添加标签的信息，请参阅AWS Batch 用户指南中的为资源添加标签。

适用于 Amazon Bedrock 的 Security Hub CSPM 控件 AgentCore

这些 AWS Security Hub CSPM 控制措施会评估 Amazon Bedrock AgentCore 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：高

资源类型：`AWS::BedrockAgentCore::Runtime`

AWS Config 规则：bedrockagentcore-runtime-private-network-required

计划类型：已触发变更

参数：无

此控件检查 Amazon Bedrock AgentCore 运行时是否配置了 VPC 网络模式。如果运行时将其网络模式设置为 PUBLIC，则控件将失败。

在 Amazon Bedrock AgentCore 运行时使用公共网络模式会将运行时直接暴露给互联网，从而增加攻击面和未经授权访问的风险。使用 VPC 网络模式配置运行时可确保运行时流量限制在您的私有网络内，从而使您能够应用网络级安全控制，例如安全组、网络 ACL 和 VPC 流日志。

修复

要纠正这一发现，请更新不合规的 Bedrock AgentCore 运行时并将其配置为 VPC 网络模式。有关说明，请参阅《亚马逊 Bedrock AgentCore 开发者指南》中的为 VPC 配置亚马逊 Bedrock AgentCore 运行时和工具。

[BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::BedrockAgentCore::Gateway`

AWS Config 规则：bedrockagentcore-gateway-authorizer-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon Bedrock AgentCore Gateway 是否需要对入站请求进行授权。如果 Bedrock AgentCore Gateway 未设置入站授权，则控制失败。

在 Amazon Bedrock AgentCore 网关上配置身份验证可确保只有经过授权的客户端才能向您的 AI 代理发送请求。如果没有授权者，任何对网关端点具有网络访问权限的实体都可以调用您的代理，这可能会导致未经授权的数据访问、资源滥用或意外成本。入站授权对尝试通过您的 AgentCore网关访问目标的用户进行验证。

修复

要为 Amazon Bedrock AgentCore Gateway 设置入站授权，请参阅《亚马逊 B edrock AgentCore 开发者指南》中的为您的网关设置入站授权。

[BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键

相关要求： 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::BedrockAgentCore::Memory`

AWS Config 规则：bedrock-agentcore-memory-encryption-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon Bedrock AgentCore 内存是否使用客户托管 AWS KMS 密钥进行静态加密。如果 Bedrock AgentCore 内存未使用客户管理的 KMS 密钥加密，则控制失败。

与默认服务托管密钥相比，使用客户托管的 KMS 密钥对 Amazon Bedrock AgentCore 内存进行加密，可以增强安全性。客户托管的 KMS 密钥使您可以完全控制加密密钥的生命周期和访问策略。此外，可以记录和监控所有加密密钥的使用情况， AWS CloudTrail 以实现可审计性。

修复

要使用客户管理的 KMS 密钥加密您的亚马逊 Bedrock AgentCore 内存，请参阅亚马逊 B edrock 开发者指南中的加密您的亚马逊 Bedrock AgentCore AgentCore 内存。

[BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键

相关要求： 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::BedrockAgentCore::Gateway`

AWS Config 规则：bedrockagentcore-gateway-encryption-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon Bedrock AgentCore Gateway 是否使用客户托管 AWS KMS 密钥进行静态加密。如果 Bedrock AgentCore Gateway 未使用客户管理的 KMS 密钥加密，则控制失败。

默认情况下，Amazon Bedrock AgentCore 使用 AWS 托管密钥对网关数据进行加密。使用客户托管的 KMS 密钥可以让您完全控制加密密钥的生命周期，包括轮换、访问策略和审计 AWS CloudTrail。这有助于满足要求对敏感的 AI 工作负载进行客户控制加密的合规性要求。

修复

要使用客户托管的 KMS 密钥加密您的 Bedrock AgentCore 网 AgentCore 关，请参阅 A mazon Bedrock AgentCore 开发者指南中的使用客户管理的 KMS 密钥加密您的网关。

[BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：高

资源类型：`AWS::BedrockAgentCore::BrowserCustom`

AWS Config 规则：bedrockagentcore-browsercustom-network-mode-not-public

计划类型：已触发变更

参数：无

此控件检查 Amazon Bedrock AgentCore 自定义浏览器是否配置了公共网络模式。如果网络模式设置为公开，则控制失败。

在 Amazon Bedrock AgentCore 自定义浏览器中使用公共网络模式会将浏览器会话直接暴露给互联网，从而增加攻击面和未经授权访问的风险。将浏览器配置为 VPC 网络模式可确保浏览器流量限制在您的私有网络内，从而使您能够应用网络级安全控制，例如安全组、网络 ACL 和 VPC 流日志。

修复

要纠正这一发现，请删除不合规的 Bedrock AgentCore 自定义浏览器，然后使用 VPC 网络模式重新创建它。有关说明，请参阅《亚马逊 Bedrock AgentCore 开发者指南》中的为 VPC 配置亚马逊 Bedrock AgentCore 运行时和工具。

[BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::BedrockAgentCore::BrowserCustom`

AWS Config 规则：bedrockagentcore-browsercustom-recording-enabled

计划类型：已触发变更

参数：无

此控件可检查 Amazon Bedrock AgentCore 自定义浏览器是否在配置了 S3 目标的情况下启用了会话录制。如果自定义浏览器未启用录制功能或未配置用于存储录制内容的 S3 位置，则控件将失败。

Bedrock AgentCore 自定义浏览器的会话记录可确保浏览器交互的完全可审计性，从而能够在自动浏览会话期间检测未经授权的访问、数据泄露或恶意活动。

修复

有关如何启用浏览器会话录制的说明，请参阅 Amazon Bedrock AgentCore 开发者指南中的会话录制和重播。

Security Hub CSPM 控件适用于 AWS Certificate Manager

这些 AWS Security Hub CSPM 控制措施评估 AWS Certificate Manager (ACM) 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

相关要求： 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

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ACM::Certificate`

AWS Config 规则：acm-certificate-expiration-check

计划类型：已触发更改且定期进行

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`daysToExpiration`	必须续订 ACM 证书的天数	整数	`14` 到 `365`	`30`

此控件检查 AWS Certificate Manager (ACM) 证书是否在指定的时间段内续订。它会检查导入的证书和 ACM 提供的证书。如果证书未在指定的时间段内续订，则控制失败。除非您为续订期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 30 天。

ACM 可以自动续订使用 DNS 验证的证书。对于使用电子邮件验证的证书，您必须回复域验证电子邮件。ACM 不会自动续订您导入的证书。您必须手动续订导入的证书。

修复

ACM 为您的 Amazon 颁发的 SSL/TLS 证书提供托管续订。这意味着 ACM 要么自动续订您的证书（如果您使用 DNS 验证），要么在证书即将到期时向您发送电子邮件通知。对于公有和私有 ACM 证书，都提供这些服务。

对于通过电子邮件验证的域

> 当证书到期 45 天后，ACM 会向域所有者发送一封针对每个域名的电子邮件。要验证域名并完成续订，您必须回复电子邮件通知。

有关更多信息，请参阅 AWS Certificate Manager 用户指南中的续订通过电子邮件验证的域。

对于通过 DNS 验证的域

ACM 自动续订使用 DNS 验证的证书。 到期前 60 天，ACM 验证证书是否可以续订。

如果无法验证域名，ACM 会发送需要手动验证的通知。它会在到期前 45 天、30 天、7 天和 1 天发送这些通知。

有关详细信息，请参阅 AWS Certificate Manager 用户指南中的通过 DNS 验证的域的续订。

[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度

相关要求：PCI DSS v4.0.1/4.2.1

类别：识别 > 库存 > 库存服务

严重性：高

资源类型：`AWS::ACM::Certificate`

AWS Config 规则：acm-certificate-rsa-check

计划类型：已触发变更

参数：无

此控件检查管理的 RSA 证书是否 AWS Certificate Manager 使用至少 2,048 位的密钥长度。如果密钥长度小于 2,048 位，则控制失败。

加密的强度与密钥大小直接相关。我们建议密钥长度至少为 2,048 位，以保护您的 AWS 资源，因为计算能力变得越来越便宜，服务器也变得更加先进。

修复

ACM 颁发的 RSA 证书的最小密钥长度已经是 2,048 位。有关使用 ACM 颁发新 RSA 证书的说明，请参阅 AWS Certificate Manager 用户指南中的颁发和管理证书。

虽然 ACM 允许您导入密钥长度较短的证书，但您必须使用至少 2,048 位的密钥才能通过此控制。导入证书后，您无法变更密钥长度。相反，您必须删除密钥长度小于 2,048 位的证书。有关将证书导入到 ACM 的更多信息，请参阅 AWS Certificate Manager 用户指南中的导入证书的先决条件。

[ACM.3] 应标记 ACM 证书

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ACM::Certificate`

AWS Config 规则:`tagged-acm-certificate`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Certificate Manager (ACM) 证书是否具有参数`requiredTagKeys`中定义的特定密钥的标签。如果证书没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查标是否存在签密键，如果证书未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ACM 证书添加标签，请参阅AWS Certificate Manager 用户指南中的标记 AWS Certificate Manager 证书。

Security Hub CSPM 控件适用于 CloudFormation

这些 Security Hub CSPM 控件用于评估 AWS CloudFormation 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudFormation.1] CloudFormation 堆栈应与简单通知服务 (SNS) 集成 Simple Notification Service

> **Important**
>
> Security Hub CSPM 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub CSPM 控件的更改日志。

相关要求：NIST.800-53.r5 SI-4（12）、NIST.800-53.r5 SI-4（5）。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::CloudFormation::Stack`

AWS Config 规则：`cloudformation-stack-notification-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon Simple Notification Service 通知是否与 CloudFormation 堆栈集成。如果没有与 CloudFormation 堆栈相关联的 SNS 通知，则该堆栈的控制将失败。

在堆栈中配置 SNS 通知有助于立即将 CloudFormation 堆栈中发生的任何事件或更改通知利益相关者。

修复

要集成堆 CloudFormation 栈和 SNS 主题，请参阅AWS CloudFormation 用户指南中的直接更新堆栈。

[CloudFormation.2] 应 CloudFormation 标记堆栈

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CloudFormation::Stack`

AWS Config 规则:`tagged-cloudformation-stack`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS CloudFormation 堆栈是否具有参数中定义的特定键的标签`requiredTagKeys`。如果堆栈没有任何标签键或未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果堆栈未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 CloudFormation 堆栈添加标签，请参阅 AWS CloudFormation API 参考CreateStack中的。

[CloudFormation.3] CloudFormation 堆栈应启用终止保护

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::CloudFormation::Stack`

AWS Config 规则：cloudformation-termination-protection-check

计划类型：已触发变更

参数：无

此控件检查 AWS CloudFormation 堆栈是否启用了终止保护。如果 CloudFormation 堆栈上未启用终止保护，则控制失败。

CloudFormation 有助于将相关资源作为一个称为堆栈的单个单元进行管理。您可以通过在堆栈上启用终止保护来防止堆栈被意外删除。如果用户尝试删除已启用终止保护的堆栈，则删除操作会失败，并且堆栈及其状态将保持不变。您可以为状态为 `DELETE_IN_PROGRESS` 或 `DELETE_COMPLETE` 之外任何状态的堆栈设置终止保护。

> **Note**
>
> 如果在堆栈上启用或禁用终止保护，则也会将相同的选择传递给属于该堆栈的任何嵌套堆栈。不能直接在嵌套堆栈上启用或禁用终止保护。您无法直接删除属于启用了终止保护的堆栈的嵌套堆栈。如果堆栈名称旁边显示 NESTED，则该堆栈为嵌套堆栈。您只能在该嵌套堆栈所属的根堆栈上更改终止保护。

修复

要在 CloudFormation 堆栈上启用终止保护，请参阅《AWS CloudFormation 用户指南》中的保护 CloudFormation 堆栈不被删除。

[CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色

类别：检测 > 安全访问管理

严重性：中

资源类型：`AWS::CloudFormation::Stack`

AWS Config 规则：cloudformation-stack-service-role-check

计划类型：已触发变更

参数：无

此控件检查 AWS CloudFormation 堆栈是否有与之关联的服务角色。如果没有服务角色与 CloudFormation 堆栈关联，则该堆栈的控制将失败。

通过 AWS Organizations 可信访问集成，服务管理 StackSets 使用执行角色。该控件还会为服务管理创建的 AWS CloudFormation 堆栈生成失败的查找结果， StackSets 因为没有与之关联的服务角色。由于服务管理的 StackSets 身份验证方式，无法为这些堆栈填充该`roleARN`字段。

在 CloudFormation 堆栈中使用服务角色有助于实现最低权限访问，方法是将 creates/updates 堆叠用户和资源所需的权限分开。 CloudFormation create/update 这降低了权限升级的风险，并有助于维护不同操作角色之间的安全边界。

> **Note**
>
> 创建堆栈后，无法删除附加到堆栈的服务角色。拥有权限，可对此堆栈执行操作的其他用户可以使用该角色，无论这些用户是否拥有 `iam:PassRole` 权限。如果该角色包含用户不应具有的权限，则您可能无意中提升了用户的权限。确保该角色授予最低权限。

修复

要将服务角色与 CloudFormation 堆栈关联，请参阅AWS CloudFormation 用户指南中的CloudFormation 服务角色。

适用于亚马逊的 Security Hub CSPM 控件 CloudFront

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon CloudFront 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudFront.1] CloudFront 发行版应配置默认根对象

相关要求： NIST.800-53.r5 SC-7(11)、 NIST.800-53.r5 SC-7 (16)、PCI DSS v4.0.1/2.6

类别：保护 > 安全访问管理 > 不可公开访问的资源

严重性：高

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-default-root-object-configured

计划类型：已触发变更

参数：无

此控件检查源为 S3 的 Amazon CloudFront 分配是否配置为返回默认根对象的特定对象。如果 CloudFront 分配使用 S3 源且未配置默认根对象，则控制失败。此控件不适用于使用自定义来源的 CloudFront 分配。

用户有时可能会请求分配的根 URL，而不是分配中的对象。发生这种情况时，指定默认根对象可以帮助您避免暴露 Web 分发的内容。

修复

要为 CloudFront 分配配置默认根对象，请参阅 Amazon CloudFront 开发者指南中的如何指定默认根对象。

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

相关要求： NIST.800-53.r5 AC-17 (2)、、(1) NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-12 NIST.800-53.r5 IA-5 (3)、3、3 (3)、(NIST.800-53.r5 SC-13)、 NIST.800-53.r5 SC-2 (4)、NIST.800-53.r5 SC-2 (1)、 NIST.800-53.r5 SC-7 (2)、nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-viewer-policy-https

计划类型：已触发变更

参数：无

此控件可检查 Amazon CloudFront 分配是否要求查看者直接使用 HTTPS 或是否使用重定向。如果 `ViewerProtocolPolicy` 对于 `defaultCacheBehavior` 或 `cacheBehaviors` 设置为 `allow-all`，则控制失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。只能允许通过 HTTPS（TLS）进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试应用程序，以了解性能概况和 TLS 的影响。

修复

要对传输中的 CloudFront 分配进行加密，请参阅《亚马逊 CloudFront 开发者指南》中的 “需要 HTTPS 才能 CloudFront在查看者之间进行通信”。

[CloudFront.4] CloudFront 发行版应配置源站故障转移

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-origin-failover-enabled

计划类型：已触发变更

参数：无

此控件会检查 Amazon CloudFront 配送是否配置了具有两个或更多来源的起源组。

CloudFront 源站故障转移可以提高可用性。如果主源不可用或返回特定的 HTTP 响应状态代码，则源失效转移会自动将流量重定向到辅助源。

修复

要为 CloudFront 分配配置源故障转移，请参阅 Amazon CloudFront 开发者指南中的创建源组。

[CloudFront.5] CloudFront 发行版应启用日志记录

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7

(8)、PCI DSS v4.0.1/10.4.2 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-accesslogs-enabled

计划类型：已触发变更

参数：无

此控件检查 CloudFront 发行版上是否启用了服务器访问日志记录。如果未为分配启用访问日志记录，则控制失败。此控件仅评估是否为分配启用了标准日志记录（旧版）。

CloudFront 访问日志提供有关 CloudFront收到的每个用户请求的详细信息。每个日志都包含诸如收到请求的日期和时间、发出请求的查看器的 IP 地址、请求的来源以及查看器请求的端口号等信息。这些日志对于安全和访问审计、取证调查等应用很有用。有关分析访问日志的更多信息，请参阅 Amazon Athena 用户指南中的查询亚马逊 CloudFront 日志。

修复

要为 CloudFront 分配配置标准日志（旧版），请参阅 Amazon CloudFront 开发者指南中的配置标准日志（旧版）。

[CloudFront.6] CloudFront 发行版应启用 WAF

相关要求： NIST.800-53.r5 AC-4(21)、PCI DSS v4.0.1/6.4.2

类别：保护 > 防护服务

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-associated-with-waf

计划类型：已触发变更

参数：无

此控件检查 CloudFront 发行版是否与 AWS WAF Classic 或 AWS WAF Web 相关联 ACLs。如果分配未与 Web ACL 关联，则控制失败。

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 APIs免受攻击。通过它，您可以配置一组规则（称为 Web 访问控制列表，即 Web ACL），基于可自定义的 Web 安全规则以及您定义的条件，允许、阻止或统计 Web 请求。确保您的 CloudFront 发行版与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。

修复

要将 AWS WAF 网页 ACL 与 CloudFront 分配相关联，请参阅 Amazon CloudFront 开发者指南中的使用 AWS WAF 来控制对内容的访问权限。

[CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

相关要求： NIST.800-53.r5 AC-17 (2)、、(1) NIST.800-53.r5 AC-4、2 NIST.800-53.r5 IA-5 (3)、3、3 (3)、(3)、 NIST.800-53.r5 SC-1 (4)、 NIST.800-53.r5 SC-2 (1)、(NIST.800-53.r5 SC-12)、 NIST.800-53.r5 SC-7 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、nist.800-171.r2 3.13.15 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-custom-ssl-certificate

计划类型：已触发变更

参数：无

此控件检查 CloudFront 发行版是否使用默认SSL/TLS certificate CloudFront provides. This control passes if the CloudFront distribution uses a custom SSL/TLS certificate. This control fails if the CloudFront distribution uses the default SSL/TLS证书。

自定义 SSL/TLS 允许您的用户使用备用域名访问内容。您可以将自定义证书存储在 AWS Certificate Manager （推荐）中，也可以存储在 IAM 中。

修复

要使用自定义 SSL/TLS 证书为 CloudFront 分配添加备用域名，请参阅亚马逊 CloudFront 开发者指南中的添加备用域名。

[CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-sni-enabled

计划类型：已触发变更

参数：无

此控件会检查 Amazon CloudFront 分发是否使用自定义 SSL/TLS 证书，以及是否配置为使用 SNI 来处理 HTTPS 请求。如果关联了自定义 SSL/TLS 证书，但 SSL/TLS 支持方法是专用 IP 地址，则此控件将失败。

服务器名称指示（SNI）是对 TLS 协议的扩展，2010 年以后发布的浏览器和客户端均支持。如果您配置 CloudFront 为使用 SNI 处理 HTTPS 请求，请 CloudFront 将您的备用域名与每个边缘站点的 IP 地址相关联。当查看器提交针对内容的 HTTPS 请求时，DNS 将该请求传送到正确边缘站点的 IP 地址。您的域名的 IP 地址是在 SSL/TLS 握手协商期间确定的；IP 地址不是专用于您的分发的。

修复

要将 CloudFront 分配配置为使用 SNI 处理 HTTPS 请求，请参阅《CloudFront开发者指南》中的“使用 SNI 处理 HTTPS 请求（适用于大多数客户端）”。有关自定义 SSL 证书的信息，请参阅使用 SSL/TLS 证书的要求 CloudFront。

[CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

相关要求： NIST.800-53.r5 AC-17 (2)、、(1) NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-12 NIST.800-53.r5 IA-5 (3)、3、3 (3)、(NIST.800-53.r5 SC-13)、 NIST.800-53.r5 SC-2 (4)、

NIST.800-53.r5 SC-2 (1)、 NIST.800-53.r5 SC-7 (2)、nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-traffic-to-origin-encrypted

计划类型：已触发变更

参数：无

此控件可检查 Amazon CloudFront 分配是否正在加密流向自定义来源的流量。对于源协议策略允许“仅限 http”的 CloudFront 分发，此控制失败。如果分配的源协议策略为“match-viewer”，而查看器协议策略为“allow-all”，则此控制也会失败。

HTTPS（TLS）可用于帮助防止侦听或操纵网络流量。只能允许通过 HTTPS（TLS）进行加密连接。

修复

要更新源协议策略以要求对 CloudFront 连接进行加密，请参阅《亚马逊 CloudFront 开发者指南》中的要求 CloudFront 与您的自定义源之间的通信需要 HTTPS。

[CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

相关要求： NIST.800-53.r5 AC-17 (2)、、(1)、2 NIST.800-53.r5 IA-5 (3) NIST.800-53.r5 AC-4、3、3、(4)、、(1)、 NIST.800-53.r5 SC-1 (NIST.800-53.r5 SC-12)、 NIST.800-53.r5 SC-2 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、 NIST.800-53.r5 SC-8 nist.800-171.r2 3.13.15、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-no-deprecated-ssl-protocols

计划类型：已触发变更

参数：无

此控件可检查 Amazon CloudFront 分配是否使用已弃用的 SSL 协议进行 CloudFront 边缘站点和您的自定义源站之间的 HTTPS 通信。如果 CloudFront 分配`OriginSslProtocols`包含 where includes，则`CustomOriginConfig`此控件将失败`SSLv3`。

2015 年，国际互联网工程任务组（IETF）正式宣布，由于该协议不够安全，应弃用 SSL 3.0。建议您使用 TLSv1 .2 或更高版本与自定义源进行 HTTPS 通信。

修复

要更新 CloudFront 分配的 Origin SSL 协议，请参阅 Amazon CloudFront 开发者指南中的要求 HTTPS 才能 CloudFront 与您的自定义源进行通信。

[CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

相关要求：NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2（2）、PCI DSS v4.0.1/2.2.6

类别：识别 > 资源配置

严重性：高

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-s3-origin-non-existent-bucket

计划类型：定期

参数：无

此控件可检查亚马逊 CloudFront 分发是否指向不存在的 Amazon S3 来源。如果源配置为指向不存在的存储桶，则 CloudFront 分配的控制将失败。此控件仅适用于没有静态网站托管的 S3 存储桶是 S3 来源的 CloudFront 分配。

当您账户中的 CloudFront 分配配置为指向不存在的存储桶时，恶意第三方可以创建引用的存储桶，并通过您的分配提供自己的内容。无论路由行为如何，我们都建议您检查所有源，以确保分布指向适当的源。

修复

要修改 CloudFront 分配以指向新的来源，请参阅《Amazon CloudFront 开发者指南》中的更新分配。

[CloudFront.13] CloudFront 发行版应使用源站访问控制

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-s3-origin-access-control-enabled

计划类型：已触发变更

参数：无

此控件检查源为 Amazon S3 的亚马逊 CloudFront 分发是否配置了源站访问控制 (OAC)。如果没有为 CloudFront分发配置 OAC，则控制失败。

使用 S3 存储桶作为 CloudFront 分配的源时，您可以启用 OAC。这仅允许通过指定的 CloudFront分配访问存储桶中的内容，并禁止直接从存储桶或其他分配进行访问。尽管 CloudFront 支持原始访问身份 (OAI)，但 OAC 提供了其他功能，使用 OAI 的发行版可以迁移到 OAC。尽管 OAI 提供了一种安全的方式来访问 S3 源，但它也有一些局限性，例如不支持精细的策略配置和使用需要 AWS 签名版本 4 (Sigv4) AWS 区域 的 POST 方法的 HTTP/HTTPS 请求。OAI 也不支持使用进行加密。 AWS Key Management Service OAC 基于使用 IAM 服务主体向 S3 源进行身份验证 AWS 的最佳实践。

修复

要为具有 S3 来源的 CloudFront 分配配置 OAC，请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amazon S3 来源的访问权限。

[CloudFront.14] 应 CloudFront 标记发行版

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则:`tagged-cloudfront-distribution`（ 自定义 Security Hub CSPM 规则 ）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件会检查 Amazon CloudFront 分配是否具有参数中定义的特定密钥的标签requiredTagKeys。如果分配没有任何标签键或未在参数 requiredTagKeys 中指定所有键，则此控件会失败。如果未提供参数 requiredTagKeys，则此控件仅会检查是否存在标签键，如果分配未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要为 CloudFront 分配添加标签，请参阅《亚马逊 CloudFront 开发者指南》中的 “为亚马逊 CloudFront分配添加标签”。

[CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::CloudFront::Distribution

AWS Config 规则：cloudfront-ssl-policy-check

计划类型：已触发变更

参数：`securityPolicies`：`TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025`（不可自定义）

此控件会检查 Amazon CloudFront 分配是否配置为使用推荐的 TLS 安全策略。如果 CloudFront 分配未配置为使用推荐的 TLS 安全策略，则控制失败。

如果您将 Amazon CloudFront 分配配置为要求查看者使用 HTTPS 访问内容，则必须选择安全策略并指定要使用的最低 SSL/TLS 协议版本。这决定了 CloudFront 使用哪个协议版本与查看者通信，以及 CloudFront 用于加密通信的密码。我们建议使用 CloudFront 提供的最新安全策略。这样可以确保 CloudFront 使用最新的密码套件来加密在查看器和分发之间传输的数据。 CloudFront

> **Note**
>
> 此控件仅为配置为使用自定义 SSL 证书且未配置为支持旧版客户端的 CloudFront 发行版生成调查结果。

修复

有关为 CloudFront 分配配置安全策略的信息，请参阅 Amazon CloudFront 开发者指南中的更新分配。当为分配配置安全策略时，请选择最新的安全策略。

[CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-origin-lambda-url-oac-enabled

计划类型：已触发变更

参数：无

此控件检查以 AWS Lambda 函数 URL 为来源的 Amazon CloudFront 分配是否启用了源站访问控制 (OAC)。如果 CloudFront分配以 Lambda 函数 URL 作为来源，并且未启用 OAC，则控制失败。

AWS Lambda 函数 URL 是 Lambda 函数的专用 HTTPS 终端节点。如果 Lambda 函数 URL 是 CloudFront 分配的来源，则该函数 URL 必须是可公开访问的。因此，作为安全最佳实践，您应该创建一个 OAC 并将其添加到分配中的 Lambda 函数 URL。OAC 使用 IAM 服务委托人对 CloudFront 和函数 URL 之间的请求进行身份验证。它还支持使用基于资源的策略，仅当请求代表策略中指定的 CloudFront 分配时才允许调用函数。

修复

有关为使用 Lambda 函数 URL 作为来源的亚马逊 CloudFront 分配配置 OAC 的信息，请参阅 CloudFront 亚马逊开发者指南中的限制 AWS Lambda 对函数 URL 来源的访问。

[CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：cloudfront-distribution-key-group-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon CloudFront 分配是否配置为使用可信密钥组进行签名 URL 或签名 Cookie 身份验证。如果 CloudFront分发使用可信签名者，或者分配未配置身份验证，则控制失败。

要使用签名 URLs 或签名的 Cookie，您需要签名者。签名者可以是您在中创建的可信密钥组 CloudFront，也可以是包含 CloudFront 密钥对的 AWS 账户。我们建议您使用可信密钥组，因为对于 CloudFront 密钥组，您无需使用 AWS 账户 root 用户来管理 CloudFront 已签名 URLs 和已签名 Cookie 的公钥。

> **Note**
>
> 此控件不评估多租户 CloudFront 分布(`connectionMode=tenant-only`)。

修复

有关使用带签名 URLs 和 Cookie 的可信密钥组的信息，请参阅《亚马逊 CloudFront 开发者指南》中的使用可信密钥组。

Security Hub CSPM 控件适用于 AWS CloudTrail

这些 AWS Security Hub CSPM 控制措施评估 AWS CloudTrail 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

相关要求：独联体 AWS 基金会基准 v5.0.0/3.1、CIS AWS 基金会基准 v1.2.0/2.1、CIS AWS 基金会基准 v1.4.0/3.1、CIS 基金会基准 v3.0.0/3.1、 NIST.800-53.r5 AC-2 (4)、(26)、(9)、(9)、NIST.800-53.r5 AC-4 (22) AWS NIST.800-53.r5 AC-6 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 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

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：multi-region-cloudtrail-enabled

计划类型：定期

参数：

- `readWriteType`：`ALL`（不可自定义）

  `includeManagementEvents`：`true`（不可自定义）

此控件检查是否至少有一个捕获读写管理事件的多区域 AWS CloudTrail 跟踪。如果 CloudTrail 禁用或没有至少一条 CloudTrail 跟踪可以捕获读写管理事件，则控件将失败。

AWS CloudTrail 记录您的账户 AWS 的 API 调用并将日志文件发送给您。记录的信息包括：

- API 调用方的身份
- API 调用的时间
- API 调用方的源 IP 地址
- 请求参数

- 返回的响应元素 AWS 服务

CloudTrail 提供账户 AWS 的 API 调用历史记录，包括通过、 AWS 管理控制台 AWS SDKs、命令行工具进行的 API 调用。历史记录还包括来自更高级别的 API 调用 ， AWS 服务 例如。 AWS CloudFormation

生成的 AWS API 调用历史记录 CloudTrail 支持安全分析、资源变更跟踪和合规性审计。多区域跟踪还提供以下好处。

- 多区域跟踪有助于检测在其他本不应使用的区域中发生的意外活动。
- 多区域跟踪可确保默认情况下为跟踪启用全局服务事件日志记录。全球服务事件日志记录记录 AWS 全球服务生成的事件。
- 对于多区域跟踪，所有读取和写入操作的管理事件可确保 CloudTrail 记录中所有资源的管理操作。AWS 账户

默认情况下，使用创建的 CloudTrail 跟踪 AWS 管理控制台 是多区域跟踪。

修复

要在中创建新的多区域跟踪 CloudTrail，请参阅AWS CloudTrail 用户指南中的创建跟踪。使用以下值：

Field	Value
其他设置，日志文件验证	已启用
选择日志事件、管理事件、API 活动	读和写。清除排除项的复选框。

要更新现有跟踪，请参阅 AWS CloudTrail 用户指南中的更新跟踪。在管理事件中，对于 API 活动，选择读取和写入。

[CloudTrail.2] CloudTrail 应该启用静态加密

相关要求：独联体 AWS 基金会基准 v5.0.0/3.5、CIS 基金会基准 v1.2.0/2.7、CIS AWS 基金会基准 v1.4.0/3.7、CIS 基金会基准 v3.0.0/3.5、(1)、(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1)、(10)、nist.800-53.r5 SI AWS -7 (6)、nist.800-171.r2 3. NIST.800-53.r5 SC-2 8、PCI DSS v3.2.1/3.4、PCI DSS v3.2.1/3.4、NIST.800-53.r5 SC-2 PCI DSS v3.2.1/3.4 I DSS v4.0.1/10.3.2 AWS NIST.800-53.r5 SC-7

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：cloud-trail-encryption-enabled

计划类型：定期

参数：无

此控件检查 CloudTrail 是否配置为使用服务器端加密 (SSE) AWS KMS key 加密。如果 `KmsKeyId` 未定义，则控制失败。

为了增加敏感 CloudTrail 日志文件的安全性，您应该使用服务器端加密和 AWS KMS keys (SSE-KMS) 对 CloudTrail 日志文件进行静态加密。请注意，默认情况下，传送 CloudTrail 到您的存储桶的日志文件由亚马逊服务器端加密，使用 Amazon S3 托管的加密密钥 (SSE-S3) 进行加密。

修复

要为 CloudTrail 日志文件启用 SSE-KMS 加密，请参阅AWS CloudTrail 用户指南中的更新跟踪以使用 KMS 密钥。

[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪

相关要求：NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7、PCI DSS v3.2.1/10.1、PCI DSS v3.2.1/10.2.1、PCI DSS v3.2.1/10.2.2、PCI DSS v3.2.1/10.2.3、PCI DSS v3.2.1/10.2.4、PCI DSS v3.2.1/10.2.5、PCI DSS v3.2.1/10.2.6、PCI DSS v3.2.1/10.2.7、PCI DSS v3.2.1/10.3.1、PCI DSS v3.2.1/10.3.2、PCI DSS v3.2.1/10.3.3、PCI DSS v3.2.1/10.3.4、PCI DSS v3.2.1/10.3.5、PCI DSS v3.2.1/10.3.6、PCI DSS v4.0.1/10.2.1

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：cloudtrail-enabled

计划类型：定期

参数：无

此控件可检查您的中是否启用了 AWS CloudTrail 跟踪 AWS 账户。如果您的账户未启用至少一条 CloudTrail 跟踪，则控制失败。

但是，某些 AWS 服务不允许记录所有 APIs 和事件。除了 “CloudTrail 支持的 CloudTrail 服务和集成”中每项服务的文档之外，您还应实施任何其他审计跟踪。

修复

要开始使用 CloudTrail 和创建跟踪，请参阅《AWS CloudTrail 用户指南》中的入门 AWS CloudTrail 教程。

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

相关要求：独联体 AWS 基金会基准 v5.0.0/3.2、独联体基金会基准 v1.2.0/2.2、独联体基金会基准 v1.4.0/3.2、独联体 AWS 基金会基准 v3.0.0/3.2、nist.800-53.r5 AU-9、nist.800-53.r5 SI AWS -4、nist.800-53.r5 SI AWS -7 (1)、nist.800-53.r5 SI-7 (3))、nist.800-53.r5 SI-7 (7)、nist.800-171.r2 3.8、PCI DSS v3.2.1/10.5.2、PCI DSS v3.2.1/10.5.2、PCI DSS v3.2.1/10.5.5、PCI DSS v4.0.1/10.3.2

类别：数据保护 > 数据完整性

严重性：低

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：cloud-trail-log-file-validation-enabled

计划类型：定期

参数：无

此控件检查是否在 CloudTrail跟踪上启用了日志文件完整性验证。

CloudTrail 日志文件验证会创建一个经过数字签名的摘要文件，其中包含 CloudTrail 写入 Amazon S3 的每个日志的哈希值。您可以使用这些摘要文件来确定日志文件在 CloudTrail 传送日志后是更改、删除还是未更改。

Security Hub CSPM 建议您在所有跟踪中启用文件验证。日志文件验证可对 CloudTrail 日志进行额外的完整性检查。

修复

要启用 CloudTrail 日志文件验证，请参阅AWS CloudTrail 用户指南 CloudTrail中的启用日志文件完整性验证。

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

相关要求：独联体 AWS 基金会基准 v5.0.0/3.4、PCI DSS v3.2.1/10.5.3、CIS 基金会基准 v1.2.0/2.4、CIS AWS 基金会基准 v1.4.0/3.4、(4)、(26)、(9)、(9)、nist.800-53.r5 SI-20、nist.800-53.r5 SI AWS -3 (8)、nist.800-53.r5 SI-3 NIST.800-53.r5 AC-2 (8)、 NIST.800-53.r5 AC-4 nist.800-53.r5 SI-3 NIST.800-53.r5 AC-6 (8) 4 (20) 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 SI-4 NIST.800-53.r5 SC-7 (5)、nist.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：cloud-trail-cloud-watch-logs-enabled

计划类型：定期

参数：无

此控件检查是否已将 CloudTrail 跟踪配置为向日志发送 CloudWatch 日志。如果跟踪的 `CloudWatchLogsLogGroupArn` 属性为空，则控制失败。

CloudTrail 记录在给定账户中进行的 AWS API 调用。记录的信息包括以下内容：

- API 调用者的身份
- API 调用时间间
- API 调用方的源 IP 地址
- 请求参数
- 返回的响应元素 AWS 服务

CloudTrail 使用 Amazon S3 进行日志文件存储和传输。您可以捕获指定 S3 存储桶中的 CloudTrail 日志以进行长期分析。要执行实时分析，您可以配置为将日志发送 CloudTrail 到 CloudWatch 日志。

对于在账户中所有区域启用的跟踪，CloudTrail 会将所有这些区域的日志文件发送到 CloudWatch 日志日志组。

Security Hub CSPM 建议您将 CloudTrail 日志发送到日志。 CloudWatch 请注意，此建议旨在确保捕获、监视账户活动并适当发出警报。你可以使用 CloudWatch Logs 来设置你的 AWS 服务。此建议并不排除使用不同的解决方案。

将 CloudTrail 日志发送到 CloudWatch 日志便于根据用户、API、资源和 IP 地址进行实时和历史活动记录。您可以使用此方法为异常或敏感账户活动建立警报和通知。

修复

要 CloudTrail 与 CloudWatch 日志集成，请参阅AWS CloudTrail 用户指南中的向 CloudWatch 日志发送事件。

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

相关要求：独联体 AWS 基金会基准 v1.2.0/2.3、CIS 基金会基准 v1.4.0/3.3、PCI DSS v AWS 4.0.1/1.4.4

类别：识别 > 日志记录

严重性：严重

资源类型：`AWS::S3::Bucket`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期计划和触发变更

参数：无

CloudTrail 记录在您的账户中进行的每个 API 调用。这些日志文件存储在 S3 存储桶中。CIS 建议将 S3 存储桶策略或访问控制列表 (ACL) 应用于 CloudTrail 记录的 S3 存储桶，以防止公众访问 CloudTrail 日志。允许公众访问 CloudTrail 日志内容可能有助于对手识别受影响账户使用或配置中的弱点。

要运行此检查，Security Hub CSPM 首先使用自定义逻辑来查找存储 CloudTrail 日志的 S3 存储桶。然后，它使用 AWS Config 托管规则来检查存储桶是否可公开访问。

如果您将日志聚合到单个集中式 S3 存储桶中，则 Security Hub CSPM 仅对集中式 S3 存储桶所在的账户和区域进行检查。对于其他账户和区域，控件状态为无数据。

如果存储桶可公开访问，则检查会生成失败的调查发现。

修复

要阻止公众访问您的 CloudTrail S3 存储桶，请参阅《A mazon 简单存储服务用户指南》中的 “为您的 S3 存储桶配置阻止公开访问设置”。选择所有四个 Amazon S3 屏蔽公共访问权限。

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

相关要求：独联体 AWS 基金会基准 v1.2.0/2.6、CIS 基金会基准 v1.4.0/3.6、CIS AWS 基金会基准 v3.0.0/3.4、PCI DSS v4.0.1/10.2.1 AWS

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：无（ 自定义 Security Hub CSPM 规则 ）

计划类型：定期

参数：无

S3 存储桶访问日志记录会生成一个日志，其中包含对 S3 存储桶发出的每个请求的访问记录。访问日志记录包含与请求有关的详细信息，如请求类型、处理过的请求中指定的资源和请求的处理时间和日期。

CIS 建议您在 S3 存储桶上启用存储 CloudTrail 桶访问日志记录。

通过在目标 S3 存储桶上启用 S3 存储桶日志记录，您可以捕获可能影响目标存储桶中对象的所有事件。将日志配置为存放在单独的存储桶中可实现对日志信息的访问，这在安全和事故响应工作流程中非常有用。

要运行此检查，Security Hub CSPM 首先使用自定义逻辑查找存储 CloudTrail 日志的存储桶，然后使用 AWS Config 托管规则检查是否启用了日志记录。

如果 AWS 账户 将多个日志文件 CloudTrail 传送到单个目标 Amazon S3 存储桶，则 Security Hub CSPM 仅针对其所在地区的目标存储桶评估此控制权。这简化了调查发现。但是，您应该 CloudTrail 在所有将日志传送到目标存储桶的账户中开启。对于除持有目标存储桶的账户以外的所有账户，控件状态均为无数据。

修复

要为 CloudTrail S3 存储桶启用服务器访问日志记录，请参阅《亚马逊简单存储服务用户指南》中的“启用 Amazon S3 服务器访问日志”。

[CloudTrail.9] CloudTrail 路径应加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则:`tagged-cloudtrail-trail`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS CloudTrail 跟踪是否具有参数中定义的特定键的标签`requiredTagKeys`。如果跟踪记录没有任何标签键或未在参数 `requiredTagKeys` 中指定所有键，则此控件会失败。如果未提供参数 `requiredTagKeys`，则此控件仅会检查是否存在标签键，如果跟踪记录未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 CloudTrail 跟踪添加标签，请参阅 AWS CloudTrail API 参考AddTags中的。

[CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys

相关要求： NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9(1)、(10)、2 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7（NIST.800-53.r5 SC-12)、 NIST.800-53.r5 SC-1 3、8、 NIST.800-53.r5 SC-2 8 (1)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::CloudTrail::EventDataStore`

AWS Config 规则：event-data-store-cmk-encryption-enabled

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`kmsKeyArns`	评估中 AWS KMS keys 要包含的 Amazon 资源名称 (ARNs) 列表。如果事件数据存储未使用列表中的 KMS 密钥进行加密，	StringList（最多 3 件商品）	1—3 个 ARNs 现有 KMS 密钥。例如：`arn:aws:kms:us-west-2:111122223333:key/1234ab`	无默认值

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
	则该控件会生成 FAILED 调查发现。		cd-12ab-34cd-56ef-1234567890ab 。	

此控件检查 AWS CloudTrail Lake 事件数据存储是否在客户托管的情况下进行静态加密 AWS KMS key。如果未使用客户自主管理型 KMS 密钥对事件数据存储进行加密，则该控件会失败。您可以选择为控件指定要包含在评估中的 KMS 密钥列表。

默认情况下， AWS CloudTrail Lake 使用 AES-256 算法使用亚马逊 S3 托管密钥 (SSE-S3) 对存储的事件数据进行加密。为了获得更多控制，您可以将 CloudTrail Lake 配置为使用客户托管 AWS KMS key (SSE-KMS) 加密事件数据存储。客户托管的 KMS 密钥 AWS KMS key 是您在自己中创建、拥有和管理的密钥 AWS 账户。您可以完全控制此类 KMS 密钥。这包括定义和维护密钥策略、管理授权、轮换加密材料、分配标签、创建别名以及启用和禁用密钥。您可以在加密操作中使用客户托管的 KMS 密钥来管理您的 CloudTrail 数据，并通过 CloudTrail 日志审核使用情况。

修复

有关使用您指定的加密 AWS CloudTrail Lake 事件数据存储的信息，请参阅AWS CloudTrail 用户指南中的更新事件数据存储。 AWS KMS key 在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

适用于亚马逊的 Security Hub CSPM 控件 CloudWatch

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon CloudWatch 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/1.1、独联体基金会基准 v1.2.0/3.3、独联体基金会基准 v1.4.0/1.7、独联体 AWS 基金会基准 v1.4.0/4.3、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.7、PCI AWS DSS v3.2.1/7.2.1 AWS

类别：检测 > 检测服务

严重性：低

资源类
型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

根用户可以不受限制地访问 AWS 账户中的所有服务和资源。我们强烈建议您避免使用根用户执行日常任务。最大限度地减少根用户的使用并采用最低权限原则进行访问管理，可以降低意外更改和意外泄露高权限凭证的风险。

作为最佳实践，仅在需要执行账户和服务管理任务时才使用根用户凭证。将 AWS Identity and Access Management (IAM) 策略直接应用于群组和角色，但不适用于用户。有关如何设置管理员以供日常使用的教程，请参阅 IAM 用户指南中的创建第一个 IAM 管理员用户和组

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.4.0中为控制1.7规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 FAILED 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 NO_DATA 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
> - 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。
>
>   我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现

在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报

相关要求：CIS AWS 基金会基准 v1.2.0/3.1、nist.800-171.r2 3.13.1、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您创建指标筛选条件并对未经授权的 API 调用发出警报。监控未经授权的 API 调用有助于发现应用程序错误，并可能减少检测恶意活动所花费的时间。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.2中为控制3.1规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。

在以下情况下，检查会导致 FAILED 调查发现：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查会导致 NO_DATA 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 ListSubscriptionsByTopic 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成WARNING控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
指标命名空间	**LogMetrics**
指标值	**1**
默认 值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.2

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您创建不受 MFA 保护的指标筛选条件和警报控制台登录。监控单因素控制台登录可提高不受 MFA 保护的账户的可见性。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.2中为控制3.2规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 `NO_DATA` 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
> - 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。
>
> 对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态

Field	Value
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.4、CIS 基金会基准 v1.4.0/4.4、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14. AWS 6、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

此控件通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报来检查您是否实时监控 API 调用。

CIS 建议您为 IAM policy 的更改创建指标筛选条件和警报。监控此类更改有助于确保身份验证和授权控制保持不变。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 `NO_DATA` 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成WARNING控件的调查结果。

修复

> **Note**
>
> 我们在这些补救步骤中推荐的筛选条件模式与 CIS 指南中的筛选条件模式不同。我们推荐的筛选条件仅针对来自 IAM API 调用的事件。

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
指标命名空间	**LogMetrics**
指标值	**1**
默认 值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态

Field	Value
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.5、CIS 基金会基准 v1.4.0/4.5、nist.800-171.r2 3.8、nist.800-171.r2 3. AWS 8、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为对 CloudTrail 配置设置的更改创建指标筛选条件和警告。监控此类更改有助于确保账户中活动的持续可见性。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.4.0中为控制4.5规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查会导致 NO_DATA 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成WARNING控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.6、CIS 基金会基准 v1.4.0/4.6、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.7 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为失败的控制台身份验证尝试创建指标筛选条件和警报。监控失败的控制台登录可能会缩短检测暴力破解凭证尝试的准备时间，这可能会提供可供您在其他事件相关性分析中使用的指标，例如源 IP。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.4.0中为控制4.6规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 `NO_DATA` 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
> - 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.7、CIS 基金会基准 v1.4.0/4.7、nist.800-171.r2 3.13.10、nist.800-171.r2 3.13. AWS 16、nist.800-171.r2 3.13.16、nist.800-171.r2 3.14.7、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为已将状态更改为禁用或计划删除的客户管理密钥创建指标筛选条件和警报。您无法再访问使用已禁用或已删除的密钥加密的数据。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.4.0中为控制4.7规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。如果 `ExcludeManagementEventSources` 包含 `kms.amazonaws.com`，则控制也会失败。

Note

当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
在以下情况下，检查会导致 `FAILED` 调查发现：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查会导致 `NO_DATA` 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。

3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.8、CIS 基金会基准 v1.4.0/4.8、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14. AWS 6、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类
型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为 S3 存储桶策略更改创建指标筛选条件和警告。监控此类更改可能会缩短检测和纠正敏感 S3 存储桶的宽松策略的时间。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.4.0中为控制4.8规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 FAILED 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 NO_DATA 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
> - 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`

Field	Value
指标命名空间	**LogMetrics**
指标值	**1**
默认 值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.9、CIS 基金会基准 v1.4.0/4.9、nist.800-171.r2 3.8、nist.800-171.r2 3. AWS 8、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为对 AWS Config 配置设置的更改创建指标筛选条件和警告。监控此类更改有助于确保账户中配置项的持续可见性。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试 v1.4.0中为控制4.9规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 `NO_DATA` 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
> - 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。
>
> 对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.10、CIS 基金会基准 v1.4.0/4.10、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.6、 AWS nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。安全组是有状态的数据包筛选器，可用于控制 VPC 的传入和传出流量。

CIS 建议您为安全组更改创建指标筛选条件和警告。监控此类更改有助于确保不会意外公开 资源和服务。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试v1.4.0中为控制4.10规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 `NO_DATA` 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。

- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurity`

Field	Value
	`GroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.11、独联体基金会基准 v1.4.0/4.11、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.6、 AWS nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（ 自定义 Security Hub CSPM 规则 ）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。 NACLs 用作无状态数据包过滤器，用于控制 VPC 中子网的入口和出口流量。

CIS 建议您创建指标筛选器并发出警报，以应对所做的更改 NACLs。监控这些更改有助于确保 AWS 资源和服务不会被无意中暴露。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试v1.4.0中为控制4.11规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

Note

当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
在以下情况下，检查会导致 `FAILED` 调查发现：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查会导致 `NO_DATA` 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.12、CIS 基金会基准 v1.4.0/4.12、nist.800-171.r2 3.3.1、nist.800-171.r2 3.1、 AWS nist.800-171.r2 3.13.1

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。需要网络网关才能向位于 VPC 以外的目标发送流量或从其接收流量。

CIS 建议您为网络网关更改创建指标筛选条件和警告。监控此类更改有助于确保所有传入和传出流量都通过受控路径穿过 VPC 边界。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试v1.2中为控制4.12规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。

在以下情况下，检查会导致 FAILED 调查发现：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查会导致 NO_DATA 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 ListSubscriptionsByTopic 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成WARNING控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
指标命名空间	**LogMetrics**
指标值	**1**
默认 值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.13、CIS 基金会基准 v1.4.0/4.13、nist.800-171.r2 3.1、nist.800-171.r2 3.13.1、nist.8 AWS 00-171.r2 3.13.1、nist.800-171.r2 3.13.1、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类
型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

此控件通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报来检查您是否实时监控 API 调用。路由表在子网和网络网关之间路由网络流量。

CIS 建议您为路由表更改创建指标筛选条件和警告。监控此类更改有助于确保所有 VPC 流量都流经预期路径。

Note

当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
在以下情况下，检查会导致 FAILED 调查发现：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查会导致 NO_DATA 控件状态：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

> **Note**
>
> 我们在这些补救步骤中推荐的筛选条件模式与 CIS 指南中的筛选条件模式不同。我们推荐的筛选条件仅针对来自 Amazon Elastic Compute Cloud（EC2）API 调用的事件。

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventN`

Field	Value
	`ame=DeleteRoute) || ($.eventN ame=DisassociateRouteTable))}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认 值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.14、CIS 基金会基准 v1.4.0/4.14、nist.800-171.r2 3.1、nist.800-171.r2 3.13.1、nist.800-171.r2 3.13.1、ni AWS st.800-171.r2 3.13.1、nist.800-171.r2 3.13.1、nist.800-171.r2 3.14.7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。一个账户中可以有多个 VPC，并且可以在两个 VPC 之间创建对等连接 VPCs，从而使网络流量能够在两个 VPC 之间进行路由 VPCs。

CIS 建议您创建指标筛选器并发出警报，以应对所做的更改 VPCs。监控此类更改有助于确保身份验证和授权控制保持不变。

为了运行此检查，Security Hub CSPM使用自定义逻辑来执行C IS AWS 基金会基准测试v1.4.0中为控制4.14规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub CSPM 对该控件执行检查时，它会查找当前账户使用的 CloudTrail 跟踪。这些跟踪可能是属于另一个账户的组织跟踪。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查会导致 `FAILED` 调查发现：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查会导致 `NO_DATA` 控件状态：
>
> - 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
> - 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。
>
>   我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。
>
> 对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub CSPM 会生成`WARNING`控件的调查结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
指标命名空间	**LogMetrics**
指标值	**1**

Field	Value
默认 值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.15] CloudWatch 警报应配置指定操作

相关要求： 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-20、nist.800-53.r5 SI-4 (12)、nist.800-53.r5 SI-4 (5)、nist.800-53.r5 SI-4 (5)、nist.800-53.r5 SI-4 (5)、nist.800-53.r5 SI-4 (5)、nist.800-53.r5 SI-4 (5) -171.r2 3.3.4，nist.800-171.r2 3.14.6

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::CloudWatch::Alarm`

AWS Config 规则：**`cloudwatch-alarm-action-check`**

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`alarmActionRequired`	如果将参数设置为 `true` 并且警报状态变更为 `ALARM` 时警	布尔值	不可自定义	`true`

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
	报会执行操作，则控件会生成PASSED 调查发现。			
insufficientDataActionRequired	如果将参数设置为 true 并且警报状态变更为 INSUFFICIENT_DATA 时警报会执行操作，则控件会生成PASSED 调查发现。	布尔值	true 或者 false	false
okActionRequired	如果将参数设置为 true 并且警报状态变更为 OK 时警报会执行操作，则控件会生成PASSED 调查发现。	布尔值	true 或者 false	false

此控件检查 Amazon CloudWatch 警报是否为该ALARM状态配置了至少一个操作。如果警报没有为 ALARM 状态配置操作，则控制失败。或者，您可以包含自定义参数值，以便也要求对 INSUFFICIENT_DATA 或 OK 状态执行警报操作。

> **Note**
>
> Security Hub CSPM 根据 CloudWatch 指标警报评估此控件。指标警报可能是复合警报的一部分，这些复合警报配置了指定操作。在以下情况下，控件会生成 FAILED 调查发现：
>
> - 没有为指标警报配置指定操作。
> - 此指标警报是某个复合警报的一部分，该复合警报配置了指定操作。

此控件侧重于 CloudWatch 警报是否配置了警报操作，而 CloudWatch.17 侧重于 CloudWatch 警报操作的激活状态。

我们建议采取 CloudWatch 警报措施，以便在监控的指标超出定义的阈值时自动提醒您。当警报进入特定状态时，监控警报可帮助您识别异常活动并快速响应安全和操作问题。最常见的警报操作类型是通过向 Amazon Simple Notification Service（Amazon SNS）主题发送消息来通知一个或多个用户。

修复

有关 CloudWatch 警报支持的操作的信息，请参阅 Amazon CloudWatch 用户指南中的警报操作。

[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留

类别：识别 > 日志记录

相关要求： 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

严重性：中

资源类型：`AWS::Logs::LogGroup`

AWS Config 规则：**`cw-loggroup-retention-period-check`**

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`minRetentionTime`	CloudWatch 日志组的最小保留期（以天为单位）	枚举	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

此控件检查 Amazon CloudWatch 日志组的保留期是否至少为指定的天数。如果保留期少于指定天数，则控制失败。除非您为保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 365 天。

CloudWatch 日志将来自所有系统、应用程序的日志集中到一个高度可扩展的服务 AWS 服务中。您可以使用 CloudWatch 日志来监控、存储和访问来自亚马逊弹性计算云 (EC2) 实例 AWS CloudTrail、Amazon Route 53 和其他来源的日志文件。将日志保留至少 1 年可以帮助您遵守日志保留标准。

修复

要配置日志保留设置，请参阅《Amazon CloudWatch 用户指南》中的 “ CloudWatch 日志” 中的 “更改日志数据保留期”。

[CloudWatch.17] 应激 CloudWatch 活警报动作

类别：检测 > 检测服务

相关要求： 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)

严重性：高

资源类型：`AWS::CloudWatch::Alarm`

AWS Config 规则：**`cloudwatch-alarm-action-enabled-check`**

计划类型：已触发变更

参数：无

此控件检查 CloudWatch 警报操作是否已激活（`ActionEnabled`应设置为 true）。如果警报的警报动作被停用， CloudWatch 则控制失败。

> **Note**
>
> Security Hub CSPM 根据 CloudWatch 指标警报评估此控件。指标警报可能是复合警报的一部分，这些复合警报已激活警报操作。在以下情况下，控件会生成 `FAILED` 调查发现：
>
> - 没有为指标警报配置指定操作。
> - 此指标警报是某个复合警报的一部分，该复合警报已激活警报操作。

此控件侧重于 CloudWatch 警报操作的激活状态，而 CloudWatch.15 侧重于 CloudWatch 警报中是否配置了任何`ALARM`操作。

当监控的指标超出定义的阈值时，警报操作会自动向您发出警报。如果警报操作被停用，则警报状态变更时不会运行任何操作，也不会提醒您注意监控指标的变化。我们建议您激活 CloudWatch 警报操作，以帮助您快速应对安全和操作问题。

修复

激活 CloudWatch 警报操作（控制台）

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中的警报下，选择所有警报。
3. 选择要激活操作的警报。
4. 在操作中，选择警报操作-新建，然后选择启用。

有关激活 CloudWatch 警报操作的更多信息，请参阅 Amazon CloudWatch 用户指南中的警报操作。

Security Hub CSPM 控件适用于 CodeArtifact

这些 Security Hub CSPM 控件用于评估 AWS CodeArtifact 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CodeArtifact.1] 应标记CodeArtifact 存储库

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CodeArtifact::Repository`

AWS Config 规则:`tagged-codeartifact-repository`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS CodeArtifact 存储库是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果存储库没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果

未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果存储库未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 CodeArtifact 仓库添加标签，请参阅《AWS CodeArtifact 用户指南》 CodeArtifact中的为仓库添加标签。

Security Hub CSPM 控件适用于 CodeBuild

这些 Security Hub CSPM 控件用于评估 AWS CodeBuild 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证

相关要求： NIST.800-53.r5 SA-3，PCI DSS v3.2.1/8.2.1，PCI DSS v4.0.1/8.3.2

类别：保护 > 安全开发

严重性：严重

资源类型：`AWS::CodeBuild::Project`

AWS Config 规则：`codebuild-project-source-repo-url-check`

计划类型：已触发变更

参数：无

此控件检查 AWS CodeBuild 项目 Bitbucket 源存储库 URL 是否包含个人访问令牌或用户名和密码。如果 Bitbucket 源存储库 URL 包含个人访问令牌或用户名和密码，则此控件将失败。

> **Note**
>
> 此控件会评估 CodeBuild 构建项目的主要来源和次要来源。有关项目源的更多信息，请参阅《AWS CodeBuild User Guide》中的 Multiple input sources and output artifacts sample。

登录凭证不应以明文形式存储或传输，也不应出现在源存储库 URL 中。与其使用个人访问令牌或登录凭证，您应该在中访问您的源提供商 CodeBuild，并将源存储库 URL 更改为仅包含 Bitbucket 存储库位置的路径。使用个人访问令牌或登录凭证可能会导致意外的数据泄露和未经授权的访问。

修复

您可以更新您的 CodeBuild 项目以供使用 OAuth。

从 CodeBuild 项目源中移除基本身份验证/(GitHub) 个人访问令牌

1. 打开 CodeBuild 控制台，网址为https://console.aws.amazon.com/codebuild/。
2. 选择包含个人访问令牌或用户名和密码的构建项目。
3. 从 Edit（编辑） 中，选择 Source（源）。
4. 从 GitHub /Bitbucket 中选择断开连接。
5. 选择 “使用连接” OAuth，然后选择 “连接到 GitHub /Bitbucke t”。
6. 出现提示时，选择相应授权。
7. 根据需要，重新配置存储库 URL 和其他配置设置。
8. 选择更新源。

有关更多信息，请参阅《AWS CodeBuild 用户指南》中基于CodeBuild 用例的示例。

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

相关要求： NIST.800-53.r5 IA-5(7)、PCI DSS v3.2.1/8.2.1 NIST.800-53.r5 SA-3、PCI DSS v4.0.1/8.3.2

类别：保护 > 安全开发

严重性：严重

资源类型：AWS::CodeBuild::Project

AWS Config 规则：codebuild-project-envvar-awscred-check

计划类型：已触发变更

参数：无

该控制检查项目是否包含环境变量 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。

身份验证凭证 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY 决不能以明文方式存储，因为这可能会导致意外的数据暴露和未经授权的访问。

修复

要从 CodeBuild 项目中移除环境变量，请参阅AWS CodeBuild 用户指南 AWS CodeBuild中的更改构建项目的设置。确保没有为环境变量选择任何内容。

您可以将带有敏感值的环境变量存储在 P AWS Systems Manager arameter Store 中 AWS Secrets Manager ，也可以从构建规范中检索它们。有关说明，请参阅 AWS CodeBuild 用户指南中“环境”部分中标有重要的方框。

[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、nist.800-53.r5 SI- NIST.800-53.r5 SC-2 7 (6)、PCI DSS v4.0.1/10.3.2

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：低

资源类型：AWS::CodeBuild::Project

AWS Config 规则：codebuild-project-s3-logs-encrypted

计划类型：已触发变更

参数：无

此控件可检查 AWS CodeBuild 项目的 Amazon S3 日志是否已加密。如果对 CodeBuild 项目的 S3 日志停用加密，则控制失败。

建议对静态数据进行加密，以在数据周围添加一层访问管理。对静态日志进行加密可以降低未经身份验证的 AWS 用户访问存储在磁盘上的数据的风险。它添加了另一组访问控制来限制未经授权的用户访问数据的能力。

修复

要更改 CodeBuild 项目 S3 日志的加密设置，请参阅AWS CodeBuild 用户指南 AWS CodeBuild中的更改构建项目的设置。

[CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

相关要求： NIST.800-53.r5 AC-2(12)、(4)、(26)、 NIST.800-53.r5 AC-2 (9)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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 SI-4、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::CodeBuild::Project`

AWS Config 规则：`codebuild-project-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查 CodeBuild 项目环境是否至少有一个日志选项，要么是 S3 日志选项，要么是启用了 CloudWatch 日志。如果 CodeBuild 项目环境没有启用至少一个日志选项，则此控件将失败。

从安全角度来看，日志记录是一项重要功能，可以在发生任何安全事件时为将来的取证工作提供支持。将 CodeBuild 项目中的异常与威胁检测关联起来，可以增强人们对这些威胁检测准确性的信心。

修复

有关如何配置 CodeBuild 项目日志设置的更多信息，请参阅《 CodeBuild 用户指南》中的创建构建项目（控制台）。

[CodeBuild.5] CodeBuild 项目环境不应启用特权模式

> **Important**
>
> Security Hub CSPM 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub CSPM 控件的更改日志。

相关要求： 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)

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::CodeBuild::Project`

AWS Config 规则：`codebuild-project-environment-privileged-check`

计划类型：已触发变更

参数：无

此控件检查 AWS CodeBuild 项目环境是启用还是禁用了特权模式。如果 CodeBuild 项目环境启用了特权模式，则控制失败。

默认情况下，Docker 容器不允许访问任何设备。特权模式将授予构建项目的 Docker 容器访问所有设备的权限。使用 `true` 值进行设置 `privilegedMode` 允许 Docker 进程守护程序在 Docker 容器内运行。Docker 进程守护程序侦听 Docker API 请求并管理 Docker 对象，例如映像、容器、网络和卷。仅当构建项目用于构建 Docker 映像时，才应将此参数设置为 true。否则，应禁用此设置，以防止意外访问 Docker APIs 以及容器的底层硬件。`privilegedMode` 设置为 `false` 有助于保护关键资源免遭篡改和删除。

修复

要配置 CodeBuild 项目环境设置，请参阅《CodeBuild 用户指南》中的创建构建项目（控制台）。在环境部分中，不要选择特权设置。

[CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::CodeBuild::ReportGroup`

AWS Config 规则：`codebuild-report-group-encrypted-at-rest`

计划类型：已触发变更

参数：无

此控件检查导出到亚马逊简单存储服务 (Amazon S3) Storage Service 存储桶 AWS CodeBuild 的报告组的测试结果是否经过静态加密。如果未对报告组进行静态加密，则此控件将失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要加密导出到 S3 的报告组，请参阅《AWS CodeBuild User Guide》中的 Update a report group。

适用于 Amazon Profiler 的 Security Hub CSPM 控件 CodeGuru

这些 Security Hub CSPM 控件用于评估 Amazon CodeGuru Profiler 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CodeGuruProfiler::ProfilingGroup`

AWS Config 规则：`codeguruprofiler-profiling-group-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon CodeGuru Profiler 分析组是否具有参数requiredKeyTags中定义的特定密钥的标签。如果分析组没有任何标签键或者未在 requiredKeyTags 参数中指定所有键，则此控件会失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果分析组未使用任何键进行标记，则此控件会失效。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 CodeGuru Profiler 分析组添加标签，请参阅 A mazon P CodeGuru rofiler 用户指南中的为分析组添加标签。

适用于 Amazon Reviewer 的 Security Hub CSPM 控件 CodeGuru

这些 Security Hub CSPM 控件用于评估 Amazon CodeGuru Reviewer 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Config 规则：`codegurureviewer-repository-association-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon CodeGuru Reviewer 存储库关联是否具有参数`requiredKeyTags`中定义的特定密钥的标签。如果存储库关联没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件会失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果存储库关联未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 CodeGuru 审阅者存储库关联添加标签，请参阅 A mazon Rev CodeGuru iewer 用户指南中的为存储库关联添加标签。

适用于亚马逊 Cognito 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Cognito 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::Cognito::UserPool`

AWS Config 规则：cognito-user-pool-advanced-security-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`SecurityMode`	控件检查的威胁防护强制模式。	字符串	`AUDIT`, `ENFORCED`	`ENFORCED`

此控件检查 Amazon Cognito 用户池是否已激活威胁防护，并将强制模式设置为采用全功能进行标准身份验证。如果用户池已停用威胁防护，或者强制模式未设置为采用全功能进行标准身份验证，则该控件会失败。除非您提供自定义参数值，否则 Security Hub CSPM 将使用默认值`ENFORCED`作为标准身份验证的强制模式设置为全功能。

创建 Amazon Cognito 用户池后，您可以激活威胁防护并自定义针对不同风险采取的操作。或者，您可以使用审计模式收集与检测到的风险相关的指标，而无需应用任何安全缓解措施。在审计模式下，威胁防护会向 Amazon 发布指标 CloudWatch。在 Amazon Cognito 生成其第一个事件后，您即可看到指标。

修复

有关为 Amazon Cognito 用户池激活威胁防护的信息，请参阅《Amazon Cognito 开发人员指南》中的具备威胁防护的高级安全功能。

[Cognito.2] Cognito 身份池不应允许未经身份验证的身份

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::Cognito::IdentityPool`

AWS Config 规则：cognito-identity-pool-unauth-access-check

计划类型：已触发变更

参数：无

此控件检查 Amazon Cognito 身份池是否配置为允许未经身份验证的身份。如果激活身份池的访客访问权限（`AllowUnauthenticatedIdentities` 参数设置为 `true`），则该控件会失败。

如果 Amazon Cognito 身份池允许未经身份验证的身份，则该身份池将向尚未通过身份提供者进行身份验证的用户（访客）提供临时 AWS 证书。这会带来安全风险，因为它允许匿名访问 AWS 资源。如果您停用访客访问权限，则可以帮助确保只有经过适当身份验证的用户才能访问您的 AWS 资源，从而降低未经授权访问和潜在安全漏洞的风险。作为最佳实践，身份池应要求通过支持的身份提供者进行身份验证。如果需要未经身份验证的访问，请务必谨慎限制未经身份验证的身份的权限，并定期审查和监控其使用情况。

修复

有关停用 Amazon Cognito 身份池的访客访问权限的信息，请参阅《Amazon Cognito 开发人员指南》中的激活或停用访客访问权限。

[Cognito.3] Cognito 用户池的密码策略应具有可靠的配置

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::Cognito::UserPool`

AWS Config 规则：cognito-user-pool-password-policy-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
minLength	密码必须包含的最少字符数。	整数	8 到 128	8
requireLowercase	密码中要求至少包含一个小写字符。	布尔值	True, False	True
requireUppercase	密码中要求至少包含一个大写字符。	布尔值	True, False	True
requireNumbers	密码中要求至少包含一个数字。	布尔值	True, False	True
requireSymbols	密码中要求至少包含一个符号。	布尔值	True, False	True
temporaryPasswordValidity	密码过期前可以存在的最长天数。	整数	1 到 365	7

此控件根据密码策略的推荐设置，检查 Amazon Cognito 用户池的密码策略是否要求使用强密码。如果用户池的密码策略不要求使用强密码，则此控件会失败。您可以选择为控件检查的策略设置指定自定义值。

强密码是 Amazon Cognito 用户池的一项安全最佳实践。弱密码可以将用户的凭证暴露给会猜测密码并尝试访问数据的系统。对于向互联网开放的应用程序来说尤其如此。密码策略是用户目录安全的核心要素。通过使用密码策略，您可以配置用户池，使其要求密码复杂度和其他符合您的安全标准和要求的设置。

修复

有关创建或更新 Amazon Cognito 用户池的密码策略的信息，请参阅《Amazon Cognito 开发人员指南》中的添加用户池密码要求。

[Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::Cognito::UserPool`

AWS Config 规则：cognito-userpool-cust-auth-threat-full-check

计划类型：已触发变更

参数：无

此控件检查 Amazon Cognito 用户池是否已激活威胁防护，并将强制模式设置为完整功能以进行自定义身份验证。如果用户池禁用了威胁防护，或者自定义身份验证的强制模式未设置为完整功能，则控制失败。

威胁防护（此前称为高级安全功能）是一组监控用户池中不必要活动的工具，也是用于自动关闭潜在恶意活动的配置工具。创建 Amazon Cognito 用户池后，您可以激活具有全功能强制模式的威胁防护，以进行自定义身份验证，并自定义为应对不同风险而采取的操作。全功能模式包括一组自动反应，用于检测不想要的活动和泄露的密码。

修复

有关为 Amazon Cognito 用户池激活威胁防护的信息，请参阅《Amazon Cognito 开发人员指南》中的具备威胁防护的高级安全功能。

[Cognito.5] 应为 Cognito 用户池启用 MFA

类别：保护 > 安全访问管理 > 多因素身份验证

严重性：中

资源类型：`AWS::Cognito::UserPool`

AWS Config 规则：cognito-user-pool-mfa-enabled

计划类型：已触发变更

参数：无

此控件检查配置了仅限密码登录策略的 Amazon Cognito 用户池是否启用了多重身份验证 (MFA)。如果配置了仅限密码登录策略的用户池未启用 MFA，则控制失败。

多重身份验证 (MFA) 在你知道的因素（通常是用户名和密码）中添加了一个你有身份验证因子。对于联合用户，Amazon Cognito 将身份验证委托给身份提供者 (IdP)，并且不提供额外的身份验证因素。但是，如果您的本地用户具有密码身份验证，则为用户池配置 MFA 可以提高他们的安全性。

> **Note**
>
> 此控件不适用于联合用户和使用无密码因素登录的用户。

修复

有关如何为 Amazon Cognito 用户池配置 MFA 的信息，请参阅 Amazon Cognito 开发者指南中的向用户池添加 MFA。

[Cognito.6] Cognito 用户池应启用删除保护

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::Cognito::UserPool`

AWS Config 规则：cognito-user-pool-deletion-protection-enabled

计划类型：已触发变更

参数：无

此控件会检查 Amazon Cognito 用户池是否启用了删除保护。如果禁用了用户池的删除保护，则控件将失败。

删除保护有助于确保您的用户池不会被意外删除。在为用户池配置删除保护时，任何用户都无法删除该池。删除保护可防止您请求删除用户池，除非您先修改用户池并停用删除保护。

修复

要为 Amazon Cognito 用户池配置删除保护，请参阅 A mazon Cognito 开发者指南中的用户池删除保护。

Security Hub CSPM 控件适用于 AWS Config

这些 Security Hub CSPM 控件用于评估 AWS Config 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

> **Note**
>
> 启用 Security Hub CSPM 和 Security Hub 后，该 Config.1 规则的状态将始终为 “已通过”。这是因为 Security Hub CSPM 可以通过与服务相关的配置记录器直接访问配置项目。此控件的参数不适用，因为内部服务相关配置记录器是使用 AWS Config 服务相关角色自动创建的。有关更多信息，请参阅 使用与服务相关的配置记录器。

相关要求：CIS AWS 基金会基准测试 v5.0。 0/3.3，CIS AWS 基金会基准 v1.2。 0/2.5，CIS AWS 基金会基准 v1.4。 0/3.5，CIS AWS 基金会基准测试 v3.0。 0/3.3、 NIST.800-53.r5 CM-3、NIST.800-53.r5 CM-6 (1)、 NIST.800-53.r5 CM-8 (2) NIST.800-53.r5 CM-8、PCI DSS v3.2。 1/10.5.2，PCI DSS v3.2。 1/11.5

类别：识别 > 清单

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：无（ 自定义 Security Hub CSPM 规则 ）

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`includeConfigServiceLinkedRoleCheck`	如果参数设置为，则控件不会评估是否 AWS Config 使用服务相关角色。`false`	布尔值	`true` 或者 `false`	`true`

此控件检查您的账户当前 AWS Config 是否已启用 AWS 区域，记录与当前区域中启用的控件对应的所有资源，并使用服务相关 AWS Config 角色。服务相关角色的名称是AWSServiceRoleForConfig。如果您不使用服务相关角色且未将`includeConfigServiceLinkedRoleCheck`参数设置为`false`，则控制失败，因为其他角色可能不具备准确记录您的资源的必要权限。 AWS Config

该 AWS Config 服务对您的账户中支持的 AWS 资源执行配置管理，并向您提供日志文件。记录的信息包括配置项目（AWS 资源）、配置项目之间的关系以及资源中的任何配置更改。全局资源是指在任何区域中都可用的资源。

控件评估方式如下：

- 如果将当前区域设置为聚合区域，则只有在记录 AWS Identity and Access Management (IAM) 全球资源时（如果您启用了需要这些资源的控件），控件才会生成PASSED调查结果。
- 如果将当前区域设置为关联区域，则此控件不会评估是否记录了 IAM 全局资源。
- 如果当前区域不在您的聚合器中，或者您的账户中未设置跨区域聚合，则此控件仅在记录了 IAM 全局资源（如果您启用了需要这些资源的控件）时，才会生成 PASSED 调查发现。

无论您选择每天还是连续记录 AWS Config中资源状态的变化，都不会影响控件的结果。但是，如果您配置了自动启用新控件或具有自动启用新控件的中心配置策略，则在发布新控件时，此控件的结果可能会发生变化。在这些情况下，如果您没有记录所有资源，则必须配置与新控件关联的资源记录才能获得 PASSED 调查发现。

Security Hub CSPM 安全检查只有 AWS Config 在所有区域中启用并针对需要它的控制配置资源记录时，才能按预期运行。

> **Note**
>
> Config.1 要求在您使用 AWS Config Security Hub CSPM 的所有区域中启用该功能。由于 Security Hub CSPM 是一项区域服务，因此对该控件执行的检查仅评估账户的当前区域。要允许针对每个区域中的 IAM 全局资源进行安全检查，您还必须记录该区域中的 IAM 全局资源。未记录 IAM 全局资源的区域将收到用于检查 IAM 全局资源的控件的默认 PASSED 调查发现。由于 IAM 全球资源各不相同 AWS 区域，因此我们建议您仅在本地区记录 IAM 全球资源（如果您的账户中启用了跨区域聚合）。IAM 资源将仅记录在已开启全局资源记录的区域中。AWS Config 支持的 IAM 全球记录资源类型包括 IAM 用户、群组、角色和客户托管策略。您可以考虑在关闭全局资源记录的区域禁用用于检查这些资源类型的 Security Hub CSPM 控件。有关更多信息，请参阅 建议在 Security Hub CSPM 中禁用的控件。

修复

在主区域和不属于聚合器的区域中，请记录当前区域中启用的控件所需的所有资源，包括 IAM 全局资源（如果您启用了需要 IAM 全局资源的控件）。

在关联的区域中，只要您 AWS Config 录制的是与当前区域中启用的控件相对应的所有资源，您就可以使用任何录制模式。在关联区域中，如果您启用了需要记录 IAM 全局资源的控件，则不会收到 FAILED 调查发现（您对其他资源的记录就已足够）。

调查发现的 Compliance 对象中的 StatusReasons 字段可帮助您确定此控件具有失败的调查发现的原因。有关更多信息，请参阅 控件调查发现的合规性详细信息。

有关必须为每个控件记录哪些资源的列表，请参阅必填 AWS Config 控制结果的资源。有关启用 AWS Config 和配置资源记录的一般信息，请参阅启用和配置 AWS Config 适用于 Security Hub CSPM。

适用于 Amazon Connect 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件会评估 Amazon Connect 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Connect.1] 应标记 Amazon Connect 客户档案对象类型

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::CustomerProfiles::ObjectType

AWS Config 规则：customerprofiles-object-type-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Connect Customer Profiles 对象类型是否具有带特定键的标签，这些键在 requiredKeyTags 参数中进行定义。如果对象类型没有任何标签键或者未在 requiredKeyTags 参数中指定所有键，则此控件会失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在

标签键，如果对象类型未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要为客户档案对象类型添加标签，请参阅 Connect 客户管理员指南中的向 Amazon Connect 客户中的资源添加标签。

[Connect.2] Connect 客户实例应启用 CloudWatch 日志记录

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Connect::Instance`

AWS Config 规则：启用连接实例日志记录

计划类型：已触发变更

参数：无

此控件检查 Connect Customer 实例是否配置为生成流日志并将其存储在 Amazon CloudWatch 日志组中。如果 Connect Customer 实例未配置为在日志组中生成和存储流日志， CloudWatch 则控制失败。

Amazon Connect 客户流日志提供有关 Amazon Connect 客户流程中事件的实时详细信息。流程定义了 Amazon Connect 客户联络中心从头到尾的客户体验。默认情况下，当您创建新的 Amazon

Connect 客户实例时，会自动创建一个 Amazon CloudWatch 日志组来存储该实例的流日志。流日志可以帮助您分析流、发现错误和监控运营指标。您还可以为流中可能发生的特定事件设置警报。

修复

有关为 Amazon Connect 客户实例启用流日志的信息，请参阅 Connect 客户管理员指南中的在亚马逊 CloudWatch 日志组中启用 Amazon Connect 客户流日志。

适用于亚马逊 Data Firehose 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件用于评估 Amazon Data Firehose 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DataFirehose.1] Firehose 传输流应在静态状态下进行加密

相关要求： NIST.800-53.r5 AC-3、 NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-1 2、 NIST.800-53.r5 SC-1 3、 NIST.800-53.r5 SC-2 8

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::KinesisFirehose::DeliveryStream`

AWS Config 规则：`kinesis-firehose-delivery-stream-encrypted`

计划类型：定期

参数：无

此控件可检查是否使用服务器端加密对 Amazon Data Firehose 传输流进行静态加密。如果未使用服务器端加密对 Firehose 传输流进行静态加密，则此控件将失败。

服务器端加密是 Amazon Data Firehose 交付流中的一项功能，它使用在 () 中创建 AWS Key Management Service 的密钥在数据静止之前自动对其进行加密。AWS KMS在数据写入 Data Firehose 流存储层之前对其进行加密，并在存储中检索之后进行解密。这样，您就可以遵守监管要求并增强您数据的安全性。

修复

要在 Firehose 传输流上启用服务器端加密，请参阅《Amazon Data Firehose 开发人员指南》中的 Amazon Data Firehose 中的数据保护。

Security Hub CSPM 控件适用于 AWS Database Migration Service

这些 AWS Security Hub CSPM 控件会评估 AWS Database Migration Service (AWS DMS) 和 AWS DMS 资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DMS.1] Database Migration Service 复制实例不应公开

相关要求： NIST.800-53.r5 AC-21、、 NIST.800-53.r5 AC-3（7）、（21） NIST.800-53.r5 AC-3、、（11）、（16） NIST.800-53.r5 AC-4、 NIST.800-53.r5 AC-4（20）、（21）、（3） NIST.800-53.r5 AC-6、（4） NIST.800-53.r5 SC-7、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7（9）、 NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1、 NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1、 NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1、 NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.2 2.1/1.3.6，PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则：dms-replication-not-public

计划类型：定期

参数：无

此控件检查 AWS DMS 复制实例是否为公共实例。为此，它会检查 `PubliclyAccessible` 字段的值。

私有复制实例具有私有 IP 地址，您无法在复制网络外部访问该地址。当源数据库和目标数据库位于同一网络时，复制实例应具有私有 IP 地址。还必须使用 VPN 或 VPC 对等连接将网络连接到复制实例的 VPC。 Direct Connect要了解有关公有和私有复制实例的更多信息，请参阅 AWS Database Migration Service 用户指南中的公有和私有复制实例。

您还应确保只有经过授权的用户才能访问您的 AWS DMS 实例配置。为此，请限制用户修改 AWS DMS 设置和资源的 IAM 权限。

修复

创建 DMS 复制实例后，您无法变更其公共访问设置。要变更公共访问设置，请删除您当前的实例，然后重新创建实例。不要选择公开访问选项。

[DMS.2] 应标记 DMS 证书

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::Certificate`

AWS Config 规则:`tagged-dms-certificate`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS DMS 证书是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果证书没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查标是否存在签密键，如果证书未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 证书添加标签，请参阅《AWS Database Migration Service User Guide》中的 Tagging resources in AWS Database Migration Service。

[DMS.3] 应标记 DMS 活动订阅

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::EventSubscription`

AWS Config 规则:`tagged-dms-eventsubscription`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS DMS 事件订阅是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果事件订阅没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果事件订阅未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 事件订阅添加标签，请参阅《AWS Database Migration Service User Guide》中的 Tagging resources in AWS Database Migration Service。

[DMS.4] 应标记 DMS 复制实例

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则:`tagged-dms-replicationinstance`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS DMS 复制实例是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果复制实例没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果复制实例未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 复制实例添加标签，请参阅《AWS Database Migration Service User Guide》中的 Tagging resources in AWS Database Migration Service。

[DMS.5] 应标记 DMS 复制子网组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::ReplicationSubnetGroup`

AWS Config 规则:`tagged-dms-replicationsubnetgroup`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS DMS 复制子网组是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果复制子网组没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果复制子网组未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 复制子网组添加标签，请参阅《AWS Database Migration Service User Guide》中的 Tagging resources in AWS Database Migration Service。

[DMS.6] DMS 复制实例应启用自动次要版本升级

相关要求：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

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则：dms-auto-minor-version-upgrade-check

计划类型：已触发变更

参数：无

此控件检查是否为 AWS DMS 复制实例启用了自动次要版本升级。如果未为 DMS 复制实例启用自动次要版本升级，则控制失败。

DMS 为每个支持的复制引擎提供自动次要版本升级，以便您可以保留复制实例 up-to-date。次要版本可以引入新的软件功能、错误修复、安全补丁和性能改进。通过在 DMS 复制实例上启用自动次要版本升级，可以在维护时段内自动应用次要升级，或者如果选择了“立即应用变更”选项，则会立即应用次要升级。

修复

要在 DMS 复制实例上启用自动次要版本升级，请参阅 AWS Database Migration Service 用户指南中的修改复制实例。

[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、PCI DSS v4.0.1/10.4.2 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::DMS::ReplicationTask`

AWS Config 规则：dms-replication-task-targetdb-logging

计划类型：已触发变更

参数：无

此控件检查是否启用了日志记录，并且 DMS 复制任务 `TARGET_APPLY` 和 `TARGET_LOAD` 的最低严重级别为 `LOGGER_SEVERITY_DEFAULT`。如果未为这些任务启用日志记录，或者最低严重性级别低于 `LOGGER_SEVERITY_DEFAULT`，则控制失败。

在迁移过程中，DMS 使用 Amazon CloudWatch 来记录信息。使用日志记录任务设置，您可以指定记录哪些组件活动以及记录多少信息。您应该为以下任务指定日志记录：

- `TARGET_APPLY`：数据和数据定义语言（DDL）语句应用于目标数据库。

- TARGET_LOAD——数据将加载到目标数据库中。

日志记录通过启用监控、故障排除、审核、性能分析、错误检测和恢复以及历史分析和报告，在 DMS 复制任务中发挥着关键作用。日志记录有助于确保数据库之间数据的成功复制，同时保持数据完整性并符合法规要求。在故障排除期间，这些组件很少需要除了 DEFAULT 以外的其他日志级别。除非特别要求由 支持变更这些组件的日志级别，否则我们建议保留这些组件的日志级别 DEFAULT。最低日志级别为 DEFAULT 可确保将信息性消息、警告和错误消息写入日志。此控件检查上述复制任务的日志记录级别是否至少为以下级别之一：LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG 或 LOGGER_SEVERITY_DETAILED_DEBUG。

修复

要启用目标数据库 DMS 复制任务的日志记录，请参阅《AWS Database Migration Service 用户指南》中的查看和管理 AWS DMS 任务日志。

[DMS.8] 源数据库的 DMS 复制任务应启用日志记录

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、PCI DSS v4.0.1/10.4.2 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

类别：识别 > 日志记录

严重性：中

资源类型：AWS::DMS::ReplicationTask

AWS Config 规则：dms-replication-task-sourcedb-logging

计划类型：已触发变更

参数：无

此控件检查是否启用了日志记录，并且 DMS 复制任务 SOURCE_CAPTURE 和 SOURCE_UNLOAD 的最低严重级别为 LOGGER_SEVERITY_DEFAULT。如果未为这些任务启用日志记录，或者最低严重性级别低于 LOGGER_SEVERITY_DEFAULT，则控制失败。

在迁移过程中，DMS 使用 Amazon CloudWatch 来记录信息。使用日志记录任务设置，您可以指定记录哪些组件活动以及记录多少信息。您应该为以下任务指定日志记录：

- SOURCE_CAPTURE：正在进行的复制或变更数据捕获（CDC）数据从源数据库或服务中捕获，并传递到 SORTER 服务组件。
- SOURCE_UNLOAD——数据在满负荷期间从源数据库或服务中卸载。

日志记录通过启用监控、故障排除、审核、性能分析、错误检测和恢复以及历史分析和报告，在 DMS 复制任务中发挥着关键作用。日志记录有助于确保数据库之间数据的成功复制，同时保持数据完整性并符合法规要求。在故障排除期间，这些组件很少需要除了 DEFAULT 以外的其他日志级别。除非特别要求由 支持变更这些组件的日志级别，否则我们建议保留这些组件的日志级别 DEFAULT。最低日志级别为 DEFAULT 可确保将信息性消息、警告和错误消息写入日志。此控件检查上述复制任务的日志记录级别是否至少为以下级别之一：LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG 或 LOGGER_SEVERITY_DETAILED_DEBUG。

修复

要启用源数据库 DMS 复制任务的日志记录，请参阅《AWS Database Migration Service 用户指南》中的查看和管理 AWS DMS 任务日志。

[DMS.9] DMS 端点应使用 SSL

相关要求： NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-1 3、3 (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 NIST.800-53.r5 SC-8 (2)、PCI DSS v4.0.1/4.2.1

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::DMS::Endpoint

AWS Config 规则：dms-endpoint-ssl-configured

计划类型：已触发变更

参数：无

此控件检查 AWS DMS 端点是否使用 SSL 连接。如果端点不使用 SSL，则控制失败。

SSL/TLS 连接通过加密 DMS 复制实例与数据库之间的连接来提供一层安全性。使用证书通过验证是否与预期数据库建立连接来提供额外的安全保护。它通过检查自动安装在您预置的所有数据库实例上的服务器证书来实现这一点。通过在 DMS 端点上启用 SSL 连接，您可以在迁移过程中保护数据的机密性。

修复

要向新的或现有的 DMS 端点添加 SSL 连接，请参阅 AWS Database Migration Service 用户指南中的将 SSL 与 AWS Database Migration Service配合使用。

[DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权

相关要求： NIST.800-53.r5 AC-2、、、 NIST.800-53.r5 AC-1 7 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

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::DMS::Endpoint`

AWS Config 规则：dms-neptune-iam-authorization-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon Neptune 数据库的 AWS DMS 终端节点是否配置了 IAM 授权。如果 DMS 端点未启用 IAM 授权，则此控件将失败。

AWS Identity and Access Management (IAM) 提供细粒度的访问控制。 AWS通过 IAM，您可以指定谁可以在哪些条件下访问哪些服务和资源。使用 IAM 策略，您可以管理员工和系统的权限，以确保最低权限。通过在 Neptune 数据库的 AWS DMS 终端节点上启用 IAM 授权，您可以使用参数指定的服务角色向 IAM 用户授予授权权限。`ServiceAccessRoleARN`

修复

要在 Neptune 数据库的 DMS 端点上启用 IAM 授权，请参阅《AWS Database Migration Service User Guide》中的 Using Amazon Neptune as a target for AWS Database Migration Service。

[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

相关要求： 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

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::DMS::Endpoint`

AWS Config 规则：dms-mongo-db-authentication-enabled

计划类型：已触发变更

参数：无

此控件检查 MongoDB 的 AWS DMS 端点是否配置了身份验证机制。如果没有为该端点设置身份验证类型，则此控件将失败。

AWS Database Migration Service 支持 MongoDB 的两种身份验证方法：MongoDB 版本 2.x 的 MONGODB-CR 和 MongoDB 版本 3.x 或更高版本的 SCRAM-SHA-1。如果用户想使用密码访问数据库，则使用这些身份验证方法对 MongoDB 密码进行身份验证和加密。 AWS DMS 端点身份验证可确保只有经过授权的用户才能访问和修改数据库之间迁移的数据。如果没有适当的身份验证，未经授权的用户可能会在迁移过程中访问敏感数据。这样可能导致数据泄露、数据丢失或其他安全事件。

修复

要在 MongoDB 的 DMS 端点上启用身份验证机制，请参阅《AWS Database Migration Service User Guide》中的 Using MongoDB as a source for AWS DMS。

[DMS.12] Redis OSS 的 DMS 端点应启用 TLS

相关要求： NIST.800-53.r5 SC-8， NIST.800-53.r5 SC-13，PCI DSS v4.0.1/4.2.1

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::DMS::Endpoint`

AWS Config 规则：dms-redis-tls-enabled

计划类型：已触发变更

参数：无

此控件检查 Redis OSS 的 AWS DMS 终端节点是否配置了 TLS 连接。如果该端点未启用 TLS，则此控件将失败。

当数据通过互联网在应用程序或数据库之间发送时，TLS 可提供 end-to-end安全性。当您为 DMS 端点配置 SSL 加密时，其会在迁移过程中启用源数据库和目标数据库之间的加密通信。这有助于防止恶意

行为者侦听和拦截敏感数据。如果没有 SSL 加密，敏感数据可能会被访问，从而导致数据泄露、数据丢失或其他安全事件。

修复

要在 Redis 的 DMS 端点上启用 TLS 连接，请参阅《AWS Database Migration Service User Guide》中的 Using Redis as a target for AWS Database Migration Service。

[DMS.13] DMS 复制实例应配置为使用多个可用区

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则：dms-replication-instance-multi-az-enabled

计划类型：已触发变更

参数：无

此控件检查 AWS Database Migration Service (AWS DMS) 复制实例是否配置为使用多个可用区（多可用区部署）。如果 AWS DMS 复制实例未配置为使用多可用区部署，则该控件会失败。

在多可用区部署中，在不同的可用区 (AZ) 中 AWS DMS 自动配置和维护复制实例的备用副本。然后，主复制实例将同步复制到备用副本。如果主复制实例发生故障或没有响应，备用副本将以最少中断恢复任何正在运行的任务。有关更多信息，请参阅《AWS Database Migration Service 用户指南》中的 Working with a replication instance。

修复

创建 AWS DMS 复制实例后，您可以更改其多可用区部署设置。有关更改现有复制实例的此设置和其他设置的信息，请参阅《AWS Database Migration Service 用户指南》中的修改复制实例。

Security Hub CSPM 控件适用于 AWS DataSync

这些 Security Hub CSPM 控件用于评估 AWS DataSync 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DataSync.1] DataSync 任务应启用日志记录

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::DataSync::Task`

AWS Config 规则：datasync-task-logging-enabled

计划类型：已触发变更

参数：无

此控件检查 AWS DataSync 任务是否启用了日志记录。如果任务未启日志记录，则此控件将失败。

审计日志跟踪和监控系统活动。它们提供了事件记录，可以帮助您检测安全漏洞、调查事件并遵守法规。审计日志还可以增强组织的整体问责制并提高组织透明度。

修复

有关为 AWS DataSync 任务配置日志的信息，请参阅AWS DataSync 用户指南中的使用 Amazon CloudWatch Logs 监控数据传输。

[DataSync.2] 应标记 DataSync 任务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DataSync::Task`

AWS Config 规则：datasync-task-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS DataSync 任务是否具有requiredKeyTags参数指定的标签密钥。如果任务没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件会失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果任务没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关为 AWS DataSync 任务添加标签的信息，请参阅《AWS DataSync 用户指南》中的为AWS DataSync 任务添加标签。

适用于 Amazon Detective 的 Security Hub CSPM 控件

此 AWS Security Hub CSPM 控件用于评估 Amazon Detective 服务和资源。该控件可能并非在所有 AWS 区域都可用。有关更多信息，请参阅 按地区划分的控件可用性。

[Detective.1] 应标记 Detective 行为图

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Detective::Graph

AWS Config 规则:tagged-detective-graph（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon Detective 行为图是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果行为图没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供参数 `requiredTagKeys`，则此控件仅检查是否存在标签键，如果行为图未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Detective 行为图添加标签，请参阅《Amazon Detective Administration Guide》中的 Adding tags to a behavior graph。

适用于亚马逊 DocumentDB 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控件评估亚马逊文档数据库（兼容 MongoDB）服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：docdb-cluster-encrypted

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 集群是否进行静态加密。如果 Amazon DocumentDB 集群未进行静态加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。Amazon DocumentDB 集群中的数据应进行静态加密，以增加安全性。Amazon DocumentDB 使用 256 位高级加密标准（AES-256），使用 AWS Key Management Service （AWS KMS）中存储的加密密钥来加密您的数据。

修复

您可以在创建 Amazon DocumentDB 集群时启用静态加密。创建集群后，您将无法变更加密设置。有关更多信息，请参阅 Amazon DocumentDB 开发人员指南中的为 Amazon DocumentDB 集群启用静态加密。

[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期

相关要求：NIST.800-53.r5 SI-12、PCI DSS v4.0.1/3.2.1

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：docdb-cluster-backup-retention-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`minimumBackupRetentionPeriod`	最小备份保留期（以天为单位）	整数	7 到 35	7	

此控件检查 Amazon DocumentDB 集群的备份保留期是否大于或等于指定时间范围。如果备份保留期小于指定时间范围，则控制失败。除非您为备份保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 7 天。

备份可帮助您更快地从安全事件中恢复并增强系统的故障恢复能力。通过自动备份 Amazon DocumentDB 集群，您将能够将系统恢复到某个时间点并最大限度地减少停机时间和数据丢失。在 Amazon DocumentDB 中，集群的默认备份保留期为 1 天。必须将其增加到 7 到 35 天之间的值才能通过此控件。

修复

要变更 Amazon DocumentDB 集群的备份保留期，请参阅 Amazon DocumentDB 开发人员指南中的修改 Amazon DocumentDB 集群。对于备份，选择备份保留期。

[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

相关要求： 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、、、(11) NIST.800-53.r5 AC-6 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)、(4)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9)、 NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::RDS::DBClusterSnapshot`

AWS Config 规则：docdb-cluster-snapshot-public-prohibited

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 手动集群快照是否是公开的。如果手动集群快照是公共的，则控制失败。

除非有意图，否则 Amazon DocumentDB 手动集群快照不应公开。如果您将未加密的手动快照公开共享，则该快照可供所有 AWS 账户使用。公开快照可能会导致意外的数据泄露。

> **Note**
>
> 此控件评估手动集群快照。您无法共享 Amazon DocumentDB 自动集群快照。但是，您可以通过复制自动快照来创建手动快照，然后共享该副本。

修复

要移除对 Amazon DocumentDB 手动集群快照的公开访问权限，请参阅 Amazon DocumentDB 开发人员指南中的共享快照。通过编程方式，您可以使用 Amazon DocumentDB `modify-db-snapshot-attribute` 操作。将 `attribute-name` 设置为 `restore`，并将 `values-to-remove` 设置为 `all`。

[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、PCI DSS v4.0.1/10.3.3 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：docdb-cluster-audit-logging-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 集群是否将审核日志发布到亚马逊 CloudWatch 日志。如果集群不向日志发布审核日 CloudWatch 志，则控制失败。

Amazon DocumentDB（与 MongoDB 兼容）允许您审核在集群中执行的事件。记录的事件的示例包括成功和失败的身份验证尝试、删除数据库中的集合或创建索引。默认情况下，审计在 Amazon DocumentDB 中处于禁用状态，需要您采取措施才能启用审计。

修复

要将 Amazon DocumentDB 审计日志发布到 CloudWatch 日志，请参阅亚马逊 DocumentDB 开发者指南中的启用审计。

[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护

相关要求： 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)

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：docdb-cluster-deletion-protection-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 集群是否已启用删除保护。如果集群未启用删除保护，则控制失败。

启用集群删除保护可提供额外保护，防止数据库意外删除或未经授权的用户删除。在启用删除保护时，无法删除 Amazon DocumentDB 集群。您必须先禁用删除保护，删除请求才能成功。当您在 Amazon DocumentDB 控制台中创建集群时，删除保护默认启用。

修复

要为现有 Amazon DocumentDB 集群启用删除保护，请参阅 Amazon DocumentDB 开发人员指南中的修改 Amazon DocumentDB 集群。在修改集群部分中，为删除保护选择启用。

[DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：docdb-cluster-encrypted-in-transit

计划类型：定期

参数： `excludeTlsParameters`：`disabled`、`enabled`（不可自定义）

此控件检查 Amazon DocumentDB 集群是否需要 TLS 才能连接到集群。如果与集群关联的集群参数组不同步，或者 TLS 集群参数设置为 `disabled` 或 `enabled`，则该控件会失败。

您可以使用 TLS 加密应用程序与 Amazon DocumentDB 集群之间的连接。使用 TLS 可帮助防止数据在应用程序和 Amazon DocumentDB 集群之间传输时被拦截。Amazon DocumentDB 集群的传输中加密通过与该集群关联的集群参数组中的 TLS 参数进行管理。启用传输中加密后，需要使用 TLS 进行安全连接才能连接到集群。我们建议使用以下 TLS 参数：`tls1.2+`、`tls1.3+` 和 `fips-140-3`。

修复

有关更改 Amazon DocumentDB 集群的 TLS 设置的信息，请参阅《Amazon DocumentDB 开发人员指南》中的加密传输中数据。

适用于 DynamoDB 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估亚马逊 DynamoDB 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DynamoDB.1] DynamoDB 表应根据需求自动扩展容量

相关要求： NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：`dynamodb-autoscaling-enabled`

计划类型：定期

参数：

参数	说明	Type	有效的自定义值	Security Hub CSPM 默认值
`minProvisionedReadCapacity`	DynamoDB 自动扩缩的预置读取容量单位的最小数量	整数	`1` 到 `40000`	无默认值
`targetReadUtilization`	读取容量的目标使用率百分比	整数	`20` 到 `90`	无默认值
`minProvisionedWriteCapacity`	DynamoDB 自动扩缩的预置写入容量单位的最小数量	整数	`1` 到 `40000`	无默认值
`targetWriteUtilization`	写入容量的目标使用率百分比	整数	`20` 到 `90`	无默认值

此控件检查 Amazon DynamoDB 表是否可以根据需要扩展其读取和写入容量。如果表不使用按需容量模式或配置了自动扩缩的预置模式，则控制失败。默认情况下，此控件只需要配置其中一种模式，而不考虑特定的读取或写入容量级别。或者，您可以提供自定义参数值，以便要求特定的读取和写入容量级别或目标利用率。

按需扩展容量可以避免节流异常，这有助于保持应用程序的可用性。使用按需容量模式的 DynamoDB 表仅受 DynamoDB 吞吐量默认表配额的限制。要提高这些配额，您可以向提交支持请求 支持。使用预置模式且具有自动扩缩功能的 DynamoDB 表会根据流量模式动态调整预置的吞吐能力。有关 DynamoDB 请求节流的更多信息，请参阅《Amazon DynamoDB 开发人员指南》中的请求节流和容量暴增。

修复

要在容量模式下对现有表启用 DynamoDB 自动扩缩，请参阅《Amazon DynamoDB 开发人员指南》中的在现有表上启用 DynamoDB 自动扩缩。

[DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time

相关要求： 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-12、nist.800-53.r5 SI-13 (5)

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：`dynamodb-pitr-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为亚马逊 DynamoDB 表启用了 point-in-time恢复 (PITR)。

备份可以帮助您更快地从安全事件中恢复。它们还增强了系统的故障恢复能力。DynamoDB 恢复功能可 point-in-time自动对 DynamoDB 表进行备份。它可以缩短从意外删除或写入操作中恢复的时间。启用 PITR 的 DynamoDB 表可以恢复到过去 35 天内的任何时间点。

修复

要将 DynamoDB 表恢复到某个时间点，请参阅 Amazon DynamoDB 开发人员指南中的将 DynamoDB 表恢复到某个时间点。

[DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::DAX::Cluster`

AWS Config 规则：`dax-encryption-enabled`

计划类型：定期

参数：无

此控件可检查是否对 Amazon DynamoDB Accelerator（DAX）集群进行了静态加密。如果 DAX 集群未进行静态加密，则此控件将失败。

对静态数据进行加密可降低存储在磁盘上的数据被未经身份验证的用户访问的风险。 AWS加密添加了另一组访问控制，以限制未经授权的用户访问数据的能力。例如，需要 API 权限才能解密数据，然后才能读取数据。

修复

创建集群后，您无法启用或禁用静态加密。您必须重新创建集群才能启用静态加密。有关如何创建启用静态加密的 DAX 集群的详细说明，请参阅 Amazon DynamoDB 开发人员指南中的使用 AWS 管理控制台启用静态加密。

[DynamoDB.4] 备份计划中应有 DynamoDB 表

相关要求： 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)

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：**`dynamodb-resources-protected-by-backup-plan`**

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`backupVaultLockCheck`	如果将参数设置为，`true`并且资源使用 AWS Backup 文件库锁定，则控件会生成PASSED结果。	布尔值	`true` 或者 `false`	无默认值

此控件评估备份计划是否涵盖了处于 ACTIVE 状态的 Amazon DynamoDB 表。如果备份计划不涵盖 DynamoDB 表，则控制失败。如果将backupVaultLockCheck参数设置为true，则只有在锁定的文件库中备份 DynamoDB 表时，控制才会通过。 AWS Backup

AWS Backup 是一项完全托管的备份服务，可帮助您集中和自动备份数据 AWS 服务。使用 AWS Backup，您可以创建定义备份要求的备份计划，例如备份数据的频率以及保留这些备份的时间。将 DynamoDB 表纳入备份计划可帮助您保护数据免遭意外丢失或删除。

修复

要向备份计划添加 DynamoDB 表，请参阅开发人员指南中的AWS Backup 为备份计划分配资源。 AWS Backup

[DynamoDB.5] 应标记 DynamoDB 表

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::DynamoDB::Table

AWS Config 规则:tagged-dynamodb-table（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	No default value

此控件可检查 Amazon DynamoDB 表是否具有带特定键的标签，这些键在 requiredTagKeys 参数中进行定义。如果表没有任何标签键或者未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签键，如果表未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DynamoDB 表添加标签，请参阅《Amazon DynamoDB 开发者指南》中的在 DynamoDB 中为资源添加标签。

[DynamodB.6] DynamoDB 表应启用删除保护

相关要求： 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)

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：**`dynamodb-table-deletion-protection-enabled`**

计划类型：已触发变更

参数：无

此控件检查 Amazon DynamoDB 表是否已启用删除保护。如果 DynamoDB 表未启用删除保护，则控制失败。

您可以使用删除保护属性保护 DynamoDB 表免遭意外删除。为表启用此属性有助于确保在管理员执行常规表管理操作期间不会意外删除表。这有助于防止您的常规业务运营受到干扰。

修复

要为 DynamoDB 表启用删除保护，请参阅《Amazon DynamoDB 开发者指南》中的使用删除保护。

[DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密

相关要求： NIST.800-53.r5 AC-17、、3、 NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 3 NIST.800-53.r5 SC-8、PCI DSS v4.0.1/4.2.1

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::DAX::Cluster`

AWS Config 规则：`dax-tls-endpoint-encryption`

计划类型：定期

参数：无

此控件可检查 Amazon DynamoDB Accelerator（DAX）集群是否在传输过程中进行加密，其端点加密类型设置为 TLS。如果 DAX 集群未在传输过程中进行加密，则此控件将失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。应该只允许通过 TLS 加密连接来访问 DAX 集群。但是，加密传输中数据可能会影响性能。您应该在启用加密的情况下测试应用程序，以了解性能概况和 TLS 的影响。

修复

创建 DAX 集群后，将无法更改 TLS 加密设置。要加密现有 DAX 集群，请创建启用了传输中加密的新集群，将应用程序的流量转移到该集群，然后删除旧集群。有关更多信息，请参阅《Amazon DynamoDB 开发人员指南》中的使用删除保护。

适用于亚马逊 EC2 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估亚马逊弹性计算云 (Amazon EC2) 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EC2.1] 不应将 Amazon EBS 快照配置为可公开还原

相关要求：PCI DSS v3.2。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.4，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、 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)

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`ebs-snapshot-public-restorable-check`

计划类型：定期

参数：无

此控件会检查 Amazon Elastic Block Store 快照是否配置为可公开恢复。如果 Amazon EBS 快照配置为所有人均可恢复，则控制失败。

EBS 快照用于将 EBS 卷上的数据在特定时间点备份到 Amazon S3。您可以使用快照还原 EBS 卷的先前状态。与公众共享快照几乎是不允许的。通常，公开共享快照的决定要么是决策错误，要么是没有完全理解其含义。此检查有助于确保所有此类共享都是完全经过规划并且是有意进行的。

修复

要将公有 EBS 快照设为私有，请参阅《Amazon EC2 用户指南》中的共享快照。在操作、修改权限中，选择私有。

[EC2.2] VPC 默认安全组不应允许入站或出站流量

相关要求：CIS AWS 基金会基准测试 v5.0。 0/5.5，PCI DSS v3.2。 1/1.2.1，PCI DSS v3.2。 1/1.3.4，PCI DSS v3.2。 1/2.1，CIS AWS 基金会基准 v1.2。 0/4.3，CIS AWS 基金会基准 v1.4。 0/5.3，CIS AWS 基金会基准测试 v3.0。 0/5.4、 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)

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：vpc-default-security-group-closed

计划类型：已触发变更

参数：无

此控件检查 VPC 的默认安全组是否允许入站或出站流量。如果安全组允许入站或出站流量，则控制失败。

默认安全组的规则允许来自分配给相同安全组的网络接口（及其关联实例）的所有出站和入站流量。我们建议您不要使用默认安全组。由于无法删除默认安全组，因此您应更改默认安全组规则设置以限制入站和出站流量。如果意外为 EC2 实例等资源配置了默认安全组，这可以防止意外的流量。

修复

要修复此问题，请先创建新的最低权限安全组。有关说明，请参阅 Amazon VPC 用户指南中的创建安全组。然后，将新的安全组分配给 EC2 实例。有关说明，请参阅《Amazon EC2 用户指南》中的更改实例的安全组。

将新安全组分配给资源后，从默认安全组中删除所有入站和出站规则。有关说明，请参阅《Amazon VPC 用户指南》中的配置安全组规则。

[EC2.3] 附加的 Amazon EBS 卷应在静态状态下进行加密

相关要求： 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::EC2::Volume

AWS Config 规则：encrypted-volumes

计划类型：已触发变更

参数：无

该控制检查处于连接状态的 EBS 卷是否已加密。要通过此检查，EBS 卷必须处于使用中并加密。如果 EBS 卷未挂载，则不需要接受此检查。

为了增加 EBS 卷中敏感数据的安全性，您应该启用静态 EBS 加密。Amazon EBS 加密提供了直接用于 EBS 资源的加密解决方案，无需您构建、维护和保护自己的密钥管理基础设施。它在创建加密卷和快照时使用 KMS 密钥。

要了解有关 Amazon EBS 加密的更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EBS 加密。

修复

没有直接对现有未加密卷或快照进行加密的方法。您只能在新的卷或快照创建时对其进行加密。

如果您启用了默认加密，Amazon EBS 使用您用于 Amazon EBS 加密的默认密钥对生成的新卷或快照实施加密。即使您未启用默认加密，也可以在创建单个卷或快照时启用加密。在这两种情况下，您都可以覆盖 Amazon EBS 加密的默认密钥并选择对称的客户管理密钥。

有关更多信息，请参阅《Amazon EC2 用户指南》中的创建 Amazon EBS 快照和复制 Amazon EBS 快照。

[EC2.4] 应在指定时间段后移除已停止的 EC2 实例

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-2、 NIST.800-53.r5 CM-2 (2)

类别：识别 > 清单

严重性：中

资源类型：`AWS::EC2::Instance`

AWS Config 规则:`ec2-stopped-instance-days-check`（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`AllowedDays`	在生成失败的调查发现之前，允许 EC2 实例处于停止状态的天数。	整数	1 到 365	30

此控件检查 Amazon EC2 实例是否已停止超过允许的天数。如果 EC2 实例的停止时间超过允许的最大时间段，则控制失败。除非您为允许的最大时间段提供自定义参数值，否则 Security Hub CSPM 将使用 30 天的默认值。

当 EC2 实例在很长一段时间内没有运行时，会造成安全风险，因为该实例没有得到积极维护（分析、修补、更新）。如果稍后启动，则由于缺乏适当的维护，可能会导致您的 AWS 环境出现意外问题。要安全地将 EC2 实例长期保持不活动状态，请定期启动已对其进行维护，然后在维护后将其停止。理想情况下，这应是一个自动化的过程。

> **Note**
>
> 此控件使用实例的时间戳来评估 EC2 实例停止的天数。`StateTransitionReason`如果`StateTransitionReason`不包含时间戳（例如实例由于内部错误而停止时），控件将改用实例的启动时间。在这种情况下，如果启动时间超过允许的最大时间段，则控件会生成失败的查找结果。

修复

要终止非活动 EC2 实例，请参阅《Amazon EC2 用户指南》中的终止实例。

[EC2.6] 应在所有 VPC 中启用 VPC 流量记录

相关要求：CIS AWS 基金会基准测试 v5.0。 0/3.7，CIS AWS 基金会基准 v1.2。 0/2.9，CIS AWS 基金会基准 v1.4。 0/3.9，CIS AWS 基金会基准 v3.0。 0/3.7、 NIST.800-53.r5 AC-4 (26)、、、NIST.800-53.r5 AU-12、 NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3、(4)、 NIST.800-53.r5 AU-6 NIST.800-53.r5 SI-7 (8)、 NIST.800-171.r2 3.1.20 NIST.800-53.r5 CA-7、3.3. NIST.800-171.r2 1、3. NIST.800-171.r2 13.1、PCI DSS v3.2。 1/10.3.3，PCI DSS v3.2。 1/10.3.4，PCI DSS v3.2。 1/10.3.5，PCI DSS v3.2。 1/10.3.6

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::EC2::VPC`

AWS Config 规则：`vpc-flow-logs-enabled`

计划类型：定期

参数：

- `trafficType`：`REJECT`（不可自定义）

此控件检查是否找到并为 VPC 启用 Amazon VPC 流日志。流量类型设置为 `Reject`。如果您账户中的 VPC 未启用 VPC 流日志，则此控件将失败。

> **Note**
>
> 此控件不会检查是否通过 Amazon Security Lake 为 AWS 账户启用了 Amazon VPC 流日志。

通过 VPC 流日志功能，您可以捕获有关进出 VPC 中网络接口的 IP 地址流量的信息。创建流日志后，可以在 CloudWatch 日志中查看和检索其数据。为了降低成本，您还可以将流日志发送到 Amazon S3。

Security Hub CSPM 建议您为 VPC 的数据包拒绝启用流量记录。流日志提供了对穿过 VPC 的网络流量的可见性，并且可以检测异常流量或在安全工作流程期间提供见解。

默认情况下，记录包括 IP 地址流的不同组件的值，包括源、目标和协议。有关日志字段的更多信息和描述，请参阅 Amazon VPC 用户指南中的 VPC 流日志。

修复

要创建 VPC 流日志，请参阅 Amazon VPC 用户指南中的创建流日志。打开 Amazon VPC 控制台后，选择您的 VPC。对于筛选条件，选择拒绝或全部。

[EC2.7] 应启用 EBS 默认加密

相关要求：CIS AWS 基金会基准测试 v5.0。 0/5.1.1，CIS AWS 基金会基准 v1.4。 0/2.2.1，CIS AWS 基金会基准 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`ec2-ebs-encryption-by-default`

计划类型：定期

参数：无

此控件检查默认情况下 Amazon Elastic Block Store（Amazon EBS）卷是否启用账户级加密。如果 EBS 卷未启用账户级别加密，则该控件会失败。

为账户启用加密后，Amazon EBS 卷和快照副本将进行静态加密。这为数据增加了一层额外的保护。有关更多信息，请参阅《Amazon EC2 用户指南》中的默认加密。

修复

要配置 Amazon EBS 卷的默认加密，请参阅《Amazon EC2 用户指南》中的默认加密。

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (imdsv2)

相关要求：CIS AWS 基金会基准测试 v5.0。 0/5.7，CIS AWS 基金会基准测试 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

类别：保护 > 网络安全

严重性：高

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-imdsv2-check`

计划类型：已触发变更

参数：无

此控件检查 EC2 实例元数据版本是否配置了实例元数据服务版本 2（IMDSv2）。如果将 `HttpTokens` 设置为对 imdsv2 是“必需”，则控制通过。如果设置为 ，`HttpTokens`则控制失败`optional`。

您可以使用实例元数据来配置或管理正在运行的实例。IMDS 提供对临时的、经常轮换的凭证的访问权限。这些凭证消除了手动或以编程方式对实例进行硬编码或分发敏感凭证的需要。IMDS 在本地连接到每个 EC2 实例。它在特殊的“链路本地地址”IP 地址 169.254.169.254。该 IP 地址只能由实例上运行的软件访问。

IMDS 版本 2 为以下类型的漏洞添加了新的保护。这些漏洞可用于尝试访问 IMDS。

- 打开网站应用程序防火墙
- 打开反向代理
- Server-side 请求伪造 (SSRF) 漏洞
- 打开第 3 层防火墙和网络地址转换（NAT）

Security Hub CSPM 建议您使用 imdsv2 配置您的 EC2 实例。

修复

要使用 IMDSv2 配置 EC2，请参阅《Amazon EC2 用户指南》中的要求 IMDSv2 的建议途径。

[EC2.9] 亚马逊 EC2 实例不应有公有 IPv4 地址

相关要求： 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)

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-instance-no-public-ip`

计划类型：已触发变更

参数：无

此控件检查 EC2 实例是否具有公有 IP 地址。如果EC2实例配置项中存在 `publicIp` 字段，则控制失败。此控件仅适用于 IPv4 地址。

公共 IPv4 地址是可从 Internet 访问的 IP 地址。如果您使用公共 IP 地址启动实例，则可以通过 Internet 访问 EC2 实例。私有 IPv4 地址是无法从 Internet 访问的 IP 地址。您可以使用私有 IPv4 地址在同一 VPC 或连接的私有网络中的 EC2 实例之间进行通信。

IPv6 地址是全球唯一的，因此可以通过 Internet 访问。但是，默认情况下，所有子网的 IPv6 寻址属性都设置为 false。有关 IPv6 的更多信息，请参阅 Amazon VPC 用户指南中的 VPC 中的 IP 地址。

如果您有合法的用例来维护带有公有 IP 地址的 EC2 实例，则可以隐藏此控件的调查发现。有关前端架构选项的更多信息，请参阅AWS 架构博客或 “这就是我的架构” 系列 AWS 视频系列。

修复

使用非默认 VPC，以便默认情况下实例不会被分配公有 IP 地址。

当您在默认 VPC 中启动 EC2 实例时，系统会为其分配一个公共 IP 地址。当您在非默认 VPC 中启动 EC2 实例时，子网配置决定其是否接收公有 IP 地址。子网具有一个属性，用于确定子网中的新 EC2 实例是否从公共 IPv4 地址池接收公共 IP 地址。

您可以将自动分配的公有 IP 地址与 EC2 实例解除关联。有关更多信息，请参阅《Amazon EC2 用户指南》中的公有 IPv4 地址和外部 DNS 主机名。

[EC2.10] 应将 Amazon EC2 配置为使用为亚马逊 EC2 服务创建的 VPC 终端节点

相关要求： 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、(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 NIST.800-53.r5 SC-7 (4)、 NIST.800-171.r2 3.1.3、3.13.1 NIST.800-171.r2

类别：保护 > 安全网络配置 > API 私有访问

严重性：中

资源类型：`AWS::EC2::VPC`

AWS Config 规则：`service-vpc-endpoint-enabled`

计划类型：定期

参数：

- `serviceName`：`ec2`（不可自定义）

此控件检查是否为每个 VPC 创建了 Amazon EC2 的服务端点。如果 VPC 没有为 Amazon EC2 服务创建 VPC 端点，则控制失败。

此控件评估单个账户中的资源。它不能描述账户之外的资源。由于而 AWS Config 且 Security Hub CSPM 不进行跨账户检查，因此您将看到跨账户`FAILED`共享的 VPC 的调查结果。Security Hub CSPM 建议你隐瞒这些`FAILED`发现。

> **Note**
>
> 此控件评估标准端点服务名称，但当前无法识别 FIPS-variant 端点服务名称（例如`com.amazonaws.us-east-1.ec2-fips`）。即使配置了通过 VPC 终端节点与服务的连接，使用 Amazon EC2 的 FIPS 终端节点的 VPC 也可能会得出`FAILED`结果。

要改善 VPC 的安全状况，您可以将 Amazon EC2 配置为使用接口 VPC 端点。接口终端节点由一项技术提供支持 AWS PrivateLink，该技术使您能够私下访问 Amazon EC2 API 操作。它将 VPC 和 Amazon EC2 之间的所有网络流量限制为 Amazon 网络。由于端点仅在同一区域内受支持，因此您无法在 VPC 和不同区域中的服务之间创建端点。这样可以防止对其他区域进行意外的 Amazon EC2 API 调用。

要了解有关为 Amazon EC2 创建 VPC 端点的更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EC2 和接口 VPC 端点。

修复

要从 Amazon VPC 控制台创建到 Amazon EC2 的接口端点，请参阅 AWS PrivateLink 指南中的创建 VPC 端点。对于服务名称，请选择 com.amazonaws。 ***region***.ec2。

您还可以创建端点策略并将其附加到 VPC 端点以控制对 Amazon EC2 API 的访问。有关创建 VPC 端点策略的说明，请参阅《Amazon EC2 用户指南》中的创建端点策略。

[EC2.12] 应移除未使用的 Amazon EC2 EIP

相关要求：PCI DSS v3.2。 1/2.4, NIST.800-53.r5 CM-8 (1)

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::EC2::EIP`

AWS Config 规则：`eip-attached`

计划类型：已触发变更

参数：无

此控件检查分配给 VPC 的弹性 IP（EIP）地址是否附加到 EC2 实例或正在使用的弹性网络接口（ENI）。

失败的调查发现表示，您可能具有未使用的 EC2 EIP。

这将帮助您在持卡人数据环境（CDE）中维护准确的 EIP 资产清单。

修复

要释放未使用的 EIP，请参阅《Amazon EC2 用户指南》中的释放弹性 IP 地址。

[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22

相关要求：CIS AWS 基金会基准测试版本 1.2。 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、3. NIST.800-171.r2 13.1、PCI DSS v3.2。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/2.2.2，PCI DSS v4.0。 1/1.3.1

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`restricted-ssh`

计划类型：已触发更改且定期进行

参数：无

此控件检查 Amazon EC2 安全组是否允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 22。如果安全组允许从 0.0.0 进入，则控制失败。 0/0或者:: /0 到端口 22。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。我们建议不要让任何安全组允许对端口 22 进行不受限制的传入访问。删除与 SSH 等远程控制台服务的自由连接可减少服务器暴露的风险。

修复

要禁止进入端口 22，请移除允许与 VPC 关联的每个安全组进行此类访问的规则。有关说明，请参阅《Amazon EC2 用户指南》中的更新安全组规则。在 Amazon EC2 控制台中选择安全组后，请选择操作、编辑入站规则。删除允许访问端口 22 的规则。

[EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389

相关要求：CIS AWS 基金会基准测试版本 1.2。 0/4.2，PCI DSS v4.0。 1/1.3.1

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::EC2::SecurityGroup

AWS Config 规则:**restricted-common-ports**（创建的规则是restricted-rdp）

计划类型：已触发更改且定期进行

参数：无

此控件检查 Amazon EC2 安全组是否允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389。如果安全组允许从 0.0.0 进入，则控制失败。 0/0或者:: /0 到端口 3389。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。我们建议不要让任何安全组允许对端口 3389 进行不受限制的传入访问。删除与 RDP 等远程控制台服务的自由连接可减少服务器暴露的风险。

修复

要禁止进入端口 3389，请移除允许与 VPC 关联的每个安全组进行此类访问的规则。有关说明，请参阅 Amazon VPC 用户指南中的更新安全组规则。在 Amazon VPC 控制台中选择安全组后，选择操作、编辑入站规则。删除允许访问端口 3389 的规则。

[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址

相关要求： 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、(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。 1/1.4.4

类别：保护 > 网络安全

严重性：中

资源类型：AWS::EC2::Subnet

AWS Config 规则：subnet-auto-assign-public-ip-disabled

计划类型：已触发变更

参数：无

此控件检查亚马逊虚拟私有云 (Amazon VPC) 子网是否配置为自动分配公有 IP 地址。如果子网配置为自动分配公有 IPv4 或 IPv6 地址，则控制失败。

子网具有决定网络接口是否自动接收公有 IPv4 和 IPv6 地址的属性。对于 IPv4，TRUE对于默认子网和FALSE非默认子网，此属性均设置为（通过 EC2 启动实例向导创建的非默认子网除外，该向导设置为）。TRUE对于 IPv6，默认情况下，所有子网FALSE的此属性均设置为。启用这些属性后，在子网中启动的实例会自动在其主网络接口上接收相应的 IP 地址（IPv4 或 IPv6）。

修复

要将子网配置为不分配公有 IP 地址，请参阅《Amazon VPC 用户指南》中的修改子网的 IP 寻址属性。

[EC2.16] 应删除未使用的网络访问控制列表

相关要求： NIST.800-53.r5 CM-8(1)、 NIST.800-171.r2 3.4.7、PCI DSS v4.0。 1/1.2.7

类别：保护 > 网络安全

严重性：低

资源类型：`AWS::EC2::NetworkAcl`

AWS Config 规则：`vpc-network-acl-unused-check`

计划类型：已触发变更

参数：无

此控件可检查您的虚拟私有云（VPC）中是否存在任何未使用的网络访问控制列表（网络 ACL）。如果网络 ACL 未与某个子网关联，则此控件将失败。此控件不会为未使用的默认网络 ACL 生成调查发现。

此控件检查资源 `AWS::EC2::NetworkAcl` 的项目配置并确定网络 ACL 的关系。

如果唯一的关系是网络 ACL 的 VPC，则此控件将失败。

如果列出了其他关系，则控件通过。

修复

有关删除未使用的网络 ACL 的说明，请参阅 Amazon VPC 用户指南中的删除网络 ACL。您无法删除默认网络 ACL 或与子网相关联的 ACL。

[EC2.17] Amazon EC2 实例不应使用多个 ENI

相关要求： NIST.800-53.r5 AC-4(21)

类别：保护 > 网络安全

严重性：低

资源类型：AWS::EC2::Instance

AWS Config 规则：ec2-instance-multiple-eni-check

计划类型：已触发变更

参数：无

此控件检查 EC2 实例是否使用多个弹性网络接口（ENI）或 Elastic Fabric Adapters（EFA）。如果使用单个网络适配器，则此控制通过。该控件包括一个可选参数列表，用于标识允许的 ENI。如果属于 Amazon EKS 集群的 EC2 实例使用多个 ENI，则此控制也会失败。如果 EC2 实例需要将多个 ENI 作为 Amazon EKS 集群的一部分，则可以隐藏这些控件调查发现。

多个 ENI 可能导致双主机实例，即具有多个子网的实例。这会增加网络安全的复杂性并引入意外的网络路径和访问。

修复

要将网络接口与 EC2 实例分离，请参阅《Amazon EC2 用户指南》中的将网络接口与实例分离。

[EC2.18] 安全组应只允许授权端口不受限制的传入流量

相关要求： 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)、3.1.3、3. NIST.800-171.r2 1.20、 NIST.800-171.r2 3.13.1 NIST.800-171.r2

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：AWS::EC2::SecurityGroup

AWS Config 规则：vpc-sg-open-only-to-authorized-ports

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
authorizedTcpPorts	授权的 TCP 端口列表	IntegerList（最少 1 件商品，最多 32 件商品）	1 到 65535	[80,443]
authorizedUdpPorts	授权的 UDP 端口列表	IntegerList（最少 1 件商品，最多 32 件商品）	1 到 65535	无默认值

此控件检查 Amazon EC2 安全组是否允许从未经授权的端口传入不受限制的流量。控制状态如下所示确定：

- 如果您使用 authorizedTcpPorts 的默认值，则当安全组允许从端口 80 和 443 以外的任何端口传入无限制流量时，则控制失败。
- 如果您为 authorizedTcpPorts 或 authorizedUdpPorts 提供自定义值，则当安全组允许从任何未列出的端口传入无限制流量时，则控制失败。

安全组提供对 AWS的传入和传出网络流量的状态筛选。安全组规则应遵循最低权限访问的原则。不受限制的访问（带有 /0 后缀的 IP 地址）会增加恶意活动的机会，例如黑客攻击、拒绝服务攻击和数据丢失。除非明确允许某个端口，否则该端口应拒绝不受限制的访问。

修复

要修改安全组，请参阅《Amazon VPC 用户指南》中的使用安全组。

[EC2.19] 安全组不应允许不受限制地访问高风险端口

相关要求： NIST.800-53.r5 AC-4、 NIST.800-53.r5 AC-4 (21)、 NIST.800-53.r5 CA-9 (1)、(2) NIST.800-53.r5 CM-2、、、 NIST.800-53.r5 CM-2 (11) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7 (16)、 NIST.800-53.r5 SC-7 (21)、(4)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5)、 NIST.800-53.r5 SC-7 3.1.3、3.1.20、 NIST.800-171.r2 3. NIST.800-171.r2 1.20、3.13.1 NIST.800-171.r2

类别：保护 > 受限网络访问

严重性：严重

资源类型：AWS::EC2::SecurityGroup

AWS Config 规则:**restricted-common-ports**（创建的规则是vpc-sg-restricted-common-ports）

计划类型：已触发更改且定期进行

参数："blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560 可自定义）

此控件检查高风险的指定端口是否可以访问 Amazon EC2 安全组的不受限制的传入流量。如果安全组中的任何规则允许来自 '0.0.0 的入口流量，则此控制失败。 0/0' 或者 ':: /0' 到这些端口。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。不受限制的访问 (0.0.0. 0/0) 增加了恶意活动的机会，例如黑客攻击、拒绝服务攻击和数据丢失。任何安全组都不应允许对以下端口进行不受限制的入口访问：

- 20、21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433、1434（MSSQL）
- 3000（Go Node.js、和 Ruby 网络开发框架）
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000（Python 网络开发框架）
- 5432 (postgresql)

- 5500 (fcp-addr-srvr1)
- 5601（仪表板）OpenSearch
- 8080（代理）
- 8088（传统的 HTTP 端口）
- 8888（备用 HTTP 端口）
- 9200 或 9300 () OpenSearch

修复

要删除安全组中的规则，请参阅《Amazon EC2 用户指南》中的删除安全组中的规则。

[EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启

相关要求： 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)、 NIST.800-171.r2 3.1.13、3.1.20 NIST.800-171.r2

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::EC2::VPNConnection`

AWS Config 规则：`vpc-vpn-2-tunnels-up`

计划类型：已触发变更

参数：无

VPN 隧道是一种加密链路，数据可以在其中从客户网络传入 VPN 连接或传出 AWS AWS Site-to-Site VPN 连接。每个 VPN 连接均包括两条 VPN 隧道，可以同时使用这两条隧道来实现高可用性。确保两个 VPN 隧道都已开通 VPN 连接对于确认 VP AWS C 和远程网络之间的安全且高度可用的连接非常重要。

此控件会检查 VPN 提供的两个 V AWS Site-to-Site PN 隧道是否都处于 UP 状态。如果一条或两条隧道都处于关闭状态，则控制失败。

修复

要修改 VPN 隧道选项，请参阅《Site-to-SiteVPN 用户指南》中的修改 AWS Site-to-Site VPN 隧道选项。

[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389

相关要求：CIS AWS 基金会基准测试 v5.0。 0/5.2，CIS AWS 基金会基准 v1.4。 0/5.1，CIS AWS 基金会基准测试 v3.0。 0/5.1、 NIST.800-53.r5 AC-4 (21)、 NIST.800-53.r5 CA-9 (1)、(2) NIST.800-53.r5 CM-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)、3.1. NIST.800-171.r2 3、3. NIST.800-171.r2 1.20、NIST.800-171.r2 3.13.1、PCI DSS v4.0。 1/1.3.1

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::EC2::NetworkAcl`

AWS Config 规则：`nacl-no-unrestricted-ssh-rdp`

计划类型：已触发变更

参数：无

此控件检查网络访问控制列表（网络 ACL）是否允许入 SSH/RDP 口流量不受限制地访问默认 TCP 端口。如果网络 ACL 入站条目允许源 CIDR 块为 '0.0.0，则控制失败。 0/0' 或者对于 TCP 端口 22 或 3389 使用 ':: /0'。此控件不会为默认网络 ACL 生成调查发现。

对远程服务器管理端口（例如端口 22（SSH）和端口 3389（RDP））的访问不应公开访问，因为这可能会允许对 VPC 内的资源进行意外访问。

修复

要编辑网络 ACL 流量规则，请参阅《Amazon VPC 用户指南》中的使用网络 ACL。

[EC2.22] 应移除未使用的 Amazon EC2 安全组

类别：识别 > 清单

严重性：中

资源类型：`AWS::EC2::NetworkInterface`、`AWS::EC2::SecurityGroup`

AWS Config 规则：`ec2-security-group-attached-to-eni-periodic`

计划类型：定期

参数：无

此控件可检查安全组是否已附加到 Amazon Elastic Compute Cloud（Amazon EC2）实例或弹性网络接口。如果安全组未与 Amazon EC2 实例或弹性网络接口关联，则此控件将失败。

> **Important**
>
> 2023 年 9 月 20 日，Security Hub CSPM 从《AWS 基础安全最佳实践》和 NIST SP 800-53 修订版 5 标准中删除了此控件。这种控制仍然是 AWS Control Tower 服务管理标准的一部分。如果安全组连接到 EC2 实例或弹性网络接口，此控件会生成一个通过的调查发现。但是，对于某些用例，未附加的安全组不会构成安全风险。您可以使用其他 EC2 控件（例如 EC2.2、、EC2.13 EC2.14 EC2.18、和 EC2.19）来监控您的安全组。

修复

要创建、分配和删除安全组，请参阅《Amazon EC2 用户指南》中的 EC2 实例的安全组。

[EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求

相关要求： NIST.800-53.r5 AC-4(21)、 NIST.800-53.r5 CA-9 (1)、 NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::TransitGateway`

AWS Config 规则：`ec2-transit-gateway-auto-vpc-attach-disabled`

计划类型：已触发变更

参数：无

此控件检查 EC2 中转网关是否自动接受共享 VPC 附件。对于自动接受共享 VPC 附件请求的中转网关，此控制失败。

开启后，中转网关将 `AutoAcceptSharedAttachments` 配置为自动接受任何跨账户 VPC 附件请求，无需验证请求或源自哪个账户。为了遵循授权和身份验证的最佳实践，我们建议关闭此功能，以确保仅接受经过授权的 VPC 附件请求。

修复

要修改中转网关，请参阅 Amazon VPC 开发人员指南中的修改中转网关。

[EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

相关要求： NIST.800-53.r5 CM-2， NIST.800-53.r5 CM-2(2)

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-paravirtual-instance-check`

计划类型：已触发变更

参数：无

此控件检查 EC2 实例的虚拟化类型是否为半虚拟化。如果 EC2 实例的 `virtualizationType` 设置为 `paravirtual`，则控制失败。

Linux 亚马逊机器映像（AMI）使用两种虚拟化类型之一：半虚拟（PV）或硬件虚拟机（HVM）。半虚拟化和 HVM AMI 之间的主要区别在于它们的启动方式，以及它们能否使用特定硬件扩展（CPU、网络和存储）实现更好的性能。

以往，半虚拟化来宾在许多情况下的性能优于 HVM 来宾，但是由于硬件虚拟机虚拟化的功能增强以及 HVM AMI 可使用半虚拟化驱动程序，情况发生了改变。有关更多信息，请参阅《Amazon EC2 用户指南》中的 Linux AMI 虚拟化类型。

修复

要将 EC2 实例更新为新的实例类型，请参阅《Amazon EC2 用户指南》中的更改实例类型。

[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

相关要求： 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、(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。 1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EC2::LaunchTemplate`

AWS Config 规则：ec2-launch-template-public-ip-disabled

计划类型：已触发变更

参数：无

此控件检查 Amazon EC2 启动模板是否配置为在启动时将公共 IP 地址分配给网络接口。如果 EC2 启动模板配置为向网络接口分配公共 IP 地址，或者至少有一个网络接口具有公共 IP 地址，则则控制失败。

公共 IP 地址是可通过 Internet 访问的地址。如果您使用公共 IP 地址配置网络接口，则可以通过 Internet 访问与这些网络接口关联的资源。EC2 资源不应公开访问，因为这可能会导致对工作负载的意外访问。

修复

要更新 EC2 启动模板，请参阅 Amazon EC2 Auto Scaling 用户指南中的变更默认网络接口设置。

[EC2.28] 备份计划应涵盖 EBS 卷

类别：恢复 > 弹性 > 启用备份

相关要求： 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)

严重性：低

资源类型：`AWS::EC2::Volume`

AWS Config 规则：**ebs-resources-protected-by-backup-plan**

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`backupVaultLockCheck`	如果将参数设置为 `true` 并且资源使用 AWS Backup 文件库	布尔值	`true` 或者 `false`	无默认值

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
	锁定，则控件会生成 PASSED 调查发现。			

此控件评估备份计划是否涵盖处于 in-use 状态的 Amazon EBS 卷。如果备份计划不涵盖某个 EBS 卷，则控制失败。如果将backupVaultLockCheck参数设置为true，则仅当 EBS 卷备份到 AWS Backup 锁定的存储库中时，控制才会通过。

备份可帮助您更快地从安全事件中恢复。它们还增强了系统的故障恢复能力。将 Amazon EBS 卷包含在备份计划中可帮助您保护数据免遭意外丢失或删除。

修复

要将 Amazon EBS 卷添加到 AWS Backup 备份计划中，请参阅AWS Backup 开发人员指南中的为备份计划分配资源。

[EC2.33] 应标记 EC2 传输网关附件

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::TransitGatewayAttachment

AWS Config 规则:tagged-ec2-transitgatewayattachment（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 中转网关连接是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果中转网关连接没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果中转网关连接没有使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 中转网关连接添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.34] 应标记 EC2 传输网关路由表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::TransitGatewayRouteTable`

AWS Config 规则:`tagged-ec2-transitgatewayroutetable`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 中转网关路由表是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果中转网关路由表没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果中转网关路由表未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 中转网关路由表添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.35] 应标记 EC2 网络接口

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::NetworkInterface`

AWS Config 规则:`tagged-ec2-networkinterface`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 网络接口是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果网络接口没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果网络接口未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 网络接口添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.36] 应标记 EC2 客户网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::CustomerGateway`

AWS Config 规则:`tagged-ec2-customergateway`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 客户网关是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果客户网关没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果客户网关未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 客户网关添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.37] 应标记 EC2 弹性 IP 地址

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::EIP`

AWS Config 规则:`tagged-ec2-eip`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 弹性 IP 地址是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果弹性 IP 地址没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果弹性 IP 地址未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 弹性 IP 地址添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.38] 应标记 EC2 实例

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::Instance`

AWS Config 规则:`tagged-ec2-instance`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 实例是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果实例没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果实例未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 实例的信息添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.39] 应标记 EC2 互联网网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::InternetGateway`

AWS Config 规则:`tagged-ec2-internetgateway`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 互联网网关是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果互联网网关没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此

控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果互联网网关未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 互联网网关添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.40] 应标记 EC2 NAT 网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::NatGateway`

AWS Config 规则:`tagged-ec2-natgateway`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 网络地址转换（NAT）网关是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果 NAT 网关没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果 NAT 网关未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 NAT 网关添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.41] 应标记 EC2 网络 ACL

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::NetworkAcl`

AWS Config 规则:`tagged-ec2-networkacl`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 网络访问控制列表（网络 ACL）是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果网络 ACL 没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果网络 ACL 未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 网络 ACL 添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.42] 应标记 EC2 路由表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::RouteTable`

AWS Config 规则:`tagged-ec2-routetable`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 路由表是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果路由表没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果路由表未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 路由表添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.43] 应标记 EC2 安全组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则:`tagged-ec2-securitygroup`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 安全组是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果安全组没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果安全组未使用任何键进行标记，则此控件将失效。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 安全组添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.44] 应标记 EC2 子网

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::Subnet`

AWS Config 规则:`tagged-ec2-subnet`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 子网是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果子网没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果子网未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 子网添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.45] 应标记 EC2 卷

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::Volume`

AWS Config 规则:`tagged-ec2-volume`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 卷是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果卷没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果

未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果卷未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 卷添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.46] 应标记 Amazon VPC

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPC`

AWS Config 规则:`tagged-ec2-vpc`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon Virtual Private Cloud（Amazon VPC）是否具有带特定键的标签，这些键在 requiredTagKeys 参数中进行定义。如果 Amazon VPC 没有任何标签键或未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签键，如果 Amazon VPC 未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 VPC 添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.47] 应标记 Amazon VPC 终端节点服务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPCEndpointService`

AWS Config 规则:`tagged-ec2-vpcendpointservice`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon VPC 端点服务是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果端点服务没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果端点服务未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 Amazon VPC 端点服务添加标签，请参阅《AWS PrivateLink 指南》配置端点服务一节中的管理标签。

[EC2.48] 应标记 Amazon VPC 流日志

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::FlowLog`

AWS Config 规则:`tagged-ec2-flowlog`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon VPC 流日志是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果流日志没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果流日志未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 Amazon VPC 流日志添加标签，请参阅《Amazon VPC 用户指南》中的标记流日志。

[EC2.49] 应标记 Amazon VPC 对等连接

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPCPeeringConnection`

AWS Config 规则:`tagged-ec2-vpcpeeringconnection`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon VPC 对等连接是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果对等连接没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果对等连接未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 Amazon VPC 对等连接添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.50] 应标记 EC2 VPN 网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPNGateway`

AWS Config 规则:`tagged-ec2-vpngateway`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EC2 VPN 网关是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果 VPN 网关没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有密钥，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果 VPN 网关未使用任何键标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 VPN 网关添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录

相关要求： NIST.800-53.r5 AC-2(12)、 NIST.800-53.r5 AC-2 (4)、(26)、 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (9)、、、、 NIST.800-53.r5 AU-10、(3) NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6 (4)、(7)、 NIST.800-53.r5 AU-6 (9)、NIST.800-53.r5 AU-9 (8) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (20)、(8)、 NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4、 NIST.800-53.r5 SI-4 (8)、 NIST.800-171.r2 3.1.12、 NIST.800-53.r5 SI-7 3.1.20、PCI DSS v NIST.800-171.r2 4.0。 1/10.2.1

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::EC2::ClientVpnEndpoint`

AWS Config 规则：**`ec2-client-vpn-connection-log-enabled`**

计划类型：已触发变更

参数：无

此控件检查 AWS Client VPN 端点是否启用了客户端连接日志记录。如果端点未启用客户端连接日志记录，则控制失败。

客户端 VPN 端点允许远程客户端安全地连接到 AWS中虚拟私有云（VPC）中的资源。连接日志允许您跟踪 VPN 端点上的用户活动并提供可见性。启用连接日志记录时，可以在日志组中指定日志流的名称。如果未指定日志流，Client VPN 服务会为您创建一个日志流。

修复

要启用连接日志记录，请参阅《AWS Client VPN 管理员指南》中的为现有 Client VPN 端点启用连接日志记录。

[EC2.52] 应标记 EC2 传输网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::TransitGateway`

AWS Config 规则:`tagged-ec2-transitgateway`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon EC2 中转网关是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果中转网关没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果中转网关未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和

AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 EC2 中转网关添加标签，请参阅《Amazon EC2 用户指南》中的标记 Amazon EC2 资源。

[EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口

相关要求：CIS AWS 基金会基准测试 v5.0。 0/5.3，CIS AWS 基金会基准测试 v3.0。 0/5.2，PCI DSS v4.0。 1/1.3.1

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`vpc-sg-port-restriction-check`

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`ipType`	IP 版本	字符串	不可自定义	`IPv4`
`restrictPorts`	应拒绝入口流量的端口列表	IntegerList	不可自定义	`22,3389`

此控件检查 Amazon EC2 安全组是否允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口（端口 22 和 3389）。如果安全组允许从 0.0.0 进入，则控制失败。 0/0 到端口 22 或 3389。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。我们建议任何安全组都不应允许使用 TDP（6）、UDP（17）或 ALL（-1）协议对远程服务器管理端口进行不受限制的入口访问，例如 SSH 到端口 22，RDP 到端口 3389。允许对这些端口进行公共访问会增加资源攻击面和资源泄露的风险。

修复

要更新 EC2 安全组规则以禁止到指定端口的入口流量，请参阅《Amazon EC2 用户指南》中的更新安全组规则。在 Amazon EC2 控制台中选择安全组后，请选择操作、编辑入站规则。删除允许访问端口 22 或 3389 的规则。

[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口

相关要求：CIS AWS 基金会基准测试 v5.0。 0/5.4，CIS AWS 基金会基准测试 v3.0。 0/5.3，PCI DSS v4.0。 1/1.3.1

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`vpc-sg-port-restriction-check`

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`ipType`	IP 版本	字符串	不可自定义	`IPv6`
`restrictPorts`	应拒绝入口流量的端口列表	IntegerList	不可自定义	`22,3389`

此控件可检查 Amazon EC2 安全组是否允许从 :: /0 进入远程服务器管理端口（端口 22 和 3389）。如果安全组允许从 ::/0 进入端口 22 或 3389，则此控件将失败。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。我们建议任何安全组都不应允许使用 TDP（6）、UDP（17）或 ALL（-1）协议对远程服务器管理端口进行不受限制的入口访问，例如 SSH 到端口 22，RDP 到端口 3389。允许对这些端口进行公共访问会增加资源攻击面和资源泄露的风险。

修复

要更新 EC2 安全组规则以禁止到指定端口的入口流量，请参阅《Amazon EC2 用户指南》中的更新安全组规则。在 Amazon EC2 控制台中选择安全组后，请选择操作、编辑入站规则。删除允许访问端口 22 或 3389 的规则。

[EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点

相关要求： 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)

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config 规则：vpc-endpoint-enabled

计划类型：定期

参数：

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`serviceNames`	必需	控件所评估的服务的名称	字符串	不可自定义	`ecr.api`
`vpcIds`	可选	Comma-separated	StringList	使用一个或多个 VPC	无默认值

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
		VPC 终端节点的亚马逊 VPC ID 列表。如果提供，则当 `serviceName` 参数中指定的服务没有这些 VPC 端点之一时，此控件会失败。		ID 进行自定义	

此控件检查您管理的虚拟私有云（VPC）是否具有用于 Amazon ECR API 的接口 VPC 端点。如果 VPC 没有用于 ECR API 的接口 VPC 端点，则此控件会失败。此控件评估单个账户中的资源。

AWS PrivateLink 使客户能够以高度可用和可扩展的方式访问托管 AWS 在上的服务，同时将所有网络流量保持在 AWS 网络内。服务用户可以私密访问 PrivateLink 由 VPC 或本地提供支持的服务，无需使用公有 IP，也无需流量通过 Internet 进行传输。

修复

要配置 VPC 终端节点，请参阅AWS PrivateLink 指南中的AWS 服务 使用接口 VPC 终端节点访问和。

[EC2.56] 应为 VPC 配置 Docker Registry 的接口端点

相关要求： 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)

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：AWS::EC2::VPC、AWS::EC2::VPCEndpoint

AWS Config 规则：vpc-endpoint-enabled

计划类型：定期

参数：

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
serviceNames	必需	控件所评估的服务的名称	字符串	不可自定义	ecr.dkr
vpcIds	可选	Comma-separated VPC 终端节点的亚马逊 VPC ID 列表。如果提供，则当 serviceName 参数中指定的服务没有这些 VPC 端点之一时，此控件会失败。	StringList	使用一个或多个 VPC ID 进行自定义	无默认值

此控件检查您管理的虚拟私有云（VPC）是否具有用于 Docker Registry 的接口 VPC 端点。如果 VPC 没有用于 Docker Registry 的接口 VPC 端点，则此控件会失败。此控件评估单个账户中的资源。

AWS PrivateLink 使客户能够以高度可用和可扩展的方式访问托管 AWS 在上的服务，同时将所有网络流量保持在 AWS 网络内。服务用户可以私密访问 PrivateLink 由 VPC 或本地提供支持的服务，无需使用公有 IP，也无需流量通过 Internet 进行传输。

修复

要配置 VPC 终端节点，请参阅AWS PrivateLink 指南中的AWS 服务 使用接口 VPC 终端节点访问和。

[EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点

相关要求： 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)

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config 规则：vpc-endpoint-enabled

计划类型：定期

参数：

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`serviceNames`	必需	控件所评估的服务的名称	字符串	不可自定义	`ssm`
`vpcIds`	可选	Comma-separated VPC 终端节点的亚马逊 VPC ID 列表。如果提供，则当 `serviceName` 参数	StringList	使用一个或多个 VPC ID 进行自定义	无默认值

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
		中指定的服务没有这些 VPC 端点之一时，此控件会失败。			

此控件检查您管理的虚拟私有云（VPC）是否具有用于 AWS Systems Manager的接口 VPC 端点。如果 VPC 没有用于 Systems Manager 的接口 VPC 端点，则此控件会失败。此控件评估单个账户中的资源。

AWS PrivateLink 使客户能够以高度可用和可扩展的方式访问托管 AWS 在上的服务，同时将所有网络流量保持在 AWS 网络内。服务用户可以私密访问 PrivateLink 由 VPC 或本地提供支持的服务，无需使用公有 IP，也无需流量通过 Internet 进行传输。

修复

要配置 VPC 终端节点，请参阅AWS PrivateLink 指南中的AWS 服务 使用接口 VPC 终端节点访问和。

[EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点

相关要求： 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)

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config 规则：vpc-endpoint-enabled

计划类型：定期

参数：

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`serviceNames`	必需	控件所评估的服务的名称	字符串	不可自定义	`ssm-contacts`
`vpcIds`	可选	Comma-separated VPC 终端节点的亚马逊 VPC ID 列表。如果提供，则当 `serviceName` 参数中指定的服务没有这些 VPC 端点之一时，此控件会失败。	StringList	使用一个或多个 VPC ID 进行自定义	无默认值

此控件检查您管理的虚拟私有云 (VPC) 是否具有用于 AWS Systems Manager 事件管理员联系人的接口 VPC 终端节点。如果 VPC 没有用于 Systems Manager Incident Manager 联系人的接口 VPC 端点，则此控件会失败。此控件评估单个账户中的资源。

AWS PrivateLink 使客户能够以高度可用和可扩展的方式访问托管 AWS 在上的服务，同时将所有网络流量保持在 AWS 网络内。服务用户可以私密访问 PrivateLink 由 VPC 或本地提供支持的服务，无需使用公有 IP，也无需流量通过 Internet 进行传输。

修复

要配置 VPC 终端节点，请参阅AWS PrivateLink 指南中的AWS 服务 使用接口 VPC 终端节点访问和。

[EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC

相关要求： 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)

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config 规则：vpc-endpoint-enabled

计划类型：定期

参数：

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`serviceNames`	必需	控件所评估的服务的名称	字符串	不可自定义	`ssm-incidents`
`vpcIds`	可选	Comma-separated VPC 终端节点的亚马逊 VPC ID 列表。如果提供，则当 `serviceName` 参数中指定的服务没有这些 VPC 端	StringList	使用一个或多个 VPC ID 进行自定义	无默认值

参数	必需	说明	Type	允许的自定义值	Security Hub CSPM 默认值
		点之一时，此控件会失败。			

此控件检查您管理的虚拟私有云 (VPC) 是否具有用于 AWS Systems Manager 事件管理器的接口 VPC 终端节点。如果 VPC 没有用于 Systems Manager Incident Manager 的接口 VPC 端点，则此控件会失败。此控件评估单个账户中的资源。

AWS PrivateLink 使客户能够以高度可用和可扩展的方式访问托管 AWS 在上的服务，同时将所有网络流量保持在 AWS 网络内。服务用户可以私密访问 PrivateLink 由 VPC 或本地提供支持的服务，无需使用公有 IP，也无需流量通过 Internet 进行传输。

修复

要配置 VPC 终端节点，请参阅AWS PrivateLink 指南中的AWS 服务 使用接口 VPC 终端节点访问和。

[EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)

相关要求：PCI DSS v4.0。 1/2.2.6

类别：保护 > 网络安全

严重性：低

资源类型：`AWS::EC2::LaunchTemplate`

AWS Config 规则：ec2-launch-template-imdsv2-check

计划类型：已触发变更

参数：无

此控件可检查 Amazon EC2 启动模板是否配置了实例元数据服务版本 2（IMDSv2）。如果设置为，`HttpTokens`则控制失败`optional`。

在支持的软件版本上运行资源可确保最佳性能、安全性和对最新功能的访问。定期更新可防止漏洞，这有助于确保稳定高效的用户体验。

修复

如果要求在 EC2 启动模板上使用 IMDSv2，请参阅《Amazon EC2 用户指南》中的配置实例元数据服务选项。

[EC2.171] EC2 VPN 连接应启用日志记录

相关要求：CIS AWS 基金会基准测试 v3.0。 0/5.3，PCI DSS v4.0。 1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::EC2::VPNConnection`

AWS Config 规则：ec2-vpn-connection-logging-enabled

计划类型：已触发变更

参数：无

此控件会检查 AWS Site-to-Site VPN 连接是否为两条隧道都启用 CloudWatch 了 Amazon Logs。如果 Site-to-Site VPN 连接没有为两条隧道启用 CloudWatch 日志，则控制失败。

AWS Site-to-Site VPN 日志可让您更深入地了解 Site-to-Site VPN 部署。使用此功能，您可以访问 Site-to-Site VPN 连接日志，这些日志提供有关 IP 安全 (IPsec) 隧道建立、互联网密钥交换 (IKE) 协商和失效对等体检测 (DPD) 协议消息的详细信息。 Site-to-Site VPN 日志可以发布到 CloudWatch 日志。此功能为客户提供了一种统一的方式来访问和分析其所有 Site-to-Site VPN 连接的详细日志。

修复

要在 EC2 VPN 连接上启用隧道日志记录，请参阅AWS Site-to-Site VPN 用户指南中的AWS Site-to-Site VPN 日志。

[EC2.172] EC2 VPC 阻止公共访问设置应阻止互联网网关流量

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：中

资源类型：`AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config 规则:`ec2-vpc-bpa-internet-gateway-blocked`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`vpcBpaInternetGatewayBlockMode`	VPC BPA 选项模式的字符串值。	枚举	`block-bidirectional` ，`block-ingress`	无默认值

此控件检查是否将 Amazon EC2 VPC 阻止公开访问（BPA）设置配置为阻止 AWS 账户中所有 Amazon VPC 的互联网网关流量。如果 VPC BPA 设置未配置为阻止互联网网关流量，则该控件会失败。要使控件通过，VPC BPA `InternetGatewayBlockMode` 必须设置为 `block-bidirectional` 或 `block-ingress`。如果提供了参数 `vpcBpaInternetGatewayBlockMode`，则只有当 `InternetGatewayBlockMode` 的 VPC BPA 值与该参数匹配时，该控件才会通过。

在中为您的账户配置 VPC BPA 设置可以阻止 AWS 区域 您在该区域拥有的 VPC 和子网中的资源通过互联网网关和仅限出口的互联网网关访问或访问互联网。如果您需要特定 VPC 和子网能够访问互联网或从互联网访问，则可以通过配置 VPC BPA 排除项来排除它们。有关创建和删除排除项的说明，请参阅《Amazon VPC 用户指南》中的创建和删除排除项。

修复

要在账户级别启用双向 BPA，请参阅《Amazon VPC 用户指南》中的为您的账户启用 BPA 双向模式。要启用仅入口 BPA，请参阅将 VPC BPA 模式更改为仅入口。要在组织级别启用 VPC BPA，请参阅在组织级别启用 VPC BPA。

[EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::EC2::SpotFleet`

AWS Config 规则：ec2-spot-fleet-request-ct-encryption-at-rest

计划类型：已触发变更

参数：无

此控件检查指定启动参数的 Amazon EC2 竞价型实例集请求是否配置为对连接到 EC2 实例的所有 Amazon Elastic Block Store（Amazon EBS）卷启用加密。如果竞价型实例集请求指定了启动参数，但未对请求中指定的一个或多个 EBS 卷启用加密，则该控件会失败。

为了进一步提高安全性，您应该为 Amazon EBS 卷启用加密。然后，加密操作会在托管 Amazon EC2 实例的服务器上进行，这有助于确保实例与其附加的 EBS 存储之间传输的静态数据和传输中数据的安全。Amazon EBS 加密是一种直接加密解决方案，适用于与 EC2 实例关联的 EBS 资源。借助 EBS 加密，您无需构建、维护和保护自己的密钥管理基础设施。创建加密卷 AWS KMS keys 时使用 EBS 加密。

> **注意**
>
> 此控件不会为使用启动模板的 Amazon EC2 竞价型实例集请求生成调查发现。对于未明确指定 `encrypted` 参数值的竞价型实例集请求，它也不会生成调查发现。

修复

没有直接对现有未加密 Amazon EBS 卷进行加密的方法。您只能在创建新卷时对其进行加密。

但是，如果您默认情况下启用加密，Amazon EBS 将使用您的 EBS 加密默认密钥对新卷进行加密。如果默认情况下未启用加密，则可以在创建单个卷时启用加密。在这两种情况下，您都可以覆盖 EBS 加密的默认密钥，并选择客户管理型 AWS KMS key。有关 EBS 加密的更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EBS 加密。

有关创建 Amazon EC2 竞价型实例集请求的信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的创建竞价型实例集。

[EC2.174] 应标记 EC2 DHCP 选项集

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::DHCPOptions`

AWS Config 规则：ec2-dhcp-options-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EC2 DHCP 选项集是否具有 requiredKeyTags 参数指定的标签键。如果选项集没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件将失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果选项集没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon EC2 DHCP 选项集添加标签的信息，请参阅《Amazon EC2 用户指南》中的标记您的 Amazon EC2 资源。

[EC2.175] 应标记 EC2 启动模板

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::LaunchTemplate

AWS Config 规则：ec2-launch-template-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EC2 启动模板是否具有 `requiredKeyTags` 参数指定的标签键。如果启动模板没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件会失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果启动模板没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon EC2 启动模板添加标签的信息，请参阅《Amazon EC2 用户指南》中的标记您的 Amazon EC2 资源。

[EC2.176] 应标记 EC2 前缀列表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::PrefixList`

AWS Config 规则：ec2-prefix-list-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EC2 前缀列表是否具有 `requiredKeyTags` 参数指定的标签键。如果前缀列表没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件将失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果前缀列表没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon EC2 前缀列表添加标签的信息，请参阅《Amazon EC2 用户指南》中的标记您的 Amazon EC2 资源。

[EC2.177] 应标记 EC2 流量镜像会话

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::TrafficMirrorSession

AWS Config 规则：ec2-traffic-mirror-session-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EC2 流量镜像会话是否具有 requiredKeyTags 参数指定的标签键。如果会话没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件将失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果会话没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon EC2 流量镜像会话添加标签的信息，请参阅《Amazon EC2 用户指南》中的标记您的 Amazon EC2 资源。

[EC2.178] 应标记 EC2 流量镜像过滤器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::TrafficMirrorFilter`

AWS Config 规则：ec2-traffic-mirror-filter-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EC2 流量镜像筛选条件是否具有 `requiredKeyTags` 参数指定的标签键。如果筛选条件没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件将失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果筛选条件没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon EC2 流量镜像筛选条件添加标签的信息，请参阅《Amazon EC2 用户指南》中的标记您的 Amazon EC2 资源。

[EC2.179] 应标记 EC2 流量镜像目标

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::TrafficMirrorTarget`

AWS Config 规则：ec2-traffic-mirror-target-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EC2 流量镜像目标是否具有 `requiredKeyTags` 参数指定的标签键。如果目标没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件将失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果目标没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和

筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon EC2 流量镜像目标添加标签的信息，请参阅《Amazon EC2 用户指南》中的标记您的 Amazon EC2 资源。

[EC2.180] EC2 网络接口应启用 source/destination 检查功能

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::EC2::NetworkInterface`

AWS Config 规则：ec2-enis-source-destination-check-enabled

计划类型：已触发变更

参数：无

此控件 source/destination 检查是否启用了对由用户管理的 Amazon EC2 弹性网络接口 (ENI) 的检查。如果禁用了对用户管理的 ENI 的 source/destination 检查，则控制失败。此控件仅检查以下类型的 ENI：`aws_codestar_connections_managed`、`branch`、`efa`、`interface`、`lambda` 和 `quicksight`。

Source/destination 应在您的 EC2 实例中一致地启用和配置 Amazon EC2 实例和附加的 ENI 的检查。每个 ENI 都有自己的 source/destination 支票设置。如果启用了 source/destination 检查，Amazon EC2 将强制执行 source/destination 地址验证，从而确保实例是其接收的任何流量的来源或目的地。这通过防止资源处理非预期流量和防止 IP 地址欺骗来提供额外网络安全层。

> **Note**
>
> 如果您将 EC2 实例用作 NAT 实例，但禁用了对其 ENI 的 source/destination 检查，则可以改用 NAT 网关。

修复

有关为 Amazon EC2 ENI 启用 source/destination 检查的信息，请参阅 A mazon EC2 用户指南中的修改网络接口属性。

[EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::EC2::LaunchTemplate`

AWS Config 规则：ec2-launch-templates-ebs-volume-encrypted

计划类型：已触发变更

参数：无

此控件检查 Amazon EC2 启动模板是否为所有连接的 EBS 卷启用加密。如果 EC2 启动模板指定的任何 EBS 卷的加密参数设置为 `False`，则该控件会失败。

Amazon EBS 加密是一种适用于与 Amazon EC2 实例关联的 EBS 资源的直接加密解决方案。借助 EBS 加密，您无需构建、维护和保护自己的密钥管理基础设施。创建加密卷和快照时，EBS 加密使用 AWS KMS keys 。加密操作会在托管 EC2 实例的服务器上进行，这有助于确保 EC2 实例与其附加的 EBS 存储之间传输的静态数据和传输中数据的安全。有关更多信息，请参阅《Amazon EBS 用户指南》中的 Amazon EBS 加密。

您可以在手动启动单个 EC2 实例期间启用 EBS 加密。然而，使用 EC2 启动模板并在这些模板中配置加密设置有很多好处。您可以将加密作为标准强制执行，并确保使用一致的加密设置。您还可以降低手动启动实例时可能会出现的错误和安全漏洞的风险。

> **Note**
>
> 当此控件检查 EC2 启动模板时，它只会评估模板明确指定的 EBS 加密设置。评估不包括继承自账户级 EBS 加密设置、AMI 块设备映射或源快照加密状态的加密设置。

修复

创建 Amazon EC2 启动模板后，您将无法对其进行修改。但是，您可以创建一个新版本的启动模板，并在该新版本的模板中更改加密设置。您还可以将新版本指定为启动模板的默认版本。然后，如果您从启动模板启动 EC2 实例，并且没有指定模板版本，则 EC2 在启动实例时会使用默认版本的设置。有关更多信息，请参阅《Amazon EC2 用户指南》中的修改启动模板。

[EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EC2::SnapshotBlockPublicAccess`

AWS Config 规则：ebs-snapshot-block-public-access

计划类型：已触发变更

参数：无

此控件检查是否启用了账户级别的封锁公开访问以防止向所有人共享 Amazon EBS 快照。如果未启用阻止公共访问以阻止向所有人共享 Amazon EBS 快照，则控制失败。

要防止公开共享您的 Amazon EBS 快照，您可以为快照启用禁止公开访问功能。在某个区域启用了对快照的封禁公共访问后，任何在该区域公开共享快照的尝试都会被自动阻止。这有助于提高快照的安全性，并保护快照数据免遭未经授权或意外访问。

修复

要启用对快照的封锁公有访问，请参阅 Amazon EBS 用户指南中的为 Amazon EBS 快照配置屏蔽公开访问。在 “阻止公共访问” 中，选择 “阻止所有公共访问”。

[EC2.183] EC2 VPN 连接应使用 IKEv2 协议

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::EC2::VPNConnection`

AWS Config 规则：ec2-vpn-connection-ike-version-check

计划类型：已触发变更

参数：无

此控件检查 AWS Site-to-Site VPN 连接是否配置为使用 IKEv2 协议。如果 Site-to-Site VPN 连接允许 IKEv1 协议或未明确限制所有 VPN 隧道上的 IKEv2，则控制失败。

与传统的 IKEv1 协议相比，IKEv2 提供了更强大的加密算法和改进的安全功能，包括针对拒绝服务攻击的内置保护和增强的身份验证机制。IKEv1 在其密钥交换过程中存在已知的漏洞和漏洞，攻击者可以利用这些漏洞来危害 VPN 隧道的安全。通过强制 IKEv2-only 连接，您可以减少攻击面，并确保 VPN 通信使用现代的行业标准加密协议，从而更好地保护传输中的数据。

修复

要更新 EC2 VPN 连接上的 VPN 隧道的 IKE 版本，请参阅 AWS Site-to-Site VPN 用户指南中的修改 AWS Site-to-Site VPN 隧道选项。

适用于 Auto Scaling 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件用于评估 Amazon A EC2 uto Scaling 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

相关要求：PCI DSS v3.2.1/2.2、、nist.800-53.r5 CP-2 (2) NIST.800-53.r5 CA-7、nist.800-53.r5 SI-2

类别：识别 > 清单

严重性：低

资源类型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 规则：`autoscaling-group-elb-healthcheck-required`

计划类型：已触发变更

参数：无

此控件检查与负载均衡器关联的 Amazon A EC2 uto Scaling 组是否使用弹性负载平衡 (ELB) 运行状况检查。如果自动扩缩组未使用 ELB 运行状况检查，则控件会失败。

ELB 运行状况检查可确保自动扩缩组可以根据负载均衡器提供的其他测试确定实例的运行状况。使用 Elastic Load Balancing 运行状况检查还有助于支持使用 EC2 Auto Scaling 组的应用程序的可用性。

修复

要添加 Elastic Load Balancing 运行状况检查，请参阅 Amazon A EC2 uto Scaling 用户指南中的添加弹性负载平衡运行状况检查。

[AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域

相关要求： NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 规则：`autoscaling-multiple-az`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`minAvailabilityZones`	可用区的最小数量	枚举	`2, 3, 4, 5, 6`	`2`	

此控件检查 Amazon A EC2 uto Scaling 组是否至少跨越指定数量的可用区 (AZs)。如果 Auto Scaling 组的跨度不超过指定数量，则控制失败 AZs。除非您为最小数量提供自定义参数值 AZs，否则 Security Hub CSPM 将使用默认值为 2。 AZs

如果配置的单个可用区不可用，不跨越多个 AZs 的 Auto Scaling 组无法在另一个可用区中启动实例来补偿。但在某些使用案例中，例如批处理作业，或需要将可用区间传输成本保持在最低时，首选具有单个可用区的自动扩缩组。在这种情况下，您可以禁用此控件或隐藏其调查发现。

修复

要 AZs 添加到现有 Auto Scaling 组，请参阅 Amazon A EC2 uto Scaling 用户指南中的添加和删除可用区。

[AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)

相关要求： NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3 (15)、(7)、、 NIST.800-53.r5 AC-3 NIST.800-53.r5 CA-9 (1)、nist.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.6 NIST.800-53.r5 AC-6

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 规则：`autoscaling-launchconfig-requires-imdsv2`

计划类型：已触发变更

参数：无

此控件会检查 Amazon A EC2 uto Scaling 群组启动的所有实例是否 IMDSv2 已启用。如果实例元数据服务 (IMDS) 版本未包含在启动配置中或配置为（ 该设置允许 IMDSv1 或 IMDSv2之一 ）`token optional`，则控制失败。

IMDS 提供有关实例的数据，您可以使用这些数据来配置或管理正在运行的实例。

IMDS 第 2 版添加了新的保护措施，这些保护措施在进一步保护您的 EC2 实例 IMDSv1 时没有这些保护措施。

修复

自动扩缩组一次与一个启动配置关联。在创建启动配置后，您将无法对其进行修改。要更改 Auto Scaling 组的启动配置，请使用现有启动配置作为 IMDSv2 启用的新启动配置的基础。有关更多信息，请参阅 Amazon EC2 用户指南中的为新实例配置实例元数据选项。

[AutoScaling.4] Auto Scaling 组启动配置的元数据响应跳跃限制不应大于 1

> **Important**
>
> Security Hub CSPM 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub CSPM 控件的更改日志。

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 规则：`autoscaling-launch-config-hop-limit`

计划类型：已触发变更

参数：无

此控件检查元数据令牌可以传输的网络跃点数。如果元数据响应跳数限制大于 1，则控制失败。

实例元数据服务 (IMDS) 提供有关 Amazon EC2 实例的元数据信息，可用于应用程序配置。将元数据服务的 HTTP PUT 响应限制为仅限 EC2 实例，可保护 IMDS 免遭未经授权的使用。

IP 数据包中的生存时间（TTL）字段每个跳点上减少一个。这种减少可用于确保包裹不会在外面传输 EC2。 IMDSv2 保护可能被错误配置为开放路由器、第 3 层防火墙 VPNs、隧道或 NAT 设备的 EC2 实例，从而防止未经授权的用户检索元数据。使用时 IMDSv2，包含密钥令牌的PUT响应无法传送到实例之外，因为默认的元数据响应跳跃限制设置为1。但是，如果此值大于1，则令牌可以离开 EC2 实例。

修复

要修改现有启动配置的元数据响应跳跃限制，请参阅 Amazon EC2 用户指南中的修改现有实例的实例元数据选项。

[Autoscaling.5] 使用 Auto Scaling 组启动配置启动的 EC2 亚马逊实例不应具有公有 IP 地址

相关要求： 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、、、(11) NIST.800-53.r5 AC-6 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)、(4)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9)、 NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：AWS::AutoScaling::LaunchConfiguration

AWS Config 规则：autoscaling-launch-config-public-ip-disabled

计划类型：已触发变更

参数：无

此控件检查自动扩缩组的关联启动配置是否为该组的实例分配了公有 IP 地址。如果关联的启动配置分配了公有 IP 地址，则控制失败。

Auto Scaling 组启动配置中的亚马逊 EC2 实例不应具有关联的公有 IP 地址，有限的边缘情况除外。Amazon EC2 实例只能从负载均衡器后面访问，而不是直接暴露在互联网上。

修复

自动扩缩组一次与一个启动配置关联。在创建启动配置后，您将无法对其进行修改。要更改 Auto Scaling 组的启动配置，请将现有的启动配置作为新启动配置的基础。然后，更新 Auto Scaling 组以使用新的启动配置。有关 step-by-step说明，请参阅 Amazon Auto Scaling 用户指南中的更改 A EC2 uto Scaling 组的启动配置。创建新的启动配置时，在其他配置下，在高级详细信息、IP 地址类型下，选择不要为任何实例分配公有 IP 地址。

变更启动配置后，自动扩缩会使用新的配置选项启动新实例。现有实例不受影响。要更新现有实例，我们建议您刷新实例，或者根据终止策略启用自动扩缩，以逐步使用较新实例替换较旧实例。有关更新 Auto Scaling 实例的更多信息，请参阅 Amazon Auto Scaling 用户指南中的更新 A EC2 uto Scaling 实例。

[AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型

相关要求： NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::AutoScaling::AutoScalingGroup

AWS Config 规则：autoscaling-multiple-instance-types

计划类型：已触发变更

参数：无

此控件用于检查 Amazon A EC2 uto Scaling 组是否使用多种实例类型。如果自动扩缩组仅定义了一个实例类型，则控制失败。

您可以跨多个可用区中运行的多个实例类型部署应用程序以提高可用性。Security Hub CSPM 建议使用多种实例类型，这样 Auto Scaling 组可以在您选择的可用区域中的实例容量不足时启动另一种实例类型。

修复

要创建具有多种实例类型的 Auto Scaling 组，请参阅 Amazon Auto Scaling 用户指南中的具有多种实例类型和购买选项的 A EC2 uto Scaling 群组。

[AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 规则：`autoscaling-launch-template`

计划类型：已触发变更

参数：无

此控件会检查 Amazon A EC2 uto Scaling 群组是否是根据 EC2 启动模板创建的。如果未使用启动模板创建 Amazon A EC2 uto Scaling 组，或者混合实例策略中未指定启动模板，则此控制将失败。

可以根据 EC2 启动模板或启动配置创建 A EC2 uto Scaling 组。但是，使用启动模板创建自动扩缩组可确保您能够访问最新功能和改进。

修复

要使用 EC2 启动模板创建 Auto Scaling 群组，请参阅 Amazon Auto Scaling 用户指南中的使用启动模板创建 A EC2 uto Scaling 群组。有关如何用启动模板替换启动配置的信息，请参阅 Amazon EC2 用户指南中的将启动配置替换为启动模板。

[AutoScaling.10] 应标记 EC2 Auto Scaling 群组

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::AutoScaling::AutoScalingGroup

AWS Config 规则:tagged-autoscaling-autoscalinggroup（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon A EC2 uto Scaling 组是否具有参数中定义的特定密钥的标签requiredTagKeys。如果自动扩缩组没有任何标签键或未在参数 requiredTagKeys 中指定所有键，则此控件会失败。如果未提供参数 requiredTagKeys，则此控件仅会检查是否存在标签键，如果自动扩缩组未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Auto Scaling 组添加标签，请参阅 Amazon Auto Scaling 用户指南中的为 EC2 自动缩放组和实例添加标签。

适用于亚马逊 ECR 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件评估亚马逊弹性容器注册表 (Amazon ECR) Container Registry 的服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ECR.1] ECR 私有存储库应配置图像扫描

相关要求： NIST.800-53.r5 RA-5，PCI DSS v4.0.1/6.2.3，PCI DSS v4.0.1/6.2.4

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::ECR::Repository`

AWS Config 规则：ecr-private-image-scanning-enabled

计划类型：定期

参数：无

此控件检查私有 Amazon ECR 存储库是否配置了图像扫描。如果未将私有 ECR 存储库配置为推送时扫描或连续扫描，则控制失败。

ECR 映像扫描有助于识别容器映像中的软件漏洞。在 ECR 存储库上配置图像扫描为所存储图像的完整性和安全性添加了一层验证。

修复

要为 ECR 存储库配置图像扫描，请参阅 Amazon Elastic Container Registry 用户指南中的图像扫描。

[ECR.2] ECR 私有存储库应配置标签不可变性

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-8 (1)

类别：识别 > 清单 > 标记

严重性：中

资源类型：AWS::ECR::Repository

AWS Config 规则：ecr-private-tag-immutability-enabled

计划类型：已触发变更

参数：无

此控件检查私有 ECR 存储库是否启用了标签不可变性。如果私有 ECR 存储库禁用了标签不可变性，则此控制失败。如果启用了标签不可变性并且具有值 IMMUTABLE，则此规则通过。

Amazon ECR 标签不变性使客户能够依靠图像的描述性标签作为跟踪和唯一识别图像的可靠机制。不可变标签是静态的，这意味着每个标签都引用一个唯一的图像。这提高了可靠性和可扩展性，因为使用静态标签总是会导致部署相同的映像。配置后，标签不变性可防止标签被覆盖，从而减少攻击面。

修复

要创建配置了不可变标签的存储库或更新现有存储库的图像标签可变性设置，请参阅 Amazon Elastic Container Registry 用户指南中的图像标签可变性。

[ECR.3] ECR 存储库应至少配置一个生命周期策略

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：识别 > 资源配置

严重性：中

资源类型：AWS::ECR::Repository

AWS Config 规则：ecr-private-lifecycle-policy-configured

计划类型：已触发变更

参数：无

此控件检查 Amazon ECR 存储库是否至少配置了一个生命定期策略。如果 ECR 存储库未配置任何生命定期策略，则此控制失败。

Amazon ECR 生命周期策略使您能够指定存储库中镜像的生命周期管理。通过配置生命周期策略，您可以根据年龄或数量自动清理未使用的映像以及到期的映像。自动执行这些任务可以帮助您避免无意中使用存储库中过时的映像。

修复

要配置生命周期策略，请参阅 Amazon Elastic Container Registry 用户指南中的创建生命周期策略预览。

[ECR.4] 应标记 ECR 公有存储库

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECR::PublicRepository`

AWS Config 规则:`tagged-ecr-publicrepository`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon ECR 公有存储库是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果公有存储库没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果公有存储库未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些

ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECR 公有存储库添加标签，请参阅《Amazon Elastic Container Registry 用户指南》中的标记 Amazon ECR 公有存储库。

[ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys

相关要求： NIST.800-53.r5 SC-12 (2)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、(10)、(1)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6)、nist.800-53.r5 NIST.800-53.r5 CA-9 (6)、nist.800-53.r5 AU-9

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::ECR::Repository`

AWS Config 规则：ecr-repository-cmk-encryption-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`kmsKeyArns`	评估中 AWS KMS keys 要包含的 Amazon 资源名称 (ARNs) 列表。如果 ECR 存储库未使用列表中的 KMS 密钥进行加	StringList（最多 10 个项目）	1—10 个 ARNs 现有 KMS 密钥。例如：`arn:aws:`	无默认值

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
	密，则该控件会生成 FAILED 调查发现。		ms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab	

此控件检查 Amazon ECR 存储库是否已使用客户管理型 AWS KMS key进行静态加密。如果未使用客户自主管理型 KMS 密钥对 ECR 存储库进行加密，则该控件会失败。您可以选择为控件指定要包含在评估中的 KMS 密钥列表。

默认情况下，Amazon ECR 使用 AES-256 算法通过 Amazon S3 托管密钥（SSE-S3）对存储库数据进行加密。为了获得更多控制，您可以将 Amazon ECR 配置为改用 AWS KMS key （SSE-KMS 或 DSSE-KMS）对数据进行加密。KMS 密钥可以是：Amazon ECR 为您创建和管理的别名为 aws/ecr 的 AWS 托管式密钥 ，或您在自己的 AWS 账户中创建和管理的客户自主管理型密钥。使用客户管理型 KMS 密钥，您可以完全控制密钥。这包括定义和维护密钥策略、管理授权、轮换加密材料、分配标签、创建别名以及启用和禁用密钥。

> **Note**
>
> AWS KMS 支持跨账户访问 KMS 密钥。如果 ECR 存储库使用其他账户拥有的 KMS 密钥进行加密，则此控件在评估存储库时不会执行跨账户检查。该控件不会评测 Amazon ECR 在对存储库执行加密操作时是否可以访问和使用密钥。

修复

您无法更改现有 ECR 存储库的加密设置。但是，您可以为后续创建的 ECR 存储库指定不同的加密设置。Amazon ECR 支持对各个存储库使用不同的加密设置。

有关 ECR 存储库的加密选项的更多信息，请参阅《Amazon ECR 用户指南》中的 Encryption at rest。有关客户管理的更多信息 AWS KMS keys，请参阅AWS Key Management Service 开发者指南AWS KMS keys中的。

适用于亚马逊 ECS 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件评估亚马逊弹性容器服务 (Amazon ECS) 的服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ECS.2] ECS 服务不应自动分配公有 IP 地址

相关要求： 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、(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。 1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::ECS::Service`

AWS Config 规则:`ecs-service-assign-public-ip-disabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 服务是否配置为自动分配公有 IP 地址。如果 `AssignPublicIP` 是 `ENABLED`，则控制失败。如果 `AssignPublicIP` 是 `DISABLED`，则此控件通过。

公有 IP 地址是指可通过 Internet 访问的 IP 地址。如果您使用公有 IP 地址启动 Amazon ECS 实例，则可以通过 Internet 访问 Amazon ECS 实例。Amazon ECS 服务不应公开访问，因为这可能会允许对容器应用程序服务器进行意外访问。

修复

首先，您必须为您的集群创建一个任务定义，该集群使用 `awsvpc` 网络模式并为 `requiresCompatibilities` 指定 FARGATE。然后，对于计算配置，请选择启动类型和 FARGATE。最后，对于网络字段，请关闭公有 IP 以禁用服务的公有 IP 自动分配。

[ECS.3] ECS 任务定义不应共享主机的进程命名空间

相关要求： NIST.800-53.r5 CA-9(1)， NIST.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-task-definition-pid-mode-check

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义是否配置为与其容器共享主机的进程命名空间。如果任务定义与其上运行的容器共享主机的进程命名空间，则控制失败。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

进程 ID（PID）命名空间提供了进程之间的分离。它防止系统进程可见，并允许重复使用 PID，包括 PID 1。如果主机的 PID 命名空间与容器共享，则容器可以看到主机系统上的所有进程。这降低了主机和容器之间进程级分离的好处。这些情况可能导致未经授权访问主机本身的进程，包括操纵和终止这些进程的能力。客户不应与其上运行的容器共享主机的进程命名空间。

修复

要对任务定义进行配置，请参阅 `pidMode` Amazon Elastic Container Service 开发人员指南中的任务定义参数。

[ECS.4] ECS 容器应以非特权身份运行

相关要求： 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

类别：保护 > 安全访问管理 >根用户访问限制

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-containers-nonprivileged

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义的容器定义中的 privileged 参数是否设置为 true。如果此参数等于，则控制失败true。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

我们建议您从 ECS 任务定义中删除提升权限。当权限参数为 true 时，容器被赋予对宿主容器实例的提升权限（类似于根用户）。

修复

要配置任务定义的 privileged 参数，请参阅 Amazon Elastic Container Service 开发人员指南中的高级容器定义参数。

[ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限

相关要求： 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

类别：保护 > 安全访问管理

严重性：高

资源类型：AWS::ECS::TaskDefinition

AWS Config 规则：ecs-containers-readonly-access

计划类型：已触发变更

参数：无

此控件检查 ECS 任务定义是否将容器配置为仅限对已安装的根文件系统的只读访问权限。如果 ECS 任务定义的容器定义中的readonlyRootFilesystem参数设置为false，或者任务定义中的容器定义中不存在该参数，则控制失败。此控件仅评估 Amazon ECS 任务定义的最新活跃版本。

如果在 Amazon ECS 任务定义中将 readonlyRootFilesystem 参数设置为 true，则 ECS 容器将获得对其根文件系统的只读访问权限。这样可减少安全攻击向量，因为如果没有对文件系统文件夹和目录具有读写权限的显式卷挂载，就无法篡改或写入容器实例的根文件系统。启用此选项还遵循最低权限原则。

> **Note**
>
> Windows 容器不支持该readonlyRootFilesystem参数。runtimePlatform配置为指定WINDOWS_SERVER操作系统系列的任务定义被标记为NOT_APPLICABLE且不会生成此控件的调查结果。

修复

要授予 Amazon ECS 容器对其根文件系统的只读访问权限，请将 `readonlyRootFilesystem` 参数添加到容器的任务定义，并将该参数的值设置为 `true`。有关任务定义参数以及如何将其添加到任务定义中的信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的 Amazon ECS 任务定义和更新任务定义。

[ECS.8] 密钥不应作为容器环境变量传递

相关要求： NIST.800-53.r5 CA-9(1)， NIST.800-53.r5 CM-2，PCI DSS v4.0。 1/8.6.2

类别：保护 > 安全开发 > 凭证未硬编码

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-no-environment-secrets

计划类型：已触发变更

参
数：`secretKeys`：`AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA`（不可自定义）

此控件检查容器定义 `environment` 参数中任何变量的键值是否包括 `AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY` 或 `ECS_ENGINE_AUTH_DATA`。如果任何容器定义中的单个环境变量等于 `AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY` 或 `ECS_ENGINE_AUTH_DATA`，则此控制失败。此控件不包括从其他位置（例如 Amazon S3）传入的环境变量。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

AWS Systems Manager Parameter Store 可以帮助您改善组织的安全状况。我们建议使用 Parameter Store 存储密钥和凭证，而不是直接将其传递到容器实例或将其硬编码到代码中。

修复

要使用 SSM 创建参数，请参阅 AWS Systems Manager 用户指南中的创建 Systems Manager 参数。有关创建指定密钥的任务定义的更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的使用 Secrets Manager 指定敏感数据。

[ECS.9] ECS 任务定义应具有日志配置

相关要求： 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)

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-task-definition-log-configuration

计划类型：已触发变更

参数：无

此控件检查最新的活动的 Amazon ECS 任务定义是否指定了日志配置。如果任务定义未定义 `logConfiguration` 属性，或者至少有一个容器定义中的 `logDriver` 值为空，则控制失败。

日志记录可帮助您保持 Amazon ECS 的可靠性、可用性和性能。从任务定义中收集数据可提供可见性，这可以帮助您调试流程并找到错误的根本原因。如果您使用的日志记录解决方案不必在 ECS 任务定义中定义（例如第三方日志解决方案），则可以在确保正确捕获和传送日志后禁用此控件。

修复

要为 Amazon ECS 任务定义定义日志配置，请参阅 Amazon Elastic Container Service 开发人员指南中的在任务定义中指定日志配置。

[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行

相关要求： 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

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::ECS::Service`

AWS Config 规则：ecs-fargate-latest-platform-version

计划类型：已触发变更

参数：

- `latestLinuxVersion: 1.4.0`（不可自定义）
- `latestWindowsVersion: 1.0.0`（不可自定义）

此控件检查 Amazon ECS Fargate 服务是否正在运行最新的 Fargate 平台版本。如果平台版本不是最新版本，则此控制失败。

AWS Fargate 平台版本是指 Fargate 任务基础架构的特定运行时环境，它是内核和容器运行时版本的组合。随着运行时系统环境的发展，将不断发布新的平台版本。例如，可能会发布新版本以进行内核或操作系统更新、新功能、错误修复或安全更新。 Fargate 任务的安全更新和补丁将自动部署。如果发现影响平台版本的安全问题，请 AWS 修补平台版本。

修复

要更新现有服务，包括其平台版本，请参阅 Amazon Elastic Container Service 开发人员指南中的更新服务。

[ECS.12] ECS 集群应使用容器见解

相关要求： 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ECS::Cluster`

AWS Config 规则：ecs-container-insights-enabled

计划类型：已触发变更

参数：无

此控件检查 ECS 集群是否使用容器见解。如果未为集群设置 Container Insights，则此控制失败。

监控是维护 Amazon ECS 集群的可靠性、可用性和性能的重要组成部分。使用 CloudWatch Container Insights 收集、汇总和汇总来自容器化应用程序和微服务的指标和日志。 CloudWatch 自动收集许多资

源的指标，例如 CPU、内存、磁盘和网络。Container Insights 还提供诊断信息（如容器重新启动失败），以帮助您查明问题并快速解决问题。您还可以对容器洞察收集的指标设置 CloudWatch 警报。

修复

要使用容器见解，请参阅 Amazon CloudWatch 用户指南中的更新服务。

[ECS.13] 应标记 ECS 服务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECS::Service`

AWS Config 规则:`tagged-ecs-service`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon ECS 服务是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果该服务没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果该服务未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些

ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECS 服务添加标签，请参阅《Amazon Elastic Container Service 开发人员指南》中的标记 Amazon ECS 资源。

[ECS.14] 应标记 ECS 群集

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECS::Cluster`

AWS Config 规则:`tagged-ecs-cluster`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon ECS 集群是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果集群没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果集群未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECS 集群添加标签，请参阅《Amazon Elastic Container Service 开发人员指南》中的标记 Amazon ECS 资源。

[ECS.15] 应标记 ECS 任务定义

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则:`tagged-ecs-taskdefinition`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon ECS 任务定义是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果任务定义没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果任务定义未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECS 任务定义添加标签，请参阅《Amazon Elastic Container Service 开发人员指南》中的标记 Amazon ECS 资源。

[ECS.16] ECS 任务集不应自动分配公有 IP 地址

相关要求：PCI DSS v4.0。 1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::ECS::TaskSet`

AWS Config 规则:`ecs-taskset-assign-public-ip-disabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件可检查 Amazon ECS 任务集是否配置为自动分配公有 IP 地址。如果设置为，`AssignPublicIP`则控制失败`ENABLED`。

可通过互联网访问公有 IP 地址。如果您使用公有 IP 地址来配置任务集，则可以通过互联网来访问与任务集关联的资源。ECS 任务集不应可公开访问，因为这可能会允许对容器应用程序服务器进行意外访问。

修复

要更新 ECS 任务集使其不使用公有 IP 地址，请参阅《Amazon Elastic Container Service 开发人员指南》中的使用控制台更新 Amazon ECS 任务定义。

[ECS.17] ECS 任务定义不应使用主机网络模式

相关要求： 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

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-task-definition-network-mode-not-host

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义的最新有效修订版是否使用 `host` 网络模式。如果 ECS 任务定义的最新有效版本使用 `host` 网络模式，则该控件会失败。

使用 `host` 网络模式时，Amazon ECS 容器的网络直接与运行该容器的底层主机绑定。因此，这种模式允许容器连接到主机上的私有环回网络服务并模拟主机。其他显著缺点是，在使用 `host` 网络模式时无法重新映射容器端口，而且每台主机只能运行一个任务的单个实例化。

修复

有关托管在 Amazon EC2 实例上的 Amazon ECS 任务的联网模式和选项的信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的 EC2 启动类型的 Amazon ECS 任务联网选项。有关创建任务定义的新修订版和指定其他网络模式的信息，请参阅该指南中的更新 Amazon ECS 任务定义。

如果 Amazon ECS 任务定义是由创建的 AWS Batch，请参阅 AWS Batch 作业的联网模式，了解联网模式和任务类型的典型用 AWS Batch 法，并选择安全选项。

[ECS.18] ECS 任务定义应对 EFS 卷使用传输中加密

类别：保护 > 传输中数据加密

严重性：中

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-task-definition-efs-encryption-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义的最新有效版本是否对 EFS 卷使用传输中加密。如果 ECS 任务定义的最新有效版本禁用了 EFS 卷的传输中加密，则控制失败。

Amazon EFS 卷提供简单、可扩展和持久的共享文件存储，用于您的 Amazon ECS 任务。Amazon EFS 支持使用传输层安全性协议（TLS）对传输中数据进行加密。在将传输中数据加密声明为 EFS 文件系统的挂载选项时，Amazon EFS 会在挂载文件系统时与您的 EFS 文件系统建立安全的 TLS 连接。

修复

有关为使用 EFS 卷的 Amazon ECS 任务定义启用传输中加密的信息，请参阅《亚马逊弹性容器服务开发人员指南》中的步骤 5：创建任务定义。

[ECS.19] ECS 容量提供商应启用托管终止保护

类别： 保护 > 数据保护

严重性：中

资源类型：`AWS::ECS::CapacityProvider`

AWS Config 规则：ecs-capacity-provider-termination-check

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 容量提供商是否启用了托管终止保护。如果未在 ECS 容量提供商上启用托管终止保护，则控制失败。

Amazon ECS 容量提供程序为集群中的任务管理基础设施的扩缩。当将 EC2 实例用于您的容量时，请使用自动扩缩组来管理 EC2 实例。通过托管式终止保护，集群自动扩缩可以控制终止哪些实例。当您使用托管式终止保护时，Amazon ECS 仅终止没有任何正在运行的 Amazon ECS 任务的 EC2 实例。

> **Note**
>
> 使用托管终止保护时，还必须使用托管扩展，否则托管终止保护将不起作用。

修复

要为 Amazon ECS 容量提供商启用托管终止保护，请参阅亚马逊弹性容器服务开发者指南中的更新 Amazon ECS 容量提供商的托管终止保护。

[ECS.20] ECS 任务定义应在 Linux 容器定义中配置非 root 用户

类别：保护 > 安全访问管理 >根用户访问限制

严重性：中

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：ecs-task-definition-linux-user-non-root

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义的最新有效版本是否将 Linux 容器配置为以非 root 用户身份运行。如果配置了默认 root 用户或者任何容器都没有用户配置，则控制将失败。

当 Linux 容器以 root 权限运行时，它们会带来一些重大的安全风险。root 用户在容器内拥有不受限制的访问权限。这种提升的访问权限增加了容器逃脱攻击的风险，在这种攻击中，攻击者有可能突破容器隔离并访问底层主机系统。如果以 root 身份运行的容器遭到入侵，攻击者可能会利用此漏洞访问或修改主机系统资源，从而影响其他容器或主机本身。此外，root 访问权限可能导致权限升级攻击，从而使攻击者能够获得超出容器预期范围的额外权限。ECS 任务定义中的用户参数可以用多种格式指定用户，包括用户名、用户 ID、带组的用户名或带有组 ID 的 UID。在配置任务定义时，请务必注意这些不

同的格式，以确保不会无意中授予 root 访问权限。遵循最低权限原则，容器应使用非 root 用户以所需的最低权限运行。这种方法可显著减少潜在的攻击面并减轻潜在安全漏洞的影响。

> **Note**
>
> 只有在任务定义中将容器定义配置为LINUX或operatingSystemFamily未配置时operatingSystemFamily，此控件才会评估任务定义中的容器定义。如果任务定义中的任何容器定义user未配置或user配置为默认 root 用户，则该控件将为已评估的任务定义生成FAILED结果。LINUX容器的默认 root 用户为"root"和"0"。

修复

有关创建 Amazon ECS 任务定义的新修订版和更新容器定义中的user参数的信息，请参阅《亚马逊弹性容器服务开发者指南》中的更新 Amazon ECS 任务定义。

[ECS.21] ECS 任务定义应在 Windows 容器定义中配置非管理员用户

类别：保护 > 安全访问管理 >根用户访问限制

严重性：中

资源类型：AWS::ECS::TaskDefinition

AWS Config 规则：ecs-task-definition-windows-user-non-admin

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义的最新有效版本是否将 Windows 容器配置为以非默认管理员的用户身份运行。如果将默认管理员配置为用户或任何容器都没有用户配置，则控制失败。

当 Windows 容器以管理员权限运行时，它们会带来多种严重的安全风险。管理员在容器内拥有不受限制的访问权限。这种提升的访问权限增加了容器逃脱攻击的风险，在这种攻击中，攻击者有可能突破容器隔离并访问底层主机系统。

> **Note**
>
> 只有在任务定义中将容器定义配置为WINDOWS_SERVER或operatingSystemFamily未配置时operatingSystemFamily，此控件才会评估任务定义中的容器定义。如果任务定义中的

任何容器定义user未配置或user配置为容器的默认管理员，则该控件将为已评估的任务定义生成FAILED结果，即"containeradministrator"。WINDOWS_SERVER

修复

有关创建 Amazon ECS 任务定义的新修订版和更新容器定义中的user参数的信息，请参阅《亚马逊弹性容器服务开发者指南》中的更新 Amazon ECS 任务定义。

适用于亚马逊 EFS 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件评估亚马逊弹性文件系统（亚马逊 EFS）服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.3.1，CIS AWS 基金会基准 v3.0。 0/2.4.1、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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::EFS::FileSystem

AWS Config 规则：efs-encrypted-check

计划类型：定期

参数：无

此控件检查 Amazon Elastic File System 是否配置为使用加密文件数据 AWS KMS。在以下情况下，检查失败。

- 在 DescribeFileSystems 响应中 Encrypted 设置为 false。
- DescribeFileSystems 响应中的 KmsKeyId 密钥与 efs-encrypted-check 的 KmsKeyId 参数不匹配。

请注意，此控件不使用 efs-encrypted-check 的 KmsKeyId 参数。它只检查 Encrypted 的值。

为了为 Amazon EFS 中的敏感数据增加一层安全保护，您应该创建加密文件系统。Amazon EFS 支持静态文件系统加密。您可以在创建 Amazon EFS 文件系统时启用静态数据加密。要了解有关 Amazon EFS 加密的更多信息，请参阅 Amazon Elastic File System 用户指南中的 Amazon EFS 中的数据加密。

修复

有关如何加密新的 Amazon EFS 文件系统的详细信息，请参阅 Amazon Elastic File System 用户指南中的加密静态数据。

[EFS.2] Amazon EFS 卷应包含在备份计划中

相关要求： 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)

分类：恢复 > 弹性 > 备份

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：efs-in-backup-plan

计划类型：定期

参数：无

此控件检查 Amazon Elastic File System（Amazon EFS）文件系统是否已添加到 AWS Backup中的备份计划中。如果 Amazon EFS 文件系统未包含在备份计划中，控制失败。

在备份计划中包括 EFS 文件系统可帮助您保护数据免遭删除和数据丢失。

修复

要为现有 Amazon EFS 文件系统启用自动备份，请参阅 AWS Backup 开发人员指南中的入门 4：创建 Amazon EFS 自动备份。

[EFS.3] EFS 接入点应强制使用根目录

相关要求： NIST.800-53.r5 AC-6(10)

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::EFS::AccessPoint`

AWS Config 规则：efs-access-point-enforce-root-directory

计划类型：已触发变更

参数：无

此控件检查 Amazon EFS 接入点是否配置为强制使用根目录。如果的 `Path` 值设置为 `/`（文件系统的默认根目录），则控制失败。

在强制执行根目录时，使用接入点的 NFS 客户端使用在接入点上配置的根目录，而不是文件系统的根目录。强制接入点使用根目录可确保接入点的用户只能访问指定子目录的文件，从而有助于限制数据访问。

修复

有关如何为 Amazon EFS 接入点强制使用根目录的说明，请参阅 Amazon Elastic File System 用户指南中的使用接入点强制使用根目录。

[EFS.4] EFS 接入点应强制使用用户身份

相关要求： NIST.800-53.r5 AC-6(2)，PCI DSS v4.0。 1/7.3.1

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::EFS::AccessPoint`

AWS Config 规则：efs-access-point-enforce-user-identity

计划类型：已触发变更

参数：无

此控件检查 Amazon EFS 接入点是否配置为强制执行用户身份。如果在创建 EFS 接入点时未定义 POSIX 用户身份，则此控制失败。

Amazon EFS 接入点是 EFS 文件系统中特定于应用程序的入口点，便于轻松地管理应用程序对共享数据集的访问。接入点可以为通过接入点发出的所有文件系统请求强制执行用户身份（包括用户的

POSIX 组）。接入点还可以为文件系统强制执行不同的根目录，以便客户端只能访问指定目录或其子目录中的数据。

修复

要强制执行 Amazon EFS 接入点的用户身份，请参阅 Amazon Elastic File System 用户指南中的使用接入点强制使用用户身份。

[EFS.5] 应标记 EFS 接入点

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EFS::AccessPoint`

AWS Config规则:`tagged-efs-accesspoint`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EFS 接入点是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果接入点没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果接入点未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些

ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EFS 接入点添加标签，请参阅《Amazon Elastic File System User Guide》中的 Tagging Amazon EFS resources。

[EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联

类别：保护 > 网络安全 > 不公开访问的资源

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：efs-mount-target-public-accessible

计划类型：定期

参数：无

此控件检查 Amazon EFS 挂载目标是否与启动时分配公有 IP 地址的子网关联。如果挂载目标与在启动时分配公共 IP 地址的子网相关联，则该控件会失败。

子网具有决定在子网中创建的网络接口是否自动接收公有 IP 地址的属性。对于 IPv4，默认子网和`FALSE`非默认子网的`MapPublicIpOnLaunch`属性均设置为（通过 EC2 启动实例向导创建的非默认子网除外，该向导设置为）。`TRUE` `TRUE`对于 IPv6，默认情况下，所有子网`FALSE`的`AssignIpv6AddressOnCreation`属性都设置为。

虽然无法为 Amazon EFS 挂载目标分配公有 IPv4 地址，但将其放置在配置为在启动时分配公有 IP 地址的子网中，表明在这类可能挂载 EFS 文件系统的子网中启动的共置实例可以自动接收公有 IP 地址，这可能会使具有公共地址的主机无法访问文件系统数据。

启用自动分配公有 IPv6 地址的子网中的挂载目标可以接收全球可路由的 IPv6 地址。

修复

要将现有挂载目标与不同的子网关联，您必须在启动时不分配公共 IP 地址的子网中创建一个新的挂载目标，然后移除旧的挂载目标。有关安全组和挂载目标的信息，请参阅《Amazon Elastic File System User Guide》中的 Creating and managing mount targets and security groups。

[EFS.7] EFS 文件系统应启用自动备份

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：efs-automatic-backups-enabled

计划类型：已触发变更

参数：无

此控件可检查 Amazon EFS 文件系统是否已启用自动备份。如果 EFS 文件系统未启用自动备份，则此控件将失败。

数据备份是系统、配置或应用程序数据的副本，与原始数据分开存储。启用定期备份有助于保护宝贵的数据免受系统故障、网络攻击或意外删除等不可预见事件的影响。拥有强大的备份策略还有助于更快地恢复、保持业务连续性，即使面对潜在的数据丢失也能倍感安心。

修复

有关用 AWS Backup 于 EFS 文件系统的信息，请参阅 Amazon Elastic File System 用户指南中的备份 EFS 文件系统。

[EFS.8] 应对 EFS 文件系统进行静态加密

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.3.1

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：efs-filesystem-ct-encrypted

计划类型：已触发变更

参数：无

此控件检查 Amazon EFS 文件系统是否使用 AWS Key Management Service (AWS KMS) 加密数据。如果文件系统未加密，则此控件将失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要为新的 EFS 文件系统启用静态加密，请参阅《Amazon Elastic File System User Guide》中的 Encrypting data at rest。

适用于亚马逊 EKS 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件用于评估亚马逊 Elastic Kubernetes 服务（亚马逊 EKS）服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EKS.1] EKS 集群终端节点不应公开访问

相关要求： 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、(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。 1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：eks-endpoint-no-public-access

计划类型：定期

参数：无

此控件检查 Amazon EKS 集群端点是否公开访问。如果 EKS 集群具有公开访问的端点，则控制失败。

当您创建新集群时，Amazon EKS 会为您用来与集群通信的托管 Kubernetes API 服务器创建一个端点。默认情况下，此 API 服务器端点可在 Internet 上公开使用。使用 (IAM) 和原生 Kubernetes 基于角色的访问控制 AWS Identity and Access Management (RBAC) 的组合来保护对 API 服务器的访问。通过移除对端点的公共访问权限，您可以避免意外暴露和访问集群。

修复

要修改现有 EKS 集群的端点访问权限，请参阅 Amazon EKS 用户指南中的修改集群端点访问权限。您可以在创建新 EKS 集群时为其设置端点访问权限。有关创建新 Amazon EKS 集群的说明，请参阅 Amazon EKS 用户指南中的创建 Amazon EKS 集群。

[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行

相关要求： 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)、(4)、 NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5)、PCI DSS v4.0。1/12.3.4

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：eks-cluster-supported-version

计划类型：已触发变更

参数：

- `oldestVersionSupported`：`1.33`（不可自定义）

此控件检查亚马逊 Elastic Kubernetes Service（Amazon EKS）集群是否在支持标准的 Kubernetes 版本上运行。如果 Amazon EKS 集群在不受支持的版本或扩展支持版本上运行，则控制失败。

如果您的应用程序不需要特定版本的 Kubernetes，我们建议您为集群使用 EKS 支持的最新可用 Kubernetes 版本。有关更多信息，请参阅《Amazon EKS 用户指南》中的 Amazon EKS Kubernetes 发布日历和了解 Amazon EKS 上的 Kubernetes 版本生命周期。

修复

要更新 EKS 集群，请参阅《Amazon EKS 用户指南》中的将现有集群更新到新的 Kubernetes 版本。

[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

相关要求： 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。 1/8.3.2

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：eks-cluster-secrets-encrypted

计划类型：定期

参数：无

此控件可检查 Amazon EKS 集群是否使用了加密的 Kubernetes 密钥。如果集群的 Kubernetes 密钥未加密，则此控件将失败。

加密密钥时，可以使用 AWS Key Management Service (AWS KMS) 密钥为集群提供存储在 etcd 中的 Kubernetes 密钥的信封加密。这种加密是对 EBS 卷加密的补充，默认情况下，对作为 EKS 集群的一部分存储在 etcd 中的所有数据（包括密钥）启用该加密。对 EKS 集群使用密钥加密，您就可以使用您定义和管理的 KMS 密钥对 Kubernetes 密钥进行加密，从而为 Kubernetes 应用程序部署深度防御策略。

> **Note**
>
> 该控件将在2026年8月10日之后停用，并从所有适用的Security Hub CSPM标准中删除。从 Kubernetes 版本 1.28 开始，Amazon EKS 集群默认使用信封加密保护 Kubernetes 机密。

修复

要在 EKS 集群上启用密钥加密，请参阅《Amazon EKS 用户指南》中的在现有集群上启用密钥加密。

[EKS.6] 应标记 EKS 集群

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EKS::Cluster`

AWS Config 规则:`tagged-eks-cluster`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EKS 集群是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果集群没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果集群未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EKS 集群添加标签，请参阅《Amazon EKS 用户指南》中的标记 Amazon EKS 资源。

[EKS.7] 应标记 EKS 身份提供商配置

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EKS::IdentityProviderConfig

AWS Config 规则:tagged-eks-identityproviderconfig（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon EKS 身份提供商配置是否具有带特定键的标签，这些键在 requiredTagKeys 参数中进行定义。如果配置没有任何标签键或未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签键，如果配置未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EKS 身份提供商配置添加标签，请参阅《Amazon EKS 用户指南》中的标记 Amazon EKS 资源。

[EKS.8] EKS 集群应启用审核日志

相关要求： NIST.800-53.r5 AC-2(12)、 NIST.800-53.r5 AC-2 (4)、(26)、 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (9)、、、、 NIST.800-53.r5 AU-10、(3) NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6 (4)、 NIST.800-53.r5 AU-6 (7)、、 NIST.800-53.r5 AU-9 (9)、(8) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (20)、 NIST.800-53.r5 SI-3 (8)、 NIST.800-53.r5 SI-4 (20) NIST.800-53.r5 SI-4、 NIST.800-53.r5 SI-7 (8)、PCI DSS v4.0。 1/10.2.1

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：eks-cluster-log-enabled

计划类型：已触发变更

参数：

- `logTypes: audit`（不可自定义）

此控件检查 Amazon EKS 集群是否启用了审核日志记录。如果没有为集群启用审核日志记录，则控制失败。

> **Note**
>
> 此控件不会检查是否通过 Amazon Security Lake 为 AWS 账户启用了 Amazon EKS 审计日志记录。

EKS 控制平面日志将审计和诊断日志直接从 EKS 控制平面提供给您账户中的 Amazon CloudWatch Logs。您可以选择所需的日志类型，日志将作为日志流发送到中每个 EKS 集群的群组 CloudWatch。

通过日志记录，可以了解 EKS 集群的访问情况和性能。通过将 EKS 集群的 EKS 控制平面 CloudWatch 日志发送到 Logs，您可以在中心位置记录用于审计和诊断目的的操作。

修复

要为您的 EKS 集群启用审核日志，请参阅《Amazon EKS 用户指南》中的启用和禁用控制面板日志。

[EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::EKS::Nodegroup`

AWS Config 规则：eks-nodegroup-supported-version-check

计划类型：已触发变更

参数：

- `oldestVersionSupported`：`1.33`（不可自定义）

此控件检查 Amazon EKS 节点组是否在支持标准的 Kubernetes 版本上运行。如果 Amazon EKS 节点组在不受支持的版本或扩展支持版本上运行，则控制失败。

在不受支持的 Kubernetes 版本上运行 EKS 节点组意味着这些节点不再收到来自的安全补丁、错误修复或兼容性更新。 AWS不支持的版本可能包含已知漏洞，这些漏洞已在新版本中得到解决，并且它们可能会遇到与 Kubernetes 生态系统中更新的 AWS 服务容器镜像和第三方工具的兼容性问题。如果您的应用程序不需要特定版本的 Kubernetes，我们建议您为节点组使用 Amazon EKS 支持的最新可用的 Kubernetes 版本。有关更多信息，请参阅 Amazon EKS Kubernetes 发布日历和《亚马逊 EKS 用户指南》中的 “了解节点更新的每个阶段”。

修复

要更新 EKS 节点组，请参阅 Amazon EKS 用户指南中的更新集群的托管节点组。

Security Hub CSPM 控件适用于 ElastiCache

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon ElastiCache 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份

相关要求： 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)

类别：恢复 > 弹性 > 启用备份

严重性：高

资源类型：`AWS::ElastiCache::CacheCluster`、`AWS:ElastiCache:ReplicationGroup`

AWS Config 规则：elasticache-redis-cluster-automatic-backup-check

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`snapshotRetentionPeriod`	最短快照保留期（以天为单位）	整数	1 到 35	1

此控件评估亚马逊 ElastiCache （Redis OSS）集群是否启用了自动备份。如果 Redis OSS 集群的 `SnapshotRetentionLimit` 小于指定时间段，则该控件会失败。除非您为快照保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 1 天。

ElastiCache （Redis OSS）集群可以备份其数据。可以使用备份还原集群或为新集群做种。备份包含集群的元数据以及集群中的所有数据。所有备份都写入 Amazon S3，后者提供持久性存储。您可以通过创建新 ElastiCache 集群并在其中填充备份中的数据来恢复数据。您可以使用 AWS 管理控制台 AWS CLI、和 ElastiCache API 管理备份。

> **Note**
>
> 此控件还会评估 ElastiCache （Redis OSS 和 Valkey）复制组。

修复

有关为 ElastiCache 集群安排自动备份的信息，请参阅 Amazon ElastiCache 用户指南中的安排自动备份。

[ElastiCache.2] ElastiCache 集群应启用自动次要版本升级

相关要求：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

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::ElastiCache::CacheCluster`

AWS Config 规则：elasticache-auto-minor-version-upgrade-check

计划类型：定期

参数：无

此控件用于评估 Amazon 是否 ElastiCache 自动对缓存集群应用次要版本升级。如果缓存集群未自动应用次要版本升级，则此控件会失败。

> **Note**
>
> 此控件不适用于 ElastiCache Memcached 集群。

自动次要版本升级是您可以在 Amazon 中启用的一项功能，以便在新的次 ElastiCache 要缓存引擎版本可用时自动升级您的缓存集群。这些升级可能包括安全补丁和错误修复。继续 up-to-date安装补丁是保护系统的重要一步。

修复

要自动对现有 ElastiCache 缓存集群应用次要版本升级，请参阅 Amazon ElastiCache 用户指南 ElastiCache中的版本管理。

[ElastiCache.3] ElastiCache 复制组应启用自动故障切换

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::ElastiCache::ReplicationGroup

AWS Config 规则：elasticache-repl-grp-auto-failover-enabled

计划类型：定期

参数：无

此控件检查 ElastiCache 复制组是否启用了自动故障转移。如果未为复制组启用自动失效转移，则此控件会失败。

为复制组启用自动失效转移后，主节点的角色将自动将失效转移到其中一个只读副本。此失效转移和副本升级可确保您可以在升级完成后恢复写入新的主数据库，从而减少发生故障时的总体停机时间。

修复

要为现有 ElastiCache 复制组启用自动故障转移，请参阅 Amazon ElastiCache 用户指南中的修改 ElastiCache 集群。如果您使用 ElastiCache 控制台，请将自动故障转移设置为启用。

[ElastiCache.4] ElastiCache 复制组应进行静态加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：AWS::ElastiCache::ReplicationGroup

AWS Config 规则：elasticache-repl-grp-encrypted-at-rest

计划类型：定期

参数：无

此控件检查 ElastiCache 复制组是否处于静态加密状态。如果未对复制组进行静态加密，则此控件会失败。

对静态数据进行加密可降低未经身份验证的用户访问存储在磁盘上的数据的风险。 ElastiCache（Redis OSS）复制组应进行静态加密，以增加安全性。

修复

要在 ElastiCache 复制组上配置静态加密，请参阅 A mazon ElastiCache 用户指南中的启用静态加密。

[ElastiCache.5] ElastiCache 复制组在传输过程中应加密

相关要求： NIST.800-53.r5 AC-17 (2)、、(1) NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-12 NIST.800-53.r5 IA-5 (3)、3、3 (3)、(NIST.800-53.r5 SC-13)、 NIST.800-53.r5 SC-2 (4)、NIST.800-53.r5 SC-2 (1)、 NIST.800-53.r5 SC-7 (2)、nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 规则：elasticache-repl-grp-encrypted-in-transit

计划类型：定期

参数：无

此控件检查 ElastiCache 复制组在传输过程中是否已加密。如果未在传输过程中加密复制组，则此控件会失败。

对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。在 ElastiCache 复制组上启用传输中的加密可在数据从一个位置移动到另一个位置时对其进行加密，例如在集群中的节点之间或集群与应用程序之间。

修复

要在 ElastiCache 复制组上配置传输中加密，请参阅 A mazon ElastiCache 用户指南中的启用传输中加密。

[ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证

相关要求： NIST.800-53.r5 AC-2(1)、(15) NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (7)、 NIST.800-53.r5 AC-6、PCI DSS v4.0.1/8.3.1

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 规则：elasticache-repl-grp-redis-auth-enabled

计划类型：定期

参数：无

此控件检查 ElastiCache （Redis OSS）复制组是否启用了 Redis OSS 身份验证。如果复制组节点的 Redis OSS 版本低于 6.0 且未使用 `AuthToken`，则此控件将失败。

当您使用 Redis 身份验证令牌或密码时，Redis 在允许客户端运行命令之前需要密码，这提高了数据安全性。对于Redis 6.0及更高版本，我们建议使用基于角色的访问控制（RBAC）。由于 6.0 之前的 Redis 版本不支持 RBAC，因此此控件仅评估无法使用 RBAC 功能的版本。

修复

要在 ElastiCache （Redis OSS）复制组上使用 Redis 身份验证，请参阅亚马逊用户指南中的修改现有 ElastiCache （Redis OSS）集群上的身份验证令牌。 ElastiCache

[ElastiCache.7] ElastiCache 群集不应使用默认子网组

相关要求： 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)

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::ElastiCache::CacheCluster`

AWS Config 规则：elasticache-subnet-group-check

计划类型：定期

参数：无

此控件检查集 ElastiCache 群是否配置了自定义子网组。如果 ElastiCache 群集的值`CacheSubnetGroupName`为该值，则控制失败`default`。

启动 ElastiCache 集群时，如果尚不存在默认子网组，则会创建一个默认子网组。默认组使用来自默认虚拟私有云（VPC）的子网。我们建议使用对集群所在子网以及集群从子网继承的网络进行更严格的限制的自定义子网组。

修复

要为 ElastiCache 集群创建新的子网组，请参阅 Amazon ElastiCache 用户指南中的创建子网组。

Elastic Beanstalk 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估 AWS Elastic Beanstalk 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

相关要求： NIST.800-53.r5 CA-7，nist.800-53.r5 SI-2

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::ElasticBeanstalk::Environment`

AWS Config 规则：`beanstalk-enhanced-health-reporting-enabled`

计划类型：已触发变更

参数：无

此控件可检查 AWS Elastic Beanstalk 环境是否启用了增强型运行状况报告。

Elastic Beanstalk 增强型运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。

Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。支持的亚马逊系统AMIs映像 () 中包含的 Elastic Beanstalk 运行状况代理用于评估环境实例的日志和指标。 EC2

有关更多信息，请参阅 AWS Elastic Beanstalk 开发人员指南中的增强型运行状况报告和监控。

修复

有关如何启用增强型运行状况报告的说明，请参阅 AWS Elastic Beanstalk 开发人员指南中的使用 Elastic Beanstalk 控制台启用增强型运行状况报告。

[ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新

相关要求：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

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::ElasticBeanstalk::Environment`

AWS Config 规则：`elastic-beanstalk-managed-updates-enabled`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`UpdateLevel`	版本更新级别	枚举	`minor`, `patch`	无默认值

此控件检查是否为 Elastic Beanstalk 环境启用了托管平台更新。如果未启用托管平台更新，则控制失败。默认情况下，如果启用了任何类型的平台更新，则控制才会通过。或者，您可以提供自定义参数值以要求特定的更新级别。

启用托管平台更新可确保为环境安装最新的可用平台修补程序、更新和功能。及时安装补丁程序是保护系统安全的重要一步。

修复

要启用托管平台更新，请参阅《AWS Elastic Beanstalk 开发人员指南》中的在托管平台更新下配置托管平台更新。

[ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch

相关要求：PCI DSS v4.0.1/10.4.2

类别：识别 > 日志记录

严重性：高

资源类型：AWS::ElasticBeanstalk::Environment

AWS Config 规则：elastic-beanstalk-logs-to-cloudwatch

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
RetentionInDays	日志事件在到期前保留的天数	枚举	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 , 400, 545, 731, 1827, 3653	无默认值

此控件检查 Elastic Beanstalk 环境是否配置为向日志发送日志。 CloudWatch 如果 Elastic Beanstalk 环境未配置为向日志发送日志，则控制失败。 CloudWatch 或者，如果您希望仅当日志在到期前保留指定天数时控制才通过，则可以为 RetentionInDays 参数提供自定义值。

CloudWatch 帮助您收集和监控应用程序和基础设施资源的各种指标。您还可以使用 CloudWatch 根据特定指标配置警报操作。我们建议将 Elastic Beanstalk 与集成，以提高您的 Ela CloudWatch stic Beanstalk 环境的可见性。Elastic Beanstalk 日志包括 eb-activity.log、来自环境 nginx 或 Apache 代理服务器的访问日志以及特定于环境的日志。

修复

要将 Elastic B CloudWatch eanstalk 与日志集成，请参阅开发者指南中的将实例日志流式传输到 CloudWatch 日志。AWS Elastic Beanstalk

适用于 Elastic Load Balancing 的 Security Hub CSPM 控制

这些 AWS Security Hub CSPM 控件会评估 Elastic Load Balancing 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

相关要求：PCI DSS v3.2.1/2.3、PCI DSS v3.2.1/4.1、 NIST.800-53.r5 AC-1 7 (2)、、(1)、2 (3)、3、3 NIST.800-53.r5 AC-4、 NIST.800-53.r5 IA-5 (3)、(3)、(4)、 NIST.800-53.r5 SC-1 (1)、 NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12)、 NIST.800-53.r5 SC-2 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：检测 > 检测服务

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：alb-http-to-https-redirection-check

计划类型：定期

参数：无

此控件检查是否在应用程序负载均衡器的所有 HTTP 侦听器上配置了 HTTP 到 HTTPS 重定向。如果应用程序负载均衡器的任何 HTTP 侦听器未配置 HTTP 到 HTTPS 重定向，则控制失败。

在开始使用应用程序负载均衡器之前，必须添加一个或多个侦听器。侦听器是使用配置的协议和端口检查连接请求的进程。侦听器支持 HTTP 和 HTTPS 协议。您可以使用 HTTPS 侦听器将加密和解密工作卸载到负载均衡器。要强制传输过程中的加密，您应该使用应用程序负载均衡器的重定向操作，将客户端 HTTP 请求重定向到端口 443 上的 HTTPS 请求。

要了解更多信息，请参阅应用程序负载均衡器用户指南中的应用程序负载均衡器的侦听器。

修复

要将 HTTP 请求重定向到 HTTPS，您必须添加应用程序负载均衡器侦听器规则或编辑现有规则。

有关添加新规则的说明，请参阅 应用程序负载均衡器用户指南中的添加规则。对于协议：端口，选择 HTTP，然后输入 **80**。对于添加操作，选择重定向到，选择 HTTPS，然后输入 **443**。

有关编辑现有规则的说明，请参阅应用程序负载均衡器用户指南中的编辑规则。对于协议：端口，选择 HTTP，然后输入 **80**。对于添加操作，选择重定向到，选择 HTTPS，然后输入 **443**。

[ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager

相关要求： NIST.800-53.r5 AC-17 (2)、、(1) NIST.800-53.r5 AC-4、2 NIST.800-53.r5 IA-5 (3)、3、3 (5)、 NIST.800-53.r5 SC-1 (4)、 NIST.800-53.r5 SC-2 (1)、 NIST.800-53.r5 SC-2 (NIST.800-53.r5

SC-12)、 NIST.800-53.r5 SC-7 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)、nist.800-171.r2 3.13.8 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：elb-acm-certificate-required

计划类型：已触发变更

参数：无

此控件检查 Classic Load Balancer 是否使用 AWS Certificate Manager (ACM) 提供的 HTTPS/SSL 证书。如果配置了 HTTPS/SSL 侦听器的 Classic Load Balancer 不使用 ACM 提供的证书，则控制失败。

要创建证书，您可以使用 ACM 或支持 SSL 和 TLS 协议的工具（例如 OpenSSL）。Security Hub CSPM 建议您使用 ACM 为负载均衡器创建或导入证书。

ACM 与经典负载均衡器集成，以便您可以在负载均衡器上部署证书。您还应该自动续订这些证书。

修复

有关如何将 ACM SSL/TLS 证书与 Classic Load Balancer 关联的信息，请参阅 AWS 知识中心文章如何将 ACM SSL/TLS 证书与经典负载均衡器、应用程序负载均衡器或网络负载均衡器相关联？

[ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止

相关要求： NIST.800-53.r5 AC-17 (2)、、(1)、2 (3) NIST.800-53.r5 AC-4、3、3 NIST.800-53.r5 IA-5 (3)、(3)、(4)、 NIST.800-53.r5 SC-1 (1)、 NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12)、NIST.800-53.r5 SC-2 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8 nist.800-171.r2 3.13.8、nist.800-171.r2 3.13.15、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：elb-tls-https-listeners-only

计划类型：已触发变更

参数：无

此控件检查经典负载均衡器侦听器是使用 HTTPS 还是 TLS 协议配置以进行前端（客户端到负载均衡器）连接。如果经典负载均衡器有侦听器，则该控件适用。如果经典负载均衡器没有配置侦听器，则该控件不会报告任何调查发现。

如果经典负载均衡器侦听器为前端连接配置了 TLS 或 HTTPS，则控制通过。

如果侦听器没有为前端连接配置 TLS 或 HTTPS，则控制失败。

在开始使用负载均衡器之前，必须添加一个或多个侦听器。侦听器是使用配置的协议和端口检查连接请求的进程。监听器可以同时支持 HTTP 和 HTTPS/TLS 协议。您应始终使用 HTTPS 或 TLS 侦听器，以便负载均衡器在传输过程中完成加密和解密工作。

修复

要修复此问题，请更新侦听器以使用 TLS 或 HTTPS 协议。

将所有不合规的监听器更改为听众 TLS/HTTPS

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中的 Load Balancing (负载平衡) 下，选择 Load Balancers (负载均衡器)。
3. 选择您的经典负载均衡器。
4. 在 Listeners 选项卡上，选择 Edit。
5. 对于所有未将负载均衡器协议设置为 HTTPS 或 SSL 的侦听器，将设置变更为 HTTPS 或 SSL。
6. 对于所有修改过的侦听器，在证书选项卡上，选择变更默认值。
7. 对于 ACM 和 IAM 证书，选择一个证书。
8. 选择另存为默认值。
9. 更新所有侦听器后，选择保存。

[ELB.4] 应将应用程序负载均衡器配置为丢弃无效的 http 标头

相关要求： NIST.800-53.r5 SC-7(4)、 NIST.800-53.r5 SC-8 (2)、PCI DSS v4.0.1/6.2.4

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：alb-http-drop-invalid-header-enabled

计划类型：已触发变更

参数：无

此控件可评估应用程序负载均衡器是否配置为丢弃无效的 HTTP 标头。如果 `false` 的值设置为 `routing.http.drop_invalid_header_fields.enabled`，则控制失败。

默认情况下，应用程序负载均衡器未配置为删除无效的 HTTP 标头值。删除这些标头值可以防止 HTTP 不同步攻击。

> **Note**
>
> 如果您的账户启用了 ELB.12，我们建议禁用此控件。有关更多信息，请参阅 [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式。

修复

要修复此问题，将负载均衡器配置为删除无效标头字段。

配置负载均衡器以删除无效标头字段

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择应用程序负载均衡器。
4. 在操作中，选择编辑属性。
5. 在删除无效标题字段下，选择启用。
6. 选择保存。

[ELB.5] 应启用应用程序和经典负载均衡器日志记录

相关要求： NIST.800-53.r5 AC-4(26)、、 NIST.800-53.r5 SC-7 (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 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`、`AWS::ElasticLoadBalancingV2::LoadBal`

AWS Config 规则：elb-logging-enabled

计划类型：已触发变更

参数：无

此控件检查应用程序负载均衡器和传统负载均衡器是否启用了日志记录。如果 `access_logs.s3.enabled` 是 `false`，则控制失败。

Elastic Load Balancing 提供了访问日志，该访问日志可捕获有关发送到负载均衡器的请求的详细信息。每个日志都包含信息（例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应）。您可以使用这些访问日志分析流量模式并解决问题。

要了解更多信息，请参阅 经典负载均衡器用户指南中的经典负载均衡器的访问日志。

修复

要启用访问日志，请参阅 应用程序负载均衡器用户指南中的步骤 3：配置访问日志。

[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：elb-deletion-protection-enabled

计划类型：已触发变更

参数：无

此控件可检查应用程序、网关或网络负载均衡器是否已启用删除保护。如果未配置删除保护，则此控件将失败。

启用删除保护以保护应用程序、网关或网络负载均衡器免遭删除。

修复

为了防止您的负载均衡器被意外删除，您可以启用删除保护。默认情况下，已为负载均衡器禁用删除保护。

如果您为负载均衡器启用删除保护，则必须先禁用删除保护，然后才能删除负载均衡器。

要启用应用程序负载均衡器的删除保护，请参阅《应用程序负载均衡器用户指南》中的删除保护。要启用网关负载均衡器的删除保护，请参阅《User Guide for Gateway Load Balancers》中的 Deletion protection。要启用网络负载均衡器的删除保护，请参阅《网络负载均衡器用户指南》中的删除保护。

[ELB.7] 经典负载均衡器应启用连接耗尽功能

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：恢复 > 弹性

严重性：低

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则:`elb-connection-draining-enabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查经典负载均衡器是否已启用连接耗尽功能。

在经典负载均衡器上启用连接耗尽可确保负载均衡器停止向正在取消注册或运行状况不佳的实例发送请求。它使现有连接保持打开状态。这对于自动扩缩组中的实例特别有用，可确保连接不会突然断开。

修复

要在经典负载均衡器上启用连接耗尽，请参阅经典负载均衡器用户指南中的为经典负载均衡器配置连接耗尽。

[ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

相关要求： NIST.800-53.r5 AC-17 (2)、、(1)、2 (3) NIST.800-53.r5 AC-4、3、3 NIST.800-53.r5 IA-5 (3)、(3)、(4)、 NIST.800-53.r5 SC-1 (1)、 NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12)、NIST.800-53.r5 SC-2 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8 nist.800-171.r2 3.13.8、nist.800-171.r2 3.13.15、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 规则：elb-predefined-security-policy-ssl-check

计划类型：已触发变更

参数：

- predefinedPolicyName：ELBSecurityPolicy-TLS-1-2-2017-01（不可自定义）

此控件可检查您的 Classic Load Balancer HTTPS/SSL 侦听器是否使用预定义的策略ELBSecurityPolicy-TLS-1-2-2017-01。如果 Classic Load Balancer HTTPS/SSL 侦听器不使用ELBSecurityPolicy-TLS-1-2-2017-01，则控制失败。

安全策略是 SSL 协议、密码和服务器顺序首选项选项的组合。预定义策略控制客户端和负载均衡器之间的 SSL 协商期间支持的密码、协议和优先顺序。

使用 ELBSecurityPolicy-TLS-1-2-2017-01 可以帮助您满足要求您禁用特定版本的 SSL 和 TLS 的合规性和安全标准。有关更多信息，请参阅经典负载均衡器用户指南中的经典负载均衡器的预定义 SSL 安全策略。

修复

有关如何在经典负载均衡器上使用预定义安全策略 ELBSecurityPolicy-TLS-1-2-2017-01 的信息，请参阅 经典负载均衡器用户指南中的配置安全设置。

[ELB.9] 经典负载均衡器应启用跨区域负载均衡器

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 规则：elb-cross-zone-load-balancing-enabled

计划类型：已触发变更

参数：无

此控件检查是否为经典负载均衡器 () CLBs 启用了跨区域负载平衡。如果负载均衡未启用跨区负载均衡，则控制失败。

负载均衡器节点仅在其可用区中的注册目标之间分配流量。禁用了跨区域负载均衡后，每个负载均衡器节点会仅在其可用区中的已注册目标之间分配流量。如果可用区中注册的目标数量不同，流量将不会均匀分布，并且与另一区域中的实例相比，一个区域中的实例可能最终会被过度利用。启用跨区域负载均衡后，经典负载均衡器的每个负载均衡器节点都会在所有已启用的可用区中的注册实例之间均匀分配请求。有关详细信息，请参阅弹性负载均衡用户指南中的跨可用区负载均衡。

修复

要在经典负载均衡器中启用跨区域负载均衡，请参阅经典负载均衡器用户指南中的启用跨区域负载均衡。

[ELB.10] 经典负载均衡器应跨越多个可用区

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：clb-multiple-az

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`minAvailabilityZones`	可用区的最小数量	枚举	`2, 3, 4, 5, 6`	`2`

此控件检查 Classic Load Balancer 是否已配置为至少跨越指定数量的可用区 (AZs)。如果 Classic Load Balancer 的跨度不超过指定数量，则控制失败 AZs。除非您为最小数量提供自定义参数值 AZs，否则 Security Hub CSPM 将使用默认值为 2。 AZs

可以将经典负载均衡器设置为跨单个可用区或多个可用区中的 Amazon EC2 实例分发传入请求。如果唯一配置的可用区不可用，则不跨多个可用区的经典负载均衡器无法将流量重定向到另一个可用区中的目标。

修复

要向经典负载均衡器添加可用区，请参阅《经典负载均衡器用户指南》中的为您的经典负载均衡器添加或删除子网。

[ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式

相关要求： NIST.800-53.r5 AC-4(21)、 NIST.800-53.r5 CA-9 (1)、nist.800-53.r5 CM-2、PCI DSS v4.0.1/6.2.4

类别：保护 >数据保护 > 数据完整性

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：alb-desync-mode-check

计划类型：已触发变更

参数：

- `desyncMode`：`defensive, strictest`（不可自定义）

此控件检查应用程序负载均衡器配置了防御模式还是最严格的异步缓解模式。如果应用程序负载均衡器未配置防御或最严格的异步缓解模式，则控制失败。

HTTP Desync 问题可能导致请求走私，并使应用程序容易受到请求队列或缓存中毒的影响。反过来，这些漏洞可能导致凭证填充或执行未经授权的命令。配置了防御性或最严格的异步缓解模式的应用程序负载均衡器可保护应用程序免受 HTTP Desync 可能导致的安全问题的影响。

修复

要更新应用程序负载均衡器的异步缓解模式，请参阅应用程序负载均衡器用户指南中的异步缓解模式。

[ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：elbv2-multiple-az

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`minAvailabilityZones`	可用区的最小数量	枚举	`2, 3, 4, 5, 6`	`2`

此控件检查 Elastic Load Balancer V2（应用程序、网络或网关负载均衡器）是否注册了至少来自指定数量的可用区（AZs）的实例。如果 Elastic Load Balancer V2 中注册的实例数量不超过指定数量，则控制失败。 AZs除非您为最小数量提供自定义参数值 AZs，否则 Security Hub CSPM 将使用默认值为 2。 AZs

弹性负载均衡 在一个或多个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。弹性负载均衡 根据传入流量随时间的变化对负载均衡器进行扩展。建议至少配置两个可用区，以保证服务的可用性，因为当一个可用区不可用时，弹性负载均衡器可以将流量引导到另一个可用区。配置多个可用区将有助于消除应用程序的单点故障。

修复

要向应用程序负载均衡器添加可用区，请参阅应用程序负载均衡器用户指南中的应用程序负载均衡器的可用区。要向网络负载均衡器添加可用区，请参阅网络负载均衡器用户指南中的网络负载均衡器。要向网关负载均衡器添加可用区，请参阅网关负载均衡器用户指南中的创建网关负载均衡器。

[ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式

相关要求： NIST.800-53.r5 AC-4(21)、 NIST.800-53.r5 CA-9 (1)、nist.800-53.r5 CM-2、PCI DSS v4.0.1/6.2.4

类别：保护 >数据保护 > 数据完整性

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：clb-desync-mode-check

计划类型：已触发变更

参数：

- `desyncMode`：`defensive, strictest`（不可自定义）

此控件检查经典负载均衡器是配置了防御模式还是最严格的异步缓解模式。如果经典负载均衡器未配置防御或最严格的异步缓解模式，则控制失败。

HTTP Desync 问题可能导致请求走私，并使应用程序容易受到请求队列或缓存中毒的影响。反过来，这些漏洞可能导致凭证劫持或执行未经授权的命令。配置了防御性或最严格的异步缓解模式的经典负载均衡器可保护应用程序免受 HTTP Desync 可能导致的安全问题的影响。

修复

要更新经典负载均衡器上的异步缓解模式，请参阅经典负载均衡器用户指南中的修改异步缓解模式。

[ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF

相关要求： NIST.800-53.r5 AC-4(21)

类别：保护 > 防护服务

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：alb-waf-enabled

计划类型：已触发变更

参数：无

此控件检查 Application Load Balancer 是与 AWS WAF 经典访问控制列表（AWS WAF Web ACL）关联还是与 Web 访问控制列表 (Web ACL) 关联。如果 AWS WAF 配置`Enabled`字段设置为，则控件将失败`false`。

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 APIs 免受攻击。使用 AWS WAF，您可以配置 Web ACL，这是一组基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求的规则。我们建议将 Application Load Balancer 与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。

修复

要将 Application Load Balancer 与 Web ACL 关联，请参阅开发者指南中的将网页 ACL 与 AWS 资源关联或取消关联。AWS WAF

[ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略

相关要求： NIST.800-53.r5 AC-17 (2)、、 NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-1 2 (3)、3、3（NIST.800-53.r5 SC-13)、（NIST.800-53.r5 SC-23)、NIST.800-53.r5 SC-2 (4)、(1)、 NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8、 NIST.800-53.r5 SC-8 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::Listener`

AWS Config 规则：elbv2-predefined-security-policy-ssl-check

计划类型：已触发变更

参数：`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`（不可自定义）

此控件检查应用程序负载均衡器的 HTTPS 侦听器或网络负载均衡器的 TLS 侦听器是否配置为使用推荐的安全策略对传输中数据进行加密。如果负载均衡器的 HTTPS 或 TLS 侦听器未配置为使用推荐的安全策略，则该控件会失败。

Elastic Load Balancing 使用 SSL 协商配置（称为安全策略）来协商客户端和负载均衡器之间的连接。安全策略指定协议和密码的组合。协议会在客户端和服务器之间建立安全连接。密码是使用加密密钥创建编码消息的加密算法。在 连接协商过程中，客户端和负载均衡器会按首选项顺序提供各自支持的密码和协议的列表。使用推荐的负载均衡器安全策略可以帮助您满足合规性和安全标准。

修复

有关推荐的安全策略以及如何更新侦听器的信息，请参阅《Elastic Load Balancing 用户指南》的以下部分：Security policies for Application Load Balancers、Security policies for Network Load Balancers、为您的应用程序负载均衡器更新 HTTPS 侦听器和更新网络负载均衡器的侦听器。

[ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::Listener`

AWS Config 规则：elbv2-listener-encryption-in-transit

计划类型：已触发变更

参数：无

此控件检查应用程序负载均衡器或网络负载均衡器的侦听器是否配置为使用安全协议对传输中数据进行加密。如果应用程序负载均衡器侦听器未配置为使用 HTTPS 协议，或者网络负载均衡器侦听器未配置为使用 TLS 协议，则该控件会失败。

要加密客户端和负载均衡器之间传输的数据，应将 Elastic Load Balancer 侦听器配置为使用行业标准的安全协议：应用程序负载均衡器的 HTTPS 或网络负载均衡器的 TLS。否则，客户端和负载均衡器之间传输的数据容易遭遇拦截、篡改和未经授权访问。侦听器使用 HTTPS 或 TLS 符合安全最佳实践，有助于确保数据在传输过程中的机密性和完整性。对于处理敏感信息或必须遵循安全标准（要求对传输中数据进行加密）的应用程序，这尤为重要。

修复

有关配置侦听器安全协议的信息，请参阅《Elastic Load Balancing 用户指南》的以下部分：为应用程序负载均衡器创建 HTTPS 侦听器和为网络负载均衡器创建侦听器。

[ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config 规则：elbv2-targetgroup-healthcheck-protocol-encrypted

计划类型：已触发变更

参数：无

此控件检查应用程序和网络负载均衡器运行状况检查的目标组是否使用加密的传输协议。如果运行状况检查协议不使用 HTTPS，则控制失败。此控件不适用于 Lambda 目标类型。

负载均衡器向注册目标发送运行状况检查请求，以确定其状态并相应地路由流量。目标组配置中指定的运行状况检查协议决定了这些检查的执行方式。当运行状况检查协议使用未加密的通信（例如 HTTP）时，请求和响应可能会在传输过程中被拦截或操纵。这使攻击者能够深入了解基础设施配置、篡改运行状况检查结果或进行影响路由决策的 man-in-the-middle攻击。使用 HTTPS 进行运行状况检查可在负载均衡器与其目标之间提供加密通信，从而保护健康状态信息的完整性和机密性。

修复

要为应用程序负载均衡器目标组配置加密运行状况检查，请参阅《Ela stic Load Balancing 用户指南》中的 “更新应用程序负载均衡器目标组的运行状况检查设置”。要为您的网络负载均衡器目标组配置加密运行状况检查，请参阅《Ela stic Load Balancing 用户指南》中的 “更新网络负载均衡器目标组的运行状况检查设置”。

[ELB.22] ELB 目标组应使用加密的传输协议

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config 规则：elbv2-targetgroup-protocol-encrypted

计划类型：已触发变更

参数：无

此控件检查 Elastic Load Balancing 目标组是否使用加密的传输协议。此控制不适用于目标类型为 Lambda 或 ALB 的目标群体，也不适用于使用 GENEVE 协议的目标群体。如果目标组不使用 HTTPS、TLS 或 QUIC 协议，则控制失败。

对传输中的数据进行加密可保护其免遭未经授权的用户拦截。使用未加密协议（HTTP、TCP、UDP）的目标组在传输数据时不加密，因此容易被窃听。使用加密协议（HTTPS、TLS、QUIC）可确保负载均衡器和目标之间传输的数据受到保护。

修复

要使用加密协议，必须使用 HTTPS、TLS 或 QUIC 协议创建新的目标组。目标组协议创建后无法修改。要创建应用程序负载均衡器目标组，请参阅《El a stic Load Balancing 用户指南》中的为应用程序负载均衡器创建目标组。要创建网络负载均衡器目标组，请参阅《El a stic Load Balancing 用户指南》中的为网络负载均衡器创建目标组。

适用于弹性搜索的 Security Hub CSPM

这些 AWS Security Hub CSPM 控件用于评估 Elasticsearch 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ES.1] Elasticsearch 域应启用静态加密

相关要求：PCI DSS v3.2。 1/3.4、 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-encrypted-at-rest`

计划类型：定期

参数：无

此控件检查 Elasticsearch 域是否启用静态加密配置。如果未启用静态加密，检查将失败。

为了在中为您的敏感数据增加一层安全性 OpenSearch，您应将您的数据配置 OpenSearch 为静态加密。Elasticsearch 域提供静态数据加密。该功能 AWS KMS 用于存储和管理您的加密密钥。为了执行加密，它使用带有 256 位密钥的高级加密标准算法（ ）AES-256。

要了解有关静 OpenSearch 态加密的更多信息，请参阅《亚马逊服务开发者指南》中的亚马逊 OpenSearch 服务静态数据加密。 OpenSearch

某些实例类型，例如 `t.small` 和 `t.medium`，不支持静态数据加密。有关详细信息，请参阅《Amazon OpenSearch 服务开发者指南》中的支持的实例类型。

修复

要为新的和现有的 Elasticsearch 域启用静态加密，请参阅《亚马逊 OpenSearch 服务开发者指南》中的启用静态数据加密。

[ES.2] Elasticsearch 域名不应公开访问

相关要求：PCI DSS v3.2。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.2，PCI DSS v3.2。 1/1.3.4，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、 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、（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。 1/1.4.4

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：严重

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-in-vpc-only`

计划类型：定期

参数：无

此控件检查 Elasticsearch 域是否位于 VPC 中。它不会评估 VPC 子网路由配置来确定公共访问。您应确保 Elasticsearch 域未附加到公共子网。请参阅《亚马逊 OpenSearch 服务开发者指南》中的Resource-based政策。您还应该确保根据建议的最佳实践配置了 VPC。请参阅 Amazon VPC 用户指南中的 VPC 安全最佳实践。

部署在 VPC 内的 Elasticsearch 域可以通过私有 AWS 网络与 VPC 资源通信，无需穿越公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。VPC 提供了许多网络控制来保护对

Elasticsearch 域的访问，包括网络 ACL 和安全组。Security Hub CSPM 建议您将公有 Elasticsearch 域迁移到 VPC 以利用这些控制措施。

修复

如果您创建一个具有公有端点的域，则以后无法将其放置在 VPC 中。您必须创建一个新的域，然后迁移数据。反之亦然。如果在 VPC 中创建一个域，则该域不能具有公有端点。您必须创建另一个域或禁用该控制。

请参阅亚马逊 OpenSearch 服务开发者指南中的在 VPC 内启动您的亚马逊 OpenSearch 服务域。

[ES.3] Elasticsearch 域应加密节点之间发送的数据

相关要求： 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 (1) NIST.800-53.r5 SC-8、 NIST.800-53.r5 SC-8 (2)、PCI DSS v4.0。 1/4.2.1

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-node-to-node-encryption-check`

计划类型：已触发变更

参数：无

此控件用于检查 Elasticsearch 域是否已启用节点到节点加密。如果 Elasticsearch 域未启用节点到节点加密，则此控件会失败。如果 Elasticsearch 版本不支持节点到节点加密检查，则此控件还会生成失败的调查发现。

HTTPS（TLS）可用于帮助防止潜在攻击者使用中间人或类似攻击来侦听或操纵网络流量。只能允许通过 HTTPS（TLS）进行加密连接。为 Elasticsearch 域启用节点到节点加密可确保集群内通信在传输过程中加密。

此配置可能会降低性能。在启用此选项之前，您应该了解并测试性能权衡。

修复

有关在新域和现有域上启用节点到节点加密的信息，请参阅 Amazon Service 开发者指南中的启用节点到节点加密。 OpenSearch

[ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志

相关要求： 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-6 (3) NIST.800-53.r5 AU-3、(4)、 NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (8)、 NIST.800-53.r5 SI-3 (20)、(8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-7 (8)

类别：识别 – 日志记录

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-logs-to-cloudwatch`

计划类型：已触发变更

参数：

- `logtype = 'error'`（不可自定义）

此控件检查 Elasticsearch 域是否配置为向日志发送错误日志。 CloudWatch

您应该为 Elasticsearch 域启用错误日志，并将这些日志发送到 CloudWatch 日志以进行保留和响应。域错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

修复

有关如何启用日志发布的信息，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用日志发布（控制台）。

[ES.5] Elasticsearch 域应启用审核日志

相关要求： 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-6 (3) NIST.800-53.r5 AU-3、(4)、 NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (8)、 NIST.800-53.r5 SI-3 (20)、(8)、 NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8)、PCI DSS v4.0。1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则:`elasticsearch-audit-logging-enabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

- `cloudWatchLogsLogGroupArnList`（不可自定义）。Security Hub CSPM 不会填充此参数。Comma-separated 应为审核 CloudWatch 日志配置的日志日志组列表。

  `NON_COMPLIANT`如果未在此参数列表中指定 Elasticsearch 域的 CloudWatch 日志组，则此规则适用。

此控件用于检查 Elasticsearch 域名是否启用了审核日志。如果 Elasticsearch 域未启用审核日志，则此控制失败。

审核日志是高度可定制的。它们允许您跟踪 Elasticsearch 集群上的用户活动，包括身份验证成功和失败、对身份验证的请求 OpenSearch、索引更改以及传入的搜索查询。

修复

有关启用审计日志的详细说明，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用审计日志。

[ES.6] Elasticsearch 域名应至少有三个数据节点

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则:`elasticsearch-data-node-fault-tolerance`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件会检查 Elasticsearch 域是否配置了至少三个数据节点，并且 `zoneAwarenessEnabled` 是 `true`。

一个 Elasticsearch 域至少需要三个数据节点才能实现高可用性和容错能力。部署至少具有三个数据节点的 Elasticsearch 域可以确保在节点发生故障时集群正常运行。

修复

修改 Elasticsearch 域中的数据节点数量

1. 打开亚马逊 OpenSearch 服务控制台，网址为https://console.aws.amazon.com/aos/。
2. 在域下，选择要编辑的域的名称。
3. 选择编辑域。
4. 在数据节点下，将节点数设置为大于或等于 3 的数字。

   对于三个可用区部署，请设置为三的倍数，以确保可用区间的分布均等。
5. 选择提交。

[ES.7] 应将 Elasticsearch 域配置为至少三个专用主节点

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config规则:`elasticsearch-primary-node-fault-tolerance`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件用于检查 Elasticsearch 域是否配置了至少三个专用主节点。如果该域不使用专用主节点，则此控件会失败。如果 Elasticsearch 域有五个专用的主节点，则此控件会通过。但是，为了降低可用性风险，可能没有必要使用三个以上的主节点，并且会导致额外的费用。

一个 Elasticsearch 域至少需要三个专用的主节点才能实现高可用性和容错能力。在 blue/green 部署数据节点期间，专用的主节点资源可能会紧张，因为还有其他节点需要管理。部署至少具有三个专用主节点的 Elasticsearch 域可以确保在节点发生故障时有足够的主节点资源容量和集群运行。

修复

修改 OpenSearch 域中专用主节点的数量

1. 打开亚马逊 OpenSearch 服务控制台，网址为https://console.aws.amazon.com/aos/。
2. 在域下，选择要编辑的域的名称。
3. 选择编辑域。
4. 在专用主节点下，将实例类型设置为所需的实例类型。
5. 将主节点数设置为等于或大于三个。
6. 选择提交。

[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密

相关要求： NIST.800-53.r5 AC-17(2)、 NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4、(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 (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

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则:`elasticsearch-https-required`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件用于检查 Elasticsearch 域端点是否配置为使用最新的 TLS 安全策略。如果 Elasticsearch 域端点未配置为使用最新支持的策略，或者如果未启用 HTTPs，则此控件会失败。当前最新支持的 TLS 安全策略是 `Policy-Min-TLS-1-2-PFS-2023-10`。

可以使用 HTTPS（TLS）帮助防止潜在攻击者使用中间人攻击或类似攻击来窃听或操纵网络流量。只能允许通过 HTTPS（TLS）进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试

应用程序，以了解性能概况和 TLS 的影响。与先前版本的 TLS 相比，TLS 1.2 提供了多项安全增强功能。

修复

要启用 TLS 加密，请使用 UpdateDomainConfig API 操作配置 DomainEndpointOptions 对象。这样会设置 TLSSecurityPolicy。

[ES.9] 应标记 Elasticsearch 域名

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Elasticsearch::Domain

AWS Config 规则:tagged-elasticsearch-domain（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	No default value

此控件用于检查 Elasticsearch 域是否具有带参数 requiredTagKeys 中定义的特定键的标签。如果该域没有任何标签键或未在参数 requiredTagKeys 中指定所有键，则此控件会失败。如果未提供 requiredTagKeys 参数，则此控件仅会检查是否存在标签键，如果该域未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些

ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Elasticsearch 域添加标签，请参阅《亚马逊 OpenSearch 服务开发者指南》中的使用标签。

适用于亚马逊 EMR 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估亚马逊 EMR（以前称为 Amazon Elastic MapReduce）服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v4.0.1/1.4.4、1、（7）、（21）、（21）、（16）、（20），(21)、(3)、(4)、(9) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EMR::Cluster`

AWS Config 规则:emr-master-no-public-ip

计划类型：定期

参数：无

此控件检查 Amazon EMR 集群上的主节点是否具有公有 IP 地址。如果公有 IP 地址与任何主节点实例相关联，则控制失败。

公有 IP 地址是在实例的 `NetworkInterfaces` 配置 `PublicIp` 字段中指定的。此控件仅检查处于 `RUNNING` 或 `WAITING` 状态的 Amazon EMR 集群。

修复

在启动期间，您可以控制是否为默认子网或非默认子网中的实例分配公有 IPv4 地址。默认情况下，默认子网的此属性设置为 `true`。非默认子网的 IPv4 公共寻址属性设置为`false`，除非它是由 Amazon EC2 启动实例向导创建的。在这种情况下，会将属性设置为 `true`。

启动后，您无法手动取消公有 IPv4 地址与您的实例的关联。

要修复失败的发现，您必须在 VPC 中启动一个新集群，该集群的私有子网的 IPv4 公有寻址属性设置为`false`。有关说明，请参阅 Amazon EMR 管理指南中的在 VPC 中启动集群。

[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置

相关要求：PCI DSS v4.0.1/1.4.4、 NIST.800-53.r5 AC-2 1、、 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（11） NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7、 NIST.800-53.r5 SC-7（16）、（20）、 NIST.800-53.r5 SC-7（21）、 NIST.800-53.r5 SC-7（21）、 NIST.800-53.r5 SC-7（3）、 NIST.800-53.r5 SC-7（4）、（9） NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：emr-block-public-access

计划类型：定期

参数：无

此控件会检查您的账户是否配置了 Amazon EMR 屏蔽公共访问权限。如果未启用屏蔽公共访问权限设置或允许除端口 22 之外的任何端口，则控制失败。

如果集群的安全配置允许来自公有 IP 地址的入站流量通过某个端口，Amazon EMR 屏蔽公共访问权限会阻止您在公有子网中启动该集群。当来自您的 AWS 账户 的用户启动集群时，Amazon EMR 会

检查该集群的安全组中的端口规则，并将其与您的入站流量规则进行比较。如果安全组有向公有 IP 地址 IPv4 0.0.0.0/0 或 IPv6 :: /0 开放端口的入站规则，并且这些端口未被指定为账户的例外情况，则 Amazon EMR 不允许用户创建集群。

> **Note**
>
> 默认情况下，阻止公有访问处于启用状态。为了增强账户保护，我们建议您将其保持启用状态。

修复

要为 Amazon EMR 配置屏蔽公共访问权限，请参阅《亚马逊 EMR 管理指南》中的使用 Amazon EMR 阻止公有访问。

[EMR.3] Amazon EMR 安全配置应静态加密

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CP-9 (8)、nist.800-53.r5 SI-12

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::EMR::SecurityConfiguration`

AWS Config 规则：emr-security-configuration-encryption-rest

计划类型：已触发变更

参数：无

此控件检查 Amazon EMR 安全配置是否启用了静态加密。如果安全配置未启用静态加密，则此控件会失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要在 Amazon EMR 安全配置中启用静态加密，请参阅《Amazon EMR 管理指南》中的配置数据加密。

[EMR.4] Amazon EMR 安全配置应在传输过程中加密

相关要求： 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-1 3、 NIST.800-53.r5 SC-2 3、 NIST.800-53.r5 SC-2 3 (3)

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::EMR::SecurityConfiguration`

AWS Config 规则：emr-security-configuration-encryption-transit

计划类型：已触发变更

参数：无

此控件检查 Amazon EMR 安全配置是否启用了传输中加密。如果安全配置未启用传输中加密，则此控件会失败。

传输中数据是指从一个位置移动到另一个位置的数据，例如在集群中的节点之间或在集群和应用程序之间。数据可能通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。

修复

要在 Amazon EMR 安全配置中启用传输中加密，请参阅《Amazon EMR 管理指南》中的配置数据加密。

Security Hub CSPM 控件适用于 EventBridge

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon EventBridge 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EventBridge.2] 应标记 EventBridge 活动总线

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Events::EventBus`

AWS Config 规则:`tagged-events-eventbus`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon EventBridge 事件总线是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果事件总线没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果事件总线未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EventBridge 事件总线添加标签，请参阅《亚马逊 EventBridge 用户指南》中的 Amazon EventBridge 标签。

[EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

相关要求： 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.800-53.r5 AC-5 NIST.800-53.r5 AC-6、PCI DSS v4.0.1/10.3.1

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：低

资源类型：`AWS::Events::EventBus`

AWS Config 规则：custom-eventbus-policy-attached

计划类型：已触发变更

参数：无

此控件会检查 Amazon EventBridge 自定义事件总线是否附加了基于资源的策略。如果自定义事件总线没有基于资源的策略，则此控制失败。

默认情况下， EventBridge 自定义事件总线不附加基于资源的策略。这允许账户中的主体访问事件总线。通过将基于资源的策略附加到事件总线，您可以将对事件总线的访问权限限制为指定账户，也可以有意向另一个账户中的实体授予访问权限。

修复

要将基于资源的策略附加到 EventBridge 自定义事件总线，请参阅《亚马逊 EventBridge 用户指南》EventBridge中的为亚马逊使用基于资源的策略。

[EventBridge.4] EventBridge 全局端点应启用事件复制

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Events::Endpoint`

AWS Config 规则：`global-endpoint-event-replication-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon EventBridge 全局终端节点启用了事件复制。如果未为全局端点启用事件复制，则控制失败。

全球端点有助于使应用程序具有区域容错能力。首先，您为端点分配一个 Amazon Route 53 运行状况检查。启动失效转移时，运行状况检查会报告“不正常”状态。在失效转移启动后的几分钟内，所有自定义事件都将路由到辅助区域的事件总线，并由该事件总线进行处理。使用全局端点时，可以启用事件复制。事件复制使用托管规则将所有自定义事件发送到主区域和次要区域的事件总线。我们建议在设置全局端点时启用事件复制。事件复制可帮助您验证全局端点配置是否正确。需要事件复制才能从失效转移事件中自动恢复。如果您未启用事件复制，则必须手动将 Route 53 运行状况检查重置为“正常”，然后才能将事件重新路由回主区域。

> **Note**
>
> 如果您使用的是自定义事件总线，则需要在每个区域中使用同一个名称和相同账户的自定义偶数总线，这样失效转移才能正常运行。启用事件复制可能会增加月度成本。有关定价的信息，请参阅 Amazon EventBridge 定价。

修复

要为 EventBridge 全局终端节点启用事件复制，请参阅 Amazon EventBridge 用户指南中的创建全局终端节点。对于事件复制，请选择启用事件复制。

适用于 Amazon Fraud Detector 的 Security Hub CSPM 控件

这些 Security Hub CSPM 控件用于评估 Amazon Fraud Detector 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FraudDetector::EntityType`

AWS Config 规则：`frauddetector-entity-type-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Fraud Detector 实体类型是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果实体类型没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果实体类型未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

向 Amazon Fraud Detector 实体类型添加标签（控制台）

1. 在 https://console.aws.amazon.com/frauddetector 上打开亚马逊 Fraud Detector 控制台。
2. 在导航窗格中，选择实体。
3. 从列表中选择一个实例类型。

4. 在实体类型标签部分，选择管理标签。
5. 选择添加新标签。输入标签的键和值。针对其他键值对重复此操作。
6. 完成添加标签后，选择保存。

[FraudDetector.2] 应标记 Amazon Fraud Detector 标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FraudDetector::Label`

AWS Config 规则：`frauddetector-label-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Fraud Detector 标签是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果标签没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果标签未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

向 Amazon Fraud Detector 标签添加标签（控制台）

1. 在 https://console.aws.amazon.com/frauddetector 上打开亚马逊 Fraud Detector 控制台。
2. 在导航窗格中，选择标签。
3. 从列表中选择一个标签。
4. 在标签标记部分，选择管理标签。
5. 选择添加新标签。输入标签的键和值。针对其他键值对重复此操作。
6. 完成添加标签后，选择保存。

[FraudDetector.3] 应标记 Amazon Fraud Detector 的结果

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FraudDetector::Outcome`

AWS Config 规则：`frauddetector-outcome-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Fraud Detector 结果是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果结果没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果结果未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

向 Amazon Fraud Detector 结果添加标签（控制台）

1. 在 https://console.aws.amazon.com/frauddetector 上打开亚马逊 Fraud Detector 控制台。
2. 在导航窗格中，选择结果。
3. 从列表中选择一个结果。
4. 在结果标签部分，选择管理标签。
5. 选择添加新标签。输入标签的键和值。针对其他键值对重复此操作。
6. 完成添加标签后，选择保存。

[FraudDetector.4] 应标记 Amazon Fraud Detector 变量

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FraudDetector::Variable`

AWS Config 规则：`frauddetector-variable-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Fraud Detector 变量是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果变量没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件会失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果变量未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

向 Amazon Fraud Detector 变量添加标签（控制台）

1. 在 https://console.aws.amazon.com/frauddetector 上打开亚马逊 Fraud Detector 控制台。

2. 在导航窗格中，选择变量。
3. 从列表中选择一个变量。
4. 在变量标签部分，选择管理标签。
5. 选择添加新标签。输入标签的键和值。针对其他键值对重复此操作。
6. 完成添加标签后，选择保存。

适用于亚马逊的 Security Hub CSPM 控件 FSx

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon FSx 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：fsx-openzfs-copy-tags-enabled

计划类型：定期

参数：无

此控件检查是否将 Amazon FSx for OpenZFS 文件系统配置为将标签复制到备份和卷。如果 OpenZFS 文件系统未配置为将标签复制到备份和卷，则控制失败。

IT 资产的识别和清点是治理和安全的一个重要方面。标签可帮助您以不同的方式对 AWS 资源进行分类，例如按用途、所有者或环境进行分类。这在您具有很多类型相同的资源时会很有用，因为您可以根据分配给特定资源的标签快速识别该资源。

修复

有关配置适用 FSx 于 OpenZFS 的文件系统以将标签复制到备份和卷的信息，请参阅 A ma FSx zon for OpenZ FS 用户指南中的更新文件系统。

[FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份

相关要求：NIST.800-53.r5 CP-9、NIST.800-53.r5 CM-8

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：fsx-lustre-copy-tags-to-backups

计划类型：定期

参数：无

此控件检查 Amazon f FSx or Lustre 文件系统是否配置为将标签复制到备份和卷。如果 Lustre 文件系统未配置为将标签复制到备份和卷，则此控件将失败。

IT 资产的识别和清点是治理和安全的一个重要方面。标签可帮助您以不同的方式对 AWS 资源进行分类，例如按用途、所有者或环境进行分类。这在您具有很多类型相同的资源时会很有用，因为您可以根据分配给特定资源的标签快速识别该资源。

修复

有关配置 for Lustre 文件系统以将标签复制到备份的信息，请参阅 Amazon FSx for Lustre 用户指南 AWS 账户中的在同一个文件系统中复制备份。 FSx

[FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：fsx-openzfs-deployment-type-check

计划类型：定期

参数：`deploymentTypes: MULTI_AZ_1`（不可自定义）

此控件会检查 Amazon FSx for OpenZFS 文件系统是否配置为使用多可用区（多可用区）部署类型。如果文件系统未配置为使用多可用区部署类型，则该控件会失败。

Amazon FSx for OpenZFS 支持多种文件系统部署类型：多可用区 (HA)、单可用区 (HA) 和单可用区（非 HA）。部署类型提供不同级别的可用性和持久性。多可用区 (HA) 文件系统由一对高可用性 (HA)

文件服务器组成，这些服务器分布在两个可用区 (AZs)。我们建议大多数生产工作负载使用多可用区（HA）部署类型，因为它提供了高可用性和持久性模型。

修复

在创建文件系统时，您可以将 Amazon for OpenZFS 文件系统配置 FSx 为使用多可用区部署类型。您无法更改现有 FSx OpenZFS 文件系统的部署类型。

有关 OpenZFS 文件系统的部署类型和选项的信息，请参阅《亚马逊版 OpenZFS 用户指南》中的 “亚马逊 FSx 适用于 OpenZFS 的可用性和持久性” 和 “管理文件系统资源 FSx ”。 FSx

[FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：fsx-ontap-deployment-type-check

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`deploymentTypes`	要包含在评估中的部署类型列表。如果文件系统未配置为使用列表中指定的部署类型，则该控件会生成 `FAILED` 调查发现。	枚举	`MULTI_AZ_1`，`MULTI_AZ_2`	`MULTI_AZ_1`，`MULTI_AZ_2`

此控件会检查 Amazon FSx f NetApp or ONTAP 文件系统是否配置为使用多可用区（多可用区）部署类型。如果文件系统未配置为使用多可用区部署类型，则该控件会失败。您可以选择执行要包含在评估中的部署类型列表。

Amazon FSx for NetApp ONTAP 支持多种文件系统的部署类型：单可用区 1、单可用区 2、多可用区 1 和多可用区 2。部署类型提供不同级别的可用性和持久性。我们建议大多数生产工作负载使用多可用

区部署类型，因为多可用区部署类型提供了高可用性和持久性模型。多可用区文件系统支持单可用区文件系统的所有可用性与持久性功能。此外，它们的设计目的是即使在可用区（AZ）不可用时也能持续提供数据可用性。

修复

您无法更改现有 Amazon FSx for NetApp ONTAP 文件系统的部署类型。但是，您可以备份数据，然后将其还原到使用多可用区部署类型的新文件系统上。

有关 ONTAP 文件系统的部署类型和选项的信息，请参阅《 FSx 适用于 ONTAP 的用户指南》FSx 中的可用性、持久性和部署选项以及管理文件系统。

[FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：fsx-windows-deployment-type-check

计划类型：定期

参数：`deploymentTypes: MULTI_AZ_1`（不可自定义）

此控件检查是否将 Amazon FSx for Windows 文件服务器文件系统配置为使用多可用区（多可用区）部署类型。如果文件系统未配置为使用多可用区部署类型，则该控件会失败。

Amazon FSx for Windows 文件服务器支持两种文件系统部署类型：单可用区和多可用区。部署类型提供不同级别的可用性和持久性。单可用区文件系统由单个 Windows 文件服务器实例和单个可用区（AZ）内的一组存储卷组成。多可用区文件系统由分布在两个可用区的 Windows 文件服务器的高可用性集群组成。我们建议大多数生产工作负载使用多可用区部署类型，因为它提供了高可用性和持久性模型。

修复

在创建文件系统时，您可以将 Amazon FSx for Windows 文件服务器文件系统配置为使用多可用区部署类型。您无法更改现有 FSx 的 Windows 文件服务器文件系统的部署类型。

有关 Windows 文件服务器文件系统的部署类型和选项的信息，请参阅《亚马逊 Windows 文件服务器用户指南》中的 “可用性和持久性：单可用区和多可用区文件系统” 和 “亚马逊 FSx 版 Windows 文件服务器入门”。 FSx FSx

全球加速器的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估 AWS Global Accelerator 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[GlobalAccelerator.1] 应标记全球加速器加速器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GlobalAccelerator::Accelerator`

AWS Config 规则:`tagged-globalaccelerator-accelerator`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Global Accelerator 加速器是否具有参数中定义的特定键的标签`requiredTagKeys`。如果加速器没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果加速器未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Global Accelerator 全局加速器添加标签，请参阅《AWS Global Accelerator Developer Guide》中的 Tagging in AWS Global Accelerator。

Security Hub CSPM 控件适用于 AWS Glue

这些 AWS Security Hub CSPM 控制措施评估 AWS Glue 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Glue.1] 应该给 AWS Glue 工作加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Glue::Job`

AWS Config 规则:`tagged-glue-job`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Glue 作业是否具有参数中定义的特定键的标签`requiredTagKeys`。如果作业没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供

`requiredTagKeys` 参数，则控件仅检查是否存在标签键，如果作业未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS Glue 作业添加标签，请参阅《AWS Glue 用户指南》AWS Glue中的AWS 标签。

[Glue.3] AWS Glue 机器学习转换应在静态时加密

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Glue::MLTransform`

AWS Config 规则：glue-ml-transform-encrypted-at-rest

计划类型：已触发变更

参数：无

此控件检查 AWS Glue 机器学习转换是否处于静态加密状态。如果未对机器学习转换进行静态加密，则此控件将失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要为 AWS Glue 机器学习转换配置加密，请参阅《AWS Glue 用户指南》中的使用机器学习转换。

[Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue

相关要求： 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)

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::Glue::Job`

AWS Config 规则：glue-spark-job-supported-version

计划类型：已触发变更

参数：`minimumSupportedGlueVersion`：`3.0`（不可自定义）

此控件检查 fo AWS Glue r Spark 作业是否配置为在支持的版本上运行 AWS Glue。如果 Spark 作业配置为在低于最低支持版本的版本上运行 AWS Glue ，则控制失败。

> **Note**
>
> 如果 versi AWS Glue on (`GlueVersion`) 属性不存在或在作业的配置项目 (CI) 中 AWS Glue 为空，则此控件还会为 for Spark 作业生成`FAILED`查找结果。在这种情况下，调查发现包含以下注释：`GlueVersion is null or missing in glueetl job configuration`。要解决此类 `FAILED` 调查发现，请将 `GlueVersion` 属性添加到作业的配置中。有关支持的版本和运行时环境的列表，请参阅《AWS Glue 用户指南》中的 AWS Glue 版本。

在当前版本上运行 AWS Glue Spark 作业 AWS Glue 可以优化性能、安全性以及对最新功能的访问 AWS Glue。它还可以帮助防范安全漏洞。例如，可能会发布新版本以提供安全更新、解决问题或引入新功能。

修复

有关将 Spark 作业迁移到支持的版本的信息 AWS Glue，请参阅《AWS Glue 用户指南》中的 Spark 作业迁移 AWS Glue。

适用于亚马逊的 Security Hub CSPM 控件 GuardDuty

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon GuardDuty 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[GuardDuty.1] GuardDuty 应该启用

相关要求： NIST.800-53.r5 AC-2(12)、、(4)、1 (1)、1 (6)、5 (2) NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7、5 NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3 (8)、(19)、(21)、(21)、(25)、(NIST.800-53.r5 SA-11)、 NIST.800-53.r5 SA-1 (3)、nist.800-53.r5 SI-20、nist.800-53.r NIST.800-53.r5 SA-1 5 SI-3 (8)、nist.800-53.r NIST.800-53.r5 SA-1 5 SI-4、 NIST.800-53.r5 SA-8 nist.800-53.r5 SI-4、 NIST.800-53.r5 SA-8 nist.800-53.r5 SI-4、 NIST.800-53.r5 SA-8 nist.800-53.r5 NIST.800-53.r5 SC-5、 NIST.800-53.r5 SC-5 nist.800-53.r5 SI-3 NIST.800-53.r5 SC-5 (8) 800-53.r5 SI-4 (1)、nist.800-53.r5 SI-4 (13)、nist.800-53.r5 SI-4 (2)、nist.800-53.r5 SI-4 (22)、nist.800-53.r5 SI-4 (25)、nist.800-53.r5 SI-4 (4)、nist.800-53.r5 SI-4 (4)、nist.800-53.r5 SI-4 (4) .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 v3.2.1/11.4，PCI DSS v4.0.1/11.5.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：guardduty-enabled-centralized

计划类型：定期

参数：无

此控件会检查您的 GuardDuty 账户和地区 GuardDuty 是否启用了 Amazon。

强烈建议您在所有支持的 AWS 区域 GuardDuty 中启用。这样 GuardDuty 做可以生成有关未经授权或异常活动的调查结果，即使在您不经常使用的地区也是如此。这还 GuardDuty 允许监控全球 CloudTrail 事件， AWS 服务 例如 IAM。

修复

要启用 GuardDuty，请参阅 Amazon GuardDuty 用户指南 GuardDuty中的入门指南。

[GuardDuty.2] 应给 GuardDuty 过滤器加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GuardDuty::Filter`

AWS Config 规则:`tagged-guardduty-filter`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件会检查 Amazon GuardDuty 筛选条件是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果筛选条件没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果筛选条件未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 GuardDuty 筛选条件添加标签，请参阅 Amazon GuardDuty API 参考TagResource中的。

[GuardDuty.3] GuardDuty IPSets 应该被标记

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GuardDuty::IPSet`

AWS Config 规则:`tagged-guardduty-ipset`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 Amazon 是否 GuardDuty IPSet 具有参数中定义的特定密钥的标签`requiredTagKeys`。如果没有任何标签密钥或参数中没有指定的所有密钥，则控件将失败`requiredTagKeys`。 IPSet 如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果未使用任何密钥进行标记，则该控 IPSet 件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向添加标签 GuardDuty IPSet，请参阅亚马逊 GuardDuty API 参考TagResource中的。

[GuardDuty.4] 应 GuardDuty 标记探测器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则:`tagged-guardduty-detector`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 Amazon GuardDuty 探测器是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果检测器没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果检测器未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 GuardDuty 探测器添加标签，请参阅 Amazon GuardDuty API 参考TagResource中的。

[GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-eks-protection-audit-enabled

计划类型：定期

参数：无

此控件检查 GuardDuty EKS 审核日志监控是否已启用。对于独立账户，如果在账户中禁用 GuardDuty EKS 审核日志监控，则控制失败。在多账户环境中，如果委派的 GuardDuty 管理员账户和所有成员账户未启用 EKS 审核日志监控，则控制失败。

在多账户环境中，该控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。只有授权的管理员才能为组织中的成员账户启用或禁用 EKS 审核日志监控功能。 GuardDuty 成员账户无法通过其账户修改此配置。如果委托的 GuardDuty 管理员有一个已暂停的成员帐户，但未启用 GuardDuty EKS 审核日志监控，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果，授权管理员必须解除这些已暂停账户的 GuardDuty关联。

GuardDuty EKS 审计日志监控可帮助您检测亚马逊 Elastic Kubernetes Service（亚马逊 EKS）集群中潜在的可疑活动。EKS 审计日志监控使用 Kubernetes 审计日志来捕获来自用户、使用 Kubernetes API 的应用程序和控制面板的按时间顺序排列的活动。

修复

要启用 GuardDuty EKS 审计日志监控，请参阅 A mazon GuardDuty 用户指南中的 EKS 审计日志监控。

[GuardDuty.6] 应启用 Lamb GuardDuty da 保护

相关要求：PCI DSS v4.0.1/11.5.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-lambda-protection-enabled

计划类型：定期

参数：无

此控件检查 GuardDuty Lambda 保护是否已启用。对于独立账户，如果在账户中禁用 GuardDuty Lambda 保护，则控制失败。在多账户环境中，如果委托的 GuardDuty 管理员账户和所有成员账户未启用 Lambda Protection，则控制失败。

在多账户环境中，该控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。只有委派的管理员才能为组织中的成员账户启用或禁用 Lambda 保护功能。 GuardDuty 成员账户无法通过其账户修改此配置。如果委托 GuardDuty 管理员有未启用 GuardDuty Lambda Protection 的已暂停成员账户，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果，授权管理员必须解除这些已暂停账户的 GuardDuty关联。

GuardDuty Lambda Protection 可帮助您在 AWS Lambda 函数被调用时识别潜在的安全威胁。启用 Lambda 保护后， GuardDuty 开始监控与中的 Lambda 函数关联的 Lambda 网络活动日志。 AWS 账户当 Lambda 函数被调用并 GuardDuty 识别出表明您的 Lambda 函数中存在潜在恶意代码的可疑网络流量时， GuardDuty 会生成调查结果。

修复

要启用 GuardDuty Lambda 保护，请参阅亚马逊用户指南中的配置 Lambda 保护。 GuardDuty

[GuardDuty.7] 应启用 GuardDuty EKS 运行时监控

相关要求：PCI DSS v4.0.1/11.5.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-eks-protection-runtime-enabled

计划类型：定期

参数：无

此控件检查是否启用了具有自动代理管理功能的 GuardDuty EKS 运行时监控。对于独立账户，如果账户中禁用了带有自动代理管理功能的 GuardDuty EKS 运行时监控，则该控制将失败。在多账户环境中，如果委派的 GuardDuty 管理员账户和所有成员账户都没有启用自动代理管理的 EKS 运行时监控，则控制失败。

在多账户环境中，该控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。只有授权的管理员才能为组织中的成员账户启用或禁用 EKS 运行时监控功能以及自动代理管理。 GuardDuty 成员账户无法通过其账户修改此配置。如果委托的 GuardDuty 管理员有一个已暂停的成员帐户，但未启用 GuardDuty EKS 运行时监控，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果，授权管理员必须解除这些已暂停账户的 GuardDuty关联。

Amazon 中的 EKS Protec GuardDuty tion 提供威胁检测覆盖范围，可帮助您保护 AWS 环境中的 Amazon EKS 集群。EKS 运行时监控使用操作系统级事件来帮助您检测 EKS 集群内的 EKS 节点和容器中的潜在威胁。

修复

要通过自动代理管理启用 EKS 运行时监控，请参阅 Amazon GuardDuty 用户指南中的启用 GuardDuty 运行时监控。

[GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-malware-protection-enabled

计划类型：定期

参数：无

此控件检查是否启用了 GuardDuty 恶意软件防护。对于独立帐户，如果该帐户中禁用了 GuardDuty 恶意软件防护，则该控制将失败。在多账户环境中，如果委派的 GuardDuty 管理员账户和所有成员账户未启用恶意软件防护，则控制失败。

在多账户环境中，该控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。只有授权的管理员才能为组织中的成员帐户启用或禁用恶意软件防护功能。 GuardDuty 成员账户无法通过其账户修改此配置。如果委托的 GuardDuty 管理员有一个已暂停但未启用 GuardDuty 恶意软件防护的成员帐户，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果，授权管理员必须解除这些已暂停账户的GuardDuty关联。

GuardDuty EC2 恶意软件防护通过扫描附加到亚马逊弹性计算云 (Amazon EC2) 实例和容器工作负载的亚马逊弹性区块存储 (Amazon EBS) 卷来帮助您检测恶意软件的潜在存在。恶意软件防护提供扫描选项，您可以在扫描时决定要包含还是排除特定的 EC2 实例和容器工作负载。它还提供了在您的 GuardDuty 账户中保留附加到 EC2 实例或容器工作负载的 EBS 卷快照的选项。只有在发现恶意软件并生成恶意软件防护调查发现时，才会保留快照。

修复

要为 EC2 启用 GuardDuty 恶意软件防护，请参阅 GuardDutyA mazon GuardDuty 用户指南中的配置启动的恶意软件扫描。

[GuardDuty.9] 应启用 GuardDuty RDS 保护

相关要求：PCI DSS v4.0.1/11.5.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-rds-protection-enabled

计划类型：定期

参数：无

此控件检查 GuardDuty RDS 保护是否已启用。对于独立账户，如果账户中禁用 GuardDuty RDS 保护，则控制失败。在多账户环境中，如果委派的 GuardDuty 管理员账户和所有成员账户未启用 RDS 保护，则控制失败。

在多账户环境中，该控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。只有授权的管理员才能为组织中的成员账户启用或禁用 RDS 保护功能。 GuardDuty 成员账户无法通过其账户修改此配置。如果委托的 GuardDuty 管理员有未启用 GuardDuty RDS 保护的已暂停成员账户，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果，授权管理员必须解除这些已暂停账户的 GuardDuty关联。

RDS Protection 可以 GuardDuty 分析和分析 RDS 登录活动，了解您的亚马逊 Aurora 数据库（兼容 Aurora MySQL 的版本和兼容 Aurora PostgreSQL 的版本）是否存在潜在的访问威胁。此功能允许您识别潜在的可疑登录行为。RDS 保护不需要额外的基础设施，其设计初衷即是为了不影响数据库实例的性能。当 RDS Protection 检测到表明您的数据库存在威胁的潜在可疑或异常登录尝试时，GuardDuty 会生成新的调查结果，其中包含有关可能受感染的数据库的详细信息。

修复

要启用 GuardDuty RDS 保护，请参阅 Amazon GuardDuty 用户指南中的 GuardDuty RDS 保护。

[GuardDuty.10] 应启用 GuardDuty S3 保护

相关要求：PCI DSS v4.0.1/11.5.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-s3-protection-enabled

计划类型：定期

参数：无

此控件检查 GuardDuty S3 保护是否已启用。对于独立账户，如果在账户中禁用 GuardDuty S3 保护，则控制失败。在多账户环境中，如果委派的 GuardDuty 管理员账户和所有成员账户未启用 S3 保护，则控制失败。

在多账户环境中，该控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。只有授权的管理员才能为组织中的成员账户启用或禁用 S3 保护功能。 GuardDuty 成员账户无法通过其账户修改此配

置。如果委派的 GuardDuty 管理员有未启用 GuardDuty S3 保护的已暂停成员账户，则此控件会生成FAILED调查结果。要获得PASSED调查结果，授权管理员必须解除这些已暂停账户的 GuardDuty关联。

S3 Protection GuardDuty 允许监控对象级 API 操作，以识别您的亚马逊简单存储服务 (Amazon S3) 存储桶中数据的潜在安全风险。 GuardDuty 通过分析 AWS CloudTrail 管理事件和 S3 数据事件来监控针对您CloudTrail 的 S3 资源的威胁。

修复

要启用 GuardDuty S3 保护，请参阅亚马逊 GuardDuty 用户指南 GuardDuty中的亚马逊 S3 保护。

[GuardDuty.11] 应启用 “ GuardDuty 运行时监控”

类别：检测 > 检测服务

严重性：高

资源类型：AWS::GuardDuty::Detector

AWS Config 规则：guardduty-runtime-monitoring-enabled

计划类型：定期

参数：无

此控件可检查 Amazon 中是否启用了运行时监控 GuardDuty。对于独立帐户，如果为该帐户禁用 GuardDuty 运行时监控，则该控制将失败。在多账户环境中，如果为委派的 GuardDuty 管理员账户和所有成员账户禁用 GuardDuty 运行时监控，则控制失败。

在多账户环境中，只有授权的 GuardDuty 管理员才能为其组织中的账户启用或禁用 GuardDuty 运行时监控。此外，只有 GuardDuty 管理员才能配置和管理 GuardDuty 用于运行时监控组织中帐户的工作 AWS 负载和资源的安全代理。 GuardDuty 成员账户无法为自己的账户启用、配置或禁用运行时监控。

GuardDuty 运行时监控可观察和分析操作系统级别、网络和文件事件，以帮助您检测环境中特定 AWS 工作负载中的潜在威胁。它使用 GuardDuty 安全代理来增加运行时行为的可见性，例如文件访问、进程执行、命令行参数和网络连接。您可以为要监控潜在威胁的每种资源类型（例如 Amazon EKS 集群和 Amazon EC2 实例）启用和管理安全代理。

修复

有关配置和启用 GuardDuty 运行时监控的信息，请参阅 GuardDuty Amazon GuardDuty 用户指南中的 GuardDuty 运行时监控和启用运行时监控。

[GuardDuty.12] 应启用 GuardDuty ECS 运行时监控

类别：检测 > 检测服务

严重性：中

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-ecs-protection-runtime-enabled

计划类型：定期

参数：无

此控件检查是否启用了亚马逊 GuardDuty 自动安全代理，以便对开启的 Amazon ECS 集群进行运行时监控 AWS Fargate。对于独立账户，如果账户禁用了安全代理，则该控件会失败。在多账户环境中，如果为委派的 GuardDuty管理员账户和所有成员账户禁用安全代理，则控制失败。

在多账户环境中，此控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。这是因为只有授权的 GuardDuty 管理员才能为其组织中的账户启用或禁用 ECS-FarGate 资源的运行时监控。 GuardDuty 成员账户无法为自己的账户执行此操作。此外，如果 GuardDuty 成员账户被暂停且成员账户禁用 ECS-Fargate 资源的运行时监控，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果，GuardDuty 管理员必须使用 GuardDuty解除被暂停的成员帐户与其管理员帐户的关联。

GuardDuty 运行时监控可观察和分析操作系统级别、网络和文件事件，以帮助您检测环境中特定 AWS 工作负载中的潜在威胁。它使用 GuardDuty 安全代理来增加运行时行为的可见性，例如文件访问、进程执行、命令行参数和网络连接。您可以为要监控潜在威胁的每种资源类型启用和管理安全代理。这包括 AWS Fargate上的 Amazon ECS 集群。

修复

要启用和管理用于对 ECS-Fargate 资源进行 GuardDuty 运行时监控的安全代理，必须直接使用。GuardDuty 对于 ECS-Fargate 资源，您无法手动启用或管理它。有关启用和管理安全代理的信息，请参阅《亚马逊 GuardDuty 用户指南》中的 AWS Fargate（仅限 Amazon ECS）支持的先决条件和管理自动安全代理 AWS Fargate（仅限 Amazon ECS）。

[GuardDuty.13] 应启用 GuardDuty EC2 运行时监控

类别：检测 > 检测服务

严重性：中

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：guardduty-ec2-protection-runtime-enabled

计划类型：定期

参数：无

此控件检查是否启用了亚马逊 GuardDuty 自动安全代理，以便对 Amazon EC2 实例进行运行时监控。对于独立账户，如果账户禁用了安全代理，则该控件会失败。在多账户环境中，如果为委派的 GuardDuty 管理员账户和所有成员账户禁用安全代理，则控制失败。

在多账户环境中，此控件仅在委派的 GuardDuty 管理员帐户中生成调查结果。这是因为只有授权的 GuardDuty 管理员才能为其组织中的账户启用或禁用 Amazon EC2 实例的运行时监控。 GuardDuty 成员账户无法为自己的账户执行此操作。此外，如果成员账户被暂停，且该成员账户 GuardDuty 的 EC2 实例运行时监控被禁用，则此控件会生成`FAILED`调查结果。要获得`PASSED`调查结果， GuardDuty 管理员必须使用 GuardDuty解除被暂停的成员帐户与其管理员帐户的关联。

GuardDuty 运行时监控可观察和分析操作系统级别、网络和文件事件，以帮助您检测环境中特定 AWS 工作负载中的潜在威胁。它使用 GuardDuty 安全代理来增加运行时行为的可见性，例如文件访问、进程执行、命令行参数和网络连接。您可以为要监控潜在威胁的每种资源类型启用和管理安全代理。这包括 Amazon EC2 实例。

修复

有关配置和管理 EC2 实例 GuardDuty 运行时监控的自动安全代理的信息，请参阅 Amazon GuardDuty 用户指南中的 Amazon EC2 实例支持的先决条件和为 Amazon EC2 实例启用自动安全代理。

Security Hub CSPM 控件适用于 AWS Identity and Access Management

这些 AWS Security Hub CSPM 控制措施评估 AWS Identity and Access Management (IAM) 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[IAM.1] IAM policy 不应允许完整的“*”管理权限

相关要求：独联体 AWS 基金会基准 v1.2.0/1.22、CIS AWS 基金会基准 v1.4.0/1.16、、NIST.800-53.r5 AC-2 (1)、、(15)、(7) NIST.800-53.r5 AC-2、、(10)、(2) NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3 (3)、 NIST.800-53.r5 AC-3 (3)、nist.800-171.r2 3.1.4 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6、 NIST.800-53.r5 AC-6 PCI DSS v3.2.1/7.2.1 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::IAM::Policy`

AWS Config 规则：`iam-policy-no-statements-with-admin-access`

计划类型：已触发变更

参数：

- `excludePermissionBoundaryPolicy: true`（不可自定义）

此控件检查 IAM policy 的默认版本（也称为客户管理型策略）是否具有管理员访问权限，方法是包含一个在 `"Resource": "*"` 上对 `"Effect": "Allow"` 和 `"Action": "*"` 的声明。如果您有带有此类声明的 IAM policy，则控制失败。

该控制仅检查您创建的客户托管策略。它不检查内联策略和 AWS 托管策略。

IAM policy 定义一组授予用户、组或角色的权限。按照标准的安全建议，AWS 建议您授予最低权限，即仅授予执行任务所需的权限。当您提供完全管理权限而不是用户所需的最低权限集时，您会将资源暴给可能有害的操作。

首先确定用户需要执行的任务，然后拟定仅限用户执行这些任务的策略，而不是允许完全管理权限。最开始只授予最低权限，然后根据需要授予其他权限，则样会更加安全。请不要一开始就授予过于宽松的权限而后再尝试收紧权限。

您应该移除包含在 `"Resource": "*"` 上对 `"Effect": "Allow"` 和 `"Action": "*"` 的声明的 IAM policy。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要修改 IAM policy 使其不允许完全的 "*" 管理权限，请参阅 IAM 用户指南中的编辑 IAM policy。

[IAM.2] IAM 用户不应附加 IAM policy

相关要求：独联体 AWS 基金会基准 v5.0.0/1.14、独联体基金会基准 v3.0.0/1.15、CIS AWS 基金会基准 v1.2.0/1.16、、（1）、（15）、（7）、、 NIST.800-53.r5 AC-2（3）、nist.800-171.r2 3.1.1、nist.800-171.r2 3.1.2、nist.800-171.r2 3.1.7、nist.800-171.r2 3.1.7、nist.800-171.r2 3.1.7 NIST.800-53.r5 AC-2、nist.800-171.r2 3.1.7 NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3 nist.800-171.r2 3.1.7、 NIST.800-53.r5 AC-3 nist.800-171.r2 r2 3.3.9 NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6 nist.800-171.r2 3.13.3、PCI AWS DSS v3.2.1/7.2.1

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::IAM::User`

AWS Config 规则：`iam-user-no-policies-check`

计划类型：已触发变更

参数：无

此控件检查 IAM 用户是否附加了策略。如果 IAM 用户附加了策略，则控制失败。相反，IAM 用户必须继承 IAM 组的权限或承担角色。

默认情况下，IAM 用户、群组和角色无权访问 AWS 资源。IAM policy 向用户、组或角色授予权限。我们建议您将 IAM policy 直接应用于组和角色，而不是用户。随着用户数量的增长，在组或角色级别分配权限可降低访问管理的复杂性。降低访问管理的复杂性有助于减少委托人意外收到或保留过多权限的机会。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在单个区域中记录全局资源，则可以在除记录全局资源的区域以外的所有区域中禁用此控件。

修复

要解决此问题，请创建一个 IAM 群组，并将该策略附加到该群组。然后，将用户添加到组中。策略将应用于组中的每一位用户。要删除直接附加到用户的策略，请参阅 IAM 用户指南中的添加和删除 IAM 身份权限。

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

相关要求：独联体 AWS 基金会基准 v5.0.0/1.13、CIS 基金会基准 v3.0.0/1.14、CIS AWS 基金会基准 v1.4.0/1.14、CIS AWS 基金会基准 v1.2.0/1.4、(1)、(3)、(15)、PCI DSS AWS v4.0.1/8.3.9、NIST.800-53.r5 AC-2 PCI DSS v4.0.1/8.6.3 NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`access-keys-rotated`

计划类型：定期

参数：

- `maxAccessKeyAge`：`90`（不可自定义）

该控制检查是否在 90 天内轮换了活动访问密钥。

我们强烈建议您不要在账户中生成和删除所有访问密钥。相反，推荐的最佳做法是创建一个或多个 IAM 角色或通过使用联合 AWS IAM Identity Center。您可以使用这些方法来允许您的用户访问 AWS 管理控制台 和 AWS CLI。

每种方法都有其使用案例。对于拥有现有中心目录或计划需要超过当前 IAM 用户限制的企业来说，联合身份验证通常更好。在 AWS 环境之外运行的应用程序需要访问密钥才能以编程方式访问 AWS 资源。

但是，如果需要编程访问权限的资源在内部运行 AWS，则最佳做法是使用 IAM 角色。通过角色，您可以授予资源访问权限，而无需在配置中硬编码访问密钥 ID 和私有访问密钥。

要了解有关保护访问密钥和帐户的更多信息，请参阅中的管理 AWS 访问密钥的最佳实践AWS 一般参考。另请参阅博客文章《使用编程访问权限 AWS 账户 时保护您的指南》。

如果你已经有了访问密钥，Security Hub CSPM 建议你每 90 天轮换一次访问密钥。轮换访问密钥可减少他人使用遭盗用账户或已终止账户关联的访问密钥的风险。这还可以确保无法使用可能已丢失、遭破解或被盗用的旧密钥访问数据。轮换访问密钥后，始终更新您的应用程序。

访问密钥包含一个访问密钥 ID 和一个私有访问密钥。它们用于签署您向 AWS发出的编程请求。用户需要自己的访问密钥才能 AWS 从 AWS CLI、Windows 工具进行编程调用 PowerShell AWS SDKs，或者使用个人的 API 操作进行直接 HTTP 调用 AWS 服务。

如果您的组织使用 AWS IAM Identity Center （ IAM 身份中心），则您的用户可以登录 Active Directory、内置的 IAM 身份中心目录或其他连接到 IAM 身份中心的身份提供商 (IdP)。然后可以将它们映射到一个 IAM 角色，使他们无需访问密钥即可运行 AWS CLI 命令或调用 AWS API 操作。要了解更多信息，请参阅AWS Command Line Interface 用户指南 AWS IAM Identity Center中的配置 AWS CLI 以使用。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要轮换超过 90 天的访问密钥，请参阅 IAM 用户指南中的轮换访问密钥。对于任何访问密钥有效期超过 90 天的用户，请按照说明进行操作。

[IAM.4] 不应存在 IAM 根用户访问密钥

相关要求：独联体 AWS 基金会基准 v5.0.0/1.3、CIS AWS 基金会基准 v3.0.0/1.4、CIS 基金会基准 v1.4.0/1.4、CIS AWS 基金会基准 v1.2.0/1.12、PCI DSS v3.2.1/2.2、PCI DSS v3.2.1/7.2.1、(1)、(15)、(7)、(10)、(2) AWS NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

类别：保护 > 安全访问管理

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`iam-root-access-key-check`

计划类型：定期

参数：无

此控件检查根用户访问密钥是否存在。

root 用户是中权限最高的用户 AWS 账户。 AWS 访问密钥提供对给定账户的编程访问权限。

Security Hub CSPM 建议您删除与根用户关联的所有访问密钥。这限制了可用于危害您的账户的向量。它还鼓励创建和使用最小权限的基于角色的账户。

修复

要删除根用户访问密钥，请参阅 IAM 用户指南中的删除根用户的访问密钥。要从中删除 root 用户访问密钥 AWS GovCloud (US)，请参阅用户指南 AWS 账户 中的删除我的 AWS GovCloud (US) 账户 root AWS GovCloud (US) 用户访问密钥。

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

相关要求：独联体 AWS 基金会基准 v5.0.0/1.9、CIS AWS 基金会基准 v3.0.0/1.10、CIS 基金会基准 v1.4.0/1.10、CIS AWS 基金会基准 v1.2.0/1.2、(1)、(15)、 NIST.800-53.r5 AC-2 (1)、(2)、(6)、(8)、 NIST.800-53.r5 AC-3 PCI AWS DSS v4.0.1/8.4.2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`mfa-enabled-for-iam-console-access`

计划类型：定期

参数：无

此控件检查是否为所有使用控制台密码的 IAM 用户启用了 AWS 多重身份验证 (MFA)。

多重身份验证（MFA）在用户名和密码之上增加了一层额外的防护。启用 MFA 后，当用户登录 AWS 网站时，系统会提示他们输入用户名和密码。此外，系统还会提示他们从 AWS MFA 设备输入身份验证码。

我们建议为拥有控制台密码的所有账户启用 MFA。MFA 旨在为控制台访问提供更高的安全性。身份验证委托人必须拥有发放具有时效性的密钥的设备，并且必须知道凭证。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要为 IAM 用户添加 MFA，请参阅 IAM 用户指南 中的在 AWS上使用多重身份验证（MFA）。

[IAM.6] 应该为根用户启用硬件 MFA

相关要求：独联体 AWS 基金会基准 v5.0.0/1.5、CIS AWS 基金会基准 v3.0.0/1.6、CIS 基金会基准 v1.4.0/1.6、CIS AWS 基金会基准 v1.2.0/1.14、PCI DSS v3.2.1/8.3.1、(1)、(15)、 NIST.800-53.r5 AC-2 (1)、(2)、(6)、(8)、PCI DSS v4.0.1/8.4.2 AWS NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

类别：保护 > 安全访问管理

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`root-account-hardware-mfa-enabled`

计划类型：定期

参数：无

此控件会检查您 AWS 账户 是否允许使用硬件多因素身份验证 (MFA) 设备使用根用户凭据登录。如果未启用硬件 MFA 或者允许虚拟 MFA 设备使用根用户凭证登录，则该控件会失败。

虚拟 MFA 无法提供与硬件 MFA 设备相同的安全水平。我们建议您仅在等待硬件购买批准或等待硬件到达时使用虚拟 MFA 设备。要了解更多信息，请参阅《IAM 用户指南》中的分配虚拟 MFA 设备（控制台）。

> **Note**
>
> Security Hub CSPM 根据中是否存在根用户凭证（登录配置文件）来评估此控件。 AWS 账户 在以下情况下，控件会生成 PASSED 调查发现：
>
> - 账户中存在根用户凭证，并且为根用户启用了硬件 MFA。
> - 账户中不存在根用户凭证。
>
> 如果账户中存在根用户凭证，并且未为根用户启用硬件 MFA，则该控件会生成 FAILED 调查发现。

修复

有关为根用户启用硬件 MFA 的信息，请参阅《IAM 用户指南》中的 AWS 账户根用户的多重身份验证。

[IAM.7] IAM 用户的密码策略应具有可靠的配置

相关要求： NIST.800-53.r5 AC-2(1)、(3)、(15)、(1)、 NIST.800-53.r5 AC-2 nist.800-171.r2 3.5.2、NIST.800-53.r5 AC-3 nist.800-171.r2 3.5.7、 NIST.800-53.r5 IA-5 nist.800-171.r2 3.5.8、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.3.9 4.0.1/8.3.10.1，PCI DSS v4.0.1/8.6.3

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`RequireUppercaseCharacters`	密码中要求至少包含一个大写字符	布尔值	`true` 或者 `false`	`true`
`RequireLowercaseCharacters`	密码中要求至少包含一个小写字符	布尔值	`true` 或者 `false`	`true`
`RequireSymbols`	密码中要求至少包含一个符号	布尔值	`true` 或者 `false`	`true`
`RequireNumbers`	密码中要求至少包含一个数字	布尔值	`true` 或者 `false`	`true`

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
MinimumPasswordLength	密码中的最少字符数	整数	8 到 128	8
PasswordReusePrevention	在可以重复使用旧密码之前的密码轮换次数	整数	12 到 24	无默认值
MaxPasswordAge	密码到期前的天数	整数	1 到 90	无默认值

此控件检查 IAM 用户的账户密码策略是否使用可靠的配置。如果密码策略未使用可靠配置，则控制失败。除非您提供自定义参数值，否则 Security Hub CSPM 将使用上表中提到的默认值。PasswordReusePrevention和MaxPasswordAge参数没有默认值，因此，如果排除这些参数，Security Hub CSPM 在评估此控件时会忽略密码轮换次数和密码期限。

要访问 AWS 管理控制台，IAM 用户需要密码。作为最佳实践，Security Hub CSPM 强烈建议您使用联合身份验证，而不是创建 IAM 用户。联合身份验证允许用户使用其现有的公司凭证登录 AWS 管理控制台。使用 AWS IAM Identity Center（IAM 身份中心）创建用户或联合用户，然后在账户中担任 IAM 角色。

要了解有关身份提供商和联合身份验证的更多信息，请参阅 IAM 用户指南中的身份提供程序和联合身份验证。要了解有关 IAM Identity Center 的更多信息，请参阅 AWS IAM Identity Center 用户指南。

如果您需要使用 IAM 用户，Security Hub CSPM 建议您强制创建强用户密码。您可以对您的设置密码策略， AWS 账户 以指定密码的复杂性要求和强制轮换周期。创建或更改密码策略时，大多数密码策略设置会在用户下次更改其密码时实施。某些设置会立即强制执行。

修复

要更新密码策略，请参阅《IAM 用户指南》中的为 IAM 用户设置账户密码策略。

[IAM.8] 应移除未使用的 IAM 用户凭证

相关要求：CIS AWS 基金会基准 v1.2.0/1.3、、 NIST.800-53.r5 AC-2 (1)、(3)、(15) NIST.800-53.r5 AC-2、 NIST.800-53.r5 AC-3 (7)、、、 NIST.800-53.r5 AC-2 nist.800-171.r2 3.1.2 NIST.800-53.r5

AC-3、 NIST.800-53.r5 AC-3 PCI DSS v3.2.1/8.1.4、PCI DSS v4.0.1/8.2.6 NIST.800-53.r5 AC-6、PCI DSS v4.0.1/8.2.6

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`iam-user-unused-credentials-check`

计划类型：定期

参数：

- `maxCredentialUsageAge`：`90`（不可自定义）

此控件可检查您的 IAM 用户是否拥有 90 天未使用的密码或有效访问密钥。

IAM 用户可以使用不同类型的证书（例如密码或访问密钥）访问 AWS 资源。

Security Hub CSPM 建议您删除或停用所有在 90 天或更长时间内未使用的证书。禁用或删除不必要的凭证可减少他人使用遭盗用账户或已弃用账户的关联凭证的风险。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

当您在 IAM 控制台中查看用户信息时，会有访问密钥年龄、密码使用期限和上次活动列。如果上述列中的任何一个中的值大于 90 天，请停用这些用户的凭证。

您还可以使用凭证报告来监控用户并识别那些连续 90 天或以上没有活动的用户。您可以从 IAM 控制台下载 `.csv` 格式的凭证报告。

确定非活动账户或未使用的凭证后，将其停用。有关说明，请参阅 IAM 用户指南中的创建、变更或删除 IAM 用户密码（控制台）。

[IAM.9] 应为根用户启用 MFA

相关要求：独联体 AWS 基金会基准 v5.0.0/1.4、PCI DSS v3.2.1/8.3.1、PCI DSS v4.0.1/8.4.2、CIS 基金会基准 v3.0.0/1.5、CIS 基金会基准 v1.4.0/1.5、CIS AWS AWS 基金会基准 v1.2.0/1.13、(1)、(1)、(2)、(6)、(8) AWS NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

类别：保护 > 安全访问管理

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`root-account-mfa-enabled`

计划类型：定期

参数：无

此控件检查是否已为的 IAM 根用户启用多重身份验证 (MFA) AWS 账户 以登录到。 AWS 管理控制台 如果账户的根用户未启用 MFA，则该控件会失败。

的 IAM 根用户可以完全访问账户中的所有服务和资源。 AWS 账户 如果启用了 MFA，则用户必须从其 AWS MFA 设备输入用户名、密码和身份验证码才能登录。 AWS 管理控制台 MFA 在用户名和密码之上增加了一层额外防护。

在以下情况下，此控件会生成 `PASSED` 调查发现：

- 账户中存在根用户凭证，并且为根用户启用了 MFA。
- 账户中不存在根用户凭证。

如果账户中存在根用户凭证，并且未为根用户启用 MFA，则该控件会生成 `FAILED` 调查发现。

修复

有关为的根用户启用 MFA 的信息 AWS 账户，请参阅《用户指南》 AWS 账户根用户中的多重身份验证。AWS Identity and Access Management

[IAM.10] IAM 用户的密码策略应具有很强的配置

相关要求：NIST.800-171.r2 3.5.2、NIST.800-171.r2 3.5.7、NIST.800-171.r2 3.5.8、PCI DSS v3.2.1/8.1.4、PCI DSS v3.2.1/8.2.3、PCI DSS v3.2.1/8.2.4、PCI DSS v3.2.1/8.2.5

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::::Account

AWS Config 规则：iam-password-policy

计划类型：定期

参数：无

此控件检查 IAM 用户的账户密码策略是否使用以下最低 PCI DSS 配置。

- RequireUppercaseCharacters——密码中要求至少包含一个大写字符。（默认值 = true）
- RequireLowercaseCharacters——密码中要求至少包含一个小写字符。（默认值 = true）
- RequireNumbers——密码中要求至少包含一个数字。（默认值 = true）
- MinimumPasswordLength——密码最小长度。（默认值 = 7 或更长）
- PasswordReusePrevention——允许重用前的密码数。（默认值 = 4）
- MaxPasswordAge – 密码到期前的天数。（默认值 = 90）

> **Note**
>
> 2025 年 5 月 30 日，Security Hub CSPM 从 PCI DSS v4.0.1 标准中删除了此控件。PCI DSS v4.0.1 现在要求密码至少包含 8 个字符。此控件继续适用于 PCI DSS v3.2.1 标准，该标准具有不同的密码要求。
>
> 要根据 PCI DSS v4.0.1 要求评估账户密码策略，可以使用 IAM.7 控件。此控件要求密码至少包含 8 个字符。它还对密码长度和其他参数支持自定义值。IAM.7 控件是 Security Hub CSPM 中 PCI DSS v4.0.1 标准的一部分。

修复

要更新您的密码策略以使用推荐的配置，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。

[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母

相关要求：CIS AWS 基金会基准 v1.2.0/1.5、nist.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.6.3

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。

CIS 建议密码策略至少需要一个大写字母。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个拉丁字母表中的大写字母（A–Z）。

[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母

相关要求：CIS AWS 基金会基准 v1.2.0/1.6、nist.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.6.3

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。CIS 建议密码策略要求包含至少一个小写字母。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个拉丁字母表中的小写字母（A–Z）。

[IAM.13] 确保 IAM 密码策略要求包含至少一个符号

相关要求：独联体 AWS 基金会基准 v1.2.0/1.7、nist.800-171.r2 3.5.7

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。

CIS 建议密码策略要求包含至少一个符号。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个非字母数字字符。

[IAM.14] 确保 IAM 密码策略要求包含至少一个数字

相关要求：CIS AWS 基金会基准 v1.2.0/1.8、nist.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.6.3

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。

CIS 建议密码策略要求包含至少一个数字。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个数字。

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

相关要求：独联体 AWS 基金会基准 v5.0.0/1.7、独联体基金会基准 v3.0.0/1.8、独联体 AWS 基金会基准 v1.4.0/1.8、独联体基金会基准 v1.2.0/1.9、nist.800 AWS -171.r2 3.5.7 AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码至少为给定长度。

CIS 建议密码策略要求最短密码长度为 14 个字符。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码最小长度，请输入 **14** 或更大的数字。

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

相关要求：独联体 AWS 基金会基准 v5.0.0/1.8、独联体基金会基准 v3.0.0/1.9、独联体 AWS 基金会基准 v1.4.0/1.9、独联体基金会基准 v1.2.0/1.10、nist.800 AWS -171.r2 3.5.8、PCI DSS v4.0.1/8.3.7 AWS

类别：保护 > 安全访问管理

严重性：低

资源类型：AWS::::Account

AWS Config 规则：iam-password-policy

计划类型：定期

参数：无

此控件检查要记住的密码数量是否设置为 24。如果该值不是 24，则控制失败。

IAM 密码策略可以阻止同一用户重复使用给定密码。

CIS 建议密码策略阻止重复使用密码。阻止重复使用密码可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。在防止密码重复使用中，输入 **24**。

[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效

相关要求：CIS AWS 基金会基准 v1.2.0/1.11、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.10.1

类别：保护 > 安全访问管理

严重性：低

资源类型：AWS::::Account

AWS Config 规则：iam-password-policy

计划类型：定期

参数：无

IAM 密码策略可以要求在给定天数后轮换密码或使密码失效。

CIS 建议密码策略在 90 天或更短时间后使密码失效。缩短密码生存期可提高账户抵抗暴力登录尝试的弹性。在以下情况下，要求定期更改密码也是非常有用的：

- 密码可能会在您不知情的情况下被窃取或泄露。系统遭受攻击、软件漏洞或内部威胁都可能导致发生这种情况。
- 某些公司和政府的 Web 筛选条件或代理服务器能够拦截和记录流量（即使流量已加密）。

- 很多用户对于许多系统（例如工作系统、电子邮件和个人系统）都使用相同的密码。
- 遭受攻击的最终用户工作站可能存在击键记录器。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于开启密码到期，请输入 **90** 或一个较小的数字。

[IAM.18] 确保已创建支持角色来管理事件 AWS 支持

相关要求：独联体 AWS 基金会基准 v5.0.0/1.16、独联体基金会基准 v3.0.0/1.17、独联体基金会基准 v1.4.0/1.17、独联体 AWS 基金会基准 v1.2.0/1.20、nist.800-171.r2 3.1.2、 AWS PCI DSS v4.0.1/12.10.3 AWS

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::::Account`

AWS Config 规则：`iam-policy-in-use`

计划类型：定期

参数：

- `policyARN`：`arn:`*`partition`*`:iam::aws:policy/AWSSupportAccess`（不可自定义）
- `policyUsageType`：`ANY`（不可自定义）

AWS 提供了一个支持中心，可用于事件通知和响应，以及技术支持和客户服务。

创建一个 IAM 角色以允许授权用户管理与 AWS Support 相关的事件。通过实施访问控制的最低权限，IAM 角色将需要相应的 IAM 策略来允许访问支持中心，以便管理事件 支持。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要纠正此问题，请创建一个角色以允许授权用户管理 支持 事件。

创建用于 支持 访问的角色

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在 IAM 导航窗格中，选择角色，然后选择创建角色。
3. 对于角色类型，选择其他 AWS 账户。
4. 在账户 AWS 账户 ID 中，输入您要 AWS 账户 向其授予资源访问权限的 ID。

   如果将代入此角色的用户或组位于同一账户中，则输入本地账户号码。

   > **Note**
   >
   > 指定账户的管理员可向该账户中的任何用户授予代入该角色的权限。为此，管理员需要将策略附加到用户或组来授予 `sts:AssumeRole` 操作的权限。在该策略中，资源必须是角色 ARN。

5. 选择下一步: 权限。
6. 搜索托管策略 `AWSSupportAccess`。
7. 选中 `AWSSupportAccess` 托管策略的复选框。
8. 选择下一步：标签。
9. （可选）要将元数据添加到角色，将标签附加为键值对。

   有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南中的标记 IAM 用户和角色。
10. 选择下一步：审核。
11. 对于 Role name (角色名称)，为您的角色输入一个名称。

    角色名称在您的角色中必须是唯一的 AWS 账户。它们不区分大小写。
12. （可选）对于角色描述，输入新角色的描述。
13. 检查该角色，然后选择创建角色。

[IAM.19] 应为所有 IAM 用户启用 MFA

相关要求： NIST.800-53.r5 AC-2(1)、(15)、(1)、(2)、 NIST.800-53.r5 AC-3 (6)、(8)、NIST.800-53.r5 IA-2 nist.800-171.r2 3.8、 NIST.800-53.r5 IA-2 nist.800-171.r2 3.5.3、

NIST.800-53.r5 IA-2 nist.800-171.r2 3.5.4、nist.800-171.r2 3.7.5、PCI DSS v3.2.1/8.3.1、PCI DSS v4.0.1/8.3.1、PCI DSS v4.0.1/8.3.1 4.2， NIST.800-53.r5 IA-2

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`iam-user-mfa-enabled`

计划类型：定期

参数：无

此控件检查 IAM 用户是否启用了多重身份验证（MFA）。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要为 IAM 用户添加 MFA，请参阅 IAM 用户指南中的为用户启用 AWS中 MFA 设备。

[IAM.20] 避免使用根用户

> **Important**
>
> Security Hub CSPM 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub CSPM 控件的更改日志。

相关要求：独联体 AWS 基金会基准 v1.2.0/1.1

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::IAM::User`

AWS Config 规则:`use-of-root-account-test`（自定义 Security Hub CSPM 规则）

计划类型：定期

参数：无

此控件检查是否对 root 用户的使用有限制。 AWS 账户 该控件评估以下资源：

- Amazon Simple Notification Service（Amazon SNS）主题
- AWS CloudTrail 步道
- 与 CloudTrail 跟踪关联的指标筛选器
- 基于筛选条件的 Amazon CloudWatch 警报

如果以下一条或多条陈述为真，此检查将导致 `FAILED` 调查发现：

- 该账户中不存在任何 CloudTrail 跟踪。
- CloudTrail 跟踪已启用，但未配置至少一个包含读写管理事件的多区域跟踪。
- CloudTrail 跟踪已启用，但未与 CloudWatch 日志日志组关联。
- 没有使用 Center for Internet Security（CIS）规定的确切指标筛选条件。规定的指标筛选条件是 `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`。
- 账户中不存在基于指标筛选条件的 CloudWatch 警报。
- CloudWatch 配置为向关联的 SNS 主题发送通知的警报不会根据警报条件触发。
- SNS 主题不符合向 SNS 主题发送消息的限制。
- SNS 主题没有至少一个订阅用户。

如果以下一条或多条陈述为真，则此检查的控件状态为 `NO_DATA`：

- 多区域跟踪基于不同区域。Security Hub CSPM 只能在跟踪所在的区域生成调查结果。
- 多区域跟踪属于不同的账户。Security Hub CSPM 只能为拥有跟踪的账户生成调查结果。

如果以下一条或多条陈述为真，则此检查的控件状态为 `WARNING`：

- 当前账号不拥有 CloudWatch 警报中提及的 SNS 话题。
- 调用 `ListSubscriptionsByTopic` SNS API 时，当前账号无权访问 SNS 主题。

> **Note**
>
> 我们建议使用组织跟踪来记录来自组织中多个账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub CSPM 仅针对成员拥有的资源生成调查结果。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在您的 Security Hub CSPM 委托管理员账户中查看这些发现。

作为最佳实践，仅在需要执行账户和服务管理任务时才使用根用户凭证。将 IAM policy 直接应用于组和角色，但不应用于用户。有关设置日常使用管理员的说明，请参阅 IAM 用户指南中的创建第一个 IAM 管理员用户和组。

修复

修复此问题的步骤包括设置 Amazon SNS 主题、 CloudTrail跟踪、指标筛选条件和指标筛选器警报。

创建 Amazon SNS 主题

1. 在 v3/home 上打开亚马逊 SNS 控制台。https://console.aws.amazon.com/sns/
2. 创建接收所有 CIS 警报的 Amazon SNS 主题。

   为该主题创建至少一个订阅者。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。

接下来，设置 CloudTrail 一个适用于所有地区的活动。为此，请按照the section called “[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪”中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 Log CloudWatch s 日志组的名称。您为该日志组创建指标筛选条件。

最后，创建指标筛选条件和警报。

创建指标筛选条件和警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择日志组。
3. 选中与您创建的 CloudTrail 跟踪关联的 Logs CloudWatch 日志组对应的复选框。
4. 从操作中，选择创建指标筛选条件。
5. 在定义模式下，请执行以下操作：

a. 复制以下模式，然后将其粘贴到筛选模式字段中。

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
 $.eventType !="AwsServiceEvent"}
```

b. 选择下一步。

6. 在分配指标下，执行以下操作：

a. 在筛选条件名称中，输入指标筛选条件的名称。

b. 对于指标命名空间，输入 **LogMetrics**。

如果您对所有 CIS 日志指标筛选条件使用相同的命名空间，则所有 CIS Benchmark 指标都会组合在一起。

c. 对于指标名称，为指标输入名称。记住指标的名称。在创建警报时，您将需要选择指标。

d. 对于 Metric value（指标值），输入 **1**。

e. 选择下一步。

7. 在查看并创建下，验证您为新指标筛选器提供的信息。选择创建指标筛选条件。

8. 在导航窗格中，选择日志组，然后选择您在指标筛选器下创建的筛选条件。

9. 选中筛选条件的复选框。选择创建警报。

10. 在指定指标和条件下，执行以下操作：

a. 在条件下，对于阈值，选择静态。

b. 对于定义警报条件，选择大于/等于。

c. 在定义阈值中输入 **1**。

d. 选择下一步。

11. 在配置操作下，执行以下操作：

a. 在警报状态触发下，选择在警报中。

b. 在选择 SNS 主题下，选择选择现有的 SNS 主题。

c. 对于发送通知至，输入您在上一过程中创建的 SNS 主题的名称。

d. 选择下一步。

12. 在添加名称和描述下，输入警报的名称和描述，例如 **CIS-1.1-RootAccountUsage**。然后选择下一步。

13. 在预览并创建下，查看警报配置。然后选择创建警报。

[IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作

相关要求： NIST.800-53.r5 AC-2、 NIST.800-53.r5 AC-2 (1)、(15)、(7)、、、(10)、(2)、NIST.800-53.r5 AC-3 (3) NIST.800-53.r5 AC-3、nist.800-171.r2 3.1.1、 NIST.800-53.r5 AC-3 nist.800-171.r2 3.1.2 NIST.800-53.r5 AC-5、nist.800-171.r2 3.1.5 NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6 nist.800-171.r2 3.1.5、 NIST.800-53.r5 AC-6 nist.800-171.r2 3.8、NIST.800-53.r5 AC-6 nist.800-171.r2 3.8、nist.800-171.r2 3.8、nist.800-171.r2 3.8、nist.800-171.r2 3.800 -171.r2 3.9、nist.800-171.r2 3.13.3、nist.800-171.r2 3.13.4

类别：检测 > 安全访问管理

严重性：低

资源类型：`AWS::IAM::Policy`

AWS Config 规则：`iam-policy-no-statements-with-full-access`

计划类型：已触发变更

参数：

- `excludePermissionBoundaryPolicy`：`True`（不可自定义）

此控制检查您创建的 IAM 基于身份的策略是否具有使用 * 通配符的允许语句来授予对任何服务的所有操作的权限。如果任何策略声明包含 `"Action": "Service:*"` 的 `"Effect": "Allow"`，则控制失败。

例如，策略中的以下语句会导致失败的调查发现。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

如果 `"Effect": "Allow"` 与 `"NotAction": "service:*"` 配合使用，控制也会失败。在这种情况下，NotAction元素提供对中所有操作的访问权限 AWS 服务，中指定的操作除外NotAction。

此控制仅适用于客户托管的 IAM policy。它不适用于由 AWS管理的 IAM policy。

当您向分配权限时 AWS 服务，请务必在您的 IAM 策略中确定允许的 IAM 操作的范围。您应将 IAM 操作限制为仅需要的操作。这可以帮助您预置最低权限权限。如果策略附加到可能不需要权限的 IAM 主体，则过于宽松的策略可能会导致权限升级。

在某些情况下，您可能需要允许具有相似前缀的 IAM 操作，例如 `DescribeFlowLogs` 和 `DescribeAvailabilityZones`。在这些授权的情况下，您可以在通用前缀中添加带后缀的通配符。例如 `ec2:Describe*`。

如果您使用带有后缀通配符的带前缀的 IAM 操作，则此控制通过。例如，策略中的以下语句会形成通过的调查发现。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

以这种方式对相关的 IAM 操作进行分组时，还可以避免超出 IAM policy 的大小限制。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要修复此问题，请更新 IAM policy，使其不允许完全的 "*" 管理权限。有关如何编辑 IAM policy 的详细信息，请参阅 IAM 用户指南中的编辑 IAM policy。

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

相关要求：独联体 AWS 基金会基准 v5.0.0/1.11、独联体基金会基准 v3.0.0/1.12、独联体 AWS 基金会基准 v1.4.0/1.12、nist.800-171.r2 3.1.2 AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：**`iam-user-unused-credentials-check`**

计划类型：定期

参数：无

此控制检查 IAM 用户是否拥有 45 天或更长时间未使用的密码或活动访问密钥。为此，它会检查 AWS Config 规则的`maxCredentialUsageAge`参数是否等于 45 或更大。

用户可以使用不同类型的凭证（例如密码或访问密钥）访问 AWS 资源。

CIS 建议您删除或停用 45 天或更长时间未使用的所有凭证。禁用或删除不必要的凭证可减少他人使用遭盗用账户或已弃用账户的关联凭证的风险。

此控件的 AWS Config 规则使用`GetCredentialReport`和 `GenerateCredentialReport`API 操作，它们仅每四小时更新一次。对 IAM 用户的更改最多可能需要四小时才能对此控件显示。

> **Note**
>
> AWS Config 应在您使用 Security Hub CSPM 的所有区域中启用。但是，您可以启用在单个区域中记录全局资源。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

当您在 IAM 控制台中查看用户信息时，会有访问密钥年龄、密码使用期限和上次活动列。如果上述列中的任何一个中的值大于 45 天，请停用这些用户的凭证。

您还可以使用凭证报告来监控用户并识别那些连续 45 天或以上没有活动的用户。您可以从 IAM 控制台下载 `.csv` 格式的凭证报告。

确定非活动账户或未使用的凭证后，将其停用。有关说明，请参阅 IAM 用户指南中的创建、变更或删除 IAM 用户密码（控制台）。

[IAM.23] 应标记 IAM Access Analyzer 分析器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AccessAnalyzer::Analyzer`

AWS Config 规则:`tagged-accessanalyzer-analyzer`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查由 AWS Identity and Access Management Access Analyzer（IAM Access Analyzer）管理的分析器是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果分析器没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果分析器未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向分析器添加标签，请参阅《AWS IAM Access Analyzer API Reference》中的 TagResource。

[IAM.24] 应标记 IAM 角色

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IAM::Role`

AWS Config 规则:`tagged-iam-role`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Identity and Access Management (IAM) 角色是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果角色没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果角色未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 IAM 角色添加标签，请参阅《IAM 用户指南》中的为 IAM 资源添加标签。

[IAM.25] 应标记 IAM 用户

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IAM::User`

AWS Config 规则:`tagged-iam-user`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Identity and Access Management (IAM) 用户是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果用户没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果用户未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 IAM 用户添加标签，请参阅《IAM 用户指南》中的为 IAM 资源添加标签。

[IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书

相关要求：独联体 AWS 基金会基准 v5.0.0/1.18、独联体基金会基准 v3.0.0/1.19 AWS

类别：标识 > 合规性

严重性：中

资源类型：`AWS::IAM::ServerCertificate`

AWS Config 规则：**`iam-server-certificate-expiration-check`**

计划类型：定期

参数：无

此控制检查在 IAM 中管理的活动 SSL/TLS 服务器证书是否已过期。如果未删除过期的 SSL/TLS 服务器证书，则控件将失败。

要在中启用与您的网站或应用程序的 HTTPS 连接 AWS，您需要 SSL/TLS 服务器证书。您可以使用 IAM 或 AWS Certificate Manager (ACM) 来存储和部署服务器证书。只有在您必须支持 ACM 不支持的 HTTPS 连接时 AWS 区域 ，才使用 IAM 作为证书管理器。IAM 安全地加密您的私有密钥并将加密的版本存储在 IAM SSL 证书存储中。IAM 支持在所有区域部署服务器证书，但您必须从外部提供商处获取证书才能使用 AWS。无法将 ACM 证书上传到 IAM。此外，也无法从 IAM 控制台管理证书。删除过期的 SSL/TLS 证书可以消除意外将无效证书部署到资源的风险，这可能会损害底层应用程序或网站的可信度。

修复

要从 IAM 中删除服务器证书，请参阅《IAM 用户指南》中的在 IAM 中管理服务器证书。

[IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess

相关要求：独联体 AWS 基金会基准 v5.0.0/1.21、CIS 基金会基准 v3.0.0/1.22 AWS

类别：保护 > 安全访问管理 > 安全的 IAM 策略

严重性：中

资源类型：AWS::IAM::Role、AWS::IAM::User、AWS::IAM::Group

AWS Config 规则：**iam-policy-blacklisted-check**

计划类型：已触发变更

参数：

- “policyarns”：“arn: aws: iam:: aws:” policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess

此控件检查 IAM 身份（用户、角色或群组）是否AWSCloudShellFullAccess附加了 AWS 托管策略。如果 IAM 身份附加了 AWSCloudShellFullAccess 策略，则此控件将失败。

AWS CloudShell 提供了一种对运行 CLI 命令的便捷方法 AWS 服务。 AWS 托管策略AWSCloudShellFullAccess提供对的完全访问权限 CloudShell，允许用户在本地系统和 CloudShell 环境之间上传和下载文件。在 CloudShell 环境中，用户具有 sudo 权限，并且可以访问互联网。因此，将此托管策略附加到 IAM 身份后，他们就可以安装文件传输软件并将数据从外部互联网服务器移动 CloudShell 到外部 Internet 服务器。我们建议遵循最低权限原则，为您的 IAM 身份附加更窄的权限。

修复

要将 AWSCloudShellFullAccess 策略与 IAM 身份分离，请参阅《IAM 用户指南》中的添加和删除 IAM 身份权限。

[IAM.28] 应启用 IAM Access Analyzer 外部访问分析器

相关要求：独联体 AWS 基金会基准 v5.0.0/1.19、CIS 基金会基准 v3.0.0/1.20 AWS

分类：检测 > 检测服务 > 特权使用监控

严重性：高

资源类型：`AWS::AccessAnalyzer::Analyzer`

AWS Config 规则：**`iam-external-access-analyzer-enabled`**

计划类型：定期

参数：无

此控件检查是否启用 AWS 账户 了 IAM 访问分析器外部访问分析器。如果该账户未在您当前选择的 AWS 区域中启用外部访问权限分析器，则此控件将失败。

IAM Access Analyzer 外部访问分析器可帮助您识别与外部实体共享的资源，例如 Amazon Simple Storage Service（Amazon S3）存储桶或 IAM 角色。这可以帮助避免意外访问您的资源和数据。IAM Access Analyzer 具有区域性，必须在每个区域中启用。为了识别与外部主体共享的资源，访问分析器使用基于逻辑的推理来分析环境中基于资源的策略。 AWS 创建外部访问分析器时，您可以为整个组织或单个账户创建并启用它。

> **Note**
>
> 如果账户是组织的一部分 AWS Organizations，则此控件不会将指定该组织指定为信任区域并已为当前区域中的组织启用的外部访问分析器考虑在内。如果您的组织使用这种类型的配置，请考虑为该区域中组织内的各个成员账户禁用此控制。

修复

有关在特定区域启用外部访问分析器的信息，请参阅《IAM 用户指南》中的开始使用 IAM Access Analyzer。您必须在要监控资源访问情况的每个区域中启用一个分析器。

适用于 Amazon Inspector 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施会评估 Amazon Inspector 的服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Inspector.1] 应启用 Amazon Inspector EC2 扫描

相关要求：PCI DSS v4.0.1/11.3.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`inspector-ec2-scan-enabled`

计划类型：定期

参数：无

此控件会检查 Amazon Inspector EC2 扫描是否已启用。对于独立账户，如果账户中禁用了 Amazon Inspector EC2 扫描，则控制失败。在多账户环境中，如果委托的 Amazon Inspector 管理员账户和所有成员账户未启用 EC2 扫描，则控制失败。

在多账户环境中，此控件仅在 Amazon Inspector 委托管理员账户中生成调查发现。只有授权的管理员才能启用或禁用组织中成员帐户的 EC2 扫描功能。Amazon Inspector 成员账户无法通过其账户修改此配置。如果委托管理员的成员账户已暂停，但未启用 Amazon Inspector EC2 扫描，则此控件会生成`FAILED`调查结果。要获得 `PASSED` 调查发现，委派管理员必须在 Amazon Inspector 中取消关联这些已暂停的账户。

Amazon Inspector EC2 扫描从您的亚马逊弹性计算云 (Amazon EC2) 实例中提取元数据，然后将这些元数据与从安全公告中收集的规则进行比较以得出结果。Amazon Inspector 会扫描实例中是否存在程序包漏洞和网络可访问性问题。有关支持的操作系统（包括不使用 SSM 代理即可扫描哪些操作系统）的信息，请参阅支持的操作系统：Amazon EC2 扫描。

修复

要启用 Amazon Inspector 扫 EC2 描，请参阅亚马逊 Inspector 用户指南中的激活扫描。

[Inspector.2] 应启用 Amazon Inspector ECR 扫描

相关要求：PCI DSS v4.0.1/11.3.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`inspector-ecr-scan-enabled`

计划类型：定期

参数：无

此控件可检查是否启用了 Amazon Inspector ECR 扫描。对于独立账户，如果账户中禁用了 Amazon Inspector ECR 扫描，则此控件将失败。在多账户环境中，如果 Amazon Inspector 委托管理员账户和所有成员账户均未启用 ECR 扫描，则此控件将失败。

在多账户环境中，此控件仅在 Amazon Inspector 委托管理员账户中生成调查发现。只有委派管理员可以为组织中的成员账户启用或禁用 ECR 扫描功能。Amazon Inspector 成员账户无法通过其账户修改此配置。如果委派管理员有一个未启用 Amazon Inspector ECR 扫描的已暂停成员账户，则此控件会生成 `FAILED` 调查发现。要获得 `PASSED` 调查发现，委派管理员必须在 Amazon Inspector 中取消关联这些已暂停的账户。

Amazon Inspector 会扫描存储在 Amazon Elastic Container Registry（Amazon ECR）中的容器映像是否存在软件漏洞，以生成程序包漏洞调查发现。为 Amazon ECR 激活 Amazon Inspector 扫描后，会将 Amazon Inspector 设置为私有注册表的首选扫描服务。这会将基本扫描（由 Amazon ECR 免费提供）替换为增强扫描（由 Amazon Inspector 提供和计费）。增强扫描让您能够在注册表级别对操作系统和编程语言包进行漏洞扫描。您可以在 Amazon ECR 控制台中，查看针对映像每一层，使用增强扫描在映像级别发现的调查发现。此外，您还可以在其他不适用于基本扫描结果的服务（包括和 Amazon）中查看 AWS Security Hub CSPM 和处理这些发现 EventBridge。

修复

要启用 Amazon Inspector ECR 扫描，请参阅《Amazon Inspector User Guide》中的 Activating scans。

[Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描

相关要求：PCI DSS v4.0.1/6.2.4、PCI DSS v4.0.1/6.3.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`inspector-lambda-code-scan-enabled`

计划类型：定期

参数：无

此控件可检查是否启用了 Amazon Inspector Lambda 扫描。对于独立账户，如果账户中禁用了 Amazon Inspector Lambda 代码扫描，则此控件将失败。在多账户环境中，如果 Amazon Inspector 委托管理员账户和所有成员账户均未启用 Lambda 代码扫描，则此控件将失败。

在多账户环境中，此控件仅在 Amazon Inspector 委托管理员账户中生成调查发现。只有委派管理员可以为组织中的成员账户启用或禁用 Lambda 代码扫描功能。Amazon Inspector 成员账户无法通过其账户修改此配置。如果委派管理员有一个未启用 Amazon Inspector Lambda 代码扫描的已暂停成员账户，则此控件会生成 `FAILED` 调查发现。要获得 `PASSED` 调查发现，委派管理员必须在 Amazon Inspector 中取消关联这些已暂停的账户。

Amazon Inspector Lambda 代码扫描会根据 AWS 安全最佳实践扫描 AWS Lambda 函数中的自定义应用程序代码，以查找代码漏洞。Lambda 代码扫描可检测注入缺陷、数据泄露、弱加密或代码中缺少加密。此功能AWS 区域 仅在特定情况下可用。您可以同时激活 Lambda 代码扫描和 Lambda 标准扫描（请参阅 [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描）。

修复

要启用 Amazon Inspector Lambda 代码扫描，请参阅《Amazon Inspector User Guide》中的 Activating scans。

[Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描

相关要求：PCI DSS v4.0.1/6.2.4、PCI DSS v4.0.1/6.3.1

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`inspector-lambda-standard-scan-enabled`

计划类型：定期

参数：无

此控件可检查是否启用了 Amazon Inspector Lambda 标准扫描。对于独立账户，如果账户中禁用了 Amazon Inspector Lambda 标准扫描，则此控件将失败。在多账户环境中，如果 Amazon Inspector 委托管理员账户和所有成员账户均未启用 Lambda 标准扫描，则此控件将失败。

在多账户环境中，此控件仅在 Amazon Inspector 委托管理员账户中生成调查发现。只有委派管理员可以为组织中的成员账户启用或禁用 Lambda 标准扫描功能。Amazon Inspector 成员账户无法通过其账

户修改此配置。如果委派管理员有未启用 Amazon Inspector Lambda 标准扫描的已暂停成员账户，则此控件会生成 FAILED 调查发现。要获得 PASSED 调查发现，委派管理员必须在 Amazon Inspector 中取消关联这些已暂停的账户。

Amazon Inspector Lambda 标准扫描可识别您添加到 AWS Lambda 函数代码和层中的应用程序包依赖项中的软件漏洞。如果 Amazon Inspector 在 Lambda 函数应用程序包依赖项中检测到漏洞，则 Amazon Inspector 会生成详细 Package Vulnerability 类型的调查发现。您可以同时激活 Lambda 代码扫描和 Lambda 标准扫描（请参阅 [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描）。

修复

要启用 Amazon Inspector Lambda 标准扫描，请参阅《Amazon Inspector User Guide》中的 Activating scans。

Security Hub CSPM 控件适用于 AWS IoT

这些 AWS Security Hub CSPM 控制措施评估 AWS IoT 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[IoT.1] 应 AWS IoT Device Defender 标记安全配置文件

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::IoT::SecurityProfile

AWS Config 规则:tagged-iot-securityprofile（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	No default value

此控件检查 AWS IoT Device Defender 安全配置文件是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果安全配置文件没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果安全配置文件未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 AWS IoT Device Defender 安全配置文件添加标签，请参阅《AWS IoT 开发人员指南》中的为AWS IoT 资源添加标签。

[IoT.2] 应 AWS IoT Core 标记缓解措施

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::MitigationAction`

AWS Config 规则:`tagged-iot-mitigationaction`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	No default value

此控件检查 AWS IoT Core 缓解操作是否具有参数中定义的特定密钥的标签requiredTagKeys。如果缓解操作没有任何标签键或未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签密钥是否存在，如果缓解操作未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 缓解操作添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[IoT.3] 应为 AWS IoT Core 维度加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::IoT::Dimension

AWS Config 规则:tagged-iot-dimension（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	No default value

此控件检查 AWS IoT Core 维度是否具有参数中定义的特定键的标签requiredTagKeys。如果维度没有任何标签键或未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签键，如果维度未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 维度添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[IoT.4] 应给 AWS IoT Core 授权者加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::Authorizer`

AWS Config 规则:`tagged-iot-authorizer`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS IoT Core 授权方是否具有参数`requiredTagKeys`中定义的特定密钥的标签。如果授权方没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果授权方未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 AWS IoT Core 授权方添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[Iot.5] 应标记 AWS IoT Core 角色别名

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::RoleAlias`

AWS Config 规则:`tagged-iot-rolealias`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合AWS 要求的标签键。	`No default value`

此控件检查 AWS IoT Core 角色别名是否具有参数中定义的特定键的标签`requiredTagKeys`。如果角色别名没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果角色别名未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 角色别名添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[IoT.6] AWS IoT Core 策略应该被标记

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::Policy`

AWS Config 规则:`tagged-iot-policy`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS IoT Core 策略是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果策略没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果策略未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 策略添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

Security Hub CSPM 控件适用于 AWS IoT Events

这些 AWS Security Hub CSPM 控件评估 AWS IoT Events 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[IoTEvents.1] AWS 应标记 IoT Events 输入内容

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTEvents::Input`

AWS Config 规则：`iotevents-input-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 I AWS oT Events 输入是否具有参数中定义的特定密钥的标签requiredKeyTags。如果输入没有任何标签键或未在参数 requiredKeyTags 中指定所有键，则此控件会失败。如果未提供参数 requiredKeyTags，则此控件仅检查是否存在标签键，如果输入未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

> **Note**
>
> 该控件将在2026年7月7日之后停用，并从所有适用的Security Hub CSPM标准中删除。 AWS 宣布从 2026 年 5 月 20 日起终止对 AWS IoT Events 服务的支持。

修复

要向 AWS IoT Even ts 输入添加标签，请参阅AWS IoT Events 开发者指南中的为 AWS IoT Events 资源添加标签。

[IoTEvents.2] AWS 应标记 IoT Events 探测器模型

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTEvents::DetectorModel`

AWS Config 规则：`iotevents-detector-model-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 I AWS oT Events 探测器模型是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果检测器模型没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件会失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果探测器模型未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

> **Note**
>
> 该控件将在2026年7月7日之后停用，并从所有适用的Security Hub CSPM标准中删除。 AWS 宣布从 2026 年 5 月 20 日起终止对 AWS IoT Events 服务的支持。

修复

要向 AWS IoT Even ts 探测器模型添加标签，请参阅AWS IoT Events 开发者指南中的为 AWS IoT Events 资源添加标签。

[IoTEvents.3] AWS 应标记 IoT Events 警报模型

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTEvents::AlarmModel`

AWS Config 规则：`iotevents-alarm-model-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 I AWS oT Events 警报模型是否具有参数中定义的特定密钥的标签requiredKeyTags。如果警报模型没有任何标签键或未在 requiredKeyTags 参数中指定所有键，则此控件将失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果警报模型未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

> **Note**
>
> 该控件将在2026年7月7日之后停用，并从所有适用的Security Hub CSPM标准中删除。 AWS 宣布从 2026 年 5 月 20 日起终止对 AWS IoT Events 服务的支持。

修复

要向 AWS IoT Even ts 警报模型添加标签，请参阅AWS IoT Events 开发者指南中的为 AWS IoT Events 资源添加标签。

适用于物联网的 Security Hub CSPM 控件 AWS SiteWise

这些 AWS Security Hub CSPM 控件评估 AWS 物联网 SiteWise 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTSiteWise::AssetModel`

AWS Config 规则：`iotsitewise-asset-model-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 SiteWise 资产模型是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果资产模型没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果资产模型未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要为 AWS 物联网 SiteWise 资产模型添加标签，请参阅AWS IoT SiteWise 用户指南中的为 AWS IoT SiteWise 资源添加标签。

[Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTSiteWise::Dashboard`

AWS Config 规则：`iotsitewise-dashboard-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 SiteWise 仪表板是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果控制面板没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则控件仅检查是否存在标签键，如果控制面板未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT SiteWise 控制面板添加标签，请参阅AWS IoT SiteWise 用户指南中的为 AWS IoT SiteWise 资源添加标签。

[Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTSiteWise::Gateway`

AWS Config 规则：`iotsitewise-gateway-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联 SiteWise 网网关是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果网关没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有密钥，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果网关未使用任何键标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT SiteWise 网关添加标签，请参阅AWS IoT SiteWise 用户指南中的为 AWS IoT SiteWise 资源添加标签。

[Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTSiteWise::Portal`

AWS Config 规则：`iotsitewise-portal-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 SiteWise 门户是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果门户没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果门户未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT SiteWise 门户添加标签，请参阅AWS IoT SiteWise 用户指南中的为 AWS IoT SiteWise 资源添加标签。

[Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTSiteWise::Project`

AWS Config 规则：`iotsitewise-project-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 SiteWise 项目是否具有参数中定义的特定密钥的标签requiredKeyTags。如果项目没有任何标签键或者未在 requiredKeyTags 参数中指定所有键，则此控件将失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果项目未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT SiteWise 项目添加标签，请参阅AWS IoT SiteWise 用户指南中的为 AWS IoT SiteWise 资源添加标签。

适用于物联网的 Security Hub CSPM 控件 AWS TwinMaker

这些 AWS Security Hub CSPM 控件评估 AWS 物联网 TwinMaker 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTTwinMaker::SyncJob`

AWS Config 规则：`iottwinmaker-sync-job-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 TwinMaker 同步作业是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果同步作业没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则控件仅检查是否存在标签键，如果同步作业未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT TwinMaker 同步任务添加标签，请参阅AWS IoT TwinMaker 用户指南TagResource中的。

[Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTTwinMaker::Workspace`

AWS Config 规则：`iottwinmaker-workspace-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 TwinMaker 工作空间是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果工作区没有任何标签键或未在参数 `requiredKeyTags` 中指定所有键，则此控件会失败。如果未提供参数 `requiredKeyTags`，则此控件仅会检查是否存在标签键，如果工作区未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT TwinMaker 工作空间添加标签，请参阅AWS IoT TwinMaker 用户指南TagResource中的。

[Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTTwinMaker::Scene`

AWS Config 规则：`iottwinmaker-scene-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 TwinMaker 场景是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果场景没有任何标签键或未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果场景未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS 物联网 TwinMaker 场景添加标签，请参阅AWS IoT TwinMaker 用户指南TagResource中的。

[Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTTwinMaker::Entity`

AWS Config 规则：`iottwinmaker-entity-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 物联网 TwinMaker 实体是否具有参数中定义的特定密钥的标签`requiredKeyTags`。如果实体没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果实体未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 I AWS oT TwinMaker 实体添加标签，请参阅AWS IoT TwinMaker 用户指南TagResource中的。

适用 AWS 于 IoT Wireless 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控件会评估 AWS IoT Wireless 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTWireless::MulticastGroup`

AWS Config 规则：`iotwireless-multicast-group-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 I AWS oT Wireless 组播组是否具有参数`requiredKeyTags`中定义的特定密钥的标签。如果组播组没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果组播组未使用任何键进行标记，则此控件将失效。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS IoT Wireless 组播组添加标签，请参阅AWS IoT Wireless 开发人员指南中的为 AWS IoT Wireless 资源添加标签。

[Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::IoTWireless::ServiceProfile

AWS Config 规则：iotwireless-service-profile-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 I AWS oT Wireless 服务配置文件是否具有参数中定义的特定密钥的标签requiredKeyTags。如果服务配置文件没有任何标签键或者未在 requiredKeyTags 参数中指定所有键，则此控件将失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果服务配置文件未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS IoT Wireless 服务配置文件添加标签，请参阅AWS IoT Wireless 开发人员指南中的为AWS IoT Wireless 资源添加标签。

[Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoTWireless::FuotaTask`

AWS Config 规则：`iotwireless-fuota-task-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合AWS 要求的标签键。	无默认值

此控件检查 I AWS oT Wireless 固件更新 over-the-air (FUOTA) 任务是否具有参数`requiredKeyTags`中定义的特定密钥的标签。如果 FUOTA 任务没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果 FUOTA 任务未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS IoT Wireless FUOTA 任务添加标签，请参阅AWS IoT Wireless 开发人员指南中的为 AWS IoT Wireless 资源添加标签。

适用于亚马逊 IVS 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估亚马逊互动视频服务 (IVS) 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[IVS.1] 应标记 IVS 播放密钥对

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IVS::PlaybackKeyPair`

AWS Config 规则：`ivs-playback-key-pair-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon IVS 播放密钥对是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果播放密钥对没有任何标签键或者未在参数 `requiredKeyTags` 中指定所有键，则此控件会失败。如

果未提供参数 `requiredKeyTags`，则此控件仅会检查是否存在标签键，如果播放密钥对未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 IVS 播放密钥对添加标签，请参阅《Amazon IVS 实时直播功能 API 参考》中的 TagResource。

[IVS.2] 应标记 IVS 录制配置

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IVS::RecordingConfiguration`

AWS Config 规则：`ivs-recording configuration-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon IVS 记录配置是否具有带参数 requiredKeyTags 中定义的特定键的标签。如果记录配置没有任何标签键或未在 requiredKeyTags 参数中指定所有键，则此控件将失败。如果未提供 requiredKeyTags 参数，则此控件仅检查是否存在标签键，如果记录配置未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 IVS 记录配置添加标签，请参阅《Amazon IVS 实时直播功能 API 参考》中的 TagResource。

[IVS.3] 应标记 IVS 频道

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::IVS::Channel

AWS Config 规则：`ivs-channel-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon IVS 频道是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果频道没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅检查是否存在标签键，如果频道未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 IVS 频道添加标签，请参阅《Amazon IVS 实时直播功能 API 参考》中的 TagResource。

Amazon Keyspaces 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Keyspaces 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Cassandra::Keyspace`

AWS Config 规则：`cassandra-keyspace-tagged`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Keyspaces 密钥空间是否具有带参数 `requiredKeyTags` 中定义的特定键的标签。如果密钥空间没有任何标签键或者未在 `requiredKeyTags` 参数中指定所有键，则此控件将失败。如果未提供 `requiredKeyTags` 参数，则此控件仅会检查是否存在标签键，如果密钥空间未使用任何键进行标记，则此控件会失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 Amazon Keyspaces 密钥空间添加标签，请参阅《Amazon Keyspaces 开发人员指南》中的向键空间添加标签。

适用于 Kinesis 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Kinesis 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Kinesis.1] Kinesis 直播应在静态状态下进行加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Kinesis::Stream`

AWS Config 规则：kinesis-stream-encrypted

计划类型：已触发变更

参数：无

此控件检查 Kinesis Data Streams 是否使用服务器端加密进行静态加密。如果 Kinesis 流未使用服务器端加密进行静态加密，则此控制失败。

服务器端加密是 Amazon Kinesis Data Streams 中的一项功能，它使用 AWS KMS key在数据静止之前自动对其进行加密。数据在写入 Kinesis 流存储层之前进行加密，并在从存储中检索后进行解密。因此，在 Amazon Kinesis Data Streams 服务中对数据进行静态加密。

修复

有关启用 Kinesis 流的服务器端加密的信息，请参阅 Amazon Kinesis 开发人员指南中的“如何开始使用服务器端加密？”。

[Kinesis.2] 应标记 Kinesis 流

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Kinesis::Stream`

AWS Config规则:`tagged-kinesis-stream`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon Kinesis 数据流是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果数据流没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果数据流未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Kinesis 数据流添加标签，请参阅《Amazon Kinesis Developer Guide》中的 Tagging your streams in Amazon Kinesis Data Streams。

[Kinesis.3] Kinesis 流应有足够的数据留存期

严重性：中

资源类型：`AWS::Kinesis::Stream`

AWS Config规则：kinesis-stream-backup-retention-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`minimumBackupRetentionPeriod`	数据应保留的最少小时数。	字符串	24 到 8760	168

此控件可检查 Amazon Kinesis 数据流的数据留存期是否大于或等于指定时间范围。如果数据留存期小于指定时间范围，则此控件将失败。除非您为数据保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 168 小时。

在 Kinesis Data Streams 中，数据流是指数据记录的有序序列，可用于执行实时写入和读取。数据记录临时存储在您流的分片中。从添加记录开始，到记录不再可供访问为止的时间段称为保留期。在缩短保留期后，Kinesis Data Streams 几乎会立即使早于新保留期的记录变得不可访问。例如，将保留期从 24 小时更改为 48 小时意味着，在 23 小时 55 分钟之前添加到流中的记录在 24 小时之后仍可用。

修复

要更改 Kinesis Data Streams 的备份保留期，请参阅《Amazon Kinesis Data Streams 开发人员指南》中的更改数据留存期。

Security Hub CSPM 控件适用于 AWS KMS

这些 AWS Security Hub CSPM 控件评估 AWS Key Management Service (AWS KMS) 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作

相关要求： 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)

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::Policy`

AWS Config 规则：iam-customer-policy-blocked-kms-actions

计划类型：已触发变更

参数：

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`（不可自定义）
- `excludePermissionBoundaryPolicy`：`True`（不可自定义）

检查 IAM 客户托管策略的默认版本是否允许委托人对所有资源使用 AWS KMS 解密操作。如果策略足够开放，可以允许对所有 KMS 密钥执行 `kms:Decrypt` 或 `kms:ReEncryptFrom` 操作，则控制失败。

该控件仅检查 Resource 元素中的 KMS 密钥，而不考虑策略的 Condition 元素中的任何条件。此外，该控件还会评估附加和独立的客户管理型策略。它不检查内联策略或 AWS 托管策略。

使用 AWS KMS，您可以控制谁可以使用您的 KMS 密钥并访问您的加密数据。IAM policy 定义了一个身份（用户、组或角色）可以对哪些资源执行哪些操作。遵循安全最佳实践， AWS 建议您允许最低权限。换句话说，您应仅授予身份 `kms:Decrypt` 或 `kms:ReEncryptFrom` 权限，并仅授予执行任务所需的密钥。否则，用户可能会使用不适合数据的密钥。

不要授予所有密钥的权限，而是确定用户访问加密数据所需的最小密钥集。然后设计允许用户仅使用这些密钥的策略。例如，不要允许对所有 KMS 密钥的 `kms:Decrypt` 权限。取而代之的是，仅允许 `kms:Decrypt` 使用特定区域中您账户的密钥。通过采用最低权限原则，您可以降低数据意外泄露的风险。

修复

要修改 IAM 客户托管策略，请参阅 IAM 用户指南中的编辑客户管理型策略。编辑策略时，在 `Resource` 字段中提供您要允许执行解密操作的一个或多个密钥的 Amazon 资源名称（ARN）。

[KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

相关要求： 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)

类别：保护 > 安全访问管理

严重性：中

资源类型：

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config 规则：iam-inline-policy-blocked-kms-actions

计划类型：已触发变更

参数：

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`（不可自定义）

此控件检查嵌入在您的 IAM 身份（角色、用户或群组）中的内联策略是否允许对所有 KMS AWS KMS 密钥执行解密和重新加密操作。如果策略足够开放，可以允许对所有 KMS 密钥执行 `kms:Decrypt` 或 `kms:ReEncryptFrom` 操作，则控制失败。

该控件仅检查 Resource 元素中的 KMS 密钥，而不考虑策略的 Condition 元素中的任何条件。

使用 AWS KMS，您可以控制谁可以使用您的 KMS 密钥并访问您的加密数据。IAM policy 定义了一个身份（用户、组或角色）可以对哪些资源执行哪些操作。遵循安全最佳实践，AWS 建议您允许最低权限。换句话说，您应该仅向身份授予他们所需的权限，并且仅授予执行任务所需的密钥。否则，用户可能会使用不适合数据的密钥。

不要授予所有密钥的权限，而是确定用户访问加密数据所需的最小密钥集。然后设计允许用户仅使用这些密钥的策略。例如，不要允许对所有 KMS 密钥的 `kms:Decrypt` 权限。相反，请仅允许对账户特定区域中的特定密钥授予权限。通过采用最低权限原则，您可以降低数据意外泄露的风险。

修复

要修改 IAM 内联策略，请参阅 IAM 用户指南中的编辑内联策略。编辑策略时，在 `Resource` 字段中提供您要允许执行解密操作的一个或多个密钥的 Amazon 资源名称（ARN）。

AWS KMS keys 不应无意中删除 [KMS.3]

相关要求： NIST.800-53.r5 SC-12、 NIST.800-53.r5 SC-1 2 (2)

类别：保护 > 数据保护 > 数据删除保护

严重性：严重

资源类型：`AWS::KMS::Key`

AWS Config 规则:`kms-cmk-not-scheduled-for-deletion-2`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查是否计划删除 KMS 密钥。如果计划删除 KMS 密钥，则控制失败。

KMS 密钥一经删除就无法恢复。如果删除 KMS 密钥，则使用 KMS 密钥加密的数据也将永久无法恢复。如果在计划删除的 KMS 密钥下加密了有意义的数据，请考虑使用新的 KMS 密钥对数据进行解密或重新加密数据，除非您故意执行加密擦除。

当计划删除 KMS 密钥时，如果计划错误，则会强制执行强制等待期，以便有时间撤消删除。默认等待期为 30 天，但当计划删除 KMS 密钥时，等待期可缩短至短至 7 天。在等待期限内，可以取消预定删除，KMS 密钥不会被删除。

有关删除 KMS 密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的删除 KMS 密钥。

修复

要取消预定的 KMS 密钥删除，请参阅 AWS Key Management Service 开发人员指南中的计划和取消密钥删除（控制台）下的取消密钥删除。

[KMS.4] 应启用 AWS KMS 密钥轮换

相关要求：独联体 AWS 基金会基准 v5.0.0/3.6、CIS 基金会基准 v3.0.0/3.6、CIS AWS 基金会基准 v1.4.0/3.8、CIS AWS 基金会基准 v1.2.0/2.8、2、2 (NIST.800-53.r5 SC-12)、8 (3)、PCI DSS AWS v3.2.1/3.6.4、PCI DSS v4.0.1/ NIST.800-53.r5 SC-1 3.7.4 NIST.800-53.r5 SC-2

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::KMS::Key`

AWS Config 规则：cmk-backing-key-rotation-enabled

计划类型：定期

参数：无

AWS KMS 允许客户轮换备用密钥，后备密钥是存储在 KMS 密钥中的 AWS KMS 密钥材料，与 KMS 密钥的密钥 ID 相关联。备用密钥被用于执行加密操作，例如加密和解密。目前，自动密钥轮换会保留所有之前的备用密钥，以便解密已加密数据的操作可以不被察觉地进行。

CIS 建议您启用 KMS 密钥轮换。轮换加密密钥有助于减少遭盗用密钥的潜在影响，因为使用可能已泄露的先前密钥无法访问使用新密钥加密的数据。

修复

要启用 KMS 密钥轮换，请参阅AWS Key Management Service 开发人员指南中的如何启用和禁用自动密钥轮换。

[KMS.5] KMS 密钥不应可公开访问

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::KMS::Key`

AWS Config 规则：kms-key-policy-no-public-access

计划类型：已触发变更

参数：无

它控制检查 AWS KMS key 是否可以公开访问。如果 KMS 密钥可公开访问，则此控件将失败。

实施最低权限访问对于降低安全风险以及错误或恶意意图的影响至关重要。如果的密钥策略 AWS KMS key 允许从外部账户进行访问，则第三方可能能够使用该密钥对数据进行加密和解密。这可能导致内部或外部威胁泄露使用密钥 AWS 服务 的数据。

> **Note**
>
> AWS KMS key 如果您的配置 AWS Config 阻止在 KMS 密钥的配置项目 (CI) 中记录密钥策略，则此控件还会返回FAILED结果。 AWS Config 要在 CI 中填充 KMS 密钥的密钥策略，AWS Config 角色必须有权使用 GetKeyPolicyAPI 调用读取密钥策略。要解决此类FAILED发现，请检查可阻止 AWS Config 角色对 KMS 密钥的密钥策略具有读取权限的策略。例如，请检查以下内容：
>
> - KMS 密钥的密钥策略。
> - 中 AWS Organizations 适用于您的账户的@@ 服务控制策略 (SCPsRCPs) 和资源控制策略 ()。
> - 该 AWS Config 角色的权限（如果您未使用AWS Config 服务相关角色）。
>
> 此外，此控件不会评估使用通配符或变量的策略条件。要生成 PASSED 调查发现，密钥策略中的条件只能使用固定值，即不包含通配符或策略变量的值。有关策略变量的信息，请参阅《AWS Identity and Access Management 用户指南》中的变量和标签。

修复

有关更新密钥策略的信息 AWS KMS key，请参阅《AWS Key Management Service 开发者指南》AWS KMS中的密钥策略。

Security Hub CSPM 控件适用于 AWS Lambda

这些 AWS Security Hub CSPM 控制措施评估 AWS Lambda 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Lambda.1] Lambda 函数策略应禁止公众访问

相关要求： 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、(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。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.2，PCI DSS v3.2。 1/1.3.4，PCI DSS v3.2。 1/7.2.1，PCI DSS v4.0。 1/7.2.1

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::Lambda::Function`

AWS Config 规则：lambda-function-public-access-prohibited

计划类型：已触发变更

参数：无

此控件检查 Lambda 函数基于资源的策略是否禁止您账户之外的公开访问。如果允许公共访问，则控制失败。如果从 Amazon S3 调用 Lambda 函数，并且该策略不包含限制公共访问的条件，则控制也会失败，例如 `AWS:SourceAccount`。我们建议在存储桶策略中使用 `AWS:SourceAccount` 与其他 S3 条件以获得更精细的访问权限。

> **Note**
>
> 此控件不会评估使用通配符或变量的策略条件。要生成 PASSED 调查发现，Lambda 函数策略中的条件必须仅使用固定值，即不包含通配符或策略变量的值。有关策略变量的信息，请参阅《AWS Identity and Access Management 用户指南》中的变量和标签。

Lambda 函数不应公开访问，因为这可能会导致意外访问函数代码。

修复

要修复此问题，您必须更新函数的基于资源的策略以移除权限或添加 `AWS:SourceAccount` 条件。您只能通过 Lambda API 或更新基于资源的策略。 AWS CLI

首先，请在 Lambda 控制台上查看基于资源的策略。确定具有公开策略的 `Principal` 字段值的策略声明，例如 `"*"` 或 `{ "AWS": "*" }`。

您无法从控制台编辑策略。要移除函数的权限，请从 AWS CLI中运行 remove-permission 命令。

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

<function-name> 替换为 Lambda 函数的名称，*<statement-id>* 替换为要删除的语句的语句 ID（`Sid`）。

[Lambda.2] Lambda 函数应使用支持的运行时

相关要求： 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)、(4)、 NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5)、PCI DSS v4.0。1/12.3.4

类别：保护 > 安全开发

严重性：中

资源类型：`AWS::Lambda::Function`

AWS Config 规则：lambda-function-settings-check

计划类型：已触发变更

参数：

- `runtime`：`dotnet10, dotnet8, java25, java21, java17, java11, java8.al2, nodejs24.x, nodejs22.x, python3.14, python3.13, python3.12, python3.11, python3.10, ruby4.0, ruby3.4, ruby3.3`（不可自定义）

此控件检查 AWS Lambda 函数运行时设置是否与每种语言中为支持的运行时设置的预期值相匹配。如果 Lambda 函数不使用支持的运行时，则此控件将失败，如“参数”部分所述。Security Hub CSPM 会忽略包类型为`Image`的函数。

Lambda 运行时系统是围绕操作系统、编程语言和需要维护和安全更新的软件库的组合构建的。护和安全更新的操作系统、编程语言和软件库的组合构建的。当安全更新不再支持某个运行时组件时，Lambda 将弃用该运行时系统。虽然您无法创建使用已弃用运行时的函数，但该函数仍可用于处理调用事件。我们建议确保 Lambda 函数处于最新状态，并且不使用已弃用的运行时环境。有关支持的运行时列表，请参阅《AWS Lambda 开发人员指南》中的 Lambda 运行时。

修复

有关支持的运行时和弃用计划的更多信息，请参阅AWS Lambda 开发人员指南中的运行时系统弃用策略。将运行时迁移到最新版本时，请遵循语言发布者的语法和指导。我们还建议应用运行时更新，以便在运行时版本不兼容的极少数情况下帮助降低对工作负载造成影响的风险。

[Lambda.3] Lambda 函数应位于 VPC 中

相关要求：PCI DSS v3.2。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.2，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、 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)

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::Lambda::Function`

AWS Config 规则：lambda-inside-vpc

计划类型：已触发变更

参数：无

此控件可检查 Lambda 函数是否部署在虚拟私有云（VPC）中。如果 Lambda 函数未部署在 VPC 中，则此控件将失败。Security Hub CSPM 不会评估 VPC 子网路由配置来确定公共可访问性。您可能会看到 Lambda @Edge 资源的失败的调查发现。

在 VPC 中部署资源可增强安全性和对网络配置的控制。此类部署还提供了跨多个可用区的可扩展性和高容错能力。您可以自定义 VPC 部署以满足不同的应用程序要求。

修复

要将现有函数配置为连接到您的 VPC 中的私有子网，请参阅 AWS Lambda 开发人员指南中的配置 VPC 访问权限。我们建议至少选择两个私有子网以实现高可用性，并至少选择一个满足功能连接要求的安全组。

[Lambda.5] VPC Lambda 函数应在多个可用区中运行

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Lambda::Function`

AWS Config 规则：lambda-vpc-multi-az-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`availabilityZones`	可用区的最小数量	枚举	`2, 3, 4, 5, 6`	2

此控件检查连接到虚拟私有云 (VPC) 的 AWS Lambda 功能是否至少在指定数量的可用区 (AZ) 中运行。如果该功能未在指定数量或更多的可用区中运行，则控制失败。除非您为最小数量的可用区提供自定义参数值，否则 Security Hub CSPM 将使用两个可用区的默认值。

跨多个可用区部署资源是确保架构内高可用性 AWS 的最佳实践。可用性是机密性、完整性和可用性三合一安全模型的核心支柱。连接到 VPC 的所有 Lambda 函数都应具有多可用区部署，以确保单个区域的故障不会导致操作完全中断。

修复

如果您将函数配置为连接到您账户中的 VPC，请指定多个可用区中的子网以确保高可用性。有关说明，请参阅 AWS Lambda 开发人员指南》中的配置 VPC 访问权限。

Lambda 自动在多个可用区中运行其他功能，以确保在单个可用区发生服务中断时可以处理事件。

[Lambda.6] 应标记 Lambda 函数

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Lambda::Function`

AWS Config 规则:`tagged-lambda-function`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Lambda 函数是否具有参数中定义的特定键的标签`requiredTagKeys`。如果函数没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果该函数未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关标记更多最佳实践，请参阅《AWS 一般参考》中的标记 AWS 资源。

修复

要向 Lambda 函数添加标签，请参阅《AWS Lambda 开发人员指南》中的在 Lambda 函数上使用标签。

[Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪

相关要求： NIST.800-53.r5 CA-7

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::Lambda::Function`

AWS Config 规则：lambda-function-xray-enabled

计划类型：已触发变更

参数：无

此控件检查是否为 AWS Lambda 函数启用了主动跟 AWS X-Ray 踪。如果对 Lambda 函数禁用了主动跟踪， X-Ray 则控件将失败。

AWS X-Ray 可以为函数提供跟踪和监控 AWS Lambda 功能，从而节省调试和操作 Lambda 函数的时间和精力。它可以通过分解 Lambda 函数的延迟来帮助您诊断错误并识别性能瓶颈、速度减慢和超时。它还可以帮助满足数据隐私和合规要求。如果您为 Lambda 函数启用主动跟踪，则会 X-Ray提供 Lambda 函数中数据流和处理的整体视图，这可以帮助您识别潜在的安全漏洞或不合规的数据处理实践。这种可见性可以帮助您维护数据的完整性、机密性以及遵守相关法规。

> **Note**
>
> AWS X-Ray 目前不支持使用适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）、自行管理 Apache Kafka、带有 ActiveMQ 和 RabbitMQ 的亚马逊 MQ 或亚马逊 DocumentDB 事件源映射的 Lambda 函数进行跟踪。

修复

有关为 AWS Lambda 函数启用主动跟踪的信息，请参阅开发人员指南 AWS X-Ray中的使用可视化 Lambda 函数调用。AWS Lambda

适用于 Macie 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Macie 服务。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Macie.1] 应启用 Amazon Macie

相关要求： NIST.800-53.r5 CA-7、 NIST.800-53.r5 CA-9 (1)、、 NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5、nist.800-53.r5 SI-4

类别：检测 > 检测服务

严重性：中

资源类型：AWS::::Account

AWS Config 规则：macie-status-check

计划类型：定期

该控件检查是否为账户启用了 Amazon Macie。如果没有为该账户启用 Macie，则控制失败。

Amazon Macie 使用机器学习和模式匹配来发现敏感数据，提供对数据安全风险的可见性，并实现针对这些风险的自动防护。Macie 会自动持续评估您的 Amazon Simple Storage Service（Amazon S3）存储桶的安全性和访问控制，并生成调查发现以通知您有关 Amazon S3 数据的安全性或隐私的潜在问题。Macie 还会自动发现和报告个人身份信息（PII）等敏感数据，，让您更好地了解在 Amazon S3 中存储的数据。要了解更多信息，请参阅《Amazon Macie 用户指南》。

修复

要启用 Macie，请参阅《Amazon Macie 》中的启用 Macie。

[Macie.2] 应启用 Macie 敏感数据自动发现

相关要求： NIST.800-53.r5 CA-7、 NIST.800-53.r5 CA-9 (1)、、 NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5、nist.800-53.r5 SI-4

类别：检测 > 检测服务

严重性：高

资源类型：AWS::::Account

AWS Config 规则：macie-auto-sensitive-data-discovery-check

计划类型：定期

该控件可检查是否为 Amazon Macie 管理员账户启用了敏感数据自动发现。如果没有为 Macie 管理员账户启用敏感数据自动发现，则此控件将失败。此控件仅适用于管理员帐户。

Macie 会自动发现并报告 Amazon Simple Storage Service（Amazon S3）存储桶中的个人身份信息（PII）等敏感数据。通过敏感数据自动发现，Macie 可以持续评估您的存储桶清单，并使用采样技术来识别和选择存储桶中具有代表性的 S3 对象。然后，Macie 会分析所选对象，检查它们是否有

敏感数据。随着分析的进行，Macie 会更新统计数据、清单数据及其提供的有关您 S3 数据的其他信息。Macie 还会生成调查发现以报告其发现的敏感数据。

修复

要创建和配置敏感数据自动发现作业以分析 S3 存储桶中的对象，请参阅《Amazon Macie User Guide》中的 Configuring automated sensitive data discovery for your account。

适用于亚马逊 MSK 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估了适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[MSK.1] MSK 集群应在代理节点之间传输时进行加密

相关要求： NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-1 3、3 (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 NIST.800-53.r5 SC-8 (2)、PCI DSS v4.0.1/4.2.1

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::MSK::Cluster`

AWS Config 规则：msk-in-cluster-node-require-tls

计划类型：已触发变更

参数：无

此控件可检查 Amazon MSK 集群在传输过程中是否在集群的代理节点之间使用 HTTPS（TLS）进行加密。如果为集群代理节点连接启用了纯文本通信，则控制失败。

HTTPS 提供了额外的安全层，因为它使用 TLS 来移动数据，可用于帮助防止潜在的攻击者使用person-in-the-middle或类似的攻击来窃听或操纵网络流量。默认情况下，Amazon MSK 使用 TLS 对传输中数据进行加密。但是，您可以在创建集群时覆盖此默认值。对于代理节点连接，我们建议使用通过 HTTPS（TLS）的加密连接。

修复

有关更新 Amazon MSK 集群的加密设置的信息，请参阅《Amazon Managed Streaming for Apache Kafka 开发人员指南》中的更新集群的安全设置。

[MSK.2] MSK 集群应配置增强型监控

相关要求： NIST.800-53.r5 CA-7，nist.800-53.r5 SI-2

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::MSK::Cluster`

AWS Config 规则：msk-enhanced-monitoring-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon MSK 集群是否配置了增强型监控，且监控级别至少指定为 `PER_TOPIC_PER_BROKER`。如果集群的监控级别设置为 `DEFAULT` 或 `PER_BROKER`，则控制失败。

`PER_TOPIC_PER_BROKER` 监控级别可以帮助您更精细地了解 MSK 集群的性能，还提供与资源利用率相关的指标，例如 CPU 和内存使用情况。这可以帮助您确定各个主题和代理的性能瓶颈和资源利用率模式。反过来，这种可见性可以优化 Kafka 代理的性能。

修复

要为 MSK 集群配置增强型监控，请完成以下步骤：

1. 在https://console.aws.amazon.com/msk/家打开亚马逊 MSK 控制台？ region=us-east-1#/home/。
2. 在导航窗格中，选择集群。然后选择一个集群。
3. 在操作中，选择编辑监控。
4. 选择增强主题级别监控选项。
5. 选择保存更改。

有关监控级别的更多信息，请参阅 Apache Managed St reaming for Apache Kafka 开发者指南 CloudWatch中的亚马逊 MSK 监控标准代理指标。

[MSK.3] MSK Connect 连接器应在传输过程中进行加密

相关要求：PCI DSS v4.0.1/4.2.1

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::KafkaConnect::Connector`

AWS Config 规则:`msk-connect-connector-encrypted`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件可检查 Amazon MSK Connect 连接器是否在传输过程中进行加密。如果连接器未在传输过程中进行加密，则此控件将失败。

传输中数据是指从一个位置移动到另一个位置的数据，例如在集群中的节点之间或在集群和应用程序之间。数据可能通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。

修复

您可以在创建 MSK Connect 连接器时启用传输中加密。创建集群后，将无法更改加密设置。有关更多信息，请参阅《Amazon Managed Streaming for Apache Kafka Developer Guide》中的 Create a connector。

[MSK.4] MSK 集群应禁用公开访问

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::MSK::Cluster`

AWS Config 规则：msk-cluster-public-access-disabled

计划类型：已触发变更

参数：无

此控件检查 Amazon MSK 集群是否已禁用公开访问。如果 MSK 集群启用了公开访问，则该控件会失败。

默认情况下，只有当客户端与 Amazon MSK 集群位于同一 VPC 中时，客户端才能访问该集群。默认情况下，Kafka 客户端与 MSK 集群之间的所有通信都是私密的，流数据不会通过互联网传输。但是，如果将 MSK 集群配置为允许公开访问，则互联网上的任何人都可以与集群内运行的 Apache Kafka 代

理建立连接。这可能会导致未经授权访问、数据泄露或漏洞利用等问题。如果通过要求身份验证和授权措施来限制对集群的访问，您可以帮助保护敏感信息并维护资源的完整性。

修复

有关管理对 Amazon MSK 集群的公开访问的信息，请参阅《Amazon Managed Streaming for Apache Kafka 开发人员指南》中的启用对预置 MSK 集群的公共访问。

[MSK.5] MSK 连接器应启用日志记录

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::KafkaConnect::Connector`

AWS Config 规则：msk-connect-connector-logging-enabled

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon MSK 连接器启用了日志记录。如果 MSK 连接器禁用了日志记录，则该控件会失败。

Amazon MSK 连接器通过不断地将流数据从数据来源复制到 Apache Kafka 集群，或不断地将数据从集群复制到数据接收器，将外部系统和 Amazon 服务与 Apache Kafka 集成。MSK Connect 可以写入日志事件，这有助于调试连接器。创建连接器时，您可以指定以下零个或多个日志目标：亚马逊 CloudWatch 日志、亚马逊 S3 和 Amazon Data Firehose。

> **Note**
>
> 如果插件未将敏感配置值定义为秘密，则这些值可能会出现在连接器日志中。Kafka Connect 对未定义的配置值的处理方式与任何其他明文值相同。

修复

要为现有 Amazon MSK 连接器启用日志记录，您必须使用适当的日志记录配置重新创建连接器。有关配置选项的信息，请参阅《Amazon Managed Streaming for Apache Kafka 开发人员指南》中的为 MSK Connect 进行日志记录。

[MSK.6] MSK 集群应禁用未经身份验证的访问

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::MSK::Cluster`

AWS Config 规则：msk-unrestricted-access-check

计划类型：已触发变更

参数：无

此控件检查 Amazon MSK 集群是否启用了未经身份验证的访问。如果 MSK 集群启用了未经身份验证的访问，则该控件会失败。

Amazon MSK 支持客户端身份验证和授权机制，可控制对集群的访问。这些机制验证连接到集群的客户端的身份，并确定客户端可以执行哪些操作。可以将 MSK 集群配置为允许未经身份验证的访问，这样任何具有网络连接的客户端无需提供凭证都可以发布和订阅 Kafka 主题。运行 MSK 集群而不要求身份验证违反了最低权限原则，并且可能使集群暴露于未经授权的访问。它允许任何客户端访问、修改或删除 Kafka 主题中的数据，这可能会导致数据泄露、未经授权的数据修改或服务中断。我们建议启用 IAM 身份验证、SASL/SCRAM 或双向 TLS 等身份验证机制，以确保适当的访问控制并保持安全合规性。

修复

有关更改亚马逊 MSK 集群身份验证设置的信息，请参阅《适用于 Apache Managed Kafka 的亚马逊托管流管理开发者指南》的以下部分：更新亚马逊 MSK 集群的安全设置以及 Apache Kafka 的身份验证和授权。 APIs

适用于亚马逊 MQ 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon MQ 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch

相关要求： 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`mq-cloudwatch-audit-log-enabled`

计划类型：已触发变更

参数：无

此控件可检查 Amazon MQ ActiveMQ 代理是否将审计日志流式传输到亚马逊日志。 CloudWatch 如果代理不将审核日志流式传输到日 CloudWatch 志，则控制失败。

通过将 ActiveMQ 代理日志发布 CloudWatch 到日志，您可以 CloudWatch 创建警报和指标，以提高安全相关信息的可见性。

修复

要将 ActiveMQ 代理日志流式传输 CloudWatch 到日志，请参阅亚马逊 MQ 开发者指南中的为 Amazon MQ 日志配置 Amazon MQ。

[MQ.4] 应给亚马逊 MQ 经纪人加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则:`tagged-amazonmq-broker`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon MQ 代理是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果代理没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果代理未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Amazon MQ 代理添加标签，请参阅《Amazon MQ Developer Guide》中的 Tagging resources。

[MQ.5] ActiveMQ 代理应使用部署模式 active/standby

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`mq-active-deployment-mode`

计划类型：已触发变更

参数：无

此控件会检查 Amazon MQ ActiveMQ 代理的部署模式是否设置为。 active/standby如果将单实例代理（默认启用）设置为部署模式，则控制失败。

Active/standby 部署为你的 Amazon MQ ActiveMQ 代理提供了高可用性。 AWS 区域 active/standby 部署模式包括位于两个不同可用区的两个代理实例，它们配置为冗余对。这些代理与应用程序同步通信，这可以减少发生故障时的停机时间和数据丢失。

修复

要使用部署模式创建新 ActiveMQ 代理 active/standby ，请参阅亚马逊 MQ 开发者指南中的创建和配置 ActiveMQ 代理。对于部署模式，请选择Active/standby 代理。您无法变更现有代理的部署模式。相反，您必须创建一个新的代理并复制旧代理的设置。

[MQ.6] RabbitMQ 代理应使用集群部署模式

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`mq-rabbit-deployment-mode`

计划类型：已触发变更

参数：无

此控件检查 Amazon MQ RabbitMQ 代理的部署模式是否设置为集群部署。如果将单实例代理（默认启用）设置为部署模式，则控制失败。

集群部署为 AWS 区域中的 Amazon MQ RabbitMQ 代理提供了高可用性。集群部署是三个 RabbitMQ 代理节点的逻辑分组，每个节点都有自己的 Amazon Elastic Block Store（Amazon EBS）卷和共享状态。集群部署确保数据被复制到集群中的所有节点，这可以减少故障时的停机时间和数据丢失。

修复

要创建具有集群部署模式的新 RabbitMQ 代理，请参阅 Amazon MQ 开发人员指南中的创建和连接 RabbitMQ 代理。对于部署模式，选择集群部署。您无法变更现有代理的部署模式。相反，您必须创建一个新的代理并复制旧代理的设置。

适用于 Neptune 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Neptune 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Neptune.1] 应对 Neptune 数据库集群进行静态加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否进行静态加密。如果 Neptune 数据库集群未在静态状态下加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。加密您的 Neptune 数据库集群可保护数据和元数据免遭未经授权的访问。它还满足了生产文件系统 data-at-rest加密的合规性要求。

修复

您可以在创建 Neptune 数据库集群时启用静态加密。创建集群后，您将无法变更加密设置。有关更多信息，请参阅 Neptune 用户指南中的加密 Neptune 静态资源。

[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、、 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-20 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 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-4 (5)、nist.800-53.r5 SI-7 (8)、I DSS v4.0.1/10.3.3

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-cloudwatch-log-export-enabled`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否将审核日志发布到 Ama CloudWatch zon 日志。如果 Neptune 数据库集群不向 CloudWatch 日志发布审核日志，则控制失败。 `EnableCloudWatchLogsExport`应设置为`Audit`。

Amazon Neptune 和亚马逊 CloudWatch 是集成在一起的，因此您可以收集和分析绩效指标。Neptune 会自动向警报发送指标 CloudWatch ，还支持 CloudWatch 警报。审核日志是高度可定制的。审计数据库时，可以监视对数据的每个操作并将其记录到审计跟踪记录中，包括有关访问哪个数据库集群以及如何访问的信息。我们建议将这些日志发送到， CloudWatch 以帮助您监控 Neptune 数据库集群。

修复

要将 Neptune 审核日志发布到日 CloudWatch 志，请参阅《Neptune 用户指南》 CloudWatch 中的 “将 Neptune 日志发布到亚马逊日志”。在日志导出部分中，选择审计。

[Neptune.3] Neptune 数据库集群快照不应公开

相关要求： 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、、、(11) NIST.800-53.r5 AC-6 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)、(4)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9)、 NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::RDS::DBClusterSnapshot`

AWS Config 规则：`neptune-cluster-snapshot-public-prohibited`

计划类型：已触发变更

参数：无

此控件检查 Neptune 手动数据库集群快照是否公开。如果 Neptune 手动数据库集群快照是公开的，则控制失败。

除非有意图，否则 Neptune 数据库集群手动快照不应公开。如果您将未加密的手动快照公开共享，则该快照可供所有 AWS 账户使用。公开快照可能会导致意外的数据泄露。

修复

要移除 Neptune 手动数据库集群快照的公共访问权限，请参阅 Neptune 用户指南中的共享数据库集群快照。

[Neptune.4] Neptune 数据库集群应启用删除保护

相关要求： 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)

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-deletion-protection-enabled`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否启用了删除保护。如果 Neptune 数据库集群未启用删除保护，则控制失败。

启用集群删除保护可提供额外保护，防止数据库意外删除或未经授权的用户删除。启用删除保护时，无法删除 Neptune 数据库集群。您必须先禁用删除保护，删除请求才能成功。

修复

要为现有 Neptune 数据库集群启用删除保护，请参阅 Amazon Aurora 用户指南中的使用控制台、CLI 和 API 修改数据库集群。

[Neptune.5] Neptune 数据库集群应启用自动备份

相关要求：NIST.800-53.r5 SI-12。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-backup-retention-check`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`minimumBackupRetentionPeriod`	最小备份保留期（以天为单位）	整数	7 到 35	7	

此控件检查 Neptune 数据库集群是否启用了自动备份，以及备份保留期是否大于或等于指定时间范围。如果没有为 Neptune 数据库集群启用备份，或者保留期小于指定时间范围，则控制失败。除非您为备份保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 7 天。

备份可帮助您更快地从安全事件中恢复并增强系统的故障恢复能力。通过自动备份 Neptune 数据库集群，您将能够将系统恢复到某个时间点，并最大限度地减少停机时间和数据丢失。

修复

要启用自动备份并为 Neptune 数据库集群设置保留期，请参阅《Amazon RDS 用户指南》中的启用自动备份。对于备份保留期，请选择大于或等于 7 的值。

[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、NIST.800-53.r5 SC-2 8、 NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、 NIST.800-53.r5 SC-7 (18)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBClusterSnapshot`

AWS Config 规则：`neptune-cluster-snapshot-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群快照是否处于静态加密状态。如果 Neptune 数据库集群未在静态状态下加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。为了增加安全性，Neptune 数据库集群快照中的数据应进行静态加密。

修复

您无法加密现有的 Neptune 数据库集群快照。相反，您必须将快照还原到新的数据库集群并在集群上启用加密。您可以从加密集群创建加密快照。有关说明，请参阅 Neptune 用户指南中的从数据库集群快照恢复和在 Neptune 中创建数据库集群快照。

[Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证

相关要求： 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

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-iam-database-authentication`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否启用了 IAM 数据库身份验证。如果未为 Neptune 数据库集群启用 IAM 数据库身份验证，则控制失败。

Amazon Neptune 数据库集群的 IAM 数据库身份验证无需在数据库配置中存储用户凭证，因为身份验证是使用 IAM 在外部管理的。启用 IAM 数据库身份验证后，每个请求都需要使用签 AWS 名版本 4 进行签名。

修复

默认情况下，创建 Neptune 数据库集群时禁用 IAM 数据库身份验证。要启用它，请参阅 Neptune 用户指南中的在 Neptune 中启用 IAM 数据库身份验证。

[Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-copy-tags-to-snapshot-enabled`

计划类型：已触发变更

参数：无

此控制会检查 Neptune 数据库集群是否配置为在创建快照时将所有标签复制到快照。如果 Neptune 数据库集群未配置为将标签复制到快照，则控制失败。

IT 资产的识别和清点是治理和安全的一个重要方面。您应使用与其父级 Amazon RDS 数据库集群相同的方式为快照添加标签。复制标签可确保数据库快照的元数据与父数据库集群的元数据匹配，并且数据库快照的访问策略也与父数据库实例的访问策略匹配。

修复

要将标签复制到 Neptune 数据库集群的快照，请参阅 Neptune 用户指南中的在 Neptune 中复制标签。

[Neptune.9] Neptune 数据库集群应跨多个可用区部署

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-multi-az-enabled`

计划类型：已触发变更

参数：无

此控件会检查 Amazon Neptune 数据库集群在多个可用区中是否有只读副本实例（ ）。AZs如果集群仅部署在一个可用区中，则控制失败。

如果可用区不可用且处于定期维护事件期间，只读副本将用作主实例的失效转移目标。也就是说，如果主实例失败，Neptune 将只读副本实例提升为主实例。相比之下，如果您的数据库集群不包含任何只读副本实例，则当主实例出现故障时，您的数据库集群将保持不可用状态，直到重新创建该实例。与提升只读副本相比，重新创建主实例所需的时间要长得多。为确保高可用性，我们建议您创建一个或多个只读副本实例，这些实例的数据库实例类别与主实例相同，并且位于不同的 AZs 主实例中。

修复

要在多个中部署 Neptune 数据库集群 AZs，请参阅《Neptune 用户指南》中的 Neptune 数据库集群中的只读副本数据库实例。

Security Hub CSPM 控件适用于 AWS Network Firewall

这些 AWS Security Hub CSPM 控制措施评估 AWS Network Firewall 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则：netfw-multi-az-enabled

计划类型：已触发变更

参数：无

此控件评估通过管理的防火墙 AWS Network Firewall 是否部署在多个可用区 (AZs)。如果防火墙仅部署在一个可用区中，则控制失败。

AWS 全球基础设施包括多个 AWS 区域。 AZs 在每个区域内都是物理上分开的、孤立的地点，通过低延迟、高吞吐量和高度冗余的网络连接。通过在多个 AZs防火墙上部署 Network Firewall 防火墙 AZs，您可以平衡和转移流量，这有助于您设计高度可用的解决方案。

修复

在多个防火墙上部署 Network Firewall AZs

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中的网络防火墙 下，选择防火墙。
3. 在防火墙页面上，选择要编辑的防火墙。
4. 在防火墙详细信息页面上，选择防火墙详细信息选项卡。
5. 在关联策略和 VPC 部分中，选择编辑
6. 要添加新的可用区，请选择添加新子网。请选择您要使用的可用区和子网。确保至少选择两个 AZs。
7. 选择保存。

[NetworkFirewall.2] 应启用 Network Firewall 日志记录

相关要求： NIST.800-53.r5 AC-2(12)、(4)、(26)、(9)、 NIST.800-53.r5 AC-2 (9)、(9)、nist.800-53.r5 SI-3 NIST.800-53.r5 AC-4 (8)、 NIST.800-53.r5 AC-6 nist.800-53.r5 SI-4 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 SI-4 NIST.800-53.r5 SC-7 (20)、nist.800-53.r5 SI-7 (8)、nist.800-171.r2 3.1.r2 3.1.r2 (20)、nist.800-53.r5 SI-7 (8) 20，nist.800-171.r2 3.13.1

类别：识别 > 日志记录

严重性：中

资源类型：AWS::NetworkFirewall::LoggingConfiguration

AWS Config 规则：netfw-logging-enabled

计划类型：定期

参数：无

此控件检查是否已为 AWS Network Firewall 防火墙启用日志记录。如果没有为至少一种日志类型启用日志记录或者日志记录目标不存在，则控制失败。

日志记录可帮助您保持防火墙的可靠性、可用性和性能。在 Network Firewall 中，日志记录为您提供有关网络流量的详细信息，包括有状态引擎接收数据包流的时间、有关数据包流的详细信息以及针对数据包流采取的任何有状态规则操作。

修复

要启用防火墙日志记录，请参阅《AWS Network Firewall 开发人员指南》中的更新防火墙的日志记录配置。

[NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-171.r2 3.1.3、nist.800-171.r2 3.13.1

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 规则：netfw-policy-rule-group-associated

计划类型：已触发变更

参数：无

此控件检查 Network Firewall 策略是否关联了任何状态或无状态规则组。如果未分配无状态或有状态规则组，则控制失败。

防火墙策略定义防火墙如何监控和处理 Amazon Virtual Private Cloud（Amazon VPC）中的流量。配置无状态和有状态规则组有助于筛选数据包和流量，并定义默认流量处理。

修复

要向 Network Firewall 策略添加规则组，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙策略。有关创建和管理规则组的信息，请参阅 AWS Network Firewall中的规则组。

[NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::NetworkFirewall::FirewallPolicy`

AWS Config 规则：netfw-policy-default-action-full-packets

计划类型：已触发变更

参数：

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`（不可自定义）

此控件检查 Network Firewall 策略中对完整数据包的默认无状态操作是丢弃还是转发。如果选择了 `Drop` 或 `Forward`，则控制通过，如果选择 `Pass` 则控制失败。

防火墙策略定义防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来筛选数据包和流量。默认为 `Pass` 可能会允许意外流量。

修复

要变更您的防火墙策略，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙策略。对于无状态默认操作，请选择编辑。然后，选择丢弃或转发到有状态的规则组作为操作。

[NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-171.r2 3.1.3、nist.800-171.r2 3.1.14、nist.800-171.r2 3.13.1、nist.800-171.r2 3.13.6

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 规则：netfw-policy-default-action-fragment-packets

计划类型：已触发变更

参数：

- statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe (不可自定义)

此控件检查 Network Firewall 策略中对碎片数据包的默认无状态操作是丢弃还是转发。如果选择了 Drop 或 Forward，则控制通过，如果选择 Pass 则控制失败。

防火墙策略定义防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来筛选数据包和流量。默认为 Pass 可能会允许意外流量。

修复

要变更您的防火墙策略，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙策略。对于无状态默认操作，请选择编辑。然后，选择丢弃或转发到有状态的规则组作为操作。

[NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

相关要求： NIST.800-53.r5 AC-4(21)、(11)、(16)、(21)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 SC-7、nist.800-171.r2 3.1.3、 NIST.800-53.r5 SC-7 nist.800-171.r2 3.1.14、nist.800-171.r2 3.1.14、nist.800-171.r2 3.13.1、nist.800-171.r2 3.13.6 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::RuleGroup

AWS Config 规则：netfw-stateless-rule-group-not-empty

计划类型：已触发变更

参数：无

此控件检查中的无状态规则组是否 AWS Network Firewall 包含规则。如果规则组中没有规则，则控制失败。

规则组包含的规则定义防火墙如何处理您的 VPC 中的流量。当防火墙策略中存在空的无状态规则组时，可能会给人一种规则组将处理流量的印象。但是，当无状态规则组为空时，它不处理流量。

修复

要将规则添加到 Network Firewall 规则组，请参阅 AWS Network Firewall 开发人员指南中的更新有状态规则组。在防火墙详细信息页面上，对于无状态规则组，选择编辑以添加规则。

[NetworkFirewall.7] 应标记 Network Firewall 防火墙

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则:`tagged-networkfirewall-firewall`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Network Firewall 防火墙是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果防火墙没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果防火墙未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些

ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Network Firewall 防火墙添加标签，请参阅《AWS Network Firewall 开发者指南》中的标记 AWS Network Firewall 资源。

[NetworkFirewall.8] 应标记 Network Firewall 防火墙策略

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::NetworkFirewall::FirewallPolicy`

AWS Config 规则:`tagged-networkfirewall-firewallpolicy`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Network Firewall 防火墙策略是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果防火墙策略没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果

防火墙策略未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Network Firewall 策略添加标签，请参阅《AWS Network Firewall 开发者指南》中的标记 AWS Network Firewall 资源。

[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

相关要求： 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)

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则：netfw-deletion-protection-enabled

计划类型：已触发变更

参数：无

此控件检查 AWS Network Firewall 防火墙是否启用了删除保护。如果未为防火墙启用删除保护，则控制失败。

AWS Network Firewall 是一项有状态的托管网络防火墙和入侵检测服务，可让您检查和过滤进出虚拟私有云或虚拟私有云之间的流量（VPCs）。删除保护设置可防止意外删除防火墙。

修复

要在现有 Network Firewall 防火墙上启用删除保护，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙。对于变更保护，选择启用。您也可以通过调用 UpdateFirewallDeleteProtectionAPI 并将该`DeleteProtection`字段设置为来`true`启用删除保护。

[NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护

相关要求： 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)

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则：netfw-subnet-change-protection-enabled

计划类型：已触发变更

参数：无

此控件检查 AWS Network Firewall 防火墙是否启用了子网更改保护。如果未为防火墙启用子网更改保护，则该控件会失败。

AWS Network Firewall 是一项有状态的托管网络防火墙和入侵检测服务，可用于检查和过滤进出虚拟私有云或虚拟私有云之间的流量（VPCs）。如果为 Network Firewall 防火墙启用子网更改保护，则可以保护防火墙免遭其子网关联意外更改。

修复

有关为现有 Network Firewall 防火墙启用子网更改保护的信息，请参阅《AWS Network Firewall 开发人员指南》中的 Updating a firewall。

适用于亚马逊服务的 Security Hub CSPM 控件 OpenSearch

这些 AWS Security Hub CSPM 控制措施评估亚马逊 OpenSearch 服务（OpenSearch 服务）服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Opensearch.1] OpenSearch 域名应启用静态加密

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、(1)、3、8、8 (1)、nist.800-53.r5 SI-7 (6) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-encrypted-at-rest`

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域名是否启用了 encryption-at-rest配置。如果未启用静态加密，检查将失败。

为了增加敏感数据的安全性，您应将 OpenSearch 服务域配置为静态加密。配置静态数据加密时，会 AWS KMS 存储和管理您的加密密钥。要执行加密，请 AWS KMS 使用带有 256 位密钥的高级加密标准算法 (AES-256)。

要了解有关静态 OpenSearch 服务加密的更多信息，请参阅《亚马逊服务开发者指南》中的亚马逊 OpenSearch 服务静态数据加密。 OpenSearch

修复

要为新域和现有 OpenSearch 域名启用静态加密，请参阅 Amazon S OpenSearch ervice 开发者指南中的启用静态数据加密。

[Opensearch.2] OpenSearch 域名不应向公众开放

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、 NIST.800-53.r5 AC-2 1、、 NIST.800-53.r5 AC-3（7）、（21）、（11）、（16）、（20）、（21）、（3） NIST.800-53.r5 AC-3、（4），(9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：严重

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-in-vpc-only`

计划类型：已触发变更

参数：无

此控件可检查 OpenSearch 域是否在 VPC 中。它不会评估 VPC 子网路由配置来确定公共访问。

您应确保 OpenSearch 域名未连接到公有子网。请参阅《Amazon OpenSearch 服务开发者指南》中的基于资源的政策。您还应该确保根据建议的最佳实践配置了 VPC。请参阅 Amazon VPC 用户指南中的 VPC 安全最佳实践。

OpenSearch 部署在 VPC 中的域可以通过私有 AWS 网络与 VPC 资源通信，无需穿越公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。 VPCs 提供多种网络控制措施来保护对 OpenSearch 域的访问，包括网络 ACL 和安全组。Security Hub 建议您将公共 OpenSearch 域迁移 VPCs 到以利用这些控制措施。

修复

如果您创建一个具有公有端点的域，则以后无法将其放置在 VPC 中。您必须创建一个新的域，然后迁移数据。反之亦然。如果在 VPC 中创建一个域，则该域不能具有公有端点。您必须创建另一个域或禁用该控制。

有关说明，请参阅《亚马逊 OpenSearch 服务开发者指南》中的在 VPC 内启动您的亚马逊 OpenSearch 服务域。

[Opensearch.3] OpenSearch 域应加密节点之间发送的数据

相关要求： NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-1 3、 NIST.800-53.r5 SC-2 3、NIST.800-53.r5 SC-2 3 (3)、 NIST.800-53.r5 SC-7 (3)、(4) NIST.800-53.r5 SC-8、 NIST.800-53.r5 SC-8 (1)、 NIST.800-53.r5 SC-8 (2)

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：opensearch-node-to-node-encryption-check

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域名是否启用了 node-to-node加密。如果在域上禁用了 node-to-node加密，则此控件将失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击窃听或操纵网络流量。只能允许通过 HTTPS（TLS）进行加密连接。为 OpenSearch 域启用 node-to-node加密可确保集群内部通信在传输过程中得到加密。

此配置可能会降低性能。在启用此选项之前，您应该了解并测试性能权衡。

修复

要在 OpenSearch 域上启用 node-to-node加密，请参阅《亚马逊 OpenSearch 服务开发者指南》中的启用 node-to-node加密。

[Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、、 NIST.800-53.r5 AC-4 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 AC-6 (8) 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 SI-4 NIST.800-53.r5 SC-7 (20)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：opensearch-logs-to-cloudwatch

计划类型：已触发变更

参数：

- logtype = 'error'（不可自定义）

此控件检查 OpenSearch 域是否配置为向日志发送错误 CloudWatch 日志。如果未为域启用错误记录功能， CloudWatch 则此控件将失败。

您应该为 OpenSearch 域启用错误日志，并将这些日志发送到 CloudWatch 日志以进行保留和响应。域错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

修复

要启用日志发布，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用日志发布（控制台）。

[Opensearch.5] OpenSearch 域应启用审核日志

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、PCI DSS v4.0.1/10.2.1 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-audit-logging-enabled`

计划类型：已触发变更

参数：

- `cloudWatchLogsLogGroupArnList`（不可自定义）— Security Hub CSPM 不填充此参数。应为审核日志配置的 CloudWatch 日志组列表，以逗号分隔。

此控件检查 OpenSearch 域名是否启用了审核日志。如果 OpenSearch 域未启用审核日志，则此控件将失败。

审核日志是高度可定制的。它们允许您跟踪OpenSearch 集群上的用户活动，包括身份验证成功和失败、对身份验证的请求OpenSearch、索引更改以及传入的搜索查询。

修复

有关启用审计日志的说明，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用审计日志。

[Opensearch.6] OpenSearch 域名应至少有三个数据节点

相关要求： 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：opensearch-data-node-fault-tolerance

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域是否配置了至少三个数据节点，并且`zoneAwarenessEnabled`是`true`。如果 OpenSearch 域小于 3 或小`instanceCount`于 3，`zoneAwarenessEnabled`则此控制失败`false`。

要实现集群级别的高可用性和容错能力，一个 OpenSearch 域应至少有三个数据节点。部署具有至少三个数据节点的 OpenSearch 域可确保在节点出现故障时集群运行。

修复

修改 OpenSearch 域中数据节点的数量

1. 登录 AWS 控制台并打开亚马逊 OpenSearch 服务控制台，网址为https://console.aws.amazon.com/aos/。
2. 在我的域名下，选择要编辑的域名，然后选择编辑。
3. 在数据节点下，将节点数设置为大于 3 的数字。如果您要部署到三个可用区，将该数字设置为三的倍数，以确保可用区间的分布均等。
4. 选择提交。

[Opensearch.7] OpenSearch 域名应启用精细的访问控制

相关要求： 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

类别：保护 > 安全访问管理 > 敏感的 API 操作受限

严重性：高

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：opensearch-access-control-enabled

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域名是否启用了细粒度访问控制。如果未启用精细访问控制，则控制失败。细粒度的访问控制需要advanced-security-options在 OpenSearch 参数中启update-domain-config用。

精细的访问控制提供了更多方法来控制对您在 Ama OpenSearch zon Service 上的数据的访问权限。

修复

要启用精细访问控制，请参阅《亚马逊服务开发者指南》中的 Amazon Service OpenSearch 中的精细访问控制。 OpenSearch

[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密

相关要求： NIST.800-53.r5 AC-17 (2)、、 NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-1 2 (3)、3、3 (NIST.800-53.r5 SC-13)、(NIST.800-53.r5 SC-23)、NIST.800-53.r5 SC-2 (4)、(1)、 NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8、 NIST.800-53.r5 SC-8 nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：opensearch-https-required

计划类型：已触发变更

参数：

- tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10 (不可自定义)

此控制检查是否将 Amazon S OpenSearch ervice 域终端节点配置为使用最新的 TLS 安全策略。如果 OpenSearch 域终端节点未配置为使用最新的支持策略或 HTTPs 未启用，则控制失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。只能允许通过 HTTPS（TLS）进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试应用程序，以了解性能概况和 TLS 的影响。与先前版本的 TLS 相比，TLS 1.2 提供了多项安全增强功能。

修复

要启用 TLS 加密，请使用 UpdateDomainConfigAPI 操作。配置DomainEndpointOptions字段以指定其值TLSSecurityPolicy。有关更多信息，请参阅《Amazon OpenSearch 服务开发者指南》中的Node-to-node 加密。

[Opensearch.9] 应该给 OpenSearch 域名加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::OpenSearch::Domain

AWS Config 规则:tagged-opensearch-domain（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	No default value

此控件会检查 Amazon S OpenSearch ervice 域名是否具有参数中定义的特定密钥的标签requiredTagKeys。如果该域没有任何标签键或未在参数 requiredTagKeys 中指定所有键，则此控件会失败。如果未提供 requiredTagKeys 参数，则此控件仅会检查是否存在标签键，如果该域未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控

制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 OpenSearch 服务域添加标签，请参阅《亚马逊 OpenSearch 服务开发者指南》中的使用标签。

[Opensearch.10] OpenSearch 域名应安装最新的软件更新

相关要求：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

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-update-check`

计划类型：已触发变更

参数：无

此控件用于检查 Amazon S OpenSearch ervice 域是否安装了最新的软件更新。如果已有可用软件更新但没有为该域安装，则控制失败。

OpenSearch 服务软件更新提供适用于该环境的最新平台修复、更新和功能。继续 up-to-date安装补丁有助于维护域的安全性和可用性。如果没有对必需更新采取任何操作，将自动更新服务软件（通常在 2 周后）。我们建议在域流量较低的时段安排更新，以最大限度地减少服务中断。

修复

要为 OpenSearch 域安装软件更新，请参阅《Amazon OpenSearch 服务开发者指南》中的启动更新。

[Opensearch.11] OpenSearch 域名应至少有三个专用的主节点

相关要求： 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

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-primary-node-fault-tolerance`

计划类型：已触发变更

参数：无

此控件会检查 Amazon S OpenSearch ervice 域是否配置了至少三个专用主节点。如果域的专用主节点少于三个，则此控件将失败。

OpenSearch 服务使用专用的主节点来提高集群稳定性。专用主节点执行集群管理任务，但不保留数据也不响应数据上传请求。我们建议您使用带备用空间的多可用区，这会向每个生产 OpenSearch 域添加三个专用的主节点。

修复

要更改 OpenSearch 域的主节点数量，请参阅《亚马逊 OpenSearch 服务开发者指南》中的创建和管理亚马逊 OpenSearch 服务域名。

Security Hub CSPM 控件适用于 AWS 私有 CA

这些 AWS Security Hub CSPM 控件评估 AWS 私有证书颁发机构 (AWS 私有 CA) 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::ACMPCA::CertificateAuthority`

AWS Config 规则：acm-pca-root-ca-disabled

计划类型：定期

参数：无

此控件检查根证书颁发机构 (CA) 是否 AWS 私有 CA 已禁用。如果启用了根 CA，则控制失败。

使用 AWS 私有 CA，您可以创建包含根 CA 和下属 CA 的 CA 层次结构 CAs。您应该尽量减少在日常任务中使用根 CA，尤其是在生产环境中。根 CA 只能用于颁发中间证书 CAs。这允许将根 CA 存储在远离危险的地方，而中间证书可以 CAs 执行签发最终实体证书的日常任务。

修复

要禁用根 CA，请参阅《AWS 私有证书颁发机构 用户指南》中的更新 CA 状态。

[PCA.2] 应标记 AWS 私有 CA 证书颁发机构

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::ACMPCA::CertificateAuthority

AWS Config 规则：acmpca-certificate-authority-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS 私有 CA 证书颁发机构是否具有参数中定义的特定密钥的标签requiredKeyTags。如果证书颁发机构没有任何标签键或者未在参数 requiredKeyTags 中指定所有键，则此控件会失败。如果未提供参数 requiredKeyTags，则该控件仅检查是否存在标签键，如果证书颁发机构未使用任何键进行标记，则此控件会失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标签最佳实践，请参阅《标签 AWS 资源和标签编辑器用户指南》中的最佳做法和策略。

修复

要向 AWS 私有 CA 机构添加标签，请参阅AWS 私有证书颁发机构 用户指南中的为私有 CA 添加标签。

适用于 Amazon RDS 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估亚马逊关系数据库服务 (Amazon RDS) 和亚马逊 RDS 资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[RDS.1] RDS 快照应该是私有的

相关要求：PCI DSS v3.2。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.4，PCI DSS v3.2。 1/1.3.6，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、 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)

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::RDS::DBClusterSnapshot`、`AWS::RDS::DBSnapshot`

AWS Config 规则：`rds-snapshots-public-prohibited`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 快照是否公有。如果 RDS 快照是公开的，则控制失败。此控件评估 RDS 实例、Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群。

RDS 快照用于备份 RDS 实例上在特定时间点的数据。它们可用于将 RDS 实例还原到之前的状态。

除非有意这样做，否则 RDS 快照不得为公有快照。如果您将未加密的手动快照作为公有快照进行共享，这会使所有 AWS 账户均可获得此快照。这可能会导致 RDS 实例意外的数据泄露。

请注意，如果将配置更改为允许公共访问，则该 AWS Config 规则可能在长达 12 小时内无法检测到更改。在 AWS Config 规则检测到更改之前，即使配置违反了规则，检查也会通过。

要了解有关共享数据库快照的更多信息，请参阅 Amazon RDS 用户指南中的共享数据库快照。

修复

要从 RDS 快照中删除公共访问权限，请参阅 Amazon RDS 用户指南中的共享快照。对于数据库快照可见性，我们选择私有。

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.2.3，CIS AWS 基金会基准测试 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、 NIST.800-53.r5 SC-7 (11)、(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。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.2，PCI DSS v3.2。 1/1.3.4，PCI DSS v3.2。 1/1.3.6，PCI DSS v3.2。 1/7.2.1，PCI DSS v4.0。 1/1.4.4

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-public-access-check`

计划类型：已触发变更

参数：无

该控制通过评估实例配置项中的 PubliclyAccessible 字段，以检查是否可以公开访问 Amazon RDS 实例。

Neptune 数据库实例和 Amazon DocumentDB 集群没有 PubliclyAccessible 标志，因此无法进行评估。但是，这种控件仍然可以为这些资源生成调查发现。您可以隐瞒这些调查发现。

RDS 实例配置中的 PubliclyAccessible 值指示是否可以公开访问数据库实例。当数据库实例配置为时PubliclyAccessible，它就是具有可公开解析的 DNS 名称的 Internet-facing 实例，该名称会解析为公有 IP 地址。如果无法公开访问数据库实例，则它是一个内部实例并具有解析为私有 IP 地址的 DNS 名称。

除非您希望 RDS 实例可公开访问，否则不应将 RDS 实例配置为 PubliclyAccessible 值。这样做可能会给数据库实例带来不必要的流量。

修复

要移除 RDS 数据库实例的公有访问权限，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。对于公有访问权限，选择否。

[RDS.3] RDS 数据库实例应启用静态加密

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.2.1，CIS AWS 基金会基准 v3.0。 0/2.3.1，CIS AWS 基金会基准 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::RDS::DBInstance

AWS Config 规则：rds-storage-encrypted

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库实例是否启用了存储加密。

此控件适用于 RDS 数据库实例。但是，它也可以生成 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的调查发现。如果这些调查发现没有用，那么您可以隐瞒它们。

为了增加 RDS 数据库实例中敏感数据的安全性，您应将 RDS 数据库实例配置为静态加密。要静态加密 RDS DB 数据库实例和快照，请启用 RDS 数据库实例的加密选项。静态加密的数据包括数据库实例的底层存储、自动备份、只读副本和快照。

RDS 加密的数据库实例使用开放标准 AES-256 加密算法对托管 RDS 数据库实例的服务器上的数据进行加密。在加密数据后，Amazon RDS 将以透明方式处理访问的身份验证和数据的解密，并且对性能产生的影响最小。您无需修改数据库客户端应用程序来使用加密。

Amazon RDS 加密当前可用于所有数据库引擎和存储类型。Amazon RDS 加密适用于大多数数据库实例类。要了解不支持 Amazon RDS 加密的数据库实例类，请参阅 Amazon RDS 用户指南中的加密 Amazon RDS 资源。

修复

有关在 Amazon RDS 中加密数据库实例的信息，请参阅 Amazon RDS 用户指南中的加密 Amazon RDS 资源。

[RDS.4] RDS 集群快照和数据库快照应在静态时加密

相关要求： 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::RDS::DBClusterSnapshot`、 `AWS::RDS::DBSnapshot`

AWS Config 规则：`rds-snapshot-encrypted`

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库快照是否已加密。如果 RDS 数据库快照未加密，则控制失败。

此控件适用于 RDS 数据库实例。但是，它也可以生成 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的快照的调查发现。如果这些调查发现没有用，那么您可以隐瞒它们。

对静态数据进行加密可降低未经身份验证的用户访问存储在磁盘上的数据的风险。为了增加安全性，RDS 快照中的数据应进行静态加密。

修复

要加密 RDS 快照，请参阅 Amazon RDS 用户指南中的加密 Amazon RDS 资源。加密 RDS 数据库实例时，加密的数据包括实例的底层存储、其自动备份、只读副本和快照。

您只能在创建 RDS 数据库实例时而不是创建该数据库实例之后加密该数据库实例。不过，由于您可以加密未加密快照的副本，因此，您可以高效地为未加密的数据库实例添加加密。也就是说，您可以创建数据库实例快照，然后创建该快照的加密副本。然后，您可以从加密快照还原数据库实例，从而获得原始数据库实例的加密副本。

[RDS.5] RDS 数据库实例应配置多个可用区

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.2.4、 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-multi-az-support`

计划类型：已触发变更

参数：无

此控件检查是否为 RDS 数据库实例启用了高可用性。如果 RDS 数据库实例未部署在多个可用区（AZ）中，则此控件将失败。此控制不适用于作为数据库集群部署一部分的 RDS Multi-AZ 数据库实例。

使用可用区配置 Amazon RDS 数据库实例有助于确保存储数据的可用性。 Multi-AZ 部署允许在可用区可用性出现问题和定期 RDS 维护期间进行自动故障转移。

修复

要在多个可用区中部署数据库实例，请在 A mazon RDS 用户指南中将 Multi-AZ 数据库实例修改为数据库实例部署。

[RDS.6] 应为 RDS 数据库实例配置增强监控

相关要求： NIST.800-53.r5 CA-7， NIST.800-53.r5 SI-2

类别：检测 > 检测服务

严重性：低

资源类型：AWS::RDS::DBInstance

AWS Config 规则：rds-enhanced-monitoring-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
monitoringInterval	监控指标收集间隔之间的秒数	枚举	1, 5, 10, 15, 30, 60	无默认值	

该控件检查是否为 Amazon Relational Database Service（Amazon RDS）数据库实例启用了增强监控。如果没有为实例启用增强监控，则控制失败。如果您为 monitoringInterval 参数提供自定义值，则仅当在按指定间隔收集实例的增强监控指标时，控制才会通过。

在 Amazon RDS 中，增强型监控可以更快地响应底层基础设施的性能变化。这些性能变化可能会导致数据可用性不足。增强监控提供 RDS 数据库实例运行的操作系统的实时指标。实例上安装了代理。与从虚拟机管理程序层相比，代理可以更准确地获取指标。

若您想了解数据库实例上不同进程或线程对 CPU 的使用差异，增强监测指标非常有用。有关更多信息，请参阅《Amazon RDS 用户指南》中的增强监控。

修复

有关为数据库实例启用增强监控的详细说明，请参阅 Amazon RDS 用户指南中的设置和启用增强监控。

[RDS.7] RDS 集群应启用删除保护

相关要求： NIST.800-53.r5 CM-3， NIST.800-53.r5 SC-5(2)

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-deletion-protection-enabled`

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库集群是否已启用删除保护。如果 RDS 数据库集群未启用删除保护，则控制失败。

此控件适用于 RDS 数据库实例。但是，它也可以生成 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的调查发现。如果这些调查发现没有用，那么您可以隐瞒它们。

启用集群删除保护是针对意外数据库删除或未经授权实体删除的额外保护层。

启用删除保护后，RDS 集群将无法被删除。在删除请求成功之前，必须禁用删除保护。

修复

要为 RDS 数据库集群启用删除保护，请参阅 Amazon RDS 用户指南中的使用控制台、CLI 和 API 修改数据库集群。对于删除保护，选择启用删除保护。

[RDS.8] RDS 数据库实例应启用删除保护

相关要求： NIST.800-53.r5 CM-3、 NIST.800-53.r5 SC-5 (2)、 NIST.800-53.r5 SI-13 (5)

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-deletion-protection-enabled`

计划类型：已触发变更

参数：

- `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`（不可自定义）

此控件会检查使用所列数据库引擎之一的 RDS 数据库实例是否启用了删除保护。如果 RDS 数据库实例未启用删除保护，则控制失败。

启用实例删除保护是针对意外数据库删除或未经授权实体删除的额外保护层。

启用删除保护后，RDS 数据库实例无法删除。在删除请求成功之前，必须禁用删除保护。

修复

要对 RDS 数据库实例启用删除保护，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。对于删除保护，选择启用删除保护。

[RDS.9] RDS 数据库实例应将日志发布到 CloudWatch 日志

相关要求： 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-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3、(4)、 NIST.800-53.r5 AU-6 (10)、(9) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (8)、 NIST.800-53.r5 SC-7 (20)、 NIST.800-53.r5 SI-3 (8)、(8)、 NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8)、PCI DSS v4.0。 1/10.2.1

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库实例是否配置为将以下日志发布到 Amazon L CloudWatch ogs。如果实例未配置为将以下日志发布到 CloudWatch 日志，则控制失败：

- Oracle：警报、审计、跟踪、侦听器
- PostgreSQL：Postgresql、升级
- MySQL：审计、错误、常规、 SlowQuery
- MariaDB：审计、错误、常规、 SlowQuery
- SQL Server：错误、代理
- Aurora-MySQL: 审计、错误、常规、 SlowQuery

- Aurora-PostgreSQL: Postgresql

RDS 数据库应启用相关日志。数据库日志记录提供向 RDS 发出的请求的详细记录。数据库日志可以协助安全和访问审计，并可以帮助诊断可用性问题。

修复

有关将 RDS 数据库日志发布到 CloudWatch 日志的信息，请参阅 Amazon RDS 用户指南中的指定要发布到 CloudWatch 日志的日志。

[RDS.10] 应为 RDS 实例配置 IAM 身份验证

相关要求： 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

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-iam-authentication-enabled`

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库实例是否启用了 IAM 数据库身份验证。如果未为 RDS 数据库实例配置 IAM 身份验证，则控制失败。此控件仅评估具有以下引擎类型的 RDS 实例：`mysql`、`postgres`、`aurora`、`aurora-mysql`、`aurora-postgresql` 和 `mariadb`。RDS 实例还必须处于以下状态之一才能生成调查发现：`available`、`backing-up`、`storage-optimization` 或 `storage-full`。

IAM 数据库身份验证允许使用身份验证令牌而不是密码对数据库实例进行身份验证。进出数据库的网络流量使用 SSL 加密。有关更多信息，请参阅《Amazon Aurora 用户指南》中的 IAM 数据库身份验证。

修复

要在 RDS 数据库实例上激活 IAM 数据库身份验证，请参阅 Amazon RDS 用户指南中的启用和禁用 IAM 数据库身份验证。

[RDS.11] RDS 实例应启用自动备份

相关要求： 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)

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`db-instance-backup-enabled`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`backupRetentionMinimum`	最小备份保留期（以天为单位）	整数	7 到 35	7
`checkReadReplicas`	检查 RDS 数据库实例是否已针对只读副本启用备份。	布尔值	不可自定义	`false`

此控件检查 Amazon Relational Database Service 实例是否启用了自动备份以及备份保留期是否大于或等于指定时间范围。只读副本不在评估范围内。如果没有为实例启用备份或保留期小于指定时间范围，则控制失败。除非您为备份保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 7 天。

备份可帮助您更快地从安全事件中恢复并增强系统的故障恢复能力。Amazon RDS 使您能够配置每日完整实例卷快照。有关 Amazon RDS 自动备份的更多信息，请参阅《Amazon RDS 用户指南》中的处理备份。

修复

要在 RDS 数据库实例上启用自动备份，请参阅 Amazon RDS 用户指南中的启用自动备份。

[RDS.12] 应为 RDS 集群配置 IAM 身份验证

相关要求： 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

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-iam-authentication-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库集群是否启用了 IAM 数据库身份验证。

IAM 数据库身份验证允许对数据库实例进行免密码身份验证。身份验证使用身份验证令牌。进出数据库的网络流量使用 SSL 加密。有关更多信息，请参阅《Amazon Aurora 用户指南》中的 IAM 数据库身份验证。

修复

要为数据库集群启用 IAM 身份验证，请参阅 Amazon Aurora 用户指南中的启用和禁用 IAM 数据库身份验证。

[RDS.13] 应启用 RDS 自动次要版本升级

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.2.2，CIS AWS 基金会基准测试 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 v4.0。 1/6.3.3

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-automatic-minor-version-upgrade-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 RDS 数据库实例启用了自动次要版本升级。

自动次要版本升级会定期将数据库更新到新近的数据库引擎版本。但是，升级可能并不始终包括最新的数据库引擎版本。如果您需要在特定时间将数据库保持在特定版本上，我们建议您根据所需的时间表，手动升级到您需要的数据库版本。在出现严重安全问题的情况下或当版本达到其终止支持日期时，Amazon RDS 可能会应用次要版本升级，即使您尚未启用自动次要版本升级选项也是如此。有关更多信息，请参阅特定数据库引擎的 Amazon RDS 升级文档：

- MariaDB 版 RDS 的自动次要版本升级
- 适用于 MySQL 的 RDS 的自动次要版本升级
- 适用于 PostgreSQL 的 RDS 的自动次要版本升级
- 亚马逊 RDS 版本上的 Db2
- 甲骨文次要版本升级
- 微软 SQL Server 数据库引擎的升级

修复

要为现有数据库实例启用自动次要版本升级，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。对于自动次要版本升级，请选择是。

[RDS.14] 亚马逊 Aurora 集群应启用回溯功能

相关要求： 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)

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`aurora-mysql-backtracking-enabled`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`BacktrackWindowInHours`	回溯 Aurora MySQL 集群所需的小时数	双精度	`0.1` 到 `72`	无默认值	

此控件检查 Amazon Aurora 集群是否启用了回溯。如果集群未启用回溯，则控制失败。如果您为 `BacktrackWindowInHours` 参数提供自定义值，则仅当集群在指定的时间长度内被回溯时，控制才会通过。

备份可以帮助您更快地从安全事件中恢复。它们还可以增强系统的弹性。Aurora 回溯可将数据库还原到某个时间点的时间。这样做不需要数据库恢复。

修复

要启用 Aurora 回溯，请参阅《Amazon Aurora 用户指南》中的配置回溯。

请注意，您无法在现有集群上启用回溯功能。相反，您可创建启用回溯功能的克隆。有关 Aurora 回溯限制的更多信息，请参阅回溯概述中的限制列表。

[RDS.15] 应为多个可用区配置 RDS 数据库集群

相关要求：CIS AWS 基金会基准测试 v5.0。 0/2.2.4、 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)

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-multi-az-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 RDS 数据库集群启用了高可用性。如果 RDS 数据库集群未部署在多个可用区（AZ）中，则控制失败。

应为多个可用区配置 RDS 数据库集群，以确保存储数据的可用性。部署到多个可用区允许在出现可用区可用性问题和定期 RDS 维护事件期间进行自动失效转移。

修复

要在多个可用区中部署数据库集群，请在 A mazon RDS 用户指南中将 Multi-AZ 数据库实例修改为数据库实例部署。

Aurora 全球数据库的修复步骤有所不同。要为 Aurora 全球数据库配置多个可用区，请选择数据库集群。然后，选择操作和添加读取器，并指定多个 AZ。有关更多信息，请参阅 Amazon Aurora 用户指南中的将 Aurora 副本添加到数据库集群。

[RDS.16] 应将 Aurora 数据库集群配置为将标签复制到数据库快照

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-2、 NIST.800-53.r5 CM-2 (2)

类别：识别 > 清单

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则:`rds-cluster-copy-tags-to-snapshots-enabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查是否已配置 Amazon Aurora 数据库集群，以便在创建快照时自动将标签复制到数据库集群的快照。如果未将 Aurora DB 集群配置为在创建集群的快照时自动将标签复制到快照，则该控件会失败。

IT 资产的识别和清点是治理和安全的一个重要方面。您需要了解所有 Amazon Aurora 数据库集群的可见性，以便评测其安全状况并对潜在的薄弱环节采取行动。Aurora 数据库快照应该与其父数据库集群具有相同的标签。在 Amazon Aurora 中，您可以配置数据库集群，使其自动将集群的所有标签复制到集群的快照中。启用此设置可确保数据库快照继承与其父数据库集群相同的标签。

修复

有关配置 Amazon Aurora 数据库集群以自动将标签复制到数据库快照的信息，请参阅《Amazon Aurora 用户指南》中的修改 Amazon Aurora 数据库集群。

[RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-2、 NIST.800-53.r5 CM-2 (2)

类别：识别 > 清单

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则:`rds-instance-copy-tags-to-snapshots-enabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控制检查 RDS 数据库实例是否配置为在创建快照时将所有标签复制到快照。

IT 资产的识别和清点是治理和安全的一个重要方面。您需要了解所有 RDS 数据库实例，以便评测其安全状况并对潜在的薄弱环节采取行动。快照的标记方式应与其父 RDS 数据库实例相同。启用此设置可确保快照继承其父级数据库实例的标签。

修复

要自动将标签复制到 RDS 数据库实例的快照，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。选择将标签复制到快照。

[RDS.19] 应为关键群集事件配置现有 RDS 事件通知订阅

相关要求： NIST.800-53.r5 CA-7， NIST.800-53.r5 SI-2

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则:`rds-cluster-event-notifications-configured`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查数据库集群的现有 Amazon RDS 事件订阅是否为以下源类型和事件类别键值对启用了通知：

```
DBCluster: ["maintenance","failure"]
```

如果账户中没有现有活动订阅，则控件通过。

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 集群事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
Source type（源类型）	集群
要包括的集群	所有集群
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅

相关要求： NIST.800-53.r5 CA-7， NIST.800-53.r5 SI-2，PCI DSS v4.0。 1/11.5.2

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则:`rds-instance-event-notifications-configured`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查数据库实例的现有 Amazon RDS 事件订阅是否为以下源类型和事件类别键值对启用了通知：

```
DBInstance: ["maintenance","configuration change","failure"]
```

如果账户中没有现有活动订阅，则控件通过。

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 实例事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
Source type（源类型）	实例
要包括的实例	所有实例
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

相关要求： NIST.800-53.r5 CA-7， NIST.800-53.r5 SI-2，PCI DSS v4.0。 1/11.5.2

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则:`rds-pg-event-notifications-configured`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查是否存在针对以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。如果账户中没有现有活动订阅，则控件通过。

```
DBParameterGroup: ["configuration change"]
```

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 数据库参数组事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
Source type（源类型）	参数组
要包括的参数组	所有参数组
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.22] 应为关键的数据库安全组事件配置 RDS 事件通知订阅

相关要求： NIST.800-53.r5 CA-7， NIST.800-53.r5 SI-2，PCI DSS v4.0。 1/11.5.2

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则:`rds-sg-event-notifications-configured`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查是否存在针对以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。如果账户中没有现有活动订阅，则控件通过。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 实例事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
Source type（源类型）	安全组
要包括的安全组	所有安全组
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.23] RDS 实例不应使用数据库引擎的默认端口

相关要求： 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)

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则:`rds-no-default-ports`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件检查 RDS 集群或实例是否使用数据库引擎默认端口以外的端口。如果 RDS 集群或实例使用默认端口，则控制失败。此控件不适用于属于集群的 RDS 实例。

如果您使用已知端口部署 RDS 集群或实例，攻击者可以猜测有关集群或实例的信息。攻击者可以将此信息与其他信息结合使用来连接到 RDS 集群或实例，或者获取有关应用程序的其他信息。

变更端口时，还必须更新用于连接到旧端口的现有连接字符串。您还应检查数据库实例的安全组，确保其包含允许在新端口上进行连接的入口规则。

修复

要修改现有 RDS 数据库实例的默认端口，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。要修改现有 RDS 数据库集群的默认端口，请参阅 Amazon Aurora 用户指南中的使用控制台、CLI 和 API 修改数据库集群。对于数据库端口，将端口值变更为非默认值。

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

相关要求： NIST.800-53.r5 CA-9(1)， NIST.800-53.r5 CM-2，PCI DSS v4.0。 1/2.2.2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-default-admin-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库集群是否已将管理员用户名从其默认值变更为其他值。该控件不适用于 neptune（Neptune 数据库）或 docdb（DocumentDB）类型的引擎。如果管理员用户名设置为默认值，则此规则将失败。

创建 Amazon RDS 数据库时，应将默认管理员用户名变更为唯一值。默认用户名是众所周知的，应在创建 RDS 数据库期间进行变更。变更默认用户名可以降低意外访问的风险。

修复

要变更与 Amazon RDS 数据库集群关联的管理员用户名，请在创建数据库时创建一个新的 RDS 数据库集群并变更默认管理员用户名。

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

相关要求： NIST.800-53.r5 CA-9(1)， NIST.800-53.r5 CM-2，PCI DSS v4.0。 1/2.2.2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-default-admin-check`

计划类型：已触发变更

参数：无

此控件检查您是否变更了 Amazon Relational Database Service（Amazon RDS）数据库实例的管理用户名，而不是默认值。如果将管理用户名设置为默认值，则控制失败。该控件不适用于 neptune（Neptune 数据库）或 docdb（DocumentDB）类型的引擎，也不适用于属于集群一部分的 RDS 实例。

Amazon RDS 数据库上的默认管理用户名是众所周知的。创建 Amazon RDS 数据库时，应将默认管理用户名变更为唯一值，以降低意外访问的风险。

修复

要变更与 RDS 数据库实例关联的管理用户名，请先创建一个新的 RDS 数据库实例。在创建数据库时变更默认的管理用户名。

[RDS.26] RDS 数据库实例应受备份计划的保护

类别：恢复 > 弹性 > 启用备份

相关要求： 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)

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：**`rds-resources-protected-by-backup-plan`**

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`backupVaultLockCheck`	如果将参数设置为 true 且资源使用 AWS Backup	布尔值	`true` 或者 `false`	无默认值	

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
	文件库锁定，则控件会生成PASSED结果。				

此控件用于评估备份计划是否涵盖 Amazon RDS 数据库实例。如果备份计划未涵盖 RDS 数据库实例，则控制失败。如果将backupVaultLockCheck参数设置为true，则仅当实例备份到 AWS Backup 锁定的文件库中时，控制才会通过。

> **Note**
>
> 此控件不评估 Neptune 和 DocumentDB 实例。它也不会评估属于集群成员的 RDS 数据库实例。

AWS Backup 是一项完全托管的备份服务，可集中和自动备份数据。 AWS 服务使用 AWS Backup，您可以创建名为备份计划的备份策略。您可以使用这些计划来定义备份要求，例如数据的备份频率以及这些备份的保留时间。将 RDS 数据库实例纳入备份计划可帮助您保护数据免遭意外丢失或删除。

修复

要将 RDS 数据库实例添加到 AWS Backup 备份计划，请参阅《AWS Backup 开发人员指南》中的为备份计划分配资源。

[RDS.27] RDS 数据库集群应进行静态加密

相关要求： 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::RDS::DBCluster

AWS Config 规则：**rds-cluster-encrypted-at-rest**

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库集群是否进行静态加密。如果 RDS 数据库集群未进行静态加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。加密 RDS 数据库集群可保护数据和元数据免遭未经授权的访问。它还满足了生产文件系统静态数据加密的合规性要求。

修复

您可以在创建 RDS 数据库集群时启用静态加密。创建集群后，您将无法变更加密设置。有关更多信息，请参阅 Amazon Aurora 用户指南中的加密 Amazon Aurora 数据库集群。

[RDS.28] 应标记 RDS 数据库集群

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则:`tagged-rds-dbcluster`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon RDS 数据库集群是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果数据库集群没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果数据库集群未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库集群添加标签，请参阅《Amazon RDS 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.29] 应标记 RDS 数据库集群快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBClusterSnapshot`

AWS Config 规则:`tagged-rds-dbclustersnapshot`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon RDS 数据库集群快照是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果数据库集群快照没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果数据库集群快照未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库集群快照添加标签，请参阅《Amazon RDS 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.30] 应标记 RDS 数据库实例

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则:`tagged-rds-dbinstance`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon RDS 数据库实例是否具有带特定键的标签，这些键在 requiredTagKeys 参数中进行定义。如果数据库实例没有任何标签键或未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签键，如果数据库实例未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库实例添加标签，请参阅《Amazon RDS 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.31] 应标记 RDS 数据库安全组

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::RDS::DBSecurityGroup

AWS Config 规则:tagged-rds-dbsecuritygroup（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredTagKeys	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon RDS 数据库安全组是否具有带特定键的标签，这些键在 requiredTagKeys 参数中进行定义。如果数据库安全组没有任何标签键或未在 requiredTagKeys 参数中指定所有键，则此控件将失败。如果未提供 requiredTagKeys 参数，则此控件仅检查是否存在标签键，如果数据库安全组未使用任何键进行标记，则此控件将失败。自动应用并以 aws: 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库安全组添加标签，请参阅《Amazon RDS 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.32] 应标记 RDS 数据库快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBSnapshot`

AWS Config 规则:`tagged-rds-dbsnapshot`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon RDS 数据库快照是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果数据库快照没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果数据库快照未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库快照添加标签，请参阅《Amazon RDS 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.33] 应标记 RDS 数据库子网组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBSubnetGroup`

AWS Config 规则:`tagged-rds-dbsubnetgroups`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon RDS 数据库子网组是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果数据库子网组没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果数据库子网组未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库子网组添加标签，请参阅《Amazon RDS 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志

相关要求： 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-6 (3) NIST.800-53.r5 AU-3、(4)、 NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (8)、 NIST.800-53.r5 SI-3 (20)、(8)、 NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8)、PCI DSS v4.0。1/10.2.1

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：**`rds-aurora-mysql-audit-logging-enabled`**

计划类型：已触发变更

参数：无

此控件检查是否将 Amazon Aurora MySQL 数据库集群配置为向亚马逊日志发布审核 CloudWatch 日志。如果集群未配置为向日志发布审核日志，则控制失败。 CloudWatch 该控件不会为 Aurora Serverless v1 数据库集群生成调查发现。

审核日志记录捕获数据库活动的记录，包括登录尝试、数据修改、架构变更和其他可以出于安全性和合规性目的进行审计的事件。当您配置 Aurora MySQL 数据库集群以将审计日志发布到 Amazon CloudWatch 日志中的日志组时，您可以对日志数据进行实时分析。 CloudWatch 日志将日志保留在高度耐用的存储空间中。您还可以在中创建警报和查看指标 CloudWatch。

> **Note**
>
> 将审计日志发布到 CloudWatch 日志的另一种方法是启用高级审计，并将集群级别的数据库参数`server_audit_logs_upload`设置为。`1server_audit_logs_upload parameter` 的默认值为 `0`。但是，我们建议您改用以下补救说明来传递此控件。

修复

要将 Aurora MySQL 数据库集群审计日志发布到 CloudWatch 日志，请参阅亚马逊 Aurora 用户指南中的将 Amazon Aurora MySQL CloudWatch 日志发布到亚马逊日志。

[RDS.35] RDS 数据库集群应启用自动次要版本升级

相关要求： 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

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：**`rds-cluster-auto-minor-version-upgrade-enable`**

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon RDS Multi-AZ 数据库集群启用了自动次要版本升级。如果未为 Multi-AZ 数据库集群启用自动次要版本升级，则控制失败。

RDS 提供自动次要版本升级，因此您可以使 Multi-AZ 数据库集群保持最新状态。次要版本可以引入新的软件功能、错误修复、安全补丁和性能改进。通过在 RDS 数据库集群上启用自动次要版本升级，当有新版本可用时，集群以及集群中的实例将收到次要版本的自动更新。更新会在维护时段自动应用。

修复

要在 Multi-AZ 数据库集群上启用自动次要版本升级，请参阅 Amazon RDS 用户指南中的修改 Multi-AZ 数据库集群。

[RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch

相关要求：PCI DSS v4.0。 1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-postgresql-logs-to-cloudwatch

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`logTypes`	Comma-separated 要发布到日志的 CloudWatch 日志类型列表	StringList	不可自定义	`postgresql`

此控件检查是否将 Amazon RDS for PostgreSQL 数据库实例配置为将日志发布到亚马逊日志。CloudWatch 如果 PostgreSQL 数据库实例未配置为将参数中`logTypes`提及的日志类型发布到日志，则控制失败。 CloudWatch

数据库日志记录提供向 RDS 实例发出的请求的详细记录。PostgreSQL 会生成事件日志，其中包含对管理员有用的信息。将这些日志发布到 Log CloudWatch s 可以集中管理日志，并帮助您对日志数据进行实时分析。 CloudWatch 日志将日志保留在高度耐用的存储空间中。您还可以在中创建警报和查看指标CloudWatch。

修复

要将 PostgreSQL 数据库实例日志发布 CloudWatch 到日志，请参阅 Amazon RDS 用户指南中的将 PostgreSQL 日志发布到 CloudWatch 亚马逊日志。

[RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch

相关要求：PCI DSS v4.0。 1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：rds-aurora-postgresql-logs-to-cloudwatch

计划类型：已触发变更

参数：无

此控件检查 Amazon Aurora PostgreSQL 数据库集群是否已配置为向亚马逊日志发布日志。CloudWatch 如果 Aurora PostgreSQL 数据库集群未配置为将 PostgreSQL 日志发布到日志，则控制失败。 CloudWatch

数据库日志记录提供向 RDS 集群发出的请求的详细记录。Aurora PostgreSQL 会生成事件日志，其中包含对管理员有用的信息。将这些日志发布到 Log CloudWatch s 可以集中管理日志，并帮助您对日志数据进行实时分析。 CloudWatch 日志将日志保留在高度耐用的存储空间中。您还可以在中创建警报和查看指标 CloudWatch。

修复

要将 Aurora PostgreSQL 数据库集群日志发布 CloudWatch 到日志，请参阅亚马逊 RDS 用户指南中的将 Aurora PostgreSQL 日志发布到 CloudWatch 亚马逊日志。

[RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-postgres-instance-encrypted-in-transit

计划类型：定期

参数：无

此控件检查与 Amazon RDS for PostgreSQL 数据库 (DB) 实例的连接在传输过程中是否经过加密。如果与实例关联的参数组的 `rds.force_ssl` 参数设置为 `0`（关闭），则此控件会失败。此控件不评估属于数据库集群的 RDS 数据库实例。

传输中数据是指从一个位置移动到另一个位置的数据，例如在集群中的节点之间或在集群和应用程序之间。数据可能通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。

修复

要要求与 RDS for PostgreSQL 数据库实例的所有连接都使用 SSL，请参阅《Amazon RDS 用户指南》中的将 SSL 与 PostgreSQL 数据库实例结合使用。

[RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-mysql-instance-encrypted-in-transit

计划类型：定期

参数：无

此控件检查与 Amazon RDS for MySQL 数据库 (DB) 实例的连接在传输过程中是否经过加密。如果与实例关联的参数组的 `rds.require_secure_transport` 参数设置为 `0`（关闭），则此控件会失败。此控件不评估属于数据库集群的 RDS 数据库实例。

传输中数据是指从一个位置移动到另一个位置的数据，例如在集群中的节点之间或在集群和应用程序之间。数据可能通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。

修复

要要求所有与 RDS for MySQL 数据库实例的连接都使用 SSL，请参阅亚马逊 RDS 用户指南中对亚马逊 RDS 上的 MySQL 数据库实例的SSL/TLS 支持。

[RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志

相关要求： 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-6 (3) NIST.800-53.r5 AU-3、(4)、 NIST.800-53.r5 AU-6 (10) NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (9)、 NIST.800-53.r5 SC-7 (8)、(20)、 NIST.800-53.r5 SI-3 (8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-sql-server-logs-to-cloudwatch

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`logTypes`	RDS for SQL Server 数据库实例应配置为发布到 CloudWatch 日志的日志类型列表。如果数据库实例未配置为发布列表中指定的日志类型，则此控制会失败。	EnumList（最多 2 件商品）	`agent`, `error`	`agent`, `error`

此控件检查适用于微软 SQL Server 的 Amazon RDS 数据库实例是否配置为将日志发布到亚马逊 CloudWatch 日志。如果 RDS for SQL Server 数据库实例未配置为向日志发布日 CloudWatch 志，则控制失败。您可以选择指定数据库实例应配置为发布的日志类型。

数据库日志记录提供向 Amazon RDS 数据库实例发出的请求的详细记录。将日志发布到 CloudWatch 日志可以集中管理日志，并帮助您对日志数据进行实时分析。 CloudWatch 日志将日志保留在高度耐用的存储空间中。此外，您可以使用它为可能发生的特定错误创建警报，例如错误日志中记录的频繁重启。同样，您可以为 SQL Server 代理日志中记录的与 SQL 代理作业相关的错误或警告创建警报。

修复

有关将日志发布到 RDS for SQL Server 数据库实例 CloudWatch 日志的信息，请参阅《亚马逊关系数据库服务用户指南》中的 Amazon RDS for Microsoft SQL Server 数据库日志文件。

[RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-sqlserver-encrypted-in-transit

计划类型：定期

参数：无

此控件检查与 Amazon RDS for Microsoft SQL Server 数据库实例的连接在传输过程中是否加密。如果与数据库实例关联的参数组的 `rds.force_ssl` 参数设置为 `0 (off)`，则该控件会失败。

传输中数据是指从一个位置移动到另一个位置的数据，例如在数据库集群中的节点之间或在数据库集群和客户端应用程序之间。数据可以通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权用户侦听网络流量的风险。

修复

SSL/TLS 有关启用与运行微软 SQL Server 的 Amazon RDS 数据库实例的连接的信息，请参阅亚马逊关系数据库服务用户指南中的在微软 SQL Server 数据库实例上使用 SS L。

[RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch

相关要求： 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-6 (3) NIST.800-53.r5 AU-3、(4)、、、 NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (10)、 NIST.800-53.r5 SC-7 (8)、(20)、 NIST.800-53.r5 SI-3 (8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：mariadb-publish-logs-to-cloudwatch-logs

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`logTypes`	MariaDB 数据库实例应配置为发布到 CloudWatch 日志的日志类型列表。如果数据库实	EnumList（最多 4 件商品）	`audit`, `error`,	`audit`, `error`

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
	例未配置为发布列表中指定的日志类型，则该控件会生成 FAILED 调查发现。		general, slowquery	

此控件检查是否将 Amazon RDS for MariaDB 数据库实例配置为将某些类型的日志发布到亚马逊 CloudWatch 日志。如果 MariaDB 数据库实例未配置为将日志发布到 CloudWatch 日志，则控制失败。您可以选择指定 MariaDB 数据库实例应配置为发布哪些类型的日志。

数据库日志记录提供向 Amazon RDS for MariaDB 数据库实例发出的请求的详细记录。将日志发布到 Amazon Log CloudWatch s 可以集中管理日志，并帮助您对日志数据进行实时分析。此外，CloudWatch Logs 会将日志保留在持久存储中，这可以支持安全性、访问权限以及可用性审查和审计。借助 CloudWatch 日志，您还可以创建警报和查看指标。

修复

有关配置 Amazon RDS for MariaDB 数据库实例以将日志发布到亚马逊 CloudWatch 日志的信息，请参阅亚马逊关系数据库服务用户指南中的将 MariaDB CloudWatch 日志发布到亚马逊日志。

[RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：AWS::RDS::DBProxy

AWS Config 规则：rds-proxy-tls-encryption

计划类型：定期

参数：无

此控件检查 Amazon RDS 数据库代理是否要求代理与底层 RDS 数据库实例之间的所有连接都使用 TLS。如果代理不要求代理与 RDS 数据库实例之间的所有连接都使用 TLS，则该控件会失败。

Amazon RDS 代理可作为客户端应用程序和底层 RDS 数据库实例之间的附加安全层。例如，即使底层数据库实例支持旧版 TLS，您也可以使用 TLS 1.3 连接到 RDS。通过使用 RDS 代理，您可以对数据库应用程序强制执行严格的身份验证要求。

修复

有关更改 Amazon RDS 代理设置以要求使用 TLS 的信息，请参阅《Amazon Relational Database Service 用户指南》中的修改 RDS 代理。

[RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-mariadb-instance-encrypted-in-transit

计划类型：定期

参数：无

此控件检查与 Amazon RDS for MariaDB 数据库实例的连接是否在传输过程中加密。如果与数据库实例关联的数据库参数组不同步，或者参数组的 `require_secure_transport` 参数未设置为 `ON`，则该控件会失败。

> **Note**
>
> 此控件不会评估使用早于 10.5 版的 MariaDB 版本的 Amazon RDS 数据库实例。`require_secure_transport` 参数仅支持 MariaDB 版本 10.5 及更高版本。

传输中数据是指从一个位置移动到另一个位置的数据，例如在数据库集群中的节点之间或在数据库集群和客户端应用程序之间。数据可以通过互联网或在私有网络内移动。对传输中数据进行加密可降低未经授权用户侦听网络流量的风险。

修复

SSL/TLS 有关启用与 Amazon RDS for MariaDB 数据库实例的连接的信息，请参阅《亚马逊关系数据库服务用户指南》中的 “要求 SSL/TLS 所有与 MariaDB 数据库实例的连接”。

[RDS.45] Aurora MySQL 数据库集群应启用审计日志

相关要求： 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-6 (3) NIST.800-53.r5 AU-3、(4)、、、 NIST.800-53.r5

AU-6 (9) NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7 (8)、(20)、 NIST.800-53.r5 SI-3 (8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：aurora-mysql-cluster-audit-logging

计划类型：定期

参数：无

此控件检查 Amazon Aurora MySQL 数据库集群是否启用了审核日志记录。如果与数据库集群关联的数据库参数组不同步、`server_audit_logging` 参数未设置为 `1` 或者 `server_audit_events` 参数设置为空值，则该控件会失败。

数据库日志可以协助安全和访问审计，并帮助诊断可用性问题。审核日志记录捕获数据库活动的记录，包括登录尝试、数据修改、架构变更和其他可以出于安全性和合规性目的进行审计的事件。

修复

有关为亚马逊 Aurora MySQL 数据库集群启用日志记录的信息，请参阅亚马逊 Aurora 用户指南中的将亚马逊 Aurora MySQL CloudWatch 日志发布到亚马逊日志。

[RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：rds-instance-subnet-igw-check

计划类型：定期

参数：无

此控件检查 Amazon RDS 数据库实例是否部署在具有通往互联网网关的路由的公共子网中。如果 RDS 数据库实例部署在具有通往互联网网关的路由的子网中，并且目标设置为 `0.0.0.0/0` 或 `::/0`，则该控件会失败。

通过在私有子网中预置 Amazon RDS 资源，您可以防止 RDS 资源接收来自公共互联网的入站流量，从而防止意外访问您的 RDS 数据库实例。如果 RDS 资源是在对互联网开放的公共子网中预置的，则可能容易面临数据泄露等风险。

修复

有关为 Amazon RDS 数据库实例配置私有子网的信息，请参阅《Amazon Relational Database Service 用户指南》中的在 VPC 中使用数据库实例。

[RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：rds-pgsql-cluster-copy-tags-to-snapshot-check

计划类型：已触发变更

参数：无

此控制检查 Amazon RDS for PostgreSQL 数据库集群是否配置为在创建快照时将所有标签复制到快照。如果 RDS for PostgreSQL 数据库集群的 `CopyTagsToSnapshot` 参数设置为 `false`，则该控件会失败。

将标签复制到数据库快照有助于在备份资源之间保持适当的资源跟踪、管理和成本分配。这样就可以在活动数据库及其快照中实现一致的资源识别、访问控制和合规性监控。正确标记的快照可以确保备份资源继承与其源数据库相同的元数据，从而提高安全运营效率。

修复

有关配置 Amazon RDS for PostgreSQL 数据库集群以自动将标签复制到数据库快照的信息，请参阅《Amazon Relational Database Service 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：rds-mysql-cluster-copy-tags-to-snapshot-check

计划类型：已触发变更

参数：无

此控制检查 Amazon RDS for MySQL 数据库集群是否配置为在创建快照时将所有标签复制到快照。如果 RDS for MySQL 数据库集群的 `CopyTagsToSnapshot` 参数设置为 `false`，则该控件会失败。

将标签复制到数据库快照有助于在备份资源之间保持适当的资源跟踪、管理和成本分配。这样就可以在活动数据库及其快照中实现一致的资源识别、访问控制和合规性监控。正确标记的快照可以确保备份资源继承与其源数据库相同的元数据，从而提高安全运营效率。

修复

有关配置 Amazon RDS for MySQL 数据库集群以自动将标签复制到数据库快照的信息，请参阅《Amazon Relational Database Service 用户指南》中的为 Amazon RDS 资源添加标签。

[RDS.50] RDS 数据库集群应设置足够的备份保留期

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：rds-cluster-backup-retention-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
`minimumBackupRetentionPeriod`	控件要检查的最短备份保留期（以天为单位）	整数	7 到 35	7	

此控件检查 RDS 数据库集群是否有最短的备份保留期。如果备份保留期小于指定的参数值，则控制失败。除非您提供自定义参数值，否则 Security Hub 使用默认值 7 天。

此控件检查 RDS 数据库集群是否有最短的备份保留期。如果备份保留期小于指定的参数值，则控制失败。除非您提供客户参数值，否则 Security Hub 使用默认值 7 天。此控件适用于所有类型的 RDS 数据库集群，包括 Aurora 数据库集群、DocumentDB 集群、NeptuneDB 集群等。

修复

要配置 RDS 数据库集群的备份保留期，请修改群集设置并将备份保留期设置为至少 7 天（或控制参数中指定的值）。有关详细说明，请参阅 Amazon Relational Database Service 用户指南中的备份保留期。对于 Aurora 数据库集群，请参阅亚马逊 Aurora 用户指南中的 Aurora 数据库集群备份和恢复 Aurora 数据库集群概述。对于其他类型的数据库集群（例如 DocumentDB 集群），请参阅相应的服务用户指南，了解如何更新集群的备份保留期。

[RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::RDS::GlobalCluster`

AWS Config 规则：rds-global-cluster-aurora-mysql-supported-version

计划类型：已触发变更

参数：

- `minSupportedEngineVersion`：`8.0.mysql_aurora.3.08.0`（不可自定义）
- `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`（不可自定义）

此控件检查 Amazon Aurora MySQL 全局集群是否在支持的最低引擎版本上运行。如果 Aurora MySQL 全局集群引擎版本低于指定的最低支持版本且未在长期支持版本参数中列出，则控制失败。

在支持的引擎版本上运行 Aurora MySQL 全局数据库有助于确保您可以访问最新的安全补丁、错误修复和性能改进。Aurora MySQL 次要版本已定义了标准支持终止日期，之后它们将不再收到关键补丁。运行不支持的版本可能会使您的全局数据库面临安全漏洞，并可能导致 Amazon RDS Extended Support 收费。由于 Aurora MySQL 遵循非连续支持生命周期，长期支持 (LTS) 版本的支持时间比后

续的非 LTS 版本更长，因此此控件还会检查仍处于标准支持之下的 LTS 版本。有关更多信息，请参阅 Aurora MySQL 的亚马逊 Aurora 发行说明中的亚马逊 Aurora MySQL 发布日历。

修复

有关将 Aurora MySQL 全球数据库升级到支持的引擎版本的信息，请参阅亚马逊 Aurora 用户指南中的升级亚马逊 Aurora 全球数据库和通过修改引擎版本升级 Aurora MySQL。

适用于亚马逊 Redshift 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Redshift 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Redshift.1] Amazon Redshift 集群应禁止公共访问

相关要求： NIST.800-53.r5 AC-21、、 NIST.800-53.r5 AC-3 (7)、(21) NIST.800-53.r5 AC-3、、、(11)、(16) NIST.800-53.r5 AC-4、 NIST.800-53.r5 AC-4 (20)、(21) NIST.800-53.r5 AC-6、(3) NIST.800-53.r5 SC-7、 NIST.800-53.r5 SC-7 (4)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9)、PCI DSS v3.2.1/1.2.1、 NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1、 NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.4 2.1/1.3.6，PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-cluster-public-access-check

计划类型：已触发变更

参数：无

此控件可检查 Amazon Redshift 集群是否公开访问。它会评估集群配置项目中的 `PubliclyAccessible` 字段。

Amazon Redshift 集群配置的 `PubliclyAccessible` 属性表示集群是否公开访问。当集群配置为 `PubliclyAccessible` 设置为 `true` 时，它是一个面向 Internet 的实例，具有可公开解析的 DNS 名称，可解析为公共 IP 地址。

当集群不可公开访问时，它是一个内部实例，其 DNS 名称可解析为私有 IP 地址。除非您希望集群可以公开访问，否则不应将集群配置为把 `PubliclyAccessible` 设置为 `true`。

修复

要更新 Amazon Redshift 集群以禁用公共访问，请参阅 Amazon Redshift 管理指南中的修改集群。将公开访问设置为否。

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

相关要求： NIST.800-53.r5 AC-4、 NIST.800-53.r5 SC-1 3、3 (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 NIST.800-53.r5 SC-8 (2)、PCI DSS v4.0.1/4.2.1

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config 规则：redshift-require-tls-ssl

计划类型：已触发变更

参数：无

此控件检查是否需要连接到 Amazon Redshift 集群才能在传输中使用加密。如果 Amazon Redshift 集群参数 `require_SSL` 未设置为 `True`，则检查将失败。

TLS 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。只应允许通过 TLS 进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试应用程序，以了解性能概况和 TLS 的影响。

修复

要将 Amazon Redshift 参数组更新为要求加密，请参阅 Amazon Redshift 管理指南中的修改参数组。将 `require_ssl` 设置为 True。

[Redshift.3] Amazon Redshift 集群应启用自动快照

相关要求： 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)

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：AWS::Redshift::Cluster

AWS Config 规则：redshift-backup-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值	
MinRetentionPeriod	最短快照保留期（以天为单位）	整数	7 到 35	7	

此控件检查 Amazon Redshift 集群是否启用了自动快照，以及保留期是否大于或等于指定的时间范围。如果没有为集群启用自动快照，或者保留期小于指定的时间范围，则控制失败。除非您为快照保留期提供自定义参数值，否则 Security Hub CSPM 将使用默认值 7 天。

备份可以帮助您更快地从安全事件中恢复。它们增强了系统的弹性。默认情况下，Amazon Redshift 会定期拍摄快照。此控件检查是否已启用自动快照并将其保留至少七天。有关 Amazon Redshift 自动快照的更多详情，请参阅 Amazon Redshift 管理指南中的自动快照。

修复

要更新 Amazon Redshift 集群的快照保留期，请参阅 Amazon Redshift 管理指南中的修改集群。对于备份，将快照保留期设置为 7 或更大。

[Redshift.4] Amazon Redshift 集群应启用审核日志记录

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、PCI DSS v4.0.1/10.2.1 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

类别：识别 > 日志记录

严重性：中

资源类型：AWS::Redshift::Cluster

AWS Config 规则:`redshift-cluster-audit-logging-enabled`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件用于检查 Amazon Redshift 集群是否启用了审核日志。

Amazon Redshift 审核日志记录提供有关集群中的连接和用户活动的其他信息。这些数据可以存储在 Amazon S3 中并加以保护，有助于安全审计和调查。有关更多信息，请参阅 Amazon Redshift 管理指南中的数据库审核日志记录。

修复

要为 Amazon Redshift 集群配置审核日志记录，请参阅 Amazon Redshift 管理指南中的使用控制台配置审计。

[Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能

相关要求： 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)、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)

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-cluster-maintenancesettings-check

计划类型：已触发变更

参数：

- `allowVersionUpgrade = true`（不可自定义）

此控件检查是否为 Amazon Redshift 集群启用了自动主要版本升级。

启用自动主要版本升级可确保在维护时段内安装 Amazon Redshift 集群的最新主要版本更新。这些更新可能包括安全补丁和错误修复。及时安装补丁程序是保护系统安全的重要一步。

修复

要从中修复此问题 AWS CLI，请使用 Amazon `modify-cluster` Redshift 命令并设置`--allow-version-upgrade`属性。 *`clustername`*是您的亚马逊 Redshift 集群的名称。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Redshift 集群应使用增强型 VPC 路由

相关要求： 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)

类别：保护 > 安全网络配置 > API 私有访问

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-enhanced-vpc-routing-enabled

计划类型：已触发变更

参数：无

此控件会检查 Amazon Redshift 集群是否已启用 `EnhancedVpcRouting`。

增强型 VPC 路由强制集群和数据存储库之间的所有 `COPY` 和 `UNLOAD` 流量通过 VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能来保护网络流量。您还可以使用 VPC Flow 日志监控网络流量。

修复

有关详细的补救说明，请参阅 Amazon Redshift 管理指南中的启用增强型 VPC 路由。

[Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-default-admin-check

计划类型：已触发变更

参数：无

此控件检查 Amazon Redshift 集群是否已将管理员用户名从其默认值变更为其他值。如果 Redshift 集群的管理员用户名设置为 `awsuser`，则此控制失败。

创建 Redshift 集群时，应将默认管理员用户名变更为唯一值。默认用户名是众所周知的，应在配置时进行变更。变更默认用户名可以降低意外访问的风险。

修复

创建 Amazon Redshift 集群后，您无法更改其管理员用户名。要使用非默认用户名创建新集群，请参阅《Amazon Redshift 入门指南》中的步骤 1：创建示例 Amazon Redshift 集群。

[Redshift.10] Redshift 集群应在静态状态下进行加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-cluster-kms-enabled

计划类型：已触发变更

参数：无

此控件会检查 Amazon Redshift 集群是否处于静态加密状态。如果 Redshift 集群未静态加密或者加密密钥与规则参数中提供的密钥不同，则则控制失败。

在 Amazon Redshift 中，您可以为集群开启数据库加密，以帮助保护静态数据。为集群开启加密时，会对集群及其快照的数据块和系统元数据进行加密。静态数据加密是推荐的最佳实践，因为它为数据添加了一层访问管理。对静态 Redshift 集群进行加密可降低未经授权的用户访问磁盘上存储的数据的风险。

修复

要将 Redshift 集群修改为使用 KMS 加密，请参阅 Amazon Redshift 管理指南中的变更集群加密。

[Redshift.11] 应标记 Redshift 集群

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则:`tagged-redshift-cluster`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon Redshift 集群是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果集群没有任何标签键或者未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果集群未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 集群添加标签，请参阅《Amazon Redshift 管理指南》中的在 Amazon Redshift 中为资源添加标签。

[Redshift.12] 应标记 Redshift 事件通知订阅

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::EventSubscription`

AWS Config 规则:`tagged-redshift-eventsubscription`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon Redshift 集群快照是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果集群快照没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果集群快照未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 事件通知订阅添加标签，请参阅《Amazon Redshift 管理指南》中的在 Amazon Redshift 中为资源添加标签。

[Redshift.13] 应标记 Redshift 集群快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::ClusterSnapshot`

AWS Config 规则:`tagged-redshift-clustersnapshot`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon Redshift 集群快照是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果集群快照没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果集群快照未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还

可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 集群快照添加标签，请参阅《Amazon Redshift 管理指南》中的在 Amazon Redshift 中为资源添加标签。

[Redshift.14] 应标记 Redshift 集群子网组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::ClusterSubnetGroup`

AWS Config 规则:`tagged-redshift-clustersubnetgroup`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon Redshift 集群子网组是否有具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果集群子网组没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果集群子网组未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 集群子网组添加标签，请参阅《Amazon Redshift 管理指南》中的在 Amazon Redshift 中为资源添加标签。

[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口

相关要求：PCI DSS v4.0.1/1.3.1

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-unrestricted-port-access

计划类型：定期

参数：无

此控件可与检查 Amazon Redshift 集群关联的安全组是否有允许从互联网访问集群端口的入口规则（0.0.0.0/0 或 ::/0）。如果安全组入口规则允许从互联网访问集群端口，则此控件将失败。

允许对 Redshift 集群端口（带有 /0 后缀的 IP 地址）进行不受限制的入站访问可能会导致未经授权的访问或安全事件。我们建议在创建安全组和配置入站规则时应用最低权限访问原则。

修复

要将 Redshift 集群端口的入口限制为受限来源，请参阅《Amazon VPC 用户指南》中的使用安全组规则。更新端口范围与 Redshift 集群端口相匹配且 IP 端口范围为 0.0.0.0/0 的规则。

[Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Redshift::ClusterSubnetGroup`

AWS Config 规则：redshift-cluster-subnet-group-multi-az

计划类型：已触发变更

参数：无

此控件检查 Amazon Redshift 集群子网组是否包含来自多个可用区（AZ）的子网。如果集群子网组没有来自至少两个不同 AZs子网的子网，则控制失败。

跨多个子网配置 AZs 有助于确保即使发生故障事件，您的 Redshift 数据仓库也能继续运行。

修复

要将 Redshift 集群子网组修改为跨多个集群子网组 AZs，请参阅《Amazon Redshift 管理指南》中的修改集群子网组。

[Redshift.17] 应标记 Redshift 集群参数组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::ClusterParameterGroup`

AWS Config 规则：redshift-cluster-parameter-group-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon Redshift 集群参数组是否具有 `requiredKeyTags` 参数指定的标签键。如果参数组没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件会失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果参数组没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 Amazon Redshift 集群参数组添加标签的信息，请参阅《Amazon Redshift 管理指南》中的在 Amazon Redshift 中为资源添加标签。

[Redshift.18] Redshift 集群应启用多可用区部署

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：redshift-cluster-multi-az-enabled

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon Redshift 集群启用了多个可用区（Multi-AZ）部署。如果没有为 Amazon Redshift 集群启用多可用区部署，则此控件会失败。

Amazon Redshift 支持对预置的集群使用多可用区（Multi-AZ）部署。如果为集群启用了多可用区部署，则在可用区（AZ）出现意外事件的故障场景中，Amazon Redshift 数据仓库可以继续运行。多可用区部署将计算资源部署在多个可用区中，这些计算资源可通过单个端点访问。如果某个可用区出现彻底故障，则第二个可用区中的剩余计算资源可用于继续处理工作负载。您可以将现有单可用区数据仓库转换为多可用区数据仓库。然后在第二个可用区预置额外的计算资源。

修复

有关为 Amazon Redshift 集群配置多可用区部署的信息，请参阅《Amazon Redshift 管理指南》中的将单可用区数据仓库转换为多可用区数据仓库。

适用于亚马逊 Redshift Serverless 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Redshift 无服务器服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：高

资源类型：`AWS::RedshiftServerless::Workgroup`

AWS Config 规则：redshift-serverless-workgroup-routes-within-vpc

计划类型：定期

参数：无

此控件检查是否为 Amazon Redshift Serverless 工作组启用了增强型 VPC 路由。如果为工作组禁用了增强型 VPC 路由，则该控件会失败。

如果对 Amazon Redshift 无服务器工作组禁用增强型 VPC 路由，Amazon Redshift 会通过互联网路由流量，包括流向网络内其他服务的流量。 AWS 如果为工作组启用增强型 VPC 路由，Amazon Redshift 会强制基于 Amazon VPC 服务通过虚拟私有云（VPC）路由集群和数据存储库之间的所有 COPY 和 UNLOAD 流量。借助增强型 VPC 路由，您可以使用标准 VPC 功能来控制 Amazon Redshift 集群与其他资源之间的数据流。这包括 VPC 安全组和终端节点策略、网络访问控制列表 (ACLs) 和域名系统 (DNS) 服务器等功能。您还可以使用 VPC 流日志来监控 COPY 和 UNLOAD 流量。

修复

有关增强型 VPC 路由以及如何为工作组启用它的更多信息，请参阅《Amazon Redshift 管理指南》中的使用 Redshift 增强型 VPC 路由控制网络流量。

[RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::RedshiftServerless::Workgroup

AWS Config 规则：redshift-serverless-workgroup-encrypted-in-transit

计划类型：定期

参数：无

此控件检查是否需要连接到 Amazon Redshift Serverless 工作组才能加密传输中数据。如果工作组的 require_ssl 配置参数设置为 false，则该控件会失败。

Amazon Redshift Serverless 工作组是一组计算资源，将 RPUs VPC 子网组和安全组等计算资源组合在一起。工作组的属性包括网络和安全设置。这些设置指定是否应要求与工作组的连接使用 SSL 加密传输中数据。

修复

有关更新 Amazon Redshift Serverless 工作组的设置以要求 SSL 连接的信息，请参阅《Amazon Redshift 管理指南》中的连接到 Amazon Redshift Serverless。

[RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::RedshiftServerless::Workgroup`

AWS Config 规则：redshift-serverless-workgroup-no-public-access

计划类型：定期

参数：无

此控件检查是否为 Amazon Redshift Serverless 工作组禁用了公开访问。它评估 Redshift Serverless 工作组的 `publiclyAccessible` 属性。如果为工作组启用了公开访问（`true`），则该控件会失败。

Amazon Redshift Serverless 工作组的公开访问（`publiclyAccessible`）设置指定是否可以从公共网络访问该工作组。如果为工作组启用了公开访问（`true`），Amazon Redshift 会创建一个弹性 IP 地址，使得可以从 VPC 外部公开访问该工作组。如果您不希望某个工作组可以公开访问，请为其禁用公开访问。

修复

有关更改 Amazon Redshift Serverless 工作组的公开访问设置的信息，请参阅《Amazon Redshift 管理指南》中的查看工作组的属性。

[RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys

相关要求： NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9(1)、(10)、2 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (NIST.800-53.r5 SC-12)、 NIST.800-53.r5 SC-1 3、8、 NIST.800-53.r5 SC-2 8 (1)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RedshiftServerless::Namespace`

AWS Config 规则：redshift-serverless-namespace-cmk-encryption

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
kmsKeyArns	评估中 AWS KMS keys 要包含的 Amazon 资源名称 (ARNs) 列表。如果 Redshift Serverless 命名空间未使用列表中的 KMS 密钥进行加密，则该控件会生成 FAILED 调查发现。	StringList （最多 3 件商品）	1—3 个 ARNs 现有 KMS 密钥。例如：arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab 。	无默认值

此控件检查 Amazon Redshift Serverless 命名空间是否使用客户管理型 AWS KMS key进行静态加密。如果未使用客户管理型 KMS 密钥对 Redshift Serverless 命名空间进行加密，则该控件会失败。您可以选择为控件指定要包含在评估中的 KMS 密钥列表。

在 Amazon Redshift Serverless 中，命名空间定义了数据库对象的逻辑容器。此控件会定期检查命名空间的加密设置是否指定由客户管理 AWS KMS key的而不是 AWS 托管的 KMS 密钥来加密命名空间中的数据。使用客户管理型 KMS 密钥，您可以完全控制密钥。这包括定义和维护密钥策略、管理授权、轮换加密材料、分配标签、创建别名以及启用和禁用密钥。

修复

有关更新 Amazon Redshift 无服务器命名空间的加密设置和指定客户托管的命名空间的信息 AWS KMS key，请参阅 Amazon Redshift 管理指南中的更改命名空间。 AWS KMS key

[RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名

类别：识别 > 资源配置

严重性：中

资源类型：AWS::RedshiftServerless::Namespace

AWS Config 规则：redshift-serverless-default-admin-check

计划类型：定期

参数：无

此控件检查 Amazon Redshift Serverless 命名空间的管理员用户名是否为默认管理员用户名 admin。如果 Redshift Serverless 命名空间的管理员用户名为 admin，则该控件会失败。

创建 Amazon Redshift Serverless 命名空间时，应为该命名空间指定自定义管理员用户名。默认管理员用户名为公共知识。例如，通过指定自定义管理员用户名，您可以帮助降低命名空间遭受暴力攻击的风险或有效性。

修复

您可以使用 Amazon Redshift Serverless 控制台或 API 更改 Amazon Redshift Serverless 命名空间的管理员用户名。要使用控制台进行更改，请选择命名空间配置，然后在操作菜单上选择编辑管理员凭证。要以编程方式对其进行更改，请使用UpdateNamespace操作，或者，如果您使用的是，则运行 update- AWS CLI namesp ace 命令。如果您更改管理员用户名，则必须同时更改管理员密码。

[RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch

类别：识别 > 日志记录

严重性：中

资源类型：AWS::RedshiftServerless::Namespace

AWS Config 规则：redshift-serverless-publish-logs-to-cloudwatch

计划类型：定期

参数：无

此控件检查 Amazon Redshift Serverless 命名空间是否配置为将连接和用户日志导出到亚马逊日志。 CloudWatch 如果 Redshift Serverless 命名空间未配置为将日志导出到日志，则控制失败。 CloudWatch

如果您将 Amazon Redshift Serverless 配置为将连接 CloudWatch 日志 (connectionloguserlog) 和用户日志 () 数据导出到 Amazon Logs 中的日志组，则可以收集日志记录并将其存储在持久存储中，

这样可以支持安全、访问和可用性审查和审计。借助 CloudWatch 日志，您还可以对日志数据进行实时分析，并 CloudWatch 用于创建警报和查看指标。

修复

要将 Amazon Redshift Serverless 命名空间的 CloudWatch 日志数据导出到 Amazon 日志，必须在该命名空间的审核日志配置设置中选择相应的日志进行导出。有关更新这些设置的信息，请参阅《Amazon Redshift 管理指南》中的编辑安全性和加密。

53 号公路的 Security Hub CSPM 控制

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon Route 53 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Route53.1] 应标记 Route53 运行状况检查

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Route53::HealthCheck`

AWS Config 规则:`tagged-route53-healthcheck`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon Route 53 运行状况检查是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果运行状况检查没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果运行状况检查未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Route 53 运行状况检查添加标签，请参阅《Amazon Route 53 开发人员指南》中的为运行状况检查命名和添加标签。

[Route53.2] Route 53 公有托管区域应记录 DNS 查询

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、PCI DSS v4.0.1/10.4.2 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

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Route53::HostedZone`

AWS Config 规则：`route53-query-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon Route 53 公共托管区域启用了 DNS 查询日志记录。如果未为 Route 53 公共托管区域启用 DNS 查询日志记录，控制将会失败。

记录 Route 53 托管区域的 DNS 查询可满足 DNS 安全性和合规性要求并授予可见性。日志包含诸如查询的域或子域、查询的日期和时间、DNS 记录类型（例如 A 或 AAAA）以及 DNS 响应代码（例如 `NoError` 或 `ServFail`）等信息。启用 DNS 查询日志记录后，Route 53 会将日志文件发布到 Amazon CloudWatch 日志。

修复

要记录 Route 53 公共托管区域的 DNS 查询，请参阅 Amazon Route 53 开发人员指南中的 DNS 查询配置日志记录。

适用于亚马逊 S3 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估了亚马逊简单存储服务 (Amazon S3) Service 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置

相关要求：CIS AWS 基金会基准 v5.0.0/2.1.4、CI AWS S 基金会基准 v3.0.0/2.1.4、CI AWS S 基金会基准 v1.4.0/2.1.5、1、、（7）、、（21）、（11）、（16）NIST.800-53.r5 AC-2、（20）NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3、（21）、（21）NIST.800-53.r5 AC-4、（3）NIST.800-53.r5 AC-4、（4）、（9）NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7、PCI DSS v3.2.1 NIST.800-53.r5 SC-7、PCI DSS v3.2.1 2.1/1.3.1 NIST.800-53.r5 SC-7、PCI DSS v3.2.1/1.3.2 NIST.800-53.r5 SC-7、PCI DSS v3.2.1/1.3.4 NIST.800-53.r5 SC-7、PCI DSS v3.2.1/1.3.6、PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：s3-account-level-public-access-blocks-periodic

计划类型：定期

参数：

- `ignorePublicAcls`：`true`（不可自定义）
- `blockPublicPolicy`：`true`（不可自定义）
- `blockPublicAcls`：`true`（不可自定义）

- `restrictPublicBuckets`：`true`（不可自定义）

此控件可检查是否在账户级别为 S3 通用存储桶配置了上述 Amazon S3 屏蔽公共访问权限设置。如果将一个或多个屏蔽公共访问权限设置设为 `false`，则此控件将失败。

如果将任何设置设置为 `false`，或者未配置任何设置，则控制失败。

Amazon S3 公有访问区块旨在提供对整个 S3 存储桶 AWS 账户 或单个 S3 存储桶级别的控制，以确保对象永远无法公开访问。通过访问控制列表 (ACLs)、存储桶策略或两者兼而有之，向存储桶和对象授予公共访问权限。

除非您打算让 S3 存储桶可公开访问，否则您应该配置账户级别 Amazon S3 屏蔽公共访问权限功能。

要了解更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 屏蔽公共访问权限。

修复

要为您启用 Amazon S3 阻止公共访问 AWS 账户，请参阅《亚马逊简单存储服务用户指南》中的为您的账户配置阻止公开访问设置。

[S3.2] S3 通用存储桶应阻止公共读取访问权限

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、 NIST.800-53.r5 AC-2 1、、 NIST.800-53.r5 AC-3（7）、（21）、（11）、（16）、（20）、（21）、（3） NIST.800-53.r5 AC-3、（4），(9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-public-read-prohibited

计划类型：定期计划和触发变更

参数：无

此控件可检查 Amazon S3 通用存储桶是否允许公共读取访问权限。它会对阻止公有访问设置、存储桶策略和存储桶访问控制列表（ACL）进行评估。如果存储桶允许公共读取访问权限，则此控件将失败。

> **Note**
>
> 如果 S3 存储桶具有存储桶策略，则此控件不会评估使用通配符或变量的策略条件。要生成 PASSED 调查发现，存储桶策略中的条件只能使用固定值，即不包含通配符或策略变量的值。有关策略变量的信息，请参阅《AWS Identity and Access Management 用户指南》中的变量和标签。

有些使用案例可能要求 Internet 上的每个人都能够从 S3 存储桶中读取数据。然而，这种情况很少见。为确保数据的完整性和安全性，您的 S3 存储桶不应可公开读取。

修复

要阻止对您的 Amazon S3 存储桶的公共读取权限，请参阅 Amazon 简单存储服务用户指南中的为 S3 存储桶配置阻止公开访问设置。

[S3.3] S3 通用存储桶应阻止公共写入访问权限

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、1、、(7)、(21)、(21)、(16)、(20)、(21)、(3)、(4)、(9) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-public-write-prohibited

计划类型：定期计划和触发变更

参数：无

此控件可检查 Amazon S3 通用存储桶是否允许公共写入访问权限。它会对阻止公有访问设置、存储桶策略和存储桶访问控制列表（ACL）进行评估。如果存储桶允许公共写入访问权限，则此控件将失败。

> **Note**
>
> 如果 S3 存储桶具有存储桶策略，则此控件不会评估使用通配符或变量的策略条件。要生成 PASSED 调查发现，存储桶策略中的条件只能使用固定值，即不包含通配符或策略变量的值。有关策略变量的信息，请参阅《AWS Identity and Access Management 用户指南》中的变量和标签。

有些使用案例要求互联网上的每个人都能写入您的 S3 存储桶。然而，这种情况很少见。为确保数据的完整性和安全性，您的 S3 存储桶不应可公开写入。

修复

要阻止对您的 Amazon S3 存储桶的公共写入权限，请参阅 Amazon 简单存储服务用户指南中的为 S3 存储桶配置阻止公开访问设置。

[S3.5] S3 通用存储桶应需要请求才能使用 SSL

相关要求：CIS AWS 基金会基准 v5.0.0/2.1.1、CIS 基金会基准 v3.0.0/2.1.1、 AWS CI AWS S 基金会基准 v1.4.0/2.1.2、7 (2)、(1)、2 (3)、3、3 (3)、(4)、(1)、(1) NIST.800-53.r5 AC-1、(2) NIST.800-53.r5 AC-4、 NIST.800-53.r5 IA-5 nist.800-53.r5 SI-7 (6) NIST.800-53.r5 SC-1、nist.800-17-17-7 (6) NIST.800-53.r5 SC-1 1.r2 3.13.8 NIST.800-53.r5 SC-2、nist.800-171.r2 3.13.15 NIST.800-53.r5 SC-8、 NIST.800-53.r5 SC-8 PCI DSS v3.2.1/4.1 NIST.800-53.r5 SC-8、PCI DSS v4.0.1/4.1、PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-ssl-requests-only

计划类型：已触发变更

参数：无

此控件可检查 Amazon S3 通用存储桶是否具有需要请求才能使用 SSL 的策略。如果存储桶策略不需要请求来使用 SSL，则此控件将失败。

S3 存储桶的策略应要求所有请求（`Action: S3:*`）在 S3 资源策略中仅接受通过 HTTPS 传输的数据，由条件密钥 `aws:SecureTransport` 表示。

修复

要更新 Amazon S3 存储桶策略以拒绝不安全传输，请参阅《Amazon Simple Storage Service 用户指南》中的使用 Amazon S3 控制台添加存储桶策略。

添加与以下策略中的策略语句相似的策略语句。将 amzn-s3-demo-bucket 替换为您要修改的存储桶的名称。

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": "*"
        }
    ]
}
```

有关更多信息，请参阅我应该使用哪个 S3 存储桶策略来遵守 AWS Config 规则 s3-bucket-ssl-requests-only？ 在AWS 官方知识中心中。

[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2、nist.800-171.r2 3.13.4

类别：保护 > 安全访问管理 > 敏感的 API 操作操作受限

严重性：高

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-blacklisted-actions-prohibited

计划类型：已触发变更

参数：

- `blacklistedactionpatterns`：`s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl`（不可自定义）

此控件可检查 Amazon S3 通用存储桶策略是否阻止其他 AWS 账户 的主体对 S3 存储桶中的资源执行被拒绝的操作。如果存储桶策略允许另一个 AWS 账户中的主体执行上述一项或多项操作，则此控件将失败。

实施最低权限访问对于降低安全风险以及错误或恶意意图的影响至关重要。如果 S3 存储桶策略允许从外部账户进行访问，则可能会导致内部威胁或攻击者泄露数据。

`blacklistedactionpatterns` 参数允许成功评估 S3 存储桶的规则。该参数授予对未包含在 `blacklistedactionpatterns` 列表中的操作模式的外部账户访问权限。

修复

要更新 Amazon S3 存储桶策略以删除权限，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 控制台添加存储桶策略。

在编辑存储桶策略页面的策略编辑文本框中，执行以下操作之一：

- 删除授予其他 AWS 账户 访问被拒绝操作的权限的语句。
- 从语句中删除允许的拒绝操作。

[S3.7] S3 通用存储桶应使用跨区域复制

相关要求：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)、(2)、nist.800-53.r5 NIST.800-53.r5 SC-5 SI-13 (5)

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-cross-region-replication-enabled

计划类型：已触发变更

参数：无

此控件可检查 Amazon S3 通用存储桶是否启用了跨区域复制。如果存储桶未启用跨区域复制，则此控件将失败。

复制是指在相同或不同的 AWS 区域存储桶之间自动异步复制对象。复制操作会将源存储桶中新创建的对象和对象更新复制到目标存储桶。 AWS 最佳实践建议对由同一 AWS 账户拥有的源存储桶和目标存储桶进行复制。除了可用性以外，您还应该考虑其他系统强化设置。

如果复制目标存储桶未启用跨区域复制，则此控件会生成该存储桶的 `FAILED` 调查发现。如果有正当理由表明目标存储桶不需要启用跨区域复制，则可以隐藏该存储桶的调查发现。

修复

要在 S3 存储桶上启用跨区域复制，请参阅 Amazon Simple Storage Service 用户指南中的为同一账户拥有的源存储桶和目标存储桶配置复制。对于源存储桶，选择应用到存储桶中的所有对象。

[S3.8] S3 通用存储桶应屏蔽公共访问权限

相关要求：CIS AWS 基金会基准 v5.0.0/2.1.4、CI AWS S 基金会基准 v3.0.02.1.4、CI AWS S 基金会基准 v1.4.0/2.1.5 NIST.800-53.r5 AC-2、1、、（7）、 NIST.800-53.r5 AC-3、（21） NIST.800-53.r5 AC-3、、（11） NIST.800-53.r5 AC-4、（16） NIST.800-53.r5 AC-4、（20） NIST.800-53.r5 AC-6、（21） NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7、（21） NIST.800-53.r5 SC-7、（3）、（4） NIST.800-53.r5 SC-7、（9） NIST.800-53.r5 SC-7、PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

类别：保护 > 安全访问管理 > 访问控制

严重性：高

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-level-public-access-prohibited

计划类型：已触发变更

参数：

- excludedPublicBuckets（不可自定义）- 已知允许的公共 S3 存储桶名称的逗号分隔列表

此控件可检查 Amazon S3 通用存储桶是否在存储桶级别屏蔽了公共访问权限。如果将以下任一设置设为 false，则此控件将失败：

- ignorePublicAcls
- blockPublicPolicy
- blockPublicAcls
- restrictPublicBuckets

S3 存储桶级别的阻止公共访问提供了控制，以确保对象永远不会具有公共访问权限。通过访问控制列表 (ACLs)、存储桶策略或两者兼而有之，向存储桶和对象授予公共访问权限。

除非您打算公开访问 S3 存储桶，否则您应该配置存储桶级别 Amazon S3 屏蔽公共访问权限功能。

修复

有关如何在存储桶级别删除公开访问权限的信息，请参阅 Amazon S3 用户指南中的阻止公众访问 Amazon S3 存储。

[S3.9] S3 通用存储桶应启用服务器访问日志记录

相关要求： NIST.800-53.r5 AC-2(4)、(26)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 (9)、nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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 SI-4 (20)、nist.800-53.r5 SI-7 (8)、nist.800-171.r2 3.8、PCI DSS v4.0.1/10.2.1

类别：识别 > 日志记录

严重性：中

资源类型：AWS::S3::Bucket

AWS Config 规则：s3-bucket-logging-enabled

计划类型：已触发变更

参数：无

此控件可检查是否为 Amazon S3 通用存储桶启用了服务器访问日志记录。如果未启用服务器访问日志记录，则此控件将失败。启用日志记录后，Amazon S3 将源存储桶的访问日志传送到选定的目标存储桶。目标存储桶必须与源存储桶位于同一 AWS 区域 存储桶中，并且不得配置默认保留期。目标日志存储桶不需要启用服务器访问日志记录，您应该隐藏该存储桶的调查发现。

服务器访问日志记录提供对存储桶发出的请求的详细记录。服务器访问日志可以帮助进行安全和访问审核。有关更多信息，请参阅 Amazon S3 的安全最佳实践：启用 Amazon S3 服务器访问日志记录。

修复

要启用 Amazon S3 服务器访问日志，请参阅 Amazon S3 用户指南中的启用 Amazon S3 服务器访问日志。

[S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置

相关要求： 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)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-version-lifecycle-policy-check

计划类型：已触发变更

参数：无

此控件可检查 Amazon S3 通用版本存储桶是否具有生命周期配置。如果存储桶不具有生命周期配置，则此控件将失败。

我们建议为 S3 存储桶配置生命周期规则，以帮助您定义希望 Amazon S3 在对象生命周期内执行的操作。

> **Tip**
>
> 在不进行生命周期管理的情况下启用版本控制可能会导致无限的存储增长和成本的增加。每次修改对象都会创建一个新版本，该版本将无限期保留。配置 S3 生命周期规则，以自动将非当前版本转换为更便宜的存储类别，或者在定义的保留期后将其过期。

修复

有关在 Amazon S3 存储桶上配置生命周期的更多信息，请参阅 Amazon S3 用户指南中的 “将 S3 版本控制与 S3 生命周期结合使用”、“在存储桶上设置生命周期配置” 和 “管理对象的生命周期”。

[S3.11] S3 通用存储桶应启用事件通知

相关要求： 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 3.8

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-event-notifications-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`eventTypes`	首选 S3 事件类型列表	EnumList（最多 28 个项目）	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`,	无默认值

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
			s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated,	

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
			s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replic	

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
			`ation:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent`	

此控件可检查 Amazon S3 通用存储桶上是否启用了 S3 事件通知。如果未在存储桶上启用 S3 事件通知，则此控件将失败。如果您为 `eventTypes` 参数提供自定义值，则仅当在为指定类型的事件启用事件通知时，此控件才会通过。

启用 S3 事件通知后，当发生影响 S3 存储桶的特定事件时，您会收到警报。例如，您可以收到有关对象创建、对象移除和对象恢复的通知。这些通知可以提醒相关团队注意可能导致未经授权的数据访问的意外或故意修改。

修复

有关检测 S3 存储桶和对象变更的信息，请参阅 Amazon S3 用户指南中的 Amazon S3 事件通知。

ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限

相关要求： 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

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-acl-prohibited

计划类型：已触发变更

参数：无

此控件可检查 Amazon S3 通用存储桶是否通过访问控制列表（ACL）为用户提供权限。如果将 ACL 配置为管理存储桶上的用户访问权限，则此控件将失败。

ACLs 是早于 IAM 的传统访问控制机制。相反 ACLs，我们建议使用 S3 存储桶策略或 AWS Identity and Access Management (IAM) 策略来管理对您的 S3 存储桶的访问权限。

修复

要传递此控制权，您应该对 ACLs S3 存储桶禁用。有关说明，请参阅《Amazon 简单存储服务用户指南》中的控制对象所有权和禁用 ACLs 存储桶。

要创建 S3 存储桶策略，请参阅使用 Amazon S3 控制台添加存储桶策略。要在 S3 存储桶上创建 IAM 用户策略，请参阅使用用户策略控制对存储桶的访问权限。

[S3.13] S3 通用存储桶应具有生命周期配置

相关要求： 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)

类别：保护 > 数据保护

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-lifecycle-policy-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
targetTransitionDays	对象创建后转换到指定存储类的天数。	整数	1 到 36500	无默认值
targetExpirationDays	对象创建后到被删除为止的天数。	整数	1 到 36500	无默认值
targetTransitionStorageClass	目标 S3 存储类类型	枚举	STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR, DEEP_ARCHIVE	无默认值

此控件可检查 Amazon S3 通用存储桶是否具有生命周期配置。如果存储桶不具有生命周期配置，则此控件将失败。如果您为前面的一个或多个参数提供自定义值，则仅当策略包含指定的存储类、删除时间或转换时间时，控制才会通过。

为 S3 存储桶创建生命周期配置可定义您希望 Amazon S3 在对象的生命周期内执行的操作。例如，您可以创建一个生命定期策略，该策略将对象转换为另一个存储类别，存档对象，或在指定时间段后将其删除。

修复

有关在 Amazon S3 存储桶上配置生命周期策略的信息，请参阅在存储桶上设置生命周期配置，并参阅 Amazon S3 用户指南中的管理存储生命周期。

[S3.14] S3 通用存储桶应启用版本控制

类别：保护 > 数据保护 > 数据删除保护

相关要求： 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 3.8 3.8

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-versioning-enabled

计划类型：已触发变更

参数：无

此控件可检查 Amazon S3 通用存储桶是否启用了版本控制。如果暂停了存储桶的版本控制，则此控件将失败。

版本控制将对象的多个变体保留在同一个 S3 存储桶中。您可以使用版本控制来保存、检索和还原存储在 S3 存储桶中的所有对象的所有版本。版本控制可帮助您从意外的用户操作和应用程序故障中恢复。

> **Tip**
>
> 在不进行生命周期管理的情况下启用版本控制可能会导致无限的存储增长和成本的增加。每次修改对象都会创建一个新版本，该版本将无限期保留。配置 S3 生命周期规则，以自动将非当前版本转换为更便宜的存储类别，或者在定义的保留期后将其过期。有关更多信息，请参阅在 S3 生命周期中使用 S3 版本控制和管理对象的生命周期。

修复

要在 S3 存储桶上使用版本控制，请参阅 Amazon S3 用户指南中的在存储桶上启用版本控制。

[S3.15] S3 通用存储桶应启用对象锁定

类别：保护 > 数据保护 > 数据删除保护

相关要求：NIST.800-53.r5 CP-6（2）、PCI DSS v4.0.1/10.5.1

严重性：中

资源类型：AWS::S3::Bucket

AWS Config 规则：s3-bucket-default-lock-enabled

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
mode	S3 对象锁定保留模式	枚举	GOVERNANCE，COMPLIANCE	无默认值

此控件可检查 Amazon S3 通用存储桶是否启用了对象锁定。如果没有为存储桶启用对象锁定，则此控件将失败。如果您为 mode 参数提供自定义值，则仅当 S3 对象锁定使用指定的保留模式时，控制才会通过。

您可以使用 S3 对象锁定通过 write-once-read-many (WORM) 模型存储对象。对象锁定可以帮助防止 S3 存储桶中的对象在固定时间内或无限期地被删除或覆盖。您可以使用 S3 对象锁定满足需要 WORM 存储的法规要求，或添加一个额外的保护层来防止对象被更改和删除。

修复

要为新的和现有 S3 存储桶配置对象锁定，请参阅《Amazon S3 用户指南》中的配置 S3 对象锁定。

[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys

类别：保护 > 数据保护 > 加密 data-at-rest

相关要求： NIST.800-53.r5 SC-12 (2)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、(10)、(1)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6)、 NIST.800-53.r5 CA-9 nist.800-53.r5 AU-9、nist.800-171.r2 3.8.9、nist.800-171.r2 3.13.16、PCI DSS v4.0.1/3.5.1

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-default-encryption-kms

计划类型：已触发变更

参数：无

此控件会检查 Amazon S3 通用存储桶是否使用 AWS KMS key （SSE-KMS 或 DSSE-KMS）进行加密。如果使用默认加密（SSE-S3）对存储桶进行加密，则此控件将失败。

服务器端加密（SSE）是接收数据的应用程序或服务在数据目的地对其进行加密。密是指由接收数据的应用程序或服务在目标位置对数据进行加密。除非您另行指定，否则 S3 存储桶默认使用 Amazon S3 托管密钥（SSE-S3）进行服务器端加密。但是，为了增加控制力，您可以选择将存储桶配置为改用服务器端加密 AWS KMS keys （SSE-KMS 或 DSSE-KMS）。当您的数据写入数据中心的磁盘时，Amazon S3 会在对象级别对其进行加密，并在您访问 AWS 数据时为您解密。

修复

要使用 SSE-KMS 加密 S3 存储桶，请参阅 Amazon S3 用户指南中的使用 AWS KMS (SSE-KMS) 指定服务器端加密。要使用 DSSE-KMS 加密 S3 存储桶，请参阅 Amazon S3 用户指南中的使用 AWS KMS keys (DSSE-KMS) 指定双层服务器端加密。

[S3.19] S3 接入点已启用屏蔽公共访问权限设置

相关要求： 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、、、(11) NIST.800-53.r5 AC-6 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)、(4)、 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9)、 NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::S3::AccessPoint`

AWS Config 规则：s3-access-point-public-access-blocks

计划类型：已触发变更

参数：无

该控件检查 Amazon S3 接入点是否启用了屏蔽公共访问权限设置。如果没有为接入点启用屏蔽公共访问权限设置，则控制失败。

Amazon S3 屏蔽公共访问权限功能可帮助您在 3 个级别上管理对 S3 资源的访问权限：账户、存储桶和接入点级别。可以独立配置每个级别的设置，从而允许您对数据设置不同级别的公共访问权限限制。接入点设置不能单独覆盖更高级别的、限制性更高的设置（账户级别或分配给接入点的存储桶）。相反，接入点级别的设置是附加的，这意味着它们作为其他级别的设置的补充，并与之配合使用。除非您打算让 S3 接入点可供公共访问，否则应启用屏蔽公共访问权限设置。

修复

Amazon S3 当前不支持在创建接入点之后更改接入点的屏蔽公共访问权限设置。默认情况下，在创建新的接入点时，将启用所有屏蔽公共访问权限设置。除非您有特定的需求要禁用任何一个设置，建议您将所有设置保持为启用状态。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的管理接入点的公共访问权限。

[S3.20] S3 通用存储桶应启用 MFA 删除

相关要求：CIS AWS 基金会基准 v5.0.0/2.1.2、CIS 基金会基准 v3.0.0/2.1.2、 AWS CI AWS S 基金会基准 v1.4.0/2.1.3、(1)、(2) NIST.800-53.r5 CA-9 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

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：s3-bucket-mfa-delete-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否启用了多重身份验证（MFA）删除。如果存储桶未启用 MFA 删除，则控件将失败。对于具有生命周期配置的存储桶，该控件不会生成任何调查发现。

如果为 S3 通用存储桶启用版本控制，则可以选择为存储桶配置 MFA 删除，从而添加另一层安全保护。如果这样做，存储桶所有者必须在删除存储桶中对象的版本或更改存储桶的版本控制状态的任何请

求中包含两种形式的身份验证。例如，如果存储桶所有者的安全凭证遭到泄露，MFA 删除可提供额外安全性。MFA 删除要求启动删除操作的用户证明其实际拥有具有 MFA 代码的 MFA 设备，并为删除操作增加额外的摩擦和安全性，这样也有助于防止存储桶被意外删除。

> **Note**
>
> 仅当 S3 通用存储桶启用 MFA 删除时，此控件才会生成 PASSED 调查发现。要为某存储桶启用 MFA 删除，还必须为该存储桶启用版本控制。存储桶版本控制是在相同的存储桶中存储 S3 对象的多个变体的方法。此外，只有以根用户身份登录的存储桶拥有者才能启用 MFA 删除并对存储桶执行删除操作。不能对具有生命周期配置的存储桶使用 MFA 删除。

修复

有关启用版本控制和为 S3 存储桶配置 MFA 删除的信息，请参阅《Amazon Simple Storage Service 用户指南》中的配置 MFA 删除。

[S3.22] S3 通用存储桶应记录对象级写入事件

相关要求：CIS AWS 基金会基准 v5.0.0/3.8、CIS 基金会基准 v3.0.0/3.8、PCI DS AWS S v4.0.1/10.2.1

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：cloudtrail-all-write-s3-data-event-check

计划类型：定期

参数：无

此控件检查是否至少 AWS 账户 有一个 AWS CloudTrail 多区域跟踪，用于记录 Amazon S3 存储桶的所有写入数据事件。如果账户没有用于记录 S3 存储桶写入数据事件的多区域跟踪，则此控件将失败。

S3 对象级操作（例如 `GetObject`、`DeleteObject` 和 `PutObject`）称为数据事件。默认情况下，CloudTrail 不记录数据事件，但您可以配置跟踪以记录 S3 存储桶的数据事件。当您为写入数据事件启用对象级日志记录时，您可以记录 S3 存储桶内每个单独的对象（文件）访问。启用对象级日志记录可

以帮助您满足数据合规性要求，执行全面的安全分析，监控您的特定用户行为模式 AWS 账户，并使用 Amazon Events 对 S3 存储桶中的对象级 API 活动采取措施。 CloudWatch 如果您配置了多区域跟踪，用于记录所有 S3 存储桶的只写或所有类型的数据事件，则此控件会生成 PASSED 调查发现。

修复

要为 S3 存储桶启用对象级日志记录，请参阅《Amaz on 简单存储服务用户指南》中的 “为 S3 存储桶和对象启用 CloudTrail 事件记录”。

[S3.23] S3 通用存储桶应记录对象级读取事件

相关要求：CIS AWS 基金会基准 v5.0.0/3.9、CIS 基金会基准 v3.0.0/3.9、PCI DS AWS S v4.0.1/10.2.1

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：cloudtrail-all-read-s3-data-event-check

计划类型：定期

参数：无

此控件检查是否至少 AWS 账户 有一个 AWS CloudTrail 多区域跟踪，用于记录 Amazon S3 存储桶的所有读取数据事件。如果账户没有用于记录 S3 存储桶读取数据事件的多区域跟踪，则此控件将失败。

S3 对象级操作（例如 `GetObject`、`DeleteObject` 和 `PutObject`）称为数据事件。默认情况下，CloudTrail 不记录数据事件，但您可以配置跟踪以记录 S3 存储桶的数据事件。当您为读取数据事件启用对象级日志记录时，您可以记录 S3 存储桶内每个单独的对象（文件）访问。启用对象级日志记录可以帮助您满足数据合规性要求，执行全面的安全分析，监控您的特定用户行为模式 AWS 账户，并使用 Amazon Events 对 S3 存储桶中的对象级 API 活动采取措施。 CloudWatch 如果您配置了多区域跟踪，用于记录所有 S3 存储桶的只读或所有类型的数据事件，则此控件会生成 PASSED 调查发现。

修复

要为 S3 存储桶启用对象级日志记录，请参阅《Amaz on 简单存储服务用户指南》中的 “为 S3 存储桶和对象启用 CloudTrail 事件记录”。

[S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置

相关要求：PCI DSS v4.0.1/1.4.4

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::S3::MultiRegionAccessPoint`

AWS Config 规则:`s3-mrap-public-access-blocked`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：无

此控件可检查 Amazon S3 多区域接入点是否启用了屏蔽公共访问权限设置。当多区域接入点未启用屏蔽公共访问权限设置时，此控件将失败。

可公开访问的资源可能会导致未经授权的访问、数据泄露或漏洞利用。通过身份验证和授权措施来限制访问有助于保护敏感信息并维护资源的完整性。

修复

默认情况下，为 S3 多区域接入点启用所有屏蔽公共访问权限设置。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用 Amazon S3 多区域接入点屏蔽公共访问权限。在创建多区域接入点之后，您无法更改其屏蔽公共访问权限设置。

[S3.25] S3 目录存储桶应具有生命周期配置

类别： 保护 > 数据保护

严重性：低

资源类型：`AWS::S3Express::DirectoryBucket`

AWS Config 规则：s3express-dir-bucket-lifecycle-rules-check

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`targetExpirationDays`	创建对象后对象应过期的天数。	整数	1 到 2147483647	无默认值

此控件检查是否为 S3 目录存储桶配置了生命周期规则。如果未为目录存储桶配置生命周期规则，或者存储桶的生命周期规则指定的过期设置与您可选指定的参数值不匹配，则该控件会失败。

在 Amazon S3 中，生命周期配置是一组规则，其定义 Amazon S3 对存储桶中的一组对象执行的操作。对于 S3 目录存储桶，您可以创建一个生命周期规则，根据期限（以天为单位）指定对象何时过期。您还可以创建一个删除未完成分段上传的生命周期规则。与其他类型的 S3 存储桶（例如通用存储桶）不同，目录存储桶对生命周期规则不支持其他类型的操作（例如在存储类别之间转换对象）。

修复

要为 S3 目录存储桶定义生命周期配置，请为该存储桶创建一个生命周期规则。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的为目录存储桶创建和管理生命周期配置。

适用于 AI 的 Security Hub CSPM 控件 SageMaker

这些 AWS Security Hub CSPM 控制措施会评估 Amazon SageMaker AI 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

相关要求： 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、(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。 1/1.2.1，PCI DSS v3.2。 1/1.3.1，PCI DSS v3.2。 1/1.3.2，PCI DSS v3.2。 1/1.3.4，PCI DSS v3.2。 1/1.3.6，PCI DSS v4.0。 1/1.4.4

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::SageMaker::NotebookInstance`

AWS Config 规则：sagemaker-notebook-no-direct-internet-access

计划类型：定期

参数：无

此控件用于检查 SageMaker AI 笔记本实例是否已禁用直接互联网接入。如果为笔记本实例启用了 `DirectInternetAccess` 字段，则此控件将失败。

如果您在没有 VPC 的情况下配置 SageMaker AI 实例，则默认情况下，您的实例将启用直接互联网访问。您应该使用 VPC 配置实例，并将默认设置变更为禁用——通过 VPC 访问 Internet。要使用笔记本电脑训练或托管模型，您需要访问 Internet。要启用互联网访问，您的 VPC 必须具有接口端点（AWS PrivateLink）或 NAT 网关，以及允许出站连接的安全组。要详细了解如何将笔记本实例连接到 VPC 中的资源，请参阅 Amazon A SageMaker I 开发人员指南中的将笔记本实例连接到 VPC 中的资源。您还应确保只有经过授权的用户才能访问您的 SageMaker AI 配置。限制允许用户更改 A SageMaker I 设置和资源的 IAM 权限。

修复

在创建笔记本实例后，您无法变更 Internet 访问设置。相反，您可以停止、删除和重新创建 Internet 访问受阻的实例。要删除允许直接访问互联网的笔记本实例，请参阅 Amazon A SageMaker I 开发者指南中的使用笔记本实例构建模型：清理。要重新创建拒绝 Internet 访问的笔记本实例，请参阅创建笔记本实例。对于网络，直接访问Internet，选择禁用-通过 VPC 访问 Internet。

[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

相关要求： 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)

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：高

资源类型：`AWS::SageMaker::NotebookInstance`

AWS Config 规则：sagemaker-notebook-instance-inside-vpc

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker AI 笔记本实例是否在自定义虚拟私有云 (VPC) 中启动。如果 A SageMaker I 笔记本实例未在自定义 VPC 内启动或在 SageMaker AI 服务 VPC 中启动，则此控制失败。

子网是 VPC 内的一系列 IP 地址。我们建议尽可能将资源保留在自定义 VPC 内，以确保为您的基础设施提供安全的网络保护。Amazon VPC 是专用于您的虚拟网络 AWS 账户。使用 Amazon VPC，您可以控制 A SageMaker I Studio 和笔记本实例的网络访问和互联网连接。

修复

在创建笔记本实例后，您无法变更 VPC 设置。相反，您可以停止、删除和重新创建实例。有关说明，请参阅 Amazon A SageMaker I 开发者指南中的使用笔记本实例构建模型：清理。

[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限

相关要求： 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)

类别：保护 > 安全访问管理 >根用户访问限制

严重性：高

资源类型：`AWS::SageMaker::NotebookInstance`

AWS Config 规则：sagemaker-notebook-instance-root-access-check

计划类型：已触发变更

参数：无

此控件检查是否已为 Amazon A SageMaker I 笔记本实例开启根访问权限。如果为 SageMaker AI 笔记本实例开启了根访问权限，则控制失败。

根据最低权限原则，建议的安全最佳实践是限制根用户对实例资源的访问权限，以避免无意中过度预置权限。

修复

要限制对 SageMaker AI 笔记本实例的根访问权限，请参阅 A mazon A SageMaker I 开发者指南中的控制 A SageMaker I 笔记本实例的根访问权限。

[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

相关要求： NIST.800-53.r5 CP-10、 NIST.800-53.r5 SC-5、 NIST.800-53.r5 SC-36、NIST.800-53.r5 SA-13

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::SageMaker::EndpointConfig`

AWS Config 规则：sagemaker-endpoint-config-prod-instance-count

计划类型：定期

参数：无

此控件会检查 Amazon A SageMaker I 终端节点的生产变体的初始实例数是否大于 1。如果端点的生产变体只有 1 个初始实例，则此控件将失败。

在实例数大于 1 的情况下运行的生产变体允许由 A SageMaker I 管理的多可用区实例冗余。跨多个可用区部署资源是在您的架构中提供高可用性 AWS 的最佳实践。高可用性可帮助您从安全事件中恢复。

> **Note**
>
> 此控件仅适用于基于实例的端点配置。

修复

有关终端节点配置参数的更多信息，请参阅 Amazon A SageMaker I 开发人员指南中的创建终端节点配置。

[SageMaker.5] SageMaker 模型应启用网络隔离

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：中

资源类型：`AWS::SageMaker::Model`

AWS Config 规则：sagemaker-model-isolation-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon A SageMaker I 托管模型是否启用了网络隔离。如果托管模型的 `EnableNetworkIsolation` 参数设置为 `False`，则该控件会失败。

SageMaker AI 训练和部署的推理容器默认支持互联网。如果您不希望 SageMaker AI 为训练或推理容器提供外部网络访问权限，则可以启用网络隔离。如果启用网络隔离，则无法通过模型容器进行入站或出站网络调用，包括通过其他 AWS 服务进行的调用。此外，容器运行时环境不提供任何 AWS 凭证。启用网络隔离有助于防止互联网意外访问您的 SageMaker AI 资源。

> **Note**
>
> 2025年8月13日，Security Hub CSPM更改了该控件的标题和描述。新的标题和描述更准确地反映了控件会检查 Amazon A SageMaker I 托管模型的`EnableNetworkIsolation`参数设置。以前，此控件的标题为：SageMaker models should block inbound traffic。

修复

有关 SageMaker AI 模型的网络隔离的更多信息，请参阅 A mazon A SageMaker I 开发者指南中的在无互联网模式下运行训练和推理容器。创建模型时，您可以通过将 `EnableNetworkIsolation` 参数的值设置为 `True` 来启用网络隔离。

[SageMaker.6] SageMaker 应用映像配置应加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SageMaker::AppImageConfig`

AWS Config 规则：sagemaker-app-image-config-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon SageMaker AI 应用程序映像配置 (AppImageConfig) 是否具有requiredKeyTags参数指定的标签密钥。如果应用程序映像配置没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件会失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果应用程序映像配置没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

要向 Amazon A SageMaker I 应用程序映像配置 (AppImageConfig) 添加标签，您可以使用 SageMaker AI API 的AddTags操作，或者，如果您使用的是 AWS CLI，则运行 add -tags 命令。

[SageMaker.7] 应给 SageMaker 图片加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::SageMaker::Image

AWS Config 规则：sagemaker-image-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 Amazon SageMaker AI 图像是否具有`requiredKeyTags`参数指定的标签密钥。如果映像没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件会失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果映像没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

要向 Amazon A SageMaker I 图像添加标签，您可以使用 SageMaker AI API 的AddTags操作，或者如果您使用的是，则可以运行 add -tags 命令。 AWS CLI

[SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行

类别：检测 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::SageMaker::NotebookInstance`

AWS Config 规则：sagemaker-notebook-instance-platform-version

计划类型：定期

参数：

- `supportedPlatformIdentifierVersions`：`notebook-al2-v3`（不可自定义）

此控件根据为笔记本实例指定的平台标识符，检查 SageMaker Amazon AI 笔记本实例是否配置为在支持的平台上运行。如果笔记本实例配置为在不再受支持的平台上运行，则该控件会失败。

如果不再支持 Amazon SageMaker AI 笔记本实例的平台，则该平台可能无法收到安全补丁、错误修复或其他类型的更新。笔记本实例可能会继续运行，但它们不会收到 SageMaker AI 安全更新或严重错误修复。使用不支持的平台所带来的风险由您自行承担。有关更多信息，请参阅 Amazon A SageMaker I 开发者指南中的JupyterLab版本控制。

修复

有关 Amazon A SageMaker I 目前支持的平台以及如何迁移到这些平台的信息，请参阅《亚马逊 A SageMaker I 开发者指南》中的 Amaz on Linux 2 笔记本实例。

[SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::SageMaker::DataQualityJobDefinition`

AWS Config 规则：sagemaker-data-quality-job-encrypt-in-transit

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker AI 数据质量任务定义是否为容器间流量启用了加密。如果监控数据质量和漂移的任务的定义没有为容器间流量启用加密，则控制失败。

启用容器间流量加密可在分布式处理期间保护敏感的机器学习数据，以进行数据质量分析。

修复

有关 Amazon AI 的容器间流量加密的更多信息，请参阅 SageMaker Amazon A SageMaker I 开发人员指南中的保护分布式训练 Job 中机器学习计算实例之间的通信。创建数据质量任务定义时，您可以通过将EnableInterContainerTrafficEncryption参数的值设置为来启用容器间流量加密。True

[SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：AWS::SageMaker::ModelExplainabilityJobDefinition

AWS Config 规则：sagemaker-model-explainability-job-encrypt-in-transit

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker 模型可解释性任务定义是否启用了容器间流量加密。如果模型可解释性任务定义未启用容器间流量加密，则控制失败。

启用容器间流量加密可在分布式处理期间保护敏感的机器学习数据，例如模型数据、训练数据集、中间处理结果、参数和模型权重，以进行可解释性分析。

修复

对于现有的 SageMaker 模型可解释性任务定义，无法在原地更新容器间流量加密。要创建启用容器间流量加密的新 SageMaker 模型可解释性任务定义，请使用 API 或 CL I 或 CloudFormation并将设置为。EnableInterContainerTrafficEncryptionTrue

[SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::SageMaker::DataQualityJobDefinition

AWS Config 规则：sagemaker-data-quality-job-isolation

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker AI 数据质量监控任务定义是否启用了网络隔离。如果监控数据质量和偏差的作业的定义禁用了网络隔离，则控制失败。

网络隔离可减少攻击。浮出水面并防止外部访问，从而防止未经授权的外部访问、意外的数据泄露和潜在的数据泄露。

修复

有关 AI 网络隔离的更多信息，请参阅 A mazon SageMaker A SageMaker I 开发者指南中的在无互联网模式下运行训练和推理容器。创建数据质量作业定义时，可以通过将`EnableNetworkIsolation`参数的值设置为来启用网络隔离`True`。

[SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离

类别：保护 > 安全网络配置 > 资源策略配置

严重性：中

资源类型：`AWS::SageMaker::ModelBiasJobDefinition`

AWS Config 规则：sagemaker-model-bias-job-isolation

计划类型：已触发变更

参数：无

此控件检查 SageMaker 模型偏差作业定义是否启用了网络隔离。如果模型偏差作业定义未启用网络隔离，则控制失败。

网络隔离可防止 SageMaker 模型偏差作业通过 Internet 与外部资源通信。通过启用网络隔离，可以确保任务的容器无法建立出站连接，从而减少攻击面并保护敏感数据免遭泄露。这对于处理受监管或敏感数据的作业尤其重要。

修复

要启用网络隔离，您必须创建一个新的模型偏差作业定义，并将`EnableNetworkIsolation`参数设置为`True`。创建作业定义后，无法修改网络隔离。要创建新的模型偏差任务定义，请参阅 Amazon A SageMaker I 开发者指南 CreateModelBiasJobDefinition中的。

[SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::SageMaker::ModelQualityJobDefinition`

AWS Config 规则：ssagemaker-model-quality-job-encrypt-in-transit

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker 模型质量任务定义是否为容器间流量启用了传输中加密。如果模型质量任务定义未启用容器间流量加密，则控制失败。

Inter-container 流量加密可保护分布式模型质量监控任务期间在容器之间传输的数据。默认情况下，容器间流量未加密。启用加密有助于在处理过程中保持数据机密性，并支持遵守传输中数据保护的监管要求。

修复

要为您的 Amazon SageMaker 模型质量任务定义启用容器间流量加密，您必须使用相应的传输中加密配置重新创建任务定义。要创建模型质量任务定义，请参阅 Amazon A SageMaker I 开发者指南 CreateModelQualityJobDefinition中的。

[SageMaker.14] SageMaker 监控计划应启用网络隔离

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::SageMaker::MonitoringSchedule`

AWS Config 规则：sagemaker-monitoring-schedule-isolation

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker 监控计划是否启用了网络隔离。如果监视计划 EnableNetworkIsolation 设置为 false 或未配置，则控制失败

网络隔离可防止监控作业进行出站网络呼叫，通过消除容器访问互联网来减少攻击面。

修复

有关在创建或更新监控计划时在 NetworkConfig 参数中配置网络隔离的信息，请参阅 Amazon A SageMaker I 开发者指南 UpdateMonitoringSchedule中的CreateMonitoringSchedule或。

[SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密

类别：保护 > 数据保护 > 传输中数据加密

严重性：中

资源类型：`AWS::SageMaker::ModelBiasJobDefinition`

AWS Config 规则：sagemaker-model-bias-job-encrypt-in-transit

计划类型：已触发变更

参数：无

此控件检查在使用多个计算实例时，Amazon SageMaker 模型偏差任务定义是否启用了容器间流量加密。如果设置`EnableInterContainerTrafficEncryption`为 false 或者没有为实例计数等于 2 或更大的作业定义进行配置，则控件将失败。

EInter-container 流量加密可保护分布式模型偏差监控作业期间计算实例之间传输的数据。加密可防止未经授权访问模型相关信息，例如实例之间传输的权重。

修复

要为 SageMaker 模型偏差任务定义启用容器间流量加密，请在任务定义使用多个计算实例`True`时将`EnableInterContainerTrafficEncryption`参数设置为。有关保护 ML 计算实例之间通信的信息，请参阅 Amazon A SageMaker I 开发人员指南中的保护分布式训练 Job 中机器学习计算实例之间的通信。

[SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：中

资源类型：`AWS::SageMaker::Model`

AWS Config 规则：sagemaker-model-private-registry-required

计划类型：已触发变更

参数：无

此控件检查 Amazon SageMaker AI 模型是否从 VPC 中的私有注册表中为主容器提取容器映像。如果未配置映像或存储库访问模式为，则控制失败`Platform`。

在 VPC 中为 SageMaker 模型容器使用私有 Docker 注册表可确保从您的 VPC 内可信、受控的来源提取容器镜像。此外，它还可确保通过 VPC 终端节点访问容器映像，而无需通过公共互联网。

修复

要为 SageMaker AI 实时推理容器配置私有 docker 注册表，请参阅 Amazon AI 开发者指南中的将私有 Docker 注册表用于 Real-Time 推理容器。 SageMaker

[SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::SageMaker::FeatureGroup`

AWS Config 规则：sagemaker-featuregroup-encryption-at-rest

计划类型：已触发变更

参数：无

此控件检查功能组的 Amazon SageMaker 离线商店是否使用 AWS KMS 密钥进行静态加密。如果功能组的离线存储 S3 存储未使用 KMS 密钥加密，则控制失败。

在 SageMaker 功能组线下商店的其余部分使用客户管理 AWS KMS keys 的加密可增强安全性。Customer-managed KMS 密钥可让您完全控制加密密钥生命周期和密钥策略。此外，可以记录和监控所有加密密钥的使用情况， AWS CloudTrail 以实现可审计性。

修复

有关使用 AWS KMS 客户管理的密钥为 SageMaker 功能商店线下商店启用静态加密的信息，请参阅 Amazon A SageMaker I 开发者指南中的安全和访问控制。

[SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键

相关要求： 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)

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：`AWS::SageMaker::FeatureGroup`

AWS Config 规则：sagemaker-featuregroup-online-store-encryption

计划类型：已触发变更

参数：无

此控件检查具有标准存储空间的功能组的 Amazon SageMaker 在线商店是否使用 AWS KMS 密钥进行静态加密。如果未为在线商店配置 KMS 密钥加密，则控制失败。

在其余 SageMaker 功能组在线商店中使用客户管理 AWS KMS keys 的加密可增强安全性。Customer-managed KMS 密钥使您可以完全控制加密密钥的生命周期和密钥策略。此外，可以记录和监控所有加密密钥的使用情况， AWS CloudTrail 以实现可审计性。

修复

有关使用 AWS KMS 客户管理的密钥为 SageMaker 功能商店在线商店启用静态加密的信息，请参阅 Amazon A SageMaker I 开发者指南中的安全和访问控制。

[SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：中

资源类型：`AWS::SageMaker::Model`

AWS Config 规则：sagemaker-model-multicontainer-private-registry

计划类型：已触发变更

参数：无

此控件可检查具有多容器推理管道的 SageMaker Amazon AI 模型是否从 VPC 中的私有 Docker 注册表中提取容器镜像。如果任何容器定义没有图像配置或存储库访问模式设置为平台，则控件将失败。

在 VPC 中使用私有 Docker 注册表进行 SageMaker 人工智能多容器推理管道，可确保从您的 VPC 中可信、受控的来源提取容器镜像。这可确保通过 VPC 端点访问容器镜像，无需通过公共互联网，从而降低供应链攻击或图像篡改的风险。

修复

要为 SageMaker AI 实时推理容器配置私有 docker 注册表，请参阅 Amazon AI 开发者指南中的将私有 Docker 注册表用于 Real-Time 推理容器。 SageMaker

Secrets Manager 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估 AWS Secrets Manager 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

相关要求： NIST.800-53.r5 AC-2(1)、 NIST.800-53.r5 AC-3 (15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

类别：保护 > 安全开发

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-rotation-enabled-check`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`maximumAllowedRotationFrequency`	密钥轮换频率的最大允许天数（以天为单位）。	整数	1 到 365	无默认值

此控件检查存储在中的密钥 AWS Secrets Manager 是否配置了自动轮换。如果密钥未配置自动轮换，则控制失败。如果您为 `maximumAllowedRotationFrequency` 参数提供自定义值，则仅当密钥在指定的时间窗口内自动轮换时，控制才会通过。

Screts Manager 可帮助您改善组织的安全状况。密钥包括数据库凭证、密码和第三方 API 密钥。您可以使用 Secrets Manager 集中存储机密、自动加密机密、控制对机密的访问以及安全自动轮换机密。

Secrets Manager 可以轮换密钥。您可以使用轮换将长期密钥替换为短期机密。轮换密钥会限制未经授权的用户使用泄露密钥的时间。因此，您应该经常轮换机密。要了解有关轮换的更多信息，请参阅《AWS Secrets Manager 用户指南》中的轮换 AWS Secrets Manager 密钥。

修复

要启用 Secrets Manager 密钥的自动轮换，请参阅《AWS Secrets Manager 用户指南》中的使用控制台为 AWS Secrets Manager 密钥设置自动轮换。必须选择和配置轮换 AWS Lambda 函数。

[SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换

相关要求： NIST.800-53.r5 AC-2(1)、 NIST.800-53.r5 AC-3 (15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

类别：保护 > 安全开发

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-scheduled-rotation-success-check`

计划类型：已触发变更

参数：无

此控件根据轮换计划检查 AWS Secrets Manager 密钥是否成功轮换。如果 `RotationOccurringAsScheduled` 是 `false`，则控制失败。该控件只评估已开启轮换。

Screts Manager 可帮助您改善组织的安全状况。密钥包括数据库凭证、密码和第三方 API 密钥。您可以使用 Secrets Manager 集中存储机密、自动加密机密、控制对机密的访问以及安全自动轮换机密。

Secrets Manager 可以轮换密钥。您可以使用轮换将长期密钥替换为短期机密。轮换密钥会限制未经授权的用户使用泄露密钥的时间。因此，您应该经常轮换机密。

除了将机密配置为自动轮换之外，您还应确保这些机密根据轮换计划成功轮换。

要了解有关轮换的更多信息，请参阅 AWS Secrets Manager 用户指南中的轮换 AWS Secrets Manager 密钥。

修复

如果自动轮换失败，那么 Secrets Manager 可能遇到了错误配置。要在 Secrets Manager 中轮换密钥，您可以使用 Lambda 函数来定义如何与拥有该密钥的数据库或服务进行交互。

有关诊断和修复与密钥轮换相关的常见错误的帮助，请参阅AWS Secrets Manager 用户指南中的密钥 AWS Secrets Manager 轮换疑难解答。

[SecretsManager.3] 移除未使用的 Secrets Manager 密钥

相关要求： NIST.800-53.r5 AC-2(1)、 NIST.800-53.r5 AC-3 (15)

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-secret-unused`

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`unusedForDays`	密钥可以保持未使用状态的最大天数	整数	1 到 365	90

此控件检查 AWS Secrets Manager 密钥是否在指定的时间范围内被访问。如果密钥在指定的时间范围之外未使用，则控制失败。除非您为访问期提供自定义参数值，否则 Security Hub CSPM 将使用 90 天的默认值。

删除未使用的机密与轮换机密一样重要。未使用的机密可能会被以前的用户滥用，他们不再需要访问这些机密。此外，随着越来越多的用户访问秘密，有人可能会处理不当并将其泄露给未经授权的实体，这增加了滥用的风险。删除未使用的密钥有助于撤销不再需要的用户的密钥访问权限。它还有助于降低 Secrets Manager 的使用 Secrets Manager 的成本。因此，必须定期删除未使用的密钥。

修复

要删除不活跃的 Sec rets Manager AWS Secrets Manager 密钥，请参阅AWS Secrets Manager 用户指南中的删除密钥。

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

相关要求： NIST.800-53.r5 AC-2(1)、 NIST.800-53.r5 AC-3 (15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-secret-periodic-rotation`

计划类型：定期

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`maxDaysSinceRotation`	密钥可以保持不变的最大天数	整数	1 到 180	90

此控件检查 AWS Secrets Manager 密钥是否在指定的时间范围内至少轮换一次。如果密钥未达到该轮换频率，则控制失败。除非您为轮换期提供自定义参数值，否则 Security Hub CSPM 将使用 90 天的默认值。

轮换密钥可以帮助您降低未经授权在 AWS 账户中使用密钥的风险。示例包括数据库凭证、密码、第三方 API 密钥，甚至任意文本。如果您长时间不更改密钥，则密钥更有可能被泄露。

随着越来越多的用户访问密钥，有人处理不当并将其泄露给未经授权的实体的可能性就变得更大。密钥可能会通过日志和缓存数据泄露出去。密钥可能会共享用于调试目的，但在调试完成后未更改或撤销。出于所有这些原因，密钥应该频繁地轮换。

您可以在 AWS Secrets Manager中为密钥配置自动轮换。通过自动轮换，您可以用短期密钥替换长期密钥，从而显着降低泄露风险。我们建议您为 Secrets Manager 密钥配置自动轮换。有关更多信息，请参阅 AWS Secrets Manager 用户指南中的轮换 AWS Secrets Manager 密钥。

修复

要启用 Secrets Manager 密钥的自动轮换，请参阅《AWS Secrets Manager 用户指南》中的使用控制台为 AWS Secrets Manager 密钥设置自动轮换。必须选择和配置轮换 AWS Lambda 函数。

[SecretsManager.5] 应标记 Secrets Manager 机密

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则:`tagged-secretsmanager-secret`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Secrets Manager 密钥是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果密钥没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果该密钥未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些

ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Secrets Manager 密钥添加标签，请参阅AWS Secrets Manager 用户指南中的标签 AWS Secrets Manager 密钥。

Security Hub CSPM 控件适用于 AWS Service Catalog

此 AWS Security Hub CSPM 控件评估 AWS Service Catalog 服务和资源。该控件可能并非在所有 AWS 区域都可用。有关更多信息，请参阅 按地区划分的控件可用性。

[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享

相关要求： 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

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::ServiceCatalog::Portfolio`

AWS Config 规则：service-catalog-shared-within-organization

计划类型：已触发变更

参数：无

此控件检查启用与 AWS Organizations 集成后，组织内是否 AWS Service Catalog 共享投资组合。如果组织内不共享产品组合，则此控件将失败。

仅在组织内共享产品组合有助于确保不会与不正确的 AWS 账户共享产品组合。要与组织中的账户共享服务目录组合，Security Hub CSPM 建议使用`ORGANIZATION_MEMBER_ACCOUNT`代替。`ACCOUNT`这

样就可以通过管理整个组织内授予账户的访问权限来简化管理。如果您有业务需要与外部账户共享 Service Catalog 产品组合，您可以从此控件自动隐藏调查发现或禁用此控件。

修复

要启用与共享电子档案夹 AWS Organizations，请参阅《AWS Service Catalog 管理员指南》 AWS Organizations中的 “与共享”。

适用于 Amazon SES 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估了亚马逊简单电子邮件服务 (Amazon SES) Service 的服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SES.1] 应标记 SES 联系人列表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SES::ContactList`

AWS Config规则:`tagged-ses-contactlist`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon SES 联系人列表中是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果联系人列表没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果联系人列表未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向亚马逊 SES 联系人列表添加标签，请参阅TagResource《亚马逊 SES API v2 参考》。

[SES.2] 应标记 SES 配置集

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SES::ConfigurationSet`

AWS Config规则:`tagged-ses-configurationset`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件可检查 Amazon SES 配置集是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果配置集没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果配置集未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Amazon SES 配置集添加标签，请参阅TagResource《亚马逊 SES API v2 参考》。

[SES.3] SES 配置集应启用 TLS 以发送电子邮件

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::SES::ConfigurationSet`

AWS Config 规则：ses-sending-tls-required

计划类型：已触发变更

参数：无

此控件检查 Amazon SES 配置集是否需要 TLS 连接。如果配置集的 TLS 策略未设置`'REQUIRE'`为，则控制失败。

默认情况下，Amazon SES 使用机会主义 TLS，这意味着如果无法与接收邮件服务器建立 TLS 连接，则可以在未加密的情况下发送电子邮件。对电子邮件发送强制执行 TLS 可确保只有在可以建立安全的加密连接时才会发送邮件。这有助于在 Amazon SES 和收件人的邮件服务器之间传输期间保护电子邮件内容的机密性和完整性。如果无法建立安全的 TLS 连接，则邮件将无法传送，从而防止敏感信息可能被泄露。

> **Note**
>
> 虽然 TLS 1.3 是 Amazon SES 的默认传送方式，但如果不通过配置集强制执行 TLS 要求，则在 TLS 连接失败时，可能会以纯文本形式传送消息。要传递此控制权，您必须在 SES 配置集的传送选项`'REQUIRE'`中将 TLS 策略配置为。如果需要 TLS，则只有在能够与接收邮件服务器建立 TLS 连接的情况下，才会传递邮件。

修复

要将 Amazon SES 配置为要求配置集使用 TLS 连接，请参阅《亚马逊 SES 开发者指南》中的 Amazon SES 和安全协议。

适用于亚马逊 SNS 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、8 (1)、(10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI- NIST.800-53.r5 SC-2 7 (6)、 NIST.800-53.r5 SC-7 nist.800-171.r2 3.13.11、nist.800-171.r2 3.13.11、nist.800-171.r2 3.13.16

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::SNS::Topic`

AWS Config 规则：`sns-encrypted-kms`

计划类型：已触发变更

参数：无

此控件可检查是否使用 AWS Key Management Service（AWS KMS）中管理的密钥对 Amazon SNS 主题进行静态加密。如果 SNS 主题未使用 KMS 密钥进行服务器端加密（SSE），则此控件将失败。默认情况下，SNS 使用磁盘加密来存储消息和文件。要传递此控件，必须选择改用 KMS 密钥进行加密。这将额外增加一层安全性，并提供更多的访问控制灵活性。

对静态数据进行加密可降低存储在磁盘上的数据被未经身份验证的用户访问的风险。 AWS需要 API 权限来解密数据，然后才能读取数据。我们建议使用 KMS 密钥加密 SNS 主题，以额外增加一层安全性。

修复

要为 SNS 主题启用 SSE，请参阅《Amazon Simple Notification Service 开发人员指南》中的为 Amazon SNS 主题启用服务器端加密（SSE）。在使用 SSE 之前，还必须配置 AWS KMS key 策略以允许对主题进行加密以及对消息进行加密和解密。有关更多信息，请参阅《Amazon 简单通知服务开发者指南》中的配置 AWS KMS 权限。

[SNS.2] 应为发送到主题的通知消息启用传输状态记录

> **Important**
>
> Security Hub CSPM 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub CSPM 控件的更改日志。

相关要求：NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::SNS::Topic`

AWS Config 规则：`sns-topic-message-delivery-notification-enabled`

计划类型：已触发变更

参数：无

此控件检查是否启用记录发送到端点的 Amazon SNS 主题的通知消息的传输状态。如果未启用邮件的传输状态通知，则此控件将失败。

日志记录是维护服务的可靠性、可用性和性能的重要组成部分。记录消息传送状态有助于提供操作见解，例如：

- 了解消息是否已传输到 Amazon SNS 端点。
- 识别从 Amazon SNS 端点发送到 Amazon SNS 的响应。
- 确定消息停留时间（发布时间戳和移交到 Amazon SNS 端点之间的时间）。

修复

要为主题配置传输状态日志，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 消息传输状态。

[SNS.3] 应标记 SNS 主题

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SNS::Topic`

AWS Config 规则:`tagged-sns-topic`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon SNS 主题是否具有带特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果主题没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果主题未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 SNS 主题添加标签，请参阅《Amazon Simple Notification Service Developer Guide》中的 Configuring Amazon SNS topic tags。

[SNS.4] SNS 主题访问策略不应允许公共访问

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::SNS::Topic`

AWS Config 规则：sns-topic-no-public-access

计划类型：已触发变更

参数：无

此控件可检查 Amazon SNS 主题访问策略是否允许公共访问。如果 SNS 主题访问策略允许公共访问，则此控件将失败。

您可以使用具有特定主题的 Amazon SNS 访问策略来限制谁能使用该主题（例如，谁能向该主题发布消息、谁能订阅该主题等）。SNS 策略可以向其他 AWS 账户人或您自己的 AWS 账户用户授予访问权限。在主题策略的 `Principal` 字段中提供通配符（`*`）以及缺乏限制主题策略的条件可能会导致数据泄露、拒绝服务或攻击者向您的服务中注入不必要的消息。

> **Note**
>
> 此控件不会评估使用通配符或变量的策略条件。要生成 PASSED 调查发现，Amazon SNS 主题访问策略中的条件必须仅使用固定值，即不包含通配符或策略变量的值。有关策略变量的信息，请参阅《AWS Identity and Access Management 用户指南》中的变量和标签。

修复

要更新 SNS 主题的访问策略，请参阅《Amazon Simple Notification Service Developer Guide》中的 Overview of managing access in Amazon SNS。

适用于亚马逊 SQS 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估亚马逊简单队列服务 (Amazon SQS) Simple Queue Service 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SQS.1] 应对 Amazon SQS 队列进行静态加密

相关要求： NIST.800-53.r5 CA-9(1)、 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3、8、NIST.800-53.r5 SC-2 8 (1)、 NIST.800-53.r5 SC-7 (10)、nist. NIST.800-53.r5 SC-2 800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::SQS::Queue`

AWS Config 规则:`sqs-queue-encrypted`（ 自定义 Security Hub CSPM 规则 ）

计划类型：已触发变更

参数：无

此控件检查是否对 Amazon SQS 队列进行了静态加密。如果队列未使用 SQS 托管密钥 (SSE-SQS) 或 () 密钥 (SSE-KMS) 加密， AWS Key Management Service 则控制失败。AWS KMS

对静态数据进行加密可降低未经身份验证的用户访问磁盘上存储的数据的风险。服务器端加密 (SSE) 使用 SQS 托管的加密密钥 (SSE-SQS) 或密钥 (SSE-KMS) 保护 SQS 队列中的消息内容。 AWS KMS

修复

要为 SQS 队列配置 SSE，请参阅《Amazon Simple Queue Service 开发人员指南》中的为队列配置服务器端加密（SSE）（控制台）。

[SQS.2] 应标记 SQS 队列

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SQS::Queue`

AWS Config 规则:`tagged-sqs-queue`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件可检查 Amazon SQS 队列是否具有特定键的标签，这些键在 `requiredTagKeys` 参数中进行定义。如果队列没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果队列未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳实践，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要使用 Amazon SQS 控制台向现有队列添加标签，请参阅《Amazon Simple Queue Service 开发人员指南》中的为 Amazon SQS 队列配置成本分配标签（控制台）。

[SQS.3] SQS 队列访问策略不应允许公开访问

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::SQS::Queue`

AWS Config 规则：sqs-queue-no-public-access

计划类型：已触发变更

参数：无

此控件检查 Amazon SQS 访问策略是否允许对 SQS 队列进行公开访问。如果 SQS 访问策略允许对队列进行公开访问，则该控件会失败。

Amazon SQS 访问策略可以允许公开访问 SQS 队列，这可能允许匿名用户或任何经过身份验证的 AWS IAM 身份访问该队列。SQS 访问策略通常通过在策略的`Principal` 元素中指定通配符（`*`）和/或不使用适当的条件限制对队列的访问来提供此访问。如果 SQS 访问策略允许公开访问，则第三方可能能够执行诸如从队列接收消息、向队列发送消息或修改队列的访问策略之类的任务。这可能会导致数据泄露、拒绝服务或威胁参与者向队列注入消息等事件。

> **Note**
>
> 此控件不会评估使用通配符或变量的策略条件。要生成 PASSED 调查发现，Amazon SQS 队列访问策略中的条件必须仅使用固定值，即不包含通配符或策略变量的值。有关策略变量的信息，请参阅《AWS Identity and Access Management 用户指南》中的变量和标签。

修复

有关配置 SQS 队列的 SQS 访问策略的信息，请参阅《Amazon Simple Queue Service 开发人员指南》中的将自定义策略与 Amazon SQS 访问策略语言配合使用。

适用于 Step Functions 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估 AWS Step Functions 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[StepFunctions.1] Step Functions 状态机应该开启日志功能

相关要求：PCI DSS v4.0.1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::StepFunctions::StateMachine`

AWS Config 规则：`step-functions-state-machine-logging-enabled`

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`logLevel`	最低日志记录级别	枚举	`ALL`, `ERROR`, `FATAL`	无默认值

此控件检查 AWS Step Functions 状态机是否已开启日志记录。如果状态机没有开启日志记录，则控制失败。如果您为 `logLevel` 参数提供自定义值，则仅当状态机开启了指定的日志记录级别时，控制才会通过。

监控可帮助您保持 Step Functions 的可靠性、可用性和性能。您应从中收集尽可能多的监控数据 AWS 服务 ，以便可以更轻松地调试多点故障。为你的 Step Function CloudWatch s 状态机定义日志配置后，你就可以在 Amazon Logs 中跟踪执行历史和结果。或者，您只能跟踪错误或致命事件。

修复

要为 Step Functions 状态机开启日志记录，请参阅 AWS Step Functions 开发人员指南中的配置日志记录。

[StepFunctions.2] 应标记 Step Functions 活动

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::StepFunctions::Activity`

AWS Config 规则:`tagged-stepfunctions-activity`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Step Functions 活动是否具有参数中定义的特定键的标签`requiredTagKeys`。如果活动没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果活动未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Step Functions 活动添加标签，请参阅《AWS Step Functions Developer Guide》中的 Tagging in Step Functions。

Systems Manager 的 Security Hub CSPM 控件

这些 AWS Security Hub CSPM 控制措施评估 AWS Systems Manager (SSM) 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

相关要求：PCI DSS v3.2.1/2.4、 NIST.800-53.r5 CA-9 (1)、5 (2)、 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(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-1 5 (8)、nist.800-53.r NIST.800-53.r5 SA-1 5 SI-2 (3) NIST.800-53.r5 SA-3

类别：识别 > 清单

严重性：中

评估的资源：`AWS::EC2::Instance`

所需的 AWS Config 录制资源：`AWS::EC2::Instance`，`AWS::SSM::ManagedInstanceInventory`

AWS Config 规则：ec2-instance-managed-by-systems-manager

计划类型：已触发变更

参数：无

此控件检查您账户中已停止和正在运行的 EC2 实例是否由管理 AWS Systems Manager。您可以使用 S AWS 服务 ystems Manager 来查看和控制您的 AWS 基础架构。

为了帮助您维护安全性和合规性，Systems Manager 会扫描已停止和正在运行的托管实例。托管实例是配置为与 Systems Manager 一起使用的机器。然后，Systems Manager 会报告其检测到的任何策略违规行为或采取纠正措施。Systems Manager 还帮助您配置和维护托管实例。要了解有关更多信息，请参阅 AWS Systems Manager 用户指南。

> **Note**
>
> 此控件会生成由管理的 AWS 弹性灾难恢复 复制服务器实例的 EC2 实例的`FAILED`调查结果 AWS。复制服务器实例是一个 EC2 实例，它由自动启动 AWS 弹性灾难恢复 ，用于支持源服务器的持续数据复制。 AWS 故意从这些实例中移除 Systems Manager (SSM) 代理，以保持隔离并帮助防止潜在的意外访问路径。

修复

有关使用管理 EC2 实例的信息 AWS Systems Manager，请参阅AWS Systems Manager 用户指南中的 Amazon EC2 主机管理。在 AWS Systems Manager 控制台的 “配置选项” 部分，您可以保留默认设置或根据需要对其进行更改，以满足您的首选配置。

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

相关要求：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）、NIST.800-53.r5 SI-2（4）、NIST.800-53.r5 SI-2（5）、NIST.800-171.r2 3.7.1、PCI DSS v3.2.1/6.2、PCI DSS v4.0.1/2.2.1、PCI DSS v4.0.1/6.3.3

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::SSM::PatchCompliance`

AWS Config 规则：ec2-managedinstance-patch-compliance-status-check

计划类型：已触发变更

参数：无

该控件在实例上安装补丁后检查 Systems Manager 补丁合规性的合规状态是否为 `COMPLIANT` 或 `NON_COMPLIANT`。如果合规性状态为 `NON_COMPLIANT`，则控制失败。该控件仅检查 Systems Manager Patch Manager 管理的实例。

根据您的组织的要求修补 EC2 实例可以减少 AWS 账户的攻击面。

修复

Systems Manager 建议使用补丁策略为您的托管实例配置补丁。您也可以使用 Systems Manager 文档（如以下过程所述）来修补实例。

修复不合规的补丁

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 对于节点管理，选择运行命令，然后选择运行命令。
3. 选择 AWS- 的选项RunPatchBaseline。
4. 将操作改为安装。
5. 选择手动选择实例，然后选择不合规的实例。
6. 选择运行。
7. 命令完成后，要监控已修补实例的新合规性状态，请在导航窗格中选择合规性。

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

相关要求： 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 v3.2.1/2.4，PCI DSS v4.0.1/2.1，PCI DSS v4.0.1/6.3.3

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::SSM::AssociationCompliance`

AWS Config 规则：ec2-managedinstance-association-compliance-status-check

计划类型：已触发变更

参数：无

此控件检查 AWS Systems Manager 关联合规性的状态是`COMPLIANT`还是关联在实例上运行`NON_COMPLIANT`之后。如果关联合规性状态为 `NON_COMPLIANT`，则控制失败。

状态管理器关联是分配给托管实例的配置。该配置定义要在实例上保持的状态。例如，关联可以指定必须在实例上安装并运行防病毒软件，或者必须关闭某些端口。

创建一个或多个状态管理器关联后，您可以立即获得合规状态信息。您可以在控制台中查看合规性状态，也可以在响应 AWS CLI 命令或相应的 Systems Manager API 操作时查看合规性状态。对于关联，配置合规性显示合规性状态（`Compliant` 或 `Non-compliant`）。它还显示分配给关联的严重性级别，例如 `Critical` 或 `Medium`。

要了解有关 State Manager 关联合规性的更多信息，请参阅 AWS Systems Manager 用户指南中的关于 State Manager 关联合规性。

修复

失败的关联可能与不同的事物相关，包括目标和 Systems Manager 文档名称。要修复此问题，您必须首先通过查看关联历史记录来识别和调查关联。有关查看关联历史记录的说明，请参阅 AWS Systems Manager 用户指南中的查看关联历史记录。

调查完成后，您可以编辑关联以更正已结果的问题。您可以编辑关联以指定新名称、计划、严重级别或目标。编辑关联后， AWS Systems Manager 创建新版本。有关编辑关联的说明，请参阅 AWS Systems Manager 用户指南中的编辑和创建关联的新版本。

[SSM.4] SSM 文档不应公开

相关要求： 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)

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::SSM::Document`

AWS Config 规则：ssm-document-not-public

计划类型：定期

参数：无

此控件检查账户拥有的 AWS Systems Manager 文档是否公开。如果所有者为 `Self` 的 Systems Manager 文档是公开的，则此控件会失败。

公开的 Systems Manager 文档可能会允许意外访问您的文档。公开的 Systems Manager 文档可能会公开有关账户、资源和内部流程的有价值的信息。

除非使用案例要求公开共享，否则我们建议您阻止对所有者为 Self 的 Systems Manager 文档进行公开共享设置。

修复

有关配置 Systems Manager 文档共享的信息，请参阅《AWS Systems Manager 用户指南》中的共享 SSM 文档。

[SSM.5] 应标记 SSM 文档

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::SSM::Document

AWS Config 规则：ssm-document-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签键区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Systems Manager 文档是否具有requiredKeyTags参数指定的标签密钥。如果文档没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件会失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果文档没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。该控件不评估 Amazon 拥有的 Systems Manager 文档。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使

用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

要向 AWS Systems Manager 文档添加标签，您可以使用 AWS Systems Manager API 的AddTagsToResource操作，或者，如果您使用的是 AWS CLI，则运行add-tags-to-resource命令。您还可以使用 AWS Systems Manager 控制台。

[SSM.6] SSM 自动化应启用日志记录 CloudWatch

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：ssm-automation-logging-enabled

计划类型：定期

参数：无

此控件检查是否已启用 Amazon CloudWatch 日志功能 AWS Systems Manager (SSM) 自动化。如果未为 SSM 自动化启用 CloudWatch 日志记录，则控件将失败。

SSM Automation 是一 AWS Systems Manager 款工具，可帮助您构建自动化解决方案，以便使用预定义或自定义运行手册大规模部署、配置和管理 AWS 资源。为了满足贵组织的运营或安全要求，您可能需要提供其运行的脚本的记录。您可以将 SSM Automation 配置为将运行手册中`aws:executeScript`操作的输出发送到您指定的 Amazon Log CloudWatch s 日志组。使用 CloudWatch 日志，您可以监控、存储和访问各种日志文件 AWS 服务。

修复

有关启用 SSM 自动化的 CloudWatch 日志记录的信息，请参阅《AWS Systems Manager 用户指南》中的使用 CloudWatch 日志记录自动化操作输出。

[SSM.7] SSM 文档应启用“阻止公开共享”设置

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：ssm-automation-block-public-sharing

计划类型：定期

参数：无

此控件检查是否为 AWS Systems Manager 文档启用了阻止公开共享设置。如果为 Systems Manager 文档禁用了阻止公开共享设置，则此控件会失败。

AWS Systems Manager (SSM) 文档的屏蔽公开共享设置是账户级别的设置。启用此设置可防止对 SSM 文档进行不需要的访问。启用此设置后，您的更改不会影响您当前与公众共享的任何 SSM 文档。除非您的使用案例要求与公众共享 SSM 文档，否则我们建议您启用阻止公开共享设置。每种设置可能有所不同 AWS 区域。

修复

有关为 AWS Systems Manager （SSM）文档启用阻止公开共享设置的信息，请参阅《AWS Systems Manager 用户指南》中的阻止 SSM 文档的公开共享。

Security Hub CSPM 控件适用于 AWS Transfer Family

这些 AWS Security Hub CSPM 控制措施评估 AWS Transfer Family 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Transfer.1] 应标记 AWS Transfer Family 工作流程

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Transfer::Workflow`

AWS Config 规则:`tagged-transfer-workflow`（自定义 Security Hub CSPM 规则）

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredTagKeys`	被评估资源必须包含的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	`No default value`

此控件检查 AWS Transfer Family 工作流程是否具有参数中定义的特定键的标签`requiredTagKeys`。如果工作流程没有任何标签键或未在 `requiredTagKeys` 参数中指定所有键，则此控件将失败。如果未提供 `requiredTagKeys` 参数，则此控件仅检查是否存在标签键，如果工作流程未使用任何键进行标记，则此控件将失败。自动应用并以 `aws:` 为开头的系统标签会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，以按用途、所有者、环境或其他标准对资源进行分类。标签可帮助您识别、组织、搜索和筛选资源。使用标签进行标记还可以帮助您跟踪负责操作和通知的资源所有者。使用标签进行标记时，可以将基于属性的访问权限控制（ABAC）作为授权策略实施，该策略根据标签来定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为 IAM 主体创建单个 ABAC 策略或者一组单独的策略。您可以将这些 ABAC 策略设计为允许在主体的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 请勿在标签中添加个人身份信息（PII）或者其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Transfer Family 工作流程（控制台）添加标签，请执行以下操作

1. 打开控制 AWS Transfer Family 台。
2. 在导航窗格中，选择工作流。然后，选择要标记的工作流程。
3. 选择管理标签，然后添加标签。

[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

相关要求： 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

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::Transfer::Server`

AWS Config 规则：transfer-family-server-no-ftp

计划类型：定期

参数：无

此控件检查 AWS Transfer Family 服务器是否使用 FTP 以外的协议进行端点连接。如果服务器使用 FTP 协议让客户端连接到服务器的端点，则此控件失败。

FTP（文件传输协议）通过未加密的通道建立端点连接，因此通过这些通道发送的数据容易被拦截。使用 SFTP（SSH 文件传输协议）、FTPS（安全文件传输协议）或AS2 （适用性声明 2）通过加密传输中的数据来提供额外的安全层，并可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。

修复

要修改 Transfer Family 服务器的协议，请参阅《AWS Transfer Family User Guide》中的 Edit the file transfer protocols。

[Transfer.3] Transfer Family 连接器应启用日志记录

相关要求： NIST.800-53.r5 AC-2(12)、(4)、(26)、 NIST.800-53.r5 AC-2 (9)、(9)、 NIST.800-53.r5 AC-4 (9)、 NIST.800-53.r5 AC-6 nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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 SI-4、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Transfer::Connector`

AWS Config 规则：transfer-connector-logging-enabled

计划类型：已触发变更

参数：无

此控件检查 AWS Transfer Family 连接器是否启用了 Amazon CloudWatch 日志记录。如果连接器未启用 CloudWatch 日志记录，则控件将失败。

Amazon CloudWatch 是一项监控和可观察性服务，可提供对您的 AWS 资源（包括 AWS Transfer Family 资源）的可视性。对于 Transfer Family， CloudWatch提供工作流程进度和结果的合并审计和日志记录。这包括 Transfer Family 为工作流定义的多个指标。您可以将 Transfer Family 配置为在中自动记录连接器事件 CloudWatch。为此，您需要为连接器指定一个日志记录角色。对于日志记录角色，您可以创建一个 IAM 角色和一个基于资源的 IAM 策略（定义该角色的权限）。

修复

有关为 Transfer Family 连接器启用 CloudWatch CloudWatch 日志记录的信息，请参阅AWS Transfer Family 用户指南中的亚马逊 AWS Transfer Family 服务器日志记录。

[Transfer.4] 应标记 Transfer Family 协议

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Transfer::Agreement`

AWS Config 规则：transfer-agreement-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Transfer Family 协议是否具有`requiredKeyTags`参数指定的标签密钥。如果协议没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件会失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果协议没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 AWS Transfer Family 协议添加标签的信息，请参阅《标记资源和标签编辑器用户指南》中的 AWS 资源标记方法。

[Transfer.5] 应标记 Transfer Family 证书

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Transfer::Certificate`

AWS Config 规则：transfer-certificate-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Transfer Family 证书是否具有requiredKeyTags参数指定的标签密钥。如果证书没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件会失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果证书没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关为 AWS Transfer Family 证书添加标签的信息，请参阅《标记资源和标签编辑器用户指南》中的 AWS 资源标记方法。

[Transfer.6] 应标记 Transfer Family 连接器

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Transfer::Connector

AWS Config 规则：transfer-connector-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
`requiredKeyTags`	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Transfer Family 连接器是否具有`requiredKeyTags`参数指定的标签密钥。如果连接器没有任何标签键，或者缺少 `requiredKeyTags` 参数指定的所有键，则该控件会失败。如果没有为 `requiredKeyTags` 参数指定任何值，则该控件仅检查是否存在标签键，如果连接器没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 `aws:` 前缀。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 AWS Transfer Family 连接器添加标签的信息，请参阅《标记资源和标签编辑器用户指南》中的 AWS 资源标记方法。

[Transfer.7] 应标记 Transfer Family 配置文件

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Transfer::Profile

AWS Config 规则：transfer-profile-tagged

计划类型：已触发变更

参数：

参数	说明	Type	允许的自定义值	Security Hub CSPM 默认值
requiredKeyTags	必须分配给所评估资源的非系统标签键列表。标签密钥区分大小写。	StringList（最多 6 件商品）	1-6 个符合 AWS 要求的标签键。	无默认值

此控件检查 AWS Transfer Family 配置文件是否具有requiredKeyTags参数指定的标签密钥。如果配置文件没有任何标签键，或者缺少 requiredKeyTags 参数指定的所有键，则该控件会失败。如果没有为 requiredKeyTags 参数指定任何值，则该控件仅检查是否存在标签键，如果配置文件没有任何标签键，则该控件会失败。该控件会忽略系统标签，这些标签会自动应用，并且带有 aws: 前缀。此控件评估本地配置文件和合作伙伴配置文件。

标签是您创建并分配给 AWS 资源的标签。每个标签都包含一个必需的标签键和一个可选的标签值。您可以使用标签，按用途、所有者、环境或其他标准对资源进行分类。它们可帮助您识别、组织、搜索和筛选资源。它们还可以帮助您跟踪资源所有者的操作和通知。您还可以使用标签来实施基于属性的访问权限控制（ABAC）作为授权策略。有关 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权根据属性定义权限。有关标签的更多信息，请参阅《标签 AWS 资源和标签编辑器用户指南》。

> **Note**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。许多人都可以访问标签 AWS 服务。它们不适合用于私有或敏感数据。

修复

有关向 AWS Transfer Family 配置文件添加标签的信息，请参阅《标记资源和标签编辑器用户指南》中的 AWS 资源标记方法。

Security Hub CSPM 控件适用于 AWS WAF

这些 AWS Security Hub CSPM 控制措施评估 AWS WAF 服务和资源。这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录

相关要求： NIST.800-53.r5 AC-4(26)、、(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 SI-7 NIST.800-53.r5 SC-7 (8)、PCI DSS v4.0.1/10.4.2

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::WAF::WebACL`

AWS Config 规则：`waf-classic-logging-enabled`

计划类型：定期

参数：无

此控件检查是否为 AWS WAF 全局 Web ACL 启用了日志记录。如果未为 Web ACL 启用日志记录，则此控制失败。

日志记录是维护 AWS WAF 全球可靠性、可用性和性能的重要组成部分。这是许多组织中的业务和合规性要求，并允许您对应用程序行为进行故障排除。它还提供有关附加到 AWS WAF的 Web ACL 所分析的流量的详细信息。

修复

要启用 AWS WAF Web ACL 的日志记录，请参阅AWS WAF 开发人员指南中的记录 Web ACL 流量信息。

[WAF.2] AWS WAF 经典区域规则应至少有一个条件

相关要求： 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)

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAFRegional::Rule

AWS Config 规则：waf-regional-rule-not-empty

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 区域规则是否至少具有一个条件。如果规则中不存在任何条件，则控制失败。

WAF 区域规则可以包含多个条件。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何条件的情况下，流量未经检查就通过。没有任何条件但带有建议允许、阻止或计数的名称或标签的 WAF 区域规则可能会导致错误地假设其中一项操作正在发生。

修复

要向空规则添加条件，请参阅 AWS WAF 开发人员指南中的在规则中添加和删除条件。

[WAF.3] AWS WAF 经典区域规则组应至少有一条规则

相关要求： 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)

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAFRegional::RuleGroup

AWS Config 规则：waf-regional-rulegroup-not-empty

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 区域规则组是否至少有一条规则。如果规则组中不存在任何规则，则控制失败。

一个 WAF 区域规则组可以包含多个规则。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何规则的情况下，流量未经检查就通过。没有规则但具有建议允许、阻止或计数的名称或标签的 WAF 区域规则组可能会导致错误地假设其中一项操作正在发生。

修复

要向空规则组添加规则和规则条件，请参阅《AWS WAF 开发者指南》中的在 AWS WAF 经典规则组中添加和删除规则以及在规则中添加和删除条件。

[WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAFRegional::WebACL`

AWS Config 规则：`waf-regional-webacl-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF Classic Regional Web ACL 是否包含任何 WAF 规则或 WAF 规则组。如果 Web ACL 不包含任何 WAF 规则或规则组，则此控制失败。

WAF Regional Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，则根据默认操作，Web 流量可以在不被 WAF 检测到或处理的情况下通过。

修复

要向空的 AWS WAF 经典区域 Web ACL 添加规则或规则组，请参阅AWS WAF 开发人员指南中的编辑 Web ACL。

[WAF.6] AWS WAF 经典全局规则应至少有一个条件

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAF::Rule`

AWS Config 规则：`waf-global-rule-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 全局规则是否包含任何条件。如果规则中不存在任何条件，则控制失败。

一个 WAF 全局规则可以包含多个条件。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何条件的情况下，流量未经检查就通过。不带条件但带有建议允许、阻止或计数的名称或标签的 WAF 全局规则可能会导致错误地假设其中一项操作正在发生。

修复

有关创建规则和添加条件的说明，请参阅 AWS WAF 开发人员指南中的创建规则和添加条件。

[WAF.7] AWS WAF 经典全局规则组应至少有一条规则

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAF::RuleGroup`

AWS Config 规则：`waf-global-rulegroup-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 全局规则组是否至少有一条规则。如果规则组中不存在任何规则，则控制失败。

一个 WAF 全局规则组可以包含多个规则。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何规则的情况下，流量未经检查就通过。没有规则但具有建议允许、阻止或计数的名称或标签的 WAF 全局规则组可能会导致错误地假设其中一项操作正在发生。

修复

有关向规则组添加规则的说明，请参阅《AWS WAF 开发人员指南》中的创建 AWS WAF 经典规则组。

[WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

相关要求： 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)

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAF::WebACL`

AWS Config 规则：`waf-global-webacl-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 全局 Web ACL 是否包含至少一个 WAF 规则或 WAF 规则组。如果 Web ACL 不包含任何 WAF 规则或规则组，则控制失败。

WAF 全局 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，则根据默认操作，Web 流量可以在不被 WAF 检测到或处理的情况下通过。

修复

要向空的 AWS WAF 全局 Web ACL 添加规则或规则组，请参阅AWS WAF 开发人员指南中的编辑 Web ACL。对于 “筛选”，选择 “全局” (CloudFront)。

[WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组

相关要求： NIST.800-53.r5 CA-9(1)、nist.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAFv2::WebACL`

AWS Config 规则：`wafv2-webacl-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF V2 Web 访问控制列表 (Web ACL) 是否至少包含一个规则或规则组。如果 Web ACL 不包含任何规则或规则组，则控制失败。

Web ACL 可让您对受保护资源响应的所有 HTTP（S）Web 请求进行精细控制。Web ACL 应包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，则 AWS WAF 根据默认操作，Web 流量可以在不被检测或处理的情况下通过。

修复

要向空的 WAFV2 Web ACL 添加规则或规则组，请参阅AWS WAF 开发人员指南中的编辑 Web ACL。

[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

相关要求： NIST.800-53.r5 AC-4(26)、(10)、 NIST.800-53.r5 SC-7 (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 SI-7 NIST.800-53.r5 SC-7 (8)、PCI DSS v4.0.1/10.4.2

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::WAFv2::WebACL`

AWS Config 规则：**`wafv2-logging-enabled`**

计划类型：定期

参数：无

此控件检查 AWS WAF V2 Web 访问控制列表 (Web ACL) 是否已激活日志记录。如果停用 Web ACL 的日志记录，则此控制失败。

> **Note**
>
> 此控件不检查是否已通过 Amazon Security Lake 为账户启用 AWS WAF 网页 ACL 日志记录。

日志记录可维护的可靠性、可用性和性能 AWS WAF。此外，在许多组织中，日志记录是一项业务和合规要求。通过记录由 Web ACL 分析的流量，您可以对应用程序行为进行故障排除。

修复

要激活 AWS WAF Web ACL 的日志记录，请参阅《AWS WAF 开发人员指南》中的管理 Web ACL 的日志记录。

[WAF.12] AWS WAF 规则应启用指标 CloudWatch

相关要求： NIST.800-53.r5 AC-4(26)、(10)、(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 SI-7 NIST.800-53.r5 SC-7 (8)、 NIST.800-53.r5 SC-7 nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.6、nist.800-171.r2 3.14.7

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::WAFv2::RuleGroup`

AWS Config 规则：**`wafv2-rulegroup-logging-enabled`**

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 规则或规则组是否启用了 Amazon CloudWatch 指标。如果规则或规则组未启用 CloudWatch 指标，则控件将失败。

在 AWS WAF 规则和规则组上配置 CloudWatch 指标可提供对流量的可见性。您可以看到哪些 ACL 规则被触发，哪些请求被接受和阻止。这种可见性可以帮助您识别关联资源上的恶意活动。

修复

要在 AWS WAF 规则组上启用 CloudWatch 指标，请调用 UpdateRuleGroupAPI。要在 AWS WAF 规则上启用 CloudWatch 指标，请调用 UpdateWebACL API。将 `CloudWatchMetricsEnabled` 字段设置为 `true`。当您使用 AWS WAF 控制台创建规则或规则组时， CloudWatch 指标会自动启用。

Security Hub CSPM 控件适用于 WorkSpaces

这些 AWS Security Hub CSPM 控制措施用于评估 Amazon WorkSpaces 服务和资源。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[WorkSpaces.1] WorkSpaces 用户卷应在静态时加密

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：AWS::WorkSpaces::Workspace

AWS Config 规则：workspaces-user-volume-encryption-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon WorkSpaces WorkSpace 中的用户卷是否处于静态加密状态。如果未对 WorkSpace 用户卷进行静态加密，则控制失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要加密 WorkSpaces 用户卷，请参阅《Amazon WorkSpaces 管理指南》 WorkSpace中的加密。

[WorkSpaces.2] WorkSpaces 根卷应在静态时加密

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：AWS::WorkSpaces::Workspace

AWS Config 规则：workspaces-root-volume-encryption-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon WorkSpaces WorkSpace 中的根卷是否处于静态加密状态。如果 WorkSpace 根卷未在静态状态下加密，则控制失败。

静态数据是指存储在持久、非易失性存储介质中的数据，无论存储时长如何。对静态数据进行加密可帮助您保护数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要加密 WorkSpaces 根卷，请参阅《Amazon WorkSpaces 管理指南》 WorkSpace中的加密。

在 Security Hub CSPM 中配置控件所需的权限

要查看有关安全控制的信息以及启用和禁用标准中的安全控制，用于访问 Security Hub CSPM 的 AWS Identity and Access Management (IAM) 角色需要调用 Sec AWS urity Hub CSPM API 的以下操作的权限。

要获得必要的权限，您可以使用 Security Hub CSPM 托管策略。或者，您可以更新自定义 IAM policy 以包含这些操作的权限。

- BatchGetSecurityControls— 返回有关当前账户和的一批安全控制措施的信息 AWS 区域。
- ListSecurityControlDefinitions——返回有关适用于指定标准的安全控件的信息。
- ListStandardsControlAssociations——确定账户中每个启用的标准中当前是启用还是禁用了安全控件。
- BatchGetStandardsControlAssociations——对于一批安全控件，标识每个控件当前是在指定标准中启用还是禁用。
- BatchUpdateStandardsControlAssociations——用于在包含该控件的标准中启用安全控件，或禁用标准中的控件。这会批量替代现有 `UpdateStandardsControl` 操作。
- BatchUpdateStandardsControlAssociations – 用于在包含安全控件的标准中启用或禁用一批控件。这会批量替代现有 `UpdateStandardsControl` 操作。
- UpdateStandardsControl – 用于在包含安全控件的标准中启用或禁用单个安全控件
- DescribeStandardsControl – 返回有关指定的安全控件的详细信息。

除上述内容外 APIs，您还应添加调用`BatchGetControlEvaluations`您的 IAM 角色的权限。要在 Security Hub CSPM 控制台上查看控件的启用和合规性状态、控件的调查发现计数以及控件的总体安全评分，需要此权限。由于只有控制台调用`BatchGetControlEvaluations`，因此此权限并不直接对应于公开记录的 Security Hub CSPM APIs 或 AWS CLI 命令。

在 Security Hub CSPM 中启用控件

在 Sec AWS urity Hub CSPM 中，控制是安全标准中的一种保护措施，可帮助组织保护其信息的机密性、完整性和可用性。每个 Security Hub CSPM 控件都与特定的 AWS 资源相关。当您启用某个控件时，Security Hub CSPM 会开始对该控件运行安全检查并生成控件的调查发现。计算安全分数时，Security Hub CSPM 还会考虑所有已启用的控件。

您可以选择针对所有适用安全标准启用控件。或者，您也可以在不同的标准中以不同的方式配置启用状态。我们建议使用前一个选项，即控件的启用状态在所有已启用的标准中保持一致。有关针对所有适用

标准启用控件的说明，请参阅针对各种标准启用控件。有关在特定标准中启用控件的说明，请参阅启用特定标准中的控件。

如果您启用了跨区域聚合并登录了某个聚合区域，Security Hub CSPM 控制台将显示在至少一个关联区域中可用的控件。如果某个控件在关联区域中可用，但在聚合区域中不可用，则无法在聚合区域启用或禁用该控件。

您可以使用 Security Hub CSPM 控制台、Security Hub CSPM API 或在每个区域启用和禁用控件。AWS CLI

启用和禁用控件的说明会因您是否使用中心配置而异。本主题介绍其中的区别。集成 Security Hub CSPM 和的用户可以使用中央配置。 AWS Organizations我们建议使用中心配置来简化在多账户、多区域环境中启用和禁用控件的过程。如果您使用中心配置，则可以通过使用配置策略启用针对多个账户和区域的控件。如果您不使用中心配置，则必须在每个账户和区域中分别启用控件。

针对各种标准启用控件

我们建议在该控件适用的所有标准中启用 Sec AWS urity Hub CSPM 控件。如果开启整合的控件调查发现，那么即使一项控件属于多个标准，您也会收到每项控件检查的调查发现。

在多账户、多区域环境中的跨标准启用

要在多个 AWS 账户 和之间启用安全控制 AWS 区域，您必须登录委派的 Security Hub CSPM 管理员帐户并使用中央配置。

使用中心配置时，委派管理员可以创建 Security Hub CSPM 配置策略，这些策略可以跨已启用标准启用指定控件。然后，您可以将配置策略与特定账户和组织单位 (OUs) 或根相关联。配置策略在您的主区域（也称为聚合区域）和所有关联区域中生效。

配置策略可自定义。例如，您可以选择启用一个 OU 中的所有控件，也可以选择在另一个 OU 中仅启用 Amazon Elastic Compute Cloud（EC2）控件。粒度级别取决于您的组织中安全覆盖范围的预期目标。有关创建配置策略（启用不同标准中的指定控件）的说明，请参阅创建和关联配置策略。

> **Note**
>
> 授权的管理员可以创建配置策略来管理除服务管理标准之外的所有标准中的控件: AWS Control Tower。应在 AWS Control Tower 服务中配置该标准的控件。

如果您希望某些账户配置自己的控件而不是委派管理员来配置，则委派管理员可以将这些账户指定为自行管理。自行管理账户必须在每个区域中单独配置控件。

单个账户和区域中的跨标准启用

如果您不使用中心配置或是自行管理账户，则无法使用配置策略在多个账户和区域中集中启用控件。但是，您可以使用以下步骤在单个账户和区域中启用控件。

Security Hub CSPM console

要在一个账户和区域中启用不同标准中的控件

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 从导航窗格中选择控件。
3. 选择已禁用选项卡。
4. 选择控件旁边的选项。
5. 选择启用控制（对于已启用的控件，此选项不会出现）。
6. 在您要在其中启用控件的每个区域中重复这些操作。

Security Hub CSPM API

要在一个账户和区域中启用不同标准中的控件

1. 调用 ListStandardsControlAssociations API。提供安全控件 ID。

   请求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. 调用 BatchUpdateStandardsControlAssociations API。提供所有未启用控件的标准的 Amazon 资源名称（ARN）。要获得标准 ARNs，请运行DescribeStandards。
3. 将 AssociationStatus 参数设置为等于 ENABLED。如果您对已启用的控件执行以下步骤，则该 API 将返回 HTTP 状态码 200 响应。

   请求示例：

   ```
   {
       "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. 在您要在其中启用控件的每个区域中重复这些操作。

AWS CLI

要在一个账户和区域中启用不同标准中的控件

1. 运行 list-standards-control-associations 命令。提供安全控件 ID。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. 运行 batch-update-standards-control-associations 命令。提供所有未启用控件的标准的 Amazon 资源名称（ARN）。要获得标准 ARNs，请运行`describe-standards`命令。
3. 将 `AssociationStatus` 参数设置为等于 `ENABLED`。如果您对已启用的控件执行这些步骤，该命令将返回 HTTP 状态代码 200 响应。

```
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. 在您要在其中启用控件的每个区域中重复这些操作。

启用特定标准中的控件

在 Sec AWS urity Hub CSPM 中启用标准时，适用于该标准的所有控件都会自动启用该标准中的所有控件（服务管理标准除外）。然后，您可以禁用并重新启用标准中的特定控件。但是，我们建议您在所有已启用的标准中调整控件的启用状态。有关在所有标准中启用控件的说明，请参阅 针对各种标准启用控件。

标准的详细信息页面包含该标准的适用控件列表，以及有关该标准当前启用和禁用哪些控件的信息。

在标准详细信息页面上，您还可以在特定标准中启用控件。您必须在每个 AWS 账户 和中分别启用特定标准中的控件 AWS 区域。在特定标准中启用控件时，它只会影响当前账户和区域。

要启用标准中的控件，您必须首先启用至少一个该控件适用的标准。有关启用标准的说明，请参阅启用安全标准。当您在一个或多个标准中启用某个控件时，Security Hub CSPM 会开始生成该控件的调查发现。Security Hub CSPM 还在总体安全分数和标准安全分数的计算中包括控件状态。即使您在多个标准中启用了控件，但如果您开启整合的控件调查发现，您也将收到一个各类标准的安全检查调查发现。有关更多信息，请参阅 Consolidated control findings。

要启用标准中的控件，该控件必须在您当前的区域中可用。有关更多信息，请参阅根据区域的控件可用性。

请按照以下步骤启用特定标准中的 Security Hub CSPM 控件。除了以下步骤之外，您还可以使用 `UpdateStandardsControl` API 操作来启用特定标准中的控件。有关在所有标准中启用控件的说明，请参阅 单个账户和区域中的跨标准启用。

Security Hub CSPM console

要启用特定标准中的控件

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 从导航窗格中选择安全标准。
3. 对于相关标准，选择查看结果。
4. 选择控件。
5. 选择启用控制（对于已启用的控件，此选项不会出现）。选择启用进行确认。

Security Hub CSPM API

要启用特定标准中的控件

1. 运行 `ListSecurityControlDefinitions` 并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 `DescribeStandards`。此 API 返回与标准无关的安全控制 IDs，而不是特定于标准的控制。 IDs

   请求示例：

   ```
   {
   ```

```
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0"
}
```

2. 运行 ListStandardsControlAssociations，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

   请求示例：

```
{
    "SecurityControlId": "IAM.1"
}
```

3. 运行 BatchUpdateStandardsControlAssociations。提供您想要在其中启用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 ENABLED。

   请求示例：

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

要启用特定标准中的控件

1. 运行 list-security-control-definitions 命令并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 describe-standards。此命令返回与标准无关的安全控制 IDs，而不是特定于标准的控制。 IDs

```
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. 运行 list-standards-control-associations 命令，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. 运行 batch-update-standards-control-associations 命令。提供您想要在其中启用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 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"}]'
```

自动启用已启用标准中的新控件

AWS Security Hub CSPM 定期发布新的控件并将其添加到一个或多个标准中。您可以选择是否在启用的标准中自动启用新控件。

我们建议使用 Security Hub CSPM 中心配置来自动启用新的安全控件。您可以创建配置策略，其中包括不同标准中要禁用的控件列表。默认情况下，所有其他控件（包括新发布的控件）均处于启用状态。或者，您可以创建策略，其中包含不同标准中要启用的控件的列表。默认情况下，所有其他控件（包括新发布的控件）均处于禁用状态。有关更多信息，请参阅 了解 Security Hub CSPM 中的中心配置。

当新控件添加到您尚未启用的标准时，Security Hub CSPM 不会启用这些控件。

以下说明仅在您不使用中心配置时适用。

选择首选访问方法，然后按照以下步骤自动启用启用的标准中的新控件。

> **Note**
>
> 按照以下说明自动启用新控件后，您可以在发布后立即在控制台中以编程方式与控件进行交互。但是，自动启用的控件的临时默认状态为已禁用。Security Hub CSPM 可能需要几天时间来处理控件发布并将控件在您的账户中指定为已启用。在处理期间，您可以手动启用或禁用某个控件，无论您是否开启了自动控件启用，Security Hub CSPM 都将保持该指定。

Security Hub CSPM console

要自动启用新控件

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置，然后选择常规选项卡。
3. 在控件下，选择编辑。
4. 在已启用的标准中开启自动启用新控件。
5. 选择保存。

Security Hub CSPM API

要自动启用新控件

1. 运行 UpdateSecurityHubConfiguration。
2. 要自动为启用的标准启用新控件，将 AutoEnableControls 设置为 true。如果您不想自动启用新控件，请设置 AutoEnableControls 为 false。

AWS CLI

要自动启用新控件

1. 运行 update-security-hub-configuration 命令。
2. 要自动为启用的标准启用新控件，请指定 --auto-enable-controls。如果您不想自动启用新控件，请指定 --no-auto-enable-controls。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

命令示例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

如果您没有自动启用新控件，则必须手动启用它们。有关说明，请参阅在 Security Hub CSPM 中启用控件。

在 Security Hub CSPM 中禁用控件

为了减少调查发现噪音，禁用与环境无关的控件可能会很有用。在 S AWS ecurity Hub CSPM 中，您可以禁用所有安全标准或仅针对特定标准的控件。

如果跨所有标准禁用控件，则会发生以下情况：

- 不再执行控件的安全检查。
- 不会为该控件生成任何其他调查发现。
- 控件的现有调查发现不再更新。
- 控件的现有调查发现通常在 3-5 天内尽力自动存档。
- Security Hub CSPM 会删除它为控件创建的所有相关 AWS Config 规则。

如果您仅针对特定标准禁用某个控件，Security Hub CSPM 会停止针对该控件或仅针对这些标准运行安全检查。这也会从每个标准的安全分数计算中移除该控件。如果在其他标准中启用了该控件，Security Hub CSPM 会保留关联的 AWS Config 规则（如果适用），并继续对该控件或其他标准运行安全检查。Security Hub CSPM 在计算其他每个标准的安全分数时会包括该控件，这会影响您的摘要安全分数。

如果禁用某标准，则适用于该标准的所有控件都会在该标准中自动禁用。但是，在其他标准中，这些控件可能会继续启用。当您禁用某个标准时，Security Hub CSPM 不会跟踪对该标准禁用哪些控件。因此，如果您稍后重新启用同一标准，则适用于该标准的所有控件都会自动启用。有关禁用标准的信息，请参阅 禁用标准。

禁用控件并非永久性操作。假设您禁用一个控件，然后启用一个包含该控件的标准。然后，为该标准启用该控件。当您在 Security Hub CSPM 中启用某个标准时，适用于该标准的所有控件都会自动启用。有关启用标准的信息，请参阅 启用标准。

主题

- 跨标准禁用控件
- 禁用特定标准中的控件
- 建议在 Security Hub CSPM 中禁用的控件

跨标准禁用控件

我们建议禁用跨标准的 S AWS ecurity Hub CSPM 控件，以保持整个组织的一致性。如果仅在特定标准中禁用了某控件，而其他标准中仍启用该控件，您可以继续接收该控件的调查发现。

多个账户和区域中的跨标准禁用

要在多个 AWS 账户 和之间禁用安全控制 AWS 区域，必须使用集中配置。

使用中心配置时，委派管理员可以创建 Security Hub CSPM 配置策略，以禁用已启用标准的指定控件。然后，您可以将配置策略与特定账户或根账户相关联。 OUs配置策略在您的主区域（也称为聚合区域）和所有关联区域中生效。

配置策略可自定义。例如，您可以选择禁用一个 OU 中的所有 AWS CloudTrail 控件，也可以选择禁用另一个 OU 中的所有 IAM 控件。粒度级别取决于您的组织中安全覆盖范围的预期目标。有关创建用于禁用不同标准中指定控件的配置策略的说明，请参阅创建和关联配置策略。

> **Note**
>
> 授权的管理员可以创建配置策略来管理除服务管理标准之外的所有标准中的控件: AWS Control Tower。应在 AWS Control Tower 服务中配置该标准的控件。

如果您希望某些账户配置自己的控件而不是委派管理员来配置，则委派管理员可以将这些账户指定为自行管理。自行管理账户必须在每个区域中单独配置控件。

单个账户和区域中的跨标准禁用

如果您未使用中心配置，或是自行管理账户，则无法使用配置策略在多个账户和区域中集中禁用控件。但是，您可以在单个账户和区域中禁用控件。

Security Hub CSPM console

要在一个账户和区域中禁用不同标准中的控件

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 从导航窗格中选择控件。
3. 选择控件旁边的选项。
4. 选择禁用控件。对于已禁用的控件，此选项不会出现。
5. 选择禁用控件的原因，然后选择禁用进行确认。
6. 在您要在其中禁用控件的每个区域中重复这些操作。

Security Hub CSPM API

要在一个账户和区域中禁用不同标准中的控件

1. 调用 ListStandardsControlAssociations API。提供安全控件 ID。

   请求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. 调用 BatchUpdateStandardsControlAssociations API。提供启用该控件的任何标准的 ARN。要获得标准 ARNs，请运行DescribeStandards。

3. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已禁用的控件执行以下步骤，API 将返回 HTTP 状态代码 200 响应。

   请求示例：

   ```
   {
       "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. 在您要在其中禁用控件的每个区域中重复这些操作。

AWS CLI

要在一个账户和区域中禁用不同标准中的控件

1. 运行 list-standards-control-associations 命令。提供安全控件 ID。

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

2. 运行 batch-update-standards-control-associations 命令。提供启用该控件的任何标准的 ARN。要获得标准 ARNs，请运行describe-standards命令。
3. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已禁用的控件执行以下步骤，该命令将返回 HTTP 状态代码 200 响应。

```
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. 在您要在其中禁用控件的每个区域中重复这些操作。

禁用特定标准中的控件

您可以仅在特定安全标准中禁用某个控件，而不是在所有标准中禁用。如果该控件适用于其他已启用的标准，则 Sec AWS urity Hub CSPM 将继续对该控件运行安全检查，并且您会继续收到该控件的调查结果。

我们建议在控件所适用的所有已启用标准中统一控件的启用状态。有关如何禁用适用于所有标准的控件的信息，请参阅跨标准禁用控件。

在标准详细信息页面上，您还可以在特定标准中禁用控件。您必须在每个 AWS 账户 和中分别禁用特定标准中的控件 AWS 区域。当您在特定标准中禁用某个控件时，它只会影响当前账户和区域。

选择您喜欢的方法，然后按照这些步骤在一个或多个特定标准中禁用控件。

Security Hub CSPM console

要禁用特定标准中的控件

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 从导航窗格中选择安全标准。对于相关标准，选择查看结果。
3. 选择控件。

4. 选择禁用控件。对于已禁用的控件，此选项不会出现。
5. 提供禁用控件的原因，然后选择禁用进行确认。

Security Hub CSPM API

要禁用特定标准中的控件

1. 运行 ListSecurityControlDefinitions 并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 DescribeStandards。此 API 返回与标准无关的安全控制 IDs，而不是特定于标准的控制。 IDs

   请求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 运行 ListStandardsControlAssociations，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

   请求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. 运行 BatchUpdateStandardsControlAssociations。提供您要在其中禁用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已禁用的控件执行以下步骤，API 将返回 HTTP 状态代码 200 响应。

   请求示例：

   ```
   {
       "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

要禁用特定标准中的控件

1. 运行 list-security-control-definitions 命令并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 describe-standards。此命令返回与标准无关的安全控制 IDs，而不是特定于标准的控制。 IDs

```
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. 运行 list-standards-control-associations 命令，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. 运行 batch-update-standards-control-associations 命令。提供您要在其中禁用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已启用的控件执行这些步骤，该命令将返回 HTTP 状态代码 200 响应。

```
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"}]'
```

建议在 Security Hub CSPM 中禁用的控件

我们建议禁用某些 Sec AWS urity Hub CSPM 控件，以减少查找噪音和使用成本。

使用全局资源的控件

有些 AWS 服务 支持全局资源，这意味着您可以从任何资源访问该资源 AWS 区域。为了节省成本 AWS Config，您可以禁用除一个区域以外的所有区域记录全球资源。但在完成此操作后，Security Hub CSPM 仍将在所有启用控件的区域进行安全检查，并将根据每个区域的每个账户的检查数量，向

您收费。因此，为了减少调查发现噪音并节省 Security Hub CSPM 的成本，还应禁用涉及到除记录全球资源的区域之外的所有区域中的全球资源的控件。

如果控件涉及全球资源，但仅在一个区域可用，则在该区域禁用该控件会让您无法获取底层资源的任何调查发现。在这种情况下，建议您使控件保持已启用状态。使用跨区域聚合时，可使用控件的区域应为聚合区域或关联区域之一。以下控件涉及全局资源，但仅在单个区域可用：

- 所有 CloudFront 控件-仅在美国东部（弗吉尼亚北部）区域可用
- GlobalAccelerator.1 — 仅在美国西部（俄勒冈）区域可用
- Route53.2 – 仅在美国东部（弗吉尼亚州北部）区域可用
- WAF.1、WAF.6、WAF.7、WAF.8 – 仅在美国东部（弗吉尼亚州北部）区域可用

> **Note**
>
> 如果您使用中心配置，Security Hub CSPM 会自动禁用涉及除主区域之外的所有区域中全局资源的控件。您选择通过配置策略启用的其他控件已在所有提供这些控件的区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。
>
> 如果涉及全局资源的已启用控件在主区域不受支持，则 Security Hub CSPM 会尝试在支持该控件的关联区域中启用该控件。使用中心配置，您无法覆盖在主区域或任何关联区域中不可用的控件。
>
> 有关中心配置的更多信息，请参阅了解 Security Hub CSPM 中的中心配置。

对于具有定期计划类型的控件，需要在 Security Hub CSPM 中将其禁用以防止计费。将 AWS Config 参数设置`includeGlobalResourceTypes`为`false`不会影响定期的 Security Hub CSPM 控制。

以下 Security Hub CSPM 控件使用全局资源：

- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF

- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

CloudTrail 日志控制

CloudTrail.2 控件评估使用 AWS Key Management Service (AWS KMS) 加密 AWS CloudTrail 跟踪日志的情况。如果您在集中式日志记录账户中记录这些跟踪，则只需在集中日志记录 AWS 区域 所在的账户中启用此控件。

如果您使用中心配置，则控件的启用状态将在主区域和关联区域之间保持一致。您无法在某些区域禁用某个控件而在其他区域启用该控件。在这种情况下，您可以抑制来自 CloudTrail .2 控件的结果，以减少查找噪音。

CloudWatch 警报控制

如果您更喜欢使用亚马逊而不是亚马逊 CloudWatch 警报 GuardDuty 进行异常检测，则可以禁用以下控件，这些控件侧重于 CloudWatch 警报：

- [CloudWatch.1] “root” 用户应有日志指标筛选器和警报
- [CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报
- [CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报
- [CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报
- [CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报
- [CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报
- [CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
- [CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

- [CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报
- [CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
- [CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
- [CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
- [CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
- [CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

了解 Security Hub CSPM 中的安全检查和分数

对于您启用的每个控件，Sec AWS urity Hub CSPM 都会运行安全检查。安全检查会生成一个调查结果，告诉您特定 AWS 资源是否符合该控件所包含的规则。

有些检查是定期进行的。其他检查仅在资源状态发生更改时运行。有关更多信息，请参阅 有关运行安全检查的计划。

许多安全检查使用 AWS Config 托管或自定义规则来确定合规性要求。要运行这些检查，您必须为所需资源设置 AWS Config 并开启资源记录。有关设置的更多信息 AWS Config，请参阅启用和配置 AWS Config 适用于 Security Hub CSPM。有关必须为每个标准记录的 AWS Config 资源列表，请参阅必填 AWS Config 控制结果的资源。其他控件使用自定义 Lambda 函数，这些函数由 Security Hub CSPM 管理，并且不需要任何先决条件。

当 Security Hub CSPM 运行安全检查时，它会生成调查发现并为其分配合规性状态。有关合规状态的更多信息，请参阅 评估 Security Hub CSPM 调查发现的合规性状态。

Security Hub CSPM 使用控件调查发现的合规性状态来确定总体控件状态。根据控件状态，Security Hub CSPM 还会计算所有已启用控件和特定标准的安全分数。有关更多信息，请参阅the section called “合规性状态和控件状态”和the section called “计算安全分数”。

如果您开启了整合的控件调查发现，即使一个控件与多个标准相关联，Security Hub CSPM 也会生成一个调查发现。有关更多信息，请参阅 整合的控件调查发现。

主题

- 必填 AWS Config 控制结果的资源
- 有关运行安全检查的计划
- 生成和更新控件调查发现
- 评估合规性状态和控件状态
- 计算安全分数

必填 AWS Config 控制结果的资源

> **Note**
>
> 如果您使用的是 Security Hub CSPM 和 Security Hub，则资源记录的配置将由您管理。Security Hub 使用与 Security Hub CSPM 支持的控件相关的所有资源创建服务关联的配置记录器， AWS Config 并直接获取有关这些资源的信息。有关更多信息，请参阅 使用与服务相关的配置记录器。

在 S AWS ecurity Hub CSPM 中，某些控件使用服务相关 AWS Config 规则来检测资源中的配置更改。 AWS 要让 Security Hub CSPM 为这些控件生成准确的调查结果，您必须在中启用 AWS Config 并打开资源记录。 AWS Config有关 Security Hub CSPM 如何使用 AWS Config 规则以及如何启用和配置的信息 AWS Config，请参阅。启用和配置 AWS Config 适用于 Security Hub CSPM有关资源记录的详细信息，请参阅《AWS Config 开发人员指南》中的使用配置记录器。

要获得准确的控制结果，您必须为已启用的控件启用 AWS Config 资源记录，并使用更改触发的计划类型。某些具有定期计划类型的控件也需要资源记录。本页列出了这些 Security Hub CSPM 控件所需的资源。

Security Hub CSPM 控件可以依赖托管 AWS Config 规则或自定义 Security Hub CSPM 规则。确保没有任何 AWS Identity and Access Management (IAM) 策略或 AWS Organizations 托管策略会 AWS Config 阻止您获得记录资源的权限。Security Hub CSPM 控件直接评估资源配置，不考虑 AWS Organizations 策略。

> **Note**
>
> AWS 区域 如果控件不可用，则相应的资源在中不可用 AWS Config。有关这些限制的列表，请参阅对 Security Hub CSPM 控件的区域限制。

主题

- 所有 Security Hub CSPM 控件所需的资源
- 所需的资源 AWS 基础安全最佳实践标准
- CIS 所需的资源 AWS 基金会基准
- NIST SP 800-53 修订版 5 标准所需的资源
- NIST SP 800-171 修订版 2 标准所需的资源

- PCI DSS v3.2.1 所需的资源
- 所需的资源 AWS 资源标签标准

所有 Security Hub CSPM 控件所需的资源

要让 Security Hub CSPM 生成已启用的变更触发控件的发现结果并使用 AWS Config 规则，您必须在中记录以下类型的资源。 AWS Config此表还指出了哪些控件评估特定类型的资源。一个控件可以评估多种类型的资源。

AWS 服务	资源类型	相关控件
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
	`AWS::ApiGateway::DomainName`	APIGateway.11
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig.1

AWS 服务	资源类型	相关控件
	`AWS::AppConfig::ConfigurationProfile`	AppConfig.2
	`AWS::AppConfig::Environment`	AppConfig.3
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
亚马逊 AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1
	`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 服务	资源类型	相关控件
	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
Amazon Bedrock AgentCore	AWS::BedrockAgentCore::BrowserCustom	BedrockAgentCore.5 BedrockAgentCore.6
	AWS::BedrockAgentCore::Gateway	BedrockAgentCore.2 BedrockAgentCore.4
	AWS::BedrockAgentCore::Memory	BedrockAgentCore.3

AWS 服务	资源类型	相关控件
	`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
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2 CloudFormation.3 CloudFormation.4

AWS 服务	资源类型	相关控件
亚马逊 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
	`AWS::CloudTrail::EventDataStore`	CloudTrail.11
亚马逊 CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17

AWS 服务	资源类型	相关控件
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 P CodeGuru rofiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2

AWS 服务	资源类型	相关控件
	`AWS::Cognito::UserPool`	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
Amazon Connect Customer	`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
	`AWS::DMS::EventSubscription`	DMS.3

AWS 服务	资源类型	相关控件
	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
	AWS::EC2::EIP	EC2.12 EC2.37

AWS 服务	资源类型	相关控件
	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
	AWS::EC2::NetworkAcl	EC2.16 EC2.21 EC2.41

AWS 服务	资源类型	相关控件
	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
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache.7

AWS 服务	资源类型	相关控件
	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
	AWS::EC2::VPC	EC2.6 EC2.46

AWS 服务	资源类型	相关控件
	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
	AWS::AutoScaling::LaunchConfiguration	AutoScaling.3 Autoscaling.5

AWS 服务	资源类型	相关控件
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
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13

AWS 服务	资源类型	相关控件
	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
Amazon Elastic Kubernetes Service（Amazon EKS）	AWS::EKS::Cluster	EKS.2 EKS.6 EKS.8

AWS 服务	资源类型	相关控件
	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

AWS 服务	资源类型	相关控件
	`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
亚马逊 EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4

AWS 服务	资源类型	相关控件
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
亚马逊 GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2
	`AWS::GuardDuty::IPSet`	GuardDuty.3

AWS 服务	资源类型	相关控件
AWS Identity and Access Management (IAM)	`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

AWS 服务	资源类型	相关控件
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
AWS IoT Events	`AWS::IoTEvents::AlarmModel`	IoTEvents.3

AWS 服务	资源类型	相关控件
	AWS::IoTEvents::DetectorModel	IoTEvents.2
	AWS::IoTEvents::Input	IoTEvents.1
AWS 物联网 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
AWS 物联网 TwinMaker	AWS::IoTTwinMaker::Entity	IoTTwinMaker.4
	AWS::IoTTwinMaker::Scene	IoTTwinMaker.3

AWS 服务	资源类型	相关控件
	`AWS::IoTTwinMaker::SyncJob`	IoTTwinMaker.1
	`AWS::IoTTwinMaker::Workspace`	IoTTwinMaker.2
AWS IoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoTWireless.1
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces（Apache Cassandra 兼容）	`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

AWS 服务	资源类型	相关控件
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

AWS 服务	资源类型	相关控件
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
亚马逊 OpenSearch 服务	`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
AWS 私有 CA	`AWS::ACMPCA::CertificateAuthority`	PCA.2

AWS 服务	资源类型	相关控件
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

AWS 服务	资源类型	相关控件
		RDS.37 RDS.47 RDS.48
	AWS::RDS::DBClusterSnapshot	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

AWS 服务	资源类型	相关控件
	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

AWS 服务	资源类型	相关控件
	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

AWS 服务	资源类型	相关控件
	`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

AWS 服务	资源类型	相关控件
	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

AWS 服务	资源类型	相关控件
	`AWS::S3Express::DirectoryBucket`	S3.25
亚马逊 SageMaker AI	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker.7
	`AWS::SageMaker::Model`	SageMaker.5 SageMaker.16 SageMaker.19
	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3
	`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 服务	资源类型	相关控件
	`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
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Systems Manager (SSM)	`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 服务	资源类型	相关控件
	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
	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
亚马逊 WorkSpaces	AWS::WorkSpaces::WorkSpace	WorkSpaces.1 WorkSpaces.2

所需的资源 AWS 基础安全最佳实践标准

为了让 Security Hub CSPM 准确报告适用于 AWS 基础安全最佳实践标准 (v.1.0.0)、已启用并使用 AWS Config 规则的变更触发控制的结果，您必须在中记录以下类型的资源。 AWS Config有关此标准的信息，请参阅 AWS Security Hub CSPM 中的基础安全最佳实践标准。

AWS 服务	资源类型
Amazon API Gateway	`AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::BrowserCustom` , `AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Runtime`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
亚马逊 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`
Amazon Connect Customer	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`

AWS 服务	资源类型
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
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

AWS 服务	资源类型
Amazon Elastic File System（Amazon EFS）	AWS::EFS::AccessPoint ，AWS::EFS::FileSystem
Amazon Elastic Kubernetes Service（Amazon EKS）	AWS::EKS::Cluster ，AWS::EKS::Nodegroup
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
AWS Identity and Access Management (IAM)	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

AWS 服务	资源类型
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`
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 Serverless	`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`
亚马逊 SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::Model` , `AWS::SageMaker::NotebookInstance`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`

AWS 服务	资源类型
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`
亚马逊 WorkSpaces	`AWS::WorkSpaces::WorkSpace`

CIS 所需的资源 AWS 基金会基准

要对适用于互联网安全中心 (CIS) AWS 基金会基准测试的已启用控件进行安全检查，Security Hub CSPM 要么执行为检查规定的确切审计步骤，要么使用特定的 AWS Config 托管规则。有关 Security Hub CSPM 中此标准的更多信息，请参阅 CIS AWS Security Hub CSPM 中的基础基准。

CIS v5.0.0 所需的资源

为使 Security Hub CSPM 能够准确报告使用 AWS Config 规则的已启用 CIS v5.0.0 更改触发的控件的调查结果，您必须在中记录以下类型的资源。 AWS Config

AWS 服务	资源类型
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`
AWS Identity and Access Management (IAM)	`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`

CIS v3.0.0 所需的资源

为了让 Security Hub CSPM 准确报告已启用 CIS v3.0.0 更改触发的使用 AWS Config 规则的控件的调查结果，您必须在中记录以下类型的资源。 AWS Config

AWS 服务	资源类型
Amazon Elastic Compute Cloud（Amazon EC2）	`AWS::EC2::Instance` ，`AWS::EC2::NetworkAcl` ，`AWS::EC2::SecurityGroup` ，`AWS::EC2::VPC`
AWS Identity and Access Management (IAM)	`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`

CIS v1.4.0 所需的 资源

为了让 Security Hub CSPM 准确报告已启用 CIS v1.4.0 更改触发的使用 AWS Config 规则的控件的调查结果，您必须在中记录以下类型的资源。 AWS Config

AWS 服务	资源类型
Amazon Elastic Compute Cloud（Amazon EC2）	`AWS::EC2::NetworkAcl` ，`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` ，`AWS::IAM::User`
Amazon Relational Database Service（Amazon RDS）	`AWS::RDS::DBInstance`
Amazon Simple Storage Service（Amazon S3）	`AWS::S3::Bucket`

CIS v1.2.0 所需的 资源

为了让 Security Hub CSPM 准确报告已启用 CIS v1.2.0 更改触发的使用 AWS Config 规则的控件的调查结果，您必须在中记录以下类型的资源。 AWS Config

AWS 服务	资源类型
Amazon Elastic Compute Cloud（Amazon EC2）	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` ，`AWS::IAM::User`

NIST SP 800-53 修订版 5 标准所需的资源

为了让 Security Hub CSPM 准确报告适用于 NIST SP 800-53 修订版 5 标准、已启用并使用 AWS Config 规则的变更触发控制的结果，您必须在中记录以下类型的资源。 AWS Config有关此标准的信息，请参阅 Security Hub CSPM 中的 NIST SP 800-53 修订版 5。

AWS 服务	资源类型
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`
亚马逊 CloudFront	`AWS::CloudFront::Distribution`
亚马逊 CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS 服务	资源类型
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
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment

AWS 服务	资源类型
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
亚马逊 ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
亚马逊 EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (IAM)	`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`
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`

AWS 服务	资源类型
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`
亚马逊 SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`

AWS 服务	资源类型
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

NIST SP 800-171 修订版 2 标准所需的资源

为了让 Security Hub CSPM 准确报告适用于 NIST SP 800-171 修订版 2 标准、已启用并使用 AWS Config 规则的变更触发控制的结果，您必须在中记录以下类型的资源。 AWS Config有关此标准的信息，请参阅 Security Hub CSPM 中的 NIST SP 800-171 修订版 2。

AWS 服务	资源类型
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
亚马逊 CloudFront	AWS::CloudFront::Distribution
亚马逊 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
AWS Identity and Access Management (IAM)	AWS::IAM::Policy ，AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias ，AWS::KMS::Key

AWS 服务	资源类型
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`

PCI DSS v3.2.1 所需的资源

为了使 Security Hub CSPM 能够为适用于支付卡行业数据安全标准（PCI DSS）v3.2.1、已启用并且使用 AWS Config 规则的控件准确报告调查发现，您必须在 AWS Config中记录以下类型的资源。有关此标准的信息，请参阅 Security Hub CSPM 中的 PCI DSS。

AWS 服务	资源类型
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`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` ，`AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`

AWS 服务	资源类型
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`

所需的资源 AWS 资源标签标准

所有适用于 AWS 资源标记标准的控件都是触发变更的，并使用 AWS Config 规则。为了让 Security Hub CSPM 准确报告这些控件的调查结果，您必须在中记录以下类型的资源。 AWS Config有关此标准的信息，请参阅 AWS Security Hub CSPM 中的资源标记标准。

AWS 服务	资源类型
AWS Amplify	`AWS::Amplify::App` ，`AWS::Amplify::Branch`
亚马逊 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 服务	资源类型
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
亚马逊 CloudFront	AWS::CloudFront::Distribution
AWS CloudTrail	AWS::CloudTrail::Trail
AWS CodeArtifact	AWS::CodeArtifact::Repository
亚马逊 CodeGuru	AWS::CodeGuruProfiler::ProfilingGroup , AWS::CodeGuruReviewer::RepositoryAssociation
Amazon Connect Customer	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

AWS 服务	资源类型
Amazon Detective	AWS::Detective::Graph
Amazon DynamoDB	AWS::DynamoDB::Trail
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

AWS 服务	资源类型
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::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
亚马逊 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`
亚马逊 GuardDuty	`AWS::GuardDuty::Detector`，`AWS::GuardDuty::Filter`，`AWS::GuardDuty::IPSet`
AWS Identity and Access Management (IAM)	`AWS::IAM::Role`，`AWS::IAM::User`
AWS Identity and Access Management Access Analyzer（IAM 访问分析器）	`AWS::AccessAnalyzer::Analyzer`

AWS 服务	资源类型
AWS IoT	AWS::IoT::Authorizer ,AWS::IoT::Dimension ,AWS::IoT::MitigationAction ,AWS::IoT::Policy ,AWS::IoT::RoleAlias ,AWS::IoT::SecurityProfile
AWS IoT 活动	AWS::IoTEvents::AlarmModel ,AWS::IoTEvents::DetectorModel ,AWS::IoTEvents::Input
AWS IoT SiteWise	AWS::IoTSiteWise::Dashboard ,AWS::IoTSiteWise::Gateway ,AWS::IoTSiteWise::Portal ,AWS::IoTSiteWise::Project
AWS IoT TwinMaker	AWS::IoTTwinMaker::Entity ,AWS::IoTTwinMaker::Scene ,AWS::IoTTwinMaker::SyncJob ,AWS::IoTTwinMaker::Workspace
AWS IoT 无线	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（Apache Cassandra 兼容）	AWS::Cassandra::Keyspace
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon MQ	AWS::AmazonMQ::Broker

AWS 服务	资源类型
AWS Network Firewall	AWS::NetworkFirewall::Firewall ，AWS::NetworkFirewall::FirewallPolicy
亚马逊 OpenSearch 服务	AWS::OpenSearch::Domain
AWS 私有证书颁发机构	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
亚马逊 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 服务	资源类型
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager (SSM)	`AWS::SSM::Document`
AWS Transfer Family	`AWS::Transfer::Agreement` ，`AWS::Transfer::Certificate` ，`AWS::Transfer::Connector` ，`AWS::Transfer::Profile` ，`AWS::Transfer::Workflow`

有关运行安全检查的计划

启用安全标准后，Securit AWS y Hub CSPM 将在两小时内开始运行所有检查。大多数检查会在 25 分钟内开始运行。 Security Hub CSPM 通过评估控件底层的规则来运行检查。在控件完成其第一次检查之前，其状态为无数据。

启用新标准后，Security Hub CSPM 最多可能需要 24 小时才能为使用与其他启用标准中的已启用控件相同的底层 AWS Config 服务关联规则的控件生成调查结果。例如，如果您在 AWS 基础安全最佳实践 (FSBP) 标准中启用 Lambda.1 控件，Security Hub CSPM 会创建与服务相关的规则，并且通常会在几分钟内生成调查结果。此后，如果您在支付卡行业数据安全标准（PCI DSS）中启用 Lambda.1 控件，Security Hub CSPM 最多可能需要 24 小时才能生成该控件的调查发现，因为它使用相同的服务相关规则。

初始检查后，每个控件的计划可以是定期的，也可以是更改触发的。对于基于托管 AWS Config 规则的控件，控件描述中包含指向《AWS Config 开发人员指南》中规则描述的链接。该描述指定规则是更改触发的还是定期性的。

定期安全检查

定期安全检查会在最近一次运行后的 12 或 24 小时内自动运行。Security Hub CSPM 确定周期性，您无法对其进行更改。定期控制反映了检查运行时的评估。

如果您更新了定期控件调查发现的工作流状态，然后在下次检查中该调查发现的合规性状态保持不变，则工作流状态将保持其已修改状态。例如，如果您找到 KMS.4 控件的查找失败（应启用AWS KMS key 轮换），然后修复了发现结果，Security Hub CSPM 会将工作流程状态从更改为。`NEW` `RESOLVED`如果您在下次定期检查之前禁用 KMS 密钥轮换，则调查发现的工作流状态将保持 `RESOLVED` 不变。

使用 Security Hub CSPM 自定义 Lambda 函数的检查是定期进行的。

更改触发的安全检查

当关联的资源状态发生变化时，会运行变更触发的安全检查。 AWS Config 允许您在连续记录资源状态变化和每日记录之间进行选择。如果您选择每日记录，则在资源状态发生变化时，会在每 24 小时结束时 AWS Config 提供资源配置数据。如果没有任何更改，则不会传送任何数据。这可能会导致 Security Hub CSPM 调查发现生成延迟，直到 24 小时周期结束。无论您选择哪个录制时间，Security Hub CSPM 都至少每 24 小时检查一次，以确保没有错过任何资源更新。 AWS Config

通常，Security Hub CSPM 尽可能使用更改触发的规则。要使资源使用变更触发的规则，它必须支持 AWS Config 配置项目。

生成和更新控件调查发现

AWS Security Hub CSPM 在对安全控制进行检查时生成并更新控制结果。控件调查发现使用 AWS 安全调查发现格式（ASFF）。

Security Hub CSPM 通常会对控件的每项安全检查收费。但是，如果多个控件使用相同的 AWS Config 规则，则 Security Hub CSPM 仅针对该规则对每项检查收取一次费用。例如，CIS AWS 基金会基准标准和 AWS 基础安全最佳实践标准中的多个控件都使用该 AWS Config `iam-password-policy`规则。每次 Security Hub CSPM 根据该规则运行检查时，它会为每个相关控件生成一个单独的控件调查发现，但只对检查收取一次费用。

如果控件调查发现的大小超过最大值 240 KB，Security Hub CSPM 将从调查发现中移除 `Resource.Details` 对象。对于由 AWS Config 资源支持的控件，您可以使用 AWS Config 控制台查看资源详细信息。

主题

- 整合的控件调查发现
- 生成、更新和存档控件调查发现
- 控件调查发现的自动化和隐藏
- 控件调查发现的合规性详细信息
- ProductFields 控制结果的详细信息
- 控件调查发现的严重性级别

整合的控件调查发现

如果您的账户启用了整合的控件调查发现，则 Security Hub 会为控件的每项安全检查生成一个调查发现或调查发现更新，即使某个控件适用于多个启用的标准。有关控件及其适用的标准列表，请参阅 Security Hub CSPM 控件参考。我们建议启用整合的控件调查发现以减少调查发现噪音。

如果您在 2023 年 2 月 23 日 AWS 账户 之前启用了 Security Hub CSPM，则可以按照本节后面的说明启用合并控制结果。如果 2023 年 2 月 23 日当天或之后启用了 Security Hub CSPM，则会自动为您的账户启用整合的控件调查发现。

如果使用 Security Hub CSPM 与 AWS Organizations的集成，或使用通过手动邀请流程邀请的成员账户，则只有在为管理员账户启用了整合的控件调查发现后，才会为成员账户启用该功能。如果为管理员账户禁用了该功能，则成员账户也会禁用。此行为适用于新的和现有的成员账户。此外，如果管理员使用中心配置来为多个账户管理 Security Hub CSPM，则它们无法使用中心配置策略来为这些账户启用或禁用整合的控件调查发现。

如果您为自己的账户禁用了整合的控件调查发现，则 Security Hub CSPM 会为每项包含控件的已启用标准生成或更新单独的控件调查发现。例如，如果您启用四个共享同一控件的标准，则在对该控件进行安全检查后，您将收到四个不同的调查发现。如果启用整合的控件调查发现，则只会收到一项调查发现。

启用整合的控件调查发现后，Security Hub CSPM 会创建与标准无关的新调查发现，并存档基于标准的原始调查发现。某些控件调查发现字段和值会发生变化，这可能会影响您的现有工作流。有关这些更改的信息，请参阅整合的控件调查发现——ASFF 的变化。启用整合的控件调查发现还可能会影响集成的第三方产品从 Security Hub CSPM 收到的调查发现。如果您在 AWS v2.0.0 上使用自动安全响应解决方案，请注意它支持整合的控制结果。

要启用或禁用整合的控件调查发现，您必须登录管理员账户或独立账户。

> **Note**
>
> 启用整合的控件调查发现后，Security Hub CSPM 最多可能需要 24 小时才能生成新的整合调查发现并存档现有基于标准的调查发现。同样，禁用整合的控件调查发现后，Security Hub CSPM 最多可能需要 24 小时才能生成基于标准的新调查发现并存档现有整合的调查发现。在此期间，您可能会在账户中同时看到与标准无关的调查发现和基于标准的调查发现。

Security Hub CSPM console

启用或禁用整合的控件调查发现

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中的设置下，选择常规。
3. 在控件部分中，选择编辑。
4. 使用整合的控件调查发现开关来启用或禁用整合的控件调查发现。
5. 选择保存。

Security Hub CSPM API

要以编程方式启用或禁用整合的控件调查发现，请使用 Security Hub CSPM API 的 UpdateSecurityHubConfiguration 操作。或者，如果您使用的是 AWS CLI，请运行该update-security-hub-configuration命令。

对于 `control-finding-generator` 参数，请指定 `SECURITY_CONTROL` 以启用整合的控件调查发现。要禁用整合的控件调查发现，请指定 `STANDARD_CONTROL`。

例如，以下 AWS CLI 命令启用合并的控制结果。

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

以下 AWS CLI 命令禁用整合控制结果。

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

生成、更新和存档控件调查发现

Security Hub CSPM 会按计划运行安全检查。Security Hub CSPM 首次对控件运行安全检查时，它会为控件检查的每个 AWS 资源生成一个新的发现。每次 Security Hub CSPM 随后对该控件运行安全检查时，它都会更新现有调查发现以报告检查结果。这意味着您可以使用各项调查发现提供的数据，根据特定控件跟踪特定资源的合规性变化。

例如，如果某个资源对于特定控件的合规性状态从 FAILED 变为 PASSED，则 Security Hub CSPM 不会生成新的调查发现。相反，Security Hub CSPM 会更新控件和资源的现有调查发现。在调查发现中，Security Hub CSPM 会将合规性状态（Compliance.Status）字段的值更改为 PASSED。Security Hub CSPM 还会更新其他字段的值以反映检查结果，例如严重性标签、工作流状态和时间戳（指明 Security Hub CSPM 最近一次运行检查并更新调查发现的时间）。

在报告合规性状态的变化时，Security Hub CSPM 可能会更新控件调查发现中的以下任何字段：

- Compliance.Status – 资源对于指定的控件的新合规性状态。
- FindingProviderFields.Severity.Label – 调查发现严重性的新定性表示，例如 LOW MEDIUM 或 HIGH。
- FindingProviderFields.Severity.Original – 调查发现严重性的新量化表示，例如合规资源为 0。
- FirstObservedAt – 资源的合规性状态最近发生变化的时间。
- LastObservedAt – Security Hub CSPM 最近对指定的控件和资源运行安全检查的时间。
- ProcessedAt – Security Hub CSPM 最近开始处理调查发现的时间。
- ProductFields.PreviousComplianceStatus：资源对于指定的控件的以前合规性状态（Compliance.Status）。
- UpdatedAt – Security Hub CSPM 最近更新调查发现的时间。
- Workflow.Status – 调查发现的调查状态，基于资源对指定的控件的新合规性状态。

Security Hub CSPM 是否更新字段主要取决于对适用控件和资源的最新安全检查的结果。例如，如果某个资源对于特定控件的合规性状态从 PASSED 变为 FAILED，则 Security Hub CSPM 会将调查发现的工作流状态更改为 NEW。要跟踪单个调查发现的更新，您可以参考调查发现的历史记录。有关调查发现中各个字段的详细信息，请参阅 AWS 安全调查发现格式（ASFF）。

在某些情况下，Security Hub CSPM 会生成新的调查发现供控件进行后续检查，而不是更新现有调查发现。如果支持控件的 AWS Config 规则存在问题，则可能会发生这种情况。如果发生这种情况，Security Hub CSPM 会存档现有调查发现，并为每个检查生成新的调查发现。在新的调查发现中，合规性状态为 NOT_AVAILABLE，记录状态为 ARCHIVED。解决 AWS Config 规则问题后，Security Hub CSPM 会生成新的发现并开始对其进行更新，以跟踪各个资源合规性状态的后续变化。

除了生成和更新控件调查发现外，Security Hub CSPM 还会自动存档符合特定标准的控件调查发现。如果禁用了控件、删除了指定的资源或指定的资源不再存在，则 Security Hub CSPM 会存档调查发

现。由于关联的服务不再使用，资源可能不再存在。更具体地说，如果控件调查发现符合以下条件之一，Security Hub CSPM 会自动存档该调查发现：

- 调查发现已 3-5 天没有更新。请注意，基于此时间范围进行的存档是尽力而为，并不保证一定能够成功。
- `NOT_APPLICABLE`针对指定资源的合规性状态返回的关联 AWS Config 评估。

要确定某调查发现是否已存档，可以参考该调查发现的记录状态（`RecordState`）字段。如果调查发现已存档，则此字段的值为 `ARCHIVED`。

Security Hub CSPM 会将存档的控件调查发现存储 30 天。30 天后，调查发现会过期，Security Hub CSPM 会将其永久删除。为了确定存档的控件调查发现是否已过期，Security Hub CSPM 会根据调查发现的 `UpdatedAt` 字段的值进行计算。

要将存档的控件调查发现存储 30 天以上，可以将调查发现导出到 S3 存储桶。您可以通过使用带有 Amazon EventBridge 规则的自定义操作来实现此目的。有关更多信息，请参阅 EventBridge 用于自动响应和补救。

> **Note**
>
> 在 2025 年 7 月 3 日之前，当资源的控件合规性状态发生变化时，Security Hub CSPM 会以不同的方式生成和更新控件调查发现。之前，Security Hub CSPM 为某个资源创建了一个新的控件调查发现并存档了现有调查发现。因此，对于特定控件和资源，您可能会有多个已存档的调查发现，直到这些调查发现过期（30 天后）。

控件调查发现的自动化和隐藏

您可以使用 Security Hub CSPM 自动化规则来更新或隐藏特定控件调查发现。如果您隐藏了某个调查发现，则可以继续访问它。但是，隐藏表明您认为无需采取任何措施来解决该调查发现。

通过隐藏调查发现，可以减少调查发现噪音。例如，您可以隐藏在测试账户中生成的控件调查发现。或者，您可以隐藏与特定资源相关的调查发现。要了解有关自动更新或隐藏调查发现的更多信息，请参阅了解 Security Hub CSPM 中的自动化规则。

当您想要更新或隐藏特定控件调查发现时，自动化规则是合适的。但是，如果某个控件与您的组织或使用案例无关，建议禁用该控件。如果禁用某个控件，Security Hub CSPM 不会对其运行安全检查，也不会向您收取控件的费用。

控件调查发现的合规性详细信息

在控制措施安全检查生成的调查结果中，合规性对象和 AWS 安全调查结果格式 (ASFF) 中的字段提供了控件所检查的各个资源的合规性详细信息。这包含以下信息：

- `AssociatedStandards` – 启用控件的已启用标准。
- `RelatedRequirements` – 所有已启用标准中控件的相关要求。这些要求源自控件的第三方安全框架，例如支付卡行业数据安全标准（PCI DSS）或 NIST SP 800-171 修订版 2 标准。
- `SecurityControlId` – Security Hub CSPM 支持的各类标准中控件的标识符。
- `Status` – Security Hub CSPM 针对控件运行的最新检查的结果。先前检查的结果会保留在调查发现的历史记录中。
- `StatusReasons` – 列出 `Status` 字段指定的值的原因的数组。对于每个原因，这包括原因代码和描述。

下表列出了调查发现可能包含在 `StatusReasons` 数组中的原因代码和描述。根据哪个控件生成了带有指定原因代码的调查发现，修复步骤会有所不同。要查看控件的修复指导，请参阅Security Hub CSPM 控件参考。

原因代码	合规性状态	说明
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	多区域 CloudTrail 跟踪没有有效的指标筛选条件。
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	多区域 CloudTrail 跟踪不存在指标筛选条件。
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	该账户没有具有所需配置的多区域 CloudTrail 跟踪。
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	多区域 CloudTrail 跟踪不在当前区域中。
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	不存在有效的警报操作。
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch 账户中不存在警报。

原因代码	合规性状态	说明
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config 状态是 ConfigError	AWS Config 访问被拒绝。 验证 AWS Config 是否已启用并已被授予足够的权限。
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config 根据规则评估了您的资源。 该规则不适用于其范围内的 AWS 资源，指定的资源已被删除，或者评估结果被删除。
CONFIG_RECORDER_CUSTOM_ROLE	FAILED（对于 Config.1）	AWS Config 记录器使用自定义 IAM 角色而不是 AWS Config 服务相关角色，并且 Config.1 的includeConfigServiceLinkedRoleCheck 自定义参数未设置为 。false
CONFIG_RECORDER_DISABLED	FAILED（对于 Config.1）	AWS Config 在配置记录器开启的情况下未启用。
CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES	FAILED（对于 Config.1）	AWS Config 并未记录与启用的 Security Hub CSPM 控件相对应的所有资源类型。为以下资源开启录制:*Resources that aren't being recorded*.

原因代码	合规性状态	说明
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	合规性状态NOT_AVAILABLE 是因为 AWS Config 返回的状态为 “不适用”。 AWS Config 未提供该状态的原因。以下是不适用状态的一些可能原因： • 该资源已从 AWS Config 规则的范围中移除。 • 该 AWS Config 规则已删除。 • 资源已删除。 • AWS Config 规则逻辑可能会生成 “不适用” 状态。
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config 状态是 ConfigError	此原因代码用于几种不同类型的评估错误。 描述提供了具体的原因信息。 错误类型可以是以下类型之一： • 由于缺乏权限而无法执行评估。描述提供缺少的特定权限。 • 参数缺少值或值无效。描述提供参数和参数值的要求。 • 从 S3 存储桶读取时出错。描述标识存储桶并提供特定错误。 • 缺少 AWS 订阅。 • 评估时出现一般超时。 • 账户暂停。

原因代码	合规性状态	说明
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config 状态是 ConfigError	该 AWS Config 规则正在创建中。
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	出现未知错误。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub CSPM 无法对自定义 Lambda 运行时执行检查。
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	该调查发现处于 WARNING 状态，因为与此规则关联的 S3 存储桶位于不同的区域或账户中。 此规则不支持跨区域或跨账户检查。 建议您在此区域或账户中禁用此控制。仅在资源所在的区域或账户中运行它。
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch 日志指标筛选条件没有有效的 Amazon SNS 订阅。
SNS_TOPIC_CROSS_ACCOUNT	WARNING	该调查发现处于一种 WARNING 状态。 与此规则关联的 SNS 主题由其他账户拥有。当前账户无法获取订阅信息。 拥有 SNS 主题的账户必须向当前账户授予访问 SNS 主题的 sns:ListSubscriptionsByTopic 权限。

原因代码	合规性状态	说明
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	该调查发现处于 WARNING 状态，因为与此规则关联的 SNS 主题位于不同的区域或账户中。 此规则不支持跨区域或跨账户检查。 建议您在此区域或账户中禁用此控制。仅在资源所在的区域或账户中运行它。
SNS_TOPIC_INVALID	FAILED	与此规则关联的 SNS 主题无效。
THROTTLING_ERROR	NOT_AVAILABLE	相关 API 操作超出了允许的速率。

ProductFields 控制结果的详细信息

在控件安全检查生成的结果中， AWS 安全调查结果格式 (ASFF) 中的ProductFields属性可以包括以下字段。

`ArchivalReasons:0/Description`

描述 Security Hub CSPM 为何存档调查发现。

例如，当您禁用某个控件或标准，或者启用或禁用整合的控件调查发现时，Security Hub CSPM 会存档现有调查发现。

`ArchivalReasons:0/ReasonCode`

指定 Security Hub CSPM 为何存档调查发现。

例如，当您禁用某个控件或标准，或者启用或禁用整合的控件调查发现时，Security Hub CSPM 会存档现有调查发现。

`PreviousComplianceStatus`

截至最近一次更新调查发现时，指定控件的资源先前合规性状态（`Compliance.Status`）。如果资源的合规性状态在最近更新期间没有发生变化，则此值与调查发现的 `Compliance.Status` 字段的值相同。有关可能的值的列表，请参阅评估合规性状态和控件状态。

`StandardsGuideArn` 或 `StandardsArn`

与控件关联的标准的 ARN。

对于 CIS AWS 基金会基准标准，字段为`StandardsGuideArn`。对于 PCI DSS 和 AWS 基础安全最佳实践标准，字段为。`StandardsArn`

如果您启用整合的控件调查发现，这些字段会被移除，取而代之的是 `Compliance.AssociatedStandards`。

`StandardsGuideSubscriptionArn` 或 `StandardsSubscriptionArn`

账户订阅该标准的 ARN。

对于 CIS AWS 基金会基准标准，字段为`StandardsGuideSubscriptionArn`。对于 PCI DSS 和 AWS 基础安全最佳实践标准，字段为。`StandardsSubscriptionArn`

如果您启用整合的控件调查发现，这些字段会被移除。

`RuleId` 或 `ControlId`

控件的标识符。

对于 CIS AWS 基金会基准标准的 1.2.0 版，字段为`RuleId`。对于其他标准，包括 CIS AWS 基金会基准标准的后续版本，字段为 `ControlId`。

如果您启用整合的控件调查发现，这些字段会被移除，取而代之的是 `Compliance.SecurityControlId`。

`RecommendationUrl`

控件的修复信息的 URL。如果您启用整合的控件调查发现，该字段会被移除，取而代之的是 `Remediation.Recommendation.Url`。

`RelatedAWSResources:0/name`

与调查发现关联的资源的名称。

`RelatedAWSResource:0/type`

与控件关联的资源类型。

`StandardsControlArn`

控件的 ARN。如果您启用整合的控件调查发现，该字段会被移除。

`aws/securityhub/ProductName`

对于控件调查发现，产品名称为 Security Hub。

`aws/securityhub/CompanyName`

对于控件调查发现，公司名称为 AWS。

`aws/securityhub/annotation`

对控件所发现问题的描述。

`aws/securityhub/FindingId`

调查发现的标识符。

如果您启用整合的控件调查发现，该字段不会引用标准。

控件调查发现的严重性级别

分配给 Security Hub CSPM 控件的严重性指明该控件的重要性。对照的严重性决定了分配给对照调查发现的严重性标签。

严重性条件

控制的严重程度是根据对以下标准的评测来确定的：

- 威胁行为者利用与控制相关的配置弱点有多困难？ 难度取决于利用弱点执行威胁场景所需的复杂程度。
- 这种弱点导致你的 AWS 账户 资源受损的可能性有多大？ 您的资源泄露意味着您的数据 AWS 账户 或 AWS 基础架构的机密性、完整性或可用性在某种程度上受到损害。泄露的可能性表明威胁情景导致您的 AWS 服务 或资源中断或泄露的可能性有多大。

例如，考虑以下配置隐患：

- 用户访问密钥不是每 90 天轮换一次。
- IAM 根用户密钥存在。

对于攻击者来说，这两个隐患同样难以利用。在这两种情况下，攻击者都可以使用凭证盗窃或其他方法来获取用户密钥。然后，他们可以使用它以未经授权的方式访问您的资源。

但是，如果威胁行为者获取了根用户访问密钥，则受到损害的可能性会更高，因为这为他们提供了更大的访问权限。因此，根用户密钥漏洞的严重性更高。

严重性未考虑底层资源的重要程度。严重性是指与调查发现关联的资源的重要性级别。例如，与任务关键型应用程序关联的资源比与非生产测试关联的资源更重要。要获取资源重要性信息，请使用 AWS 安全调查结果格式 (ASFF) 的`Criticality`字段。

下表将漏洞利用的难度和受损的可能性映射到安全标签。

	极有可能受损	可能受损	不太可能受损	受损的可能性极小
非常容易被利用	重大	重大	高	中
有点容易被利用	重大	高	中	中
有点难以利用	高	中	中	低
很难被利用	中	中	低	低

严重性定义

严重性标签的定义如下：

严重——应立即修复问题以避免问题升级。

例如，开放的 S3 存储桶被视为具有“严重”严重性的调查发现。由于许多威胁行为者会扫描开放的 S3 存储桶，因此暴露的 S3 存储桶中的数据很可能会被其他人发现和访问。

一般而言，公开访问的资源被视为关键的安全问题。您应该以最紧迫的态度对待严重调查发现。您还应该考虑资源的重要程度。

高——该问题必须作为近期优先事项予以解决。

例如，如果默认 VPC 安全组对入站和出站流量开放，则其被视为高严重性。使用这种方法，威胁行为者很容易入侵 VPC。一旦资源进入 VPC，威胁行为者也有可能破坏或泄露资源。

Security Hub CSPM 建议您将高严重性调查发现视为近期优先事项。您应该立即采取补救措施。您还应该考虑资源的重要程度。

中度——该问题应作为中期优先事项加以解决。

例如，对传输中数据缺乏加密被认为是中等严重性的调查发现。它需要复杂的 man-in-the-middle攻击才能利用这个弱点。换句话说，这有点困难。如果威胁情景成功，某些数据可能会被泄露。

Security Hub CSPM 建议您尽早调查受影响的资源。您还应该考虑资源的重要程度。

低——无需针对问题执行任何操作。

例如，未能收集取证信息被视为严重性较低。这种控制可以帮助防止未来的受损，但是缺乏取证并不能直接导致受损。

您无需对低严重性调查发现立即采取操作，但是当您将这些调查发现与其他问题关联时，它们可以提供背景信息。

信息性：未找到任何配置漏洞。

换言之，状态为 PASSED、WARNING 或 NOT_AVAILABLE。

没有建议的操作。信息性调查发现可帮助客户证明其处于合规状态。

评估合规性状态和控件状态

AWS 安全调查结果格式的Compliance.Status字段描述了控制结果的结果。 AWS Security Hub CSPM 使用控制结果的合规性状态来确定总体控制状态。控件状态将在 Security Hub CSPM 控制台上控件的详细信息页面上显示。

评估 Security Hub CSPM 调查发现的合规性状态

为每个调查发现的合规性状态分配以下值之一：

- PASSED – 表示控件通过了调查发现的安全检查。这会自动将 Security Hub CSPM Workflow.Status 设置为 RESOLVED。
- FAILED – 表示控件未通过调查发现的安全检查。
- WARNING – 表示 Security Hub CSPM 无法确定资源是处于 PASSED 还是 FAILED 状态。例如，没有为相应的资源类型启用 AWS Config 资源记录。
- NOT_AVAILABLE— 表示无法完成检查，原因是服务器出现故障、资源已删除或 AWS Config 评估结果失败NOT_APPLICABLE。如果 AWS Config 评估结果为NOT_APPLICABLE，Security Hub CSPM 会自动将发现结果存档。

如果调查发现的合规性状态从 PASSED 更改为 FAILED、WARNING 或 NOT_AVAILABLE，并且 Workflow.Status 是 NOTIFIED 或 RESOLVED，则 Security Hub CSPM 会自动将 Workflow.Status 更改为 NEW。

如果您没有与控件对应的资源，Security Hub CSPM 会在账户级别生成 PASSED 调查发现。如果您有与控件对应的资源，但随后删除了该资源，Security Hub CSPM 会创建 NOT_AVAILABLE 调查发现并立即将其存档。18 小时后，您会收到一个 PASSED 调查发现，因为您不再拥有与该控件对应的资源。

从合规性状态获取控件状态

Security Hub CSPM 根据控件调查发现的合规性状态得出总体控件状态。在确定控件状态时，Security Hub CSPM 会忽略 RecordState 为 ARCHIVED 的调查发现和 Workflow.Status 为 SUPPRESSED 的调查发现。

为控件状态分配以下值之一：

- 通过 – 表示所有调查发现的合规性状态均为 PASSED。
- 未通过 – 表示至少一个调查发现的合规性状态为 FAILED。
- 未知 – 表示至少一个调查发现的合规性状态为 WARNING 或 NOT_AVAILABLE。如果没有调查发现，则合规性状态为 FAILED。
- 无数据：表示控件没有调查发现。例如，新启用的控件在 Security Hub CSPM 开始为其生成调查发现之前一直处于此状态。如果所有标准的状态为 SUPPRESSED 或在当前 AWS 区域中不可用，则控件也具有此状态。
- 已禁用 – 表示当前账户和区域中的控件已禁用。目前没有对当前账户和区域中的此控件进行安全检查。然而，已禁用控件的调查发现在禁用后最多 24 小时内可能仍有合规性状态的值。

对于管理员账户，控件状态反映了管理员账户和成员账户的控件状态。具体而言，如果控件在管理员账户或任何成员账户中有一个或多个失败的调查发现，则该控件的总体状态将显示为失败。如果您设置了聚合区域，则聚合区域中的控件状态将反映聚合区域和关联区域的控件状态。具体而言，如果控件在聚合区域或任何关联区域中有一个或多个失败的调查发现，则该控件的总体状态将显示为失败。

Security Hub CSPM 通常会在您首次访问 Security Hub CSPM 控制台上的摘要页面或安全标准页面后 30 分钟内生成初始控件状态。此外，必须配置 AWS Config 资源记录才能显示控件状态。首次生成控件状态后，Security Hub CSPM 会根据前 24 小时的调查发现每 24 小时更新一次控件状态。控件详细信息页面上的时间戳表示控件状态的上次更新时间。

> **Note**
>
> 首次启用控件后，最长可能需要 24 小时才能在中国地区和 AWS GovCloud (US) Region生成控件状态。

计算安全分数

在 Sec AWS urity Hub CSPM 控制台上，“摘要” 页面和 “控制” 页面显示所有已启用标准的安全分数摘要。在安全标准页面上，Security Hub CSPM 还会显示每个已启用标准的安全分数（介于 0-100% 之间）。

首次启用 Security Hub CSPM 时，Security Hub CSPM 会在您首次访问控制台上的摘要或安全标准页面 30 分钟内计算出摘要安全分数和标准安全分数。仅针对您访问控制台上的这些页面时启用的标准生成分数。此外，必须配置 AWS Config 资源记录才能显示分数。摘要安全评分是标准安全评分的平均值。要查看当前启用的标准列表，你可以使用 Security Hub CSPM API 的GetEnabledStandards操作。

首次生成分数后，Security Hub CSPM 每 24 小时更新一次安全分数。Security Hub CSPM 显示时间戳以指示安全分数上次更新的时间。请注意，在中国区域和 AWS GovCloud (US) Regions生成首次安全分数最多需要 24 小时。

如果您启用整合的控件调查发现，则最长可能需要 24 小时才能更新安全分数。此外，启用新的聚合区域或更新关联区域会重置现有的安全分数。Security Hub CSPM 最多可能需要 24 小时才能生成包含来自更新区域的数据的新安全分数。

计算安全分数的方法

安全分数表示通过的控件与已启用的控件的比例。分数显示为四舍五入到最接近的整数的百分比。

Security Hub CSPM 会计算所有已启用标准的摘要安全分数。Security Hub CSPM 还会计算每个已启用标准的安全分数。为了计算分数，启用的控件包括状态为通过、失败和未知的控件。状态为无数据的控件将排除在分数计算之外。

在计算控件状态时，Security Hub CSPM 会忽略已存档和隐藏的调查发现。这可能会影响安全分数。例如，如果您隐藏控件的所有失败的调查发现，则其状态将变为已通过，这反过来可以提高安全分数。有关控件状态的详细信息，请参阅 评估合规性状态和控件状态。

评分示例：

标准	已通过的控件	失败的控件	未知控件	标准分数
AWS 基础安全最佳实践 v1.0.0	168	22	0	88%
独联体 AWS 基金会基准测试 v1.4.0	8	29	0	22%
独联体 AWS 基金会基准测试 v1.2.0	6	35	0	15%
NIST 特别出版物 800-53 第 5 版	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

在计算摘要安全分数时，Security Hub CSPM 在各类标准中只计算每个控件一次。例如，如果您启用了一个适用于三个启用标准的控件，则出于评分目的，它仅算作一个启用的控件。

在此示例中，虽然跨已启用标准的已启用控件总数为 528 个，但出于评分目的，Security Hub CSPM 仅对每个唯一控件进行一次计数。唯一启用的控件的数量可能低于 528。如果我们假设唯一启用的控件的数量为 515，并且唯一通过的控件的数量为 357，则汇总分数为 69%。该分数的计算方法是将唯一通过的控件数量除以唯一启用的控件数量。

即使您在当前区域的账户中只启用了一个标准，摘要分数也可能与标准安全分数不同。如果您登录到管理员账户并且成员账户启用了其他标准或不同的标准，则可能会发生这种情况。如果您正在查看聚合区域的分数并且在链接的区域中启用了其他标准或不同的标准，也可能会发生这种情况。

管理员账户的安全评分

如果您登录了管理员账户，则摘要安全分数和标准分数会说明管理员账户和所有成员账户中的控件状态。

如果一个成员账户中的控件状态为失败，则管理员账户中的控件状态为失败，这会影响管理员账户的分数。

如果您已登录管理员账户并正在查看聚合区域的分数，则安全分数会考虑所有成员账户和所有关联区域中的控件状态。

安全分数（如果您已设置聚合区域）

如果您设置了聚合 AWS 区域，则摘要安全分数和标准分数将全部考虑控制状态 关联的地区。

即使在一个关联区域中，控件的状态也为失败，则其在聚合区域中的状态为 失败，这会影响聚合区域分数。

如果您已登录管理员账户并正在查看聚合区域的分数，则安全分数会考虑所有成员账户和所有关联区域中的控件状态。

Security Hub CSPM 中的控件类别

每个控件都被分配了一个类别。控件的类别反映了它应用于的安全功能。

类别值包含类别、类别内的子类别以及可选的子类别内的分类器。例如：

- 识别 > 清单
- 保护 > 数据保护 > 传输中数据加密

以下是对可用类别、子类别和分类器的描述。

识别

了解组织情况以管理系统、资产、数据和功能面临的网络安全风险。

库存

该服务是否实施了正确的资源标记策略？ 标记策略是否包含资源拥有者？

该服务使用哪些资源？ 该服务是否有权使用这些资源？

您是否知道批准的库存？ 例如，您是否使用诸如 Amazon S EC2 ystems Manager 和 Service Catalog 之类的服务？

日志记录

您是否已安全启用该服务的所有相关日志记录？ 日志文件的示例包括以下内容：

- Amazon VPC 流日志
- Elastic Load Balancing 访问日志
- 亚马逊 CloudFront 日志
- Amazon CloudWatch 日志
- Amazon Relational Database Service 日志

- 亚马逊 OpenSearch 服务慢速索引日志
- X-Ray 跟踪
- AWS Directory Service 日志
- AWS Config 物品
- 快照

保护

制定并实施适当的保护措施，以确保提供关键基础设施服务和安全编码实践。

安全访问管理

该服务是否在其 IAM 或资源策略中使用最低权限实践？

密码和密钥是否足够复杂？ 它们是否已适当轮换？

该服务是否使用多重身份验证（MFA）？

该服务是否避开根用户？

基于资源的策略是否允许公有访问？

安全网络配置

该服务是否避免公有和不安全的远程网络访问？

该服务是否 VPCs 正常使用？ 例如，是否需要作业才能运行 VPCs？

该服务是否已正确分割和隔离敏感资源？

数据保护

静态数据加密——该服务是否加密静态数据？

加密传输中数据——该服务是否对数据进行传输中加密？

数据完整性——该服务是否验证数据的完整性？

数据删除保护——该服务是否保护数据免遭意外删除？

数据管理/使用——您是否使用 Amazon Macie 等服务来跟踪敏感数据的位置？

API 保护

该服务是否 AWS PrivateLink 用于保护服务 API 操作？

保护性服务

是否有适当的保护性服务？ 它们是否提供了正确的覆盖范围？

保护性服务可帮助您转移针对该服务的攻击和破坏。中的保护性服务示例 AWS 包括 AWS Control Tower、、、Vanta AWS WAF AWS Shield Advanced、Secrets Manager、IAM Access Analyzer 和 AWS Resource Access Manager。

安全开发

您是否使用了安全编码实践？

您是否避免了诸如开放 Web 应用程序安全项目（OWASP）十大漏洞之类的漏洞？

Detect

制定并实施适当的活动，以识别网络安全事件的发生。

检测服务

是否有适当的检测服务？

它们是否提供了正确的覆盖范围？

AWS 检测服务的示例包括亚马逊 GuardDuty、Sec AWS urity Hub CSPM、Amazon Inspector、Amazon Detective AWS IoT Device Defender、Amazon CloudWatch Alarms 和。AWS Trusted Advisor

响应

制定并实施适当的活动，以便对检测到的网络安全事件采取措施。

响应措施

您是否能迅速对安全事件做出响应？

您现在是否有任何“严重”或“高”严重性的调查发现？

取证

您是否能够安全地获取服务的取证数据？ 例如，您是否获取与实际正面调查发现相关的 Amazon EBS 快照？

您是否设立了取证账户？

恢复

制定并实施适当的活动，以维护恢复能力计划，恢复因网络安全事件而受损的任何能力或服务。

恢复能力

服务配置是否支持正常故障转移、弹性扩展和高可用性？

您是否已创建备份？

查看 Security Hub CSPM 中的控件的详细信息

在 Security Hub CSPM 控制台的控件页面或标准详细信息页面上选择控件会让您进入控件详细信息页面。

控件详细信息页面的顶部指示控件状态。控件状态根据控件调查发现的合规性状态总结控件的性能。Security Hub CSPM 通常会在您首次访问 Security Hub CSPM 控制台上的摘要页面或安全标准页面后 30 分钟内生成初始控件状态。状态仅适用于您访问这些页面时启用的控件。

控件详细信息页面还细分了过去 24 小时内控件调查发现的合规性状态。有关控件状态和合规性状态的更多信息，请参阅评估合规性状态和控件状态。

AWS Config 必须配置资源记录才能显示控制状态。首次生成控件状态后，Security Hub CSPM 会根据前 24 小时的调查发现每 24 小时更新一次控件状态。

管理员账户可以看到管理员账户和成员账户的聚合控件状态。如果您设置了聚合区域，则控件状态包括所有关联区域的调查发现。有关控件状态的详细信息，请参阅 the section called “合规性状态和控件状态”。

您还可以在控件详细信息页面上启用或禁用控件。

> **Note**
>
> 启用控件后，最长可能需要 24 小时才能在中国地区和 AWS GovCloud (US) Regions生成首次控件状态。

标准和要求选项卡列出了可启用控件的标准以及来自不同合规框架的与该控件相关的要求。

检查选项卡列出了过去 24 小时内控件的活跃调查发现。控件调查发现是 Security Hub CSPM 针对控件运行安全检查时生成和更新的。此选项卡上的列表不包括存档的调查发现。

对于每项调查发现，该列表都提供对调查发现详细信息的访问权限，例如合规性状态和相关资源。您还可以设置每个调查发现的工作流状态，并将调查发现发送到自定义操作。有关更多信息，请参阅 查看和管理控件调查发现。

查看控件的详细信息

选择首选访问方法，然后按照以下步骤查看控件的详细信息。详细信息适用于当前账户和地区，包括以下内容：

- 控件的标题和描述。
- 指向失败的控件调查发现的修复指导的链接。
- 控件的严重性。
- 控件的状态。

在控制台上，您还可以查看控件的最新调查发现列表。要以编程方式执行此操作，您可以使用 Security Hub CSPM API 的 GetFindings 操作。

Security Hub CSPM console

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中选择控件。
3. 选择控件。

Security Hub CSPM API

1. 运行ListSecurityControlDefinitions，并提供一个或多个标准 ARNs 以获取该标准 IDs的控制列表。要获得标准 ARNs，请运行DescribeStandards。如果你不提供标准 ARN，则此 API 会返回所有 Security Hub CSPM 控制权。 IDs此 API 返回与标准无关的安全控制 IDs，而不是这些功能发布之前存在的基于标准 IDs 的控件。

   请求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 运行BatchGetSecurityControls以获取有关当前 AWS 账户 和中一个或多个控件的详细信息 AWS 区域。

   请求示例：

```
{
    "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. 运行list-security-control-definitions命令，并提供一个或多个标准 ARNs 以获取控件列表 IDs。要获得标准 ARNs，请运行describe-standards命令。如果您未提供标准 ARN，则此命令将返回所有 Security Hub CSPM 控件。 IDs此命令返回与标准无关的安全控制 IDs，而不是这些功能发布之前存在的基于标准 IDs 的控件。

```
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. 运行 batch-get-security-controls 命令以获取有关当前 AWS 账户 和 AWS 区域中一个或多个控件的详细信息。

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Security Hub CSPM 中的筛选和排序控件

在 Sec AWS urity Hub CSPM 控制台上，您可以使用 “控件” 页面查看当前版本中可用的控件表。AWS 区域聚合区域除外。如果您配置了某个聚合区域并登录到该区域，控制台将显示聚合区域或者一个或多个关联区域中可用的控件。

要关注控件的特定子集，您可以对控件表进行排序和筛选。通过表旁边的筛选依据选项，您可以快速专注于以下特定子集：

- 所有已启用控件，在至少一个已启用标准中启用的控件。
- 所有已禁用控件，在所有标准中禁用的控件。

- 所有具有特定控件状态（例如失败）的已启用控件。无数据选项仅显示那些当前没有调查发现的控件。有关控件状态的信息，请参阅评估合规性状态和控件状态。

除了筛选依据选项外，您可以通过在表上方的筛选条件控件框中输入筛选条件来对表进行筛选。例如，您可以按控件 ID 或严重性进行筛选。

默认情况下，状态为失败的控件会首先按严重性降序列出。您可以通过选择不同的列标题来更改排序顺序。

> **Tip**
>
> 如果您有基于控件调查发现的自动化工作流，我们建议使用 `SecurityControlId` 或 `SecurityControlArn` ASFF 字段作为筛选条件，而不是 `Title` 或 `Description` 字段。后面的字段偶尔会发生变化，而控件 ID 和 ARN 是静态标识符。

如果您登录了 Security Hub CSPM 管理员账户，则已启用控件包含在至少一个成员账户中启用的控件。如果您配置了聚合区域，则已启用控件将包含在至少一个关联区域中启用的控件。

如果您选择了某个已启用控件旁边的选项，则将显示一个面板，显示当前启用该控件的标准。您还可以查看当前禁用该控件的标准。在此面板中，您可以在所有标准中禁用控件。有关更多信息，请参阅 在 Security Hub CSPM 中禁用控件。对于管理员账户，面板中的信息反映了所有成员账户的设置。

要以编程方式检索控件列表，您可以使用 Security Hub CSPM API 的 ListSecurityControlDefinitions 操作。要检索各个控件的详细信息，请使用 BatchGetSecurityControls 操作。

了解 Security Hub CSPM 中的控件参数

Sec AWS urity Hub CSPM 中的某些控件使用的参数会影响控件的评估方式。通常，此类控件是根据 Security Hub CSPM 定义的默认参数值进行评估的。但是，对于这些控件的子集，您可以修改参数值。当您修改控件参数值时，Security Hub CSPM 会开始根据您指定的值评估控件。如果控件底层的资源满足自定义值，Security Hub CSPM 会生成 `PASSED` 调查发现。如果资源不满足自定义值，Security Hub CSPM 会生成 `FAILED` 调查发现。

通过自定义控件参数，您可以优化 Security Hub CSPM 推荐和监控的安全最佳实践，使其符合您的业务需求和安全期望。您可以自定义控件的一个或多个参数以获得符合您安全需求的调查发现，而不是隐藏控件的调查发现。

以下是一些修改控件参数和设置自定义值的示例用例：

- [CloudWatch.16]- CloudWatch 日志组应在指定的时间段内保留

  您可以指定保留期限。
- [IAM.7]—IAM 用户的密码策略应具有可靠的配置

  您可以指定与密码强度相关的参数。
- [EC2.18]-安全组应只允许授权端口不受限制的传入流量

  您可以指定哪些端口有权允许不受限制的传入流量。
- [Lambda.5]—VPC Lambda 函数应在多个可用区内运行

  您可以指定生成通过的调查发现的可用区的最小数量。

本节介绍修改控件参数时的注意事项。

修改控件参数值的影响

更改参数值后，还会触发新的安全检查，根据新值对控件进行评估。然后，Security Hub CSPM 会根据新值生成新的控件调查发现。在定期更新控件调查发现期间，Security Hub CSPM 也会使用新的参数值。如果您更改了控件的参数值，但尚未启用任何包含该控件的标准，则 Security Hub CSPM 不会使用新值进行任何安全检查。您必须至少启用一个相关标准，Security Hub CSPM 才能根据新的参数值评估控件。

一个控件可以有一个或多个可自定义的参数。控件参数可能具有的数据类型如下：

- 布尔值
- 双精度
- 枚举
- EnumList
- 整数
- IntegerList
- 字符串
- StringList

自定义参数值会应用于您启用的各种标准。您无法为当前区域不支持的控件自定义参数。有关各个控件的区域限制列表，请参阅对 Security Hub CSPM 控件的区域限制。

对于某些控件，可接受的参数值必须介于指定范围之内才有效。在这些情况下，Security Hub CSPM 会提供可接受的范围。

Security Hub CSPM 会选择默认参数值，并且可能偶尔会对其进行更新。自定义控制参数后，除非您对其值进行更改，否则它会一直为您为该参数指定的值。也就是说，即使该参数的自定义值与 Security Hub CSPM 定义的当前默认值匹配，该参数也不会再跟踪对默认 Security Hub CSPM 值的更新。以下是控件 [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订的示例：

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

在前面的示例中，`daysToExpiration` 参数的自定义值为 `30`。此参数的当前默认值也可以是 `30`。如果 Security Hub CSPM 将默认值更改为 `14`，则此示例中的参数将不会跟踪该更改。它将保留值 `30`。

如果要跟踪对某参数的默认 Security Hub CSPM 值的更新，请将 `ValueType` 字段设置为 `DEFAULT`，而不是 `CUSTOM`。有关更多信息，请参阅 在一个账户和区域中恢复为默认参数值。

支持自定义参数的控件

有关支持自定义参数的安全控件列表，请参阅 Security Hub CSPM 控制台的控件页面或 Security Hub CSPM 控件参考。要以编程方式检索此列表，您可以使用 ListSecurityControlDefinitions 操作。在响应中，`CustomizableProperties` 对象指示哪些控件支持可自定义的参数。

查看当前控件参数值

在修改控件参数之前，了解其当前值会很有用。

您可以查看账户中各个控制参数的当前值。如果您使用集中配置，则委派的 S AWS ecurity Hub CSPM 管理员还可以查看配置策略中指定的参数值。

选择您的首选方法，然后按照以下步骤查看当前控制参数值。

Security Hub CSPM console

查看当前控件参数值（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择控件。选择控件。
3. 选择参数选项卡。此选项卡显示控件的当前参数值。

Security Hub CSPM API

查看当前控件参数值（API）

调用 BatchGetSecurityControlsAPI，并提供一个或多个安全控制 IDs 或 ARNs。响应中的 `Parameters` 对象显示指定控件的当前参数值。

例如，以下 AWS CLI 命令显示`APIGatway.1`、`CloudWatch.15`、和的当前参数值`IAM.7`。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

选择您的首选方法以查看中心配置策略中的当前参数值。

Security Hub CSPM console

查看配置策略中的当前控件参数值（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 在策略选项卡上，选择配置策略，然后选择查看详细信息。然后将显示策略详细信息，包括当前参数值。

Security Hub CSPM API

查看配置策略中的当前控件参数值（API）

1. 从主区域的委派管理员账户调用 GetConfigurationPolicy API。
2. 提供您要查看其详细信息的配置策略的 ARN 或 ID。响应包含当前参数值。

例如，以下 AWS CLI 命令检索指定配置策略中的当前控制参数值。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

控件调查发现还包含控件参数的当前值。在 AWS 安全调查结果格式 (ASFF)中，这些值出现在 Compliance 对象的 Parameters 字段中。要在 Security Hub CSPM 上查看调查发现，在导航窗格中选择调查发现。要以编程方式查看调查发现，请使用 Security Hub CSPM API 的 GetFindings 操作。

自定义控件参数值

根据您是否在 Sec AWS urity Hub CSPM 中使用中央配置，自定义控制参数的说明会有所不同。中央配置是一项功能，委派的 Security Hub CSPM 管理员可以使用它来跨 AWS 区域账户和组织单位配置 Security Hub CSPM 功能（ ）。OUs

如果您的组织使用中心配置，则委派管理员可以创建包含自定义控制参数的配置策略。这些政策可以与集中管理的成员账户相关联 OUs，并在您所在的地区和所有关联的地区生效。委派管理员还可以将一个或多个账户指定为自行管理，这允许账户所有者在每个区域中单独配置自己的参数。如果您的组织不使用中心配置，则必须在每个账户和区域中分别自定义控制参数。

我们建议使用中心配置，因为它允许您在组织的不同部门之间调整控制参数值。例如，您的所有测试账户都可能使用特定的参数值，而所有生产账户使用的可能是不同的值。

自定义多个账户和区域中的控件参数

如果您是使用中心配置的组织的 Security Hub CSPM 委派管理员，请选择您喜欢的方法，然后按照步骤自定义多个账户和区域的控件参数。

Security Hub CSPM console

自定义多个账户和区域中的控件参数值（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

   确保您已登录到主区域。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。
4. 要创建包含自定义参数的新配置策略，请选择创建策略。要在现有配置策略中指定自定义参数，请选择策略，然后选择编辑。

   创建具有自定义控件参数值的新的配置策略

   1. 在自定义策略部分，选择要启用的安全标准和控件。
   2. 选择自定义控制参数。
   3. 选择一个控件，然后为一个或多个参数指定自定义值。
   4. 要自定义更多控件的参数，请选择自定义其他控件。
   5. 在账户部分，选择要应用策略的账户或 OUs 账户。
   6. 选择下一步。
   7. 选择创建策略并应用。在您的主区域和所有关联区域中，此操作将覆盖与 OUs 该配置策略关联的账户的现有配置设置。账户和 OUs 可以通过直接应用或从父级继承来与配置策略相关联。

   自定义现有配置策略中的控件参数值

   1. 在控制部分的自定义策略下，指定所需的新自定义参数值。
   2. 如果这是您第一次自定义此策略中的控制参数，请选择自定义控制参数，然后选择要自定义的控件。要自定义更多控件的参数，请选择自定义其他控件。
   3. 在“帐户”部分中，验证要应用策略的账户或 OUs 账户。
   4. 选择下一步。
   5. 再次检查您的更改，确认正确无误。完成后，选择保存策略并应用。在您的主区域和所有关联区域中，此操作将覆盖与 OUs 该配置策略关联的账户的现有配置设置。账户和 OUs 可以通过直接应用或从父级继承来与配置策略相关联。

自定义多个账户和区域中的控件参数值（API）

创建具有自定义控件参数值的新的配置策略

1. 从主区域的委派管理员账户调用 CreateConfigurationPolicy API。
2. 对于 SecurityControlCustomParameters 对象，请提供要自定义的每个控件的标识符。
3. 对于 Parameters 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 CUSTOM 作为 ValueType 的值。对于 Value，请提供参数的数据类型和自定义值。当 ValueType 的值为 CUSTOM 时，该 Value 字段不能为空。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过调用 GetSecurityControlDefinition API，您可以找到控件支持的参数、数据类型和有效值。

自定义现有配置策略中的控件参数值

1. 从主区域的委派管理员账户调用 UpdateConfigurationPolicy API。
2. 对于 Identifier 字段，提供要更新配置策略的 Amazon 资源名称（ARN）或 ID。
3. 对于 SecurityControlCustomParameters 对象，请提供要自定义的每个控件的标识符。
4. 对于 Parameters 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 CUSTOM 作为 ValueType 的值。对于 Value，请提供参数的数据类型和自定义值。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过调用 GetSecurityControlDefinition API，您可以找到控件支持的参数、数据类型和有效值。

例如，以下 AWS CLI 命令使用daysToExpiration参数的自定义值创建新的配置策略ACM.1。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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}}}]}}}'
```

在单个账户和区域中自定义控制参数

如果您不使用中心配置，或拥有自行管理账户，则仅可以一次在一个区域内为账户自定义控件参数。

选择您的首选方法，然后按照步骤自定义控制参数。您的更改仅适用于当前区域中的账户。要自定义其他区域中的控制参数，请在要自定义参数的每个其他账户和区域中重复以下步骤。同一个控件可以在不同的区域中使用不同的参数值。

Security Hub CSPM console

自定义一个账户和区域中的控件参数值（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择控件。在表中，选择支持自定义参数且想要更改其参数的控件。自定义参数列指示哪些控件支持自定义参数。
3. 在控件的详细信息页面上，选择参数选项卡，然后选择编辑。
4. 指定所需的参数值。
5. 或者，在更改原因部分中，选择自定义参数的原因。
6. 选择保存。

Security Hub CSPM API

在一个账户和区域中自定义控件参数值（API）

1. 调用 UpdateSecurityControl API。
2. 对于 `SecurityControlId`，请提供要自定义的控件的 ID。
3. 对于 `Parameters` 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 `CUSTOM` 作为 `ValueType` 的值。对于 `Value`，请提供参数的数据类型和自定义值。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过调用 GetSecurityControlDefinition API，您可以找到控件支持的参数、数据类型和有效值。
4. （可选）对于 `LastUpdateReason`，提供自定义控制参数的理由。

例如，以下 AWS CLI 命令为的daysToExpiration参数定义了自定义值ACM.1。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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"
```

恢复为默认控制参数值

控制参数可以具有 Sec AWS urity Hub CSPM 定义的默认值。Security Hub CSPM 偶尔也会更新参数的默认值，以反映不断演变的安全最佳实践。如果您还没有为控制参数指定自定义值，则该控件会自动跟踪这些更新并使用新的默认值。

您可以恢复为使用控件的默认参数值。恢复说明取决于您是否在 Security Hub CSPM 中使用中心配置。中央配置是一项功能，委派的 Security Hub CSPM 管理员可以使用它来跨 AWS 区域账户和组织单位配置 Security Hub CSPM 功能（ ）。OUs

> **Note**
>
> 并非所有控件参数都具有默认 Security Hub CSPM 值。在此类情况下，当 ValueType 设置为 DEFAULT 时，没有 Security Hub CSPM 可使用的特定默认值。相反，如果没有自定义值，Security Hub CSPM 将忽略该参数。

在多个账户和区域中恢复为默认控件参数

如果您使用中央配置，则可以恢复多个集中管理账户以及主区域和关联区域 OUs 中的控制参数。

选择您的首选方法，然后按照以下步骤，使用中心配置在多个账户和区域中恢复为默认参数值。

Security Hub CSPM console

恢复多个账户和区域中的默认控件参数值（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

使用主区域中的 Security Hub CSPM 委派管理员账户的凭证登录。

2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。
4. 选择一个策略，然后选择编辑。
5. 在自定义策略下，控件部分显示了您为其指定自定义参数的控件列表。
6. 找到具有一个或多个要恢复的参数值的控件。然后，选择删除以恢复为默认值。
7. 在“帐户”部分中，验证要应用策略的账户或 OUs 账户。
8. 选择下一步。
9. 再次检查您的更改，确认正确无误。完成后，选择保存策略并应用。在您的主区域和所有关联区域中，此操作将覆盖与 OUs 该配置策略关联的账户的现有配置设置。账户和 OUs 可以通过直接应用或从父级继承来与配置策略相关联。

Security Hub CSPM API

恢复多个账户和区域中的默认控件参数值（API）

1. 从主区域的委派管理员账户调用 UpdateConfigurationPolicy API。
2. 对于 `Identifier` 字段，提供要更新策略的 Amazon 资源名称（ARN）或 ID。
3. 对于 `SecurityControlCustomParameters` 对象，请提供要为其恢复一个或多个参数的每个控件的标识符。
4. 在 `Parameters` 对象中，为要恢复的每个参数提供 `DEFAULT` 作为 `ValueType` 字段的值。当 `ValueType` 设置为 `DEFAULT` 时，无需为该 `Value` 字段提供值。如果您的请求中包含了值，Security Hub CSPM 会将其忽略。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。

> **Warning**
>
> 如果在 `SecurityControlCustomParameters` 字段中省略控件对象，Security Hub CSPM 会将该控件的所有自定义参数恢复为其默认值。`SecurityControlCustomParameters` 的列表完全为空会将所有控件的自定义参数恢复为其默认值。

例如，以下 AWS CLI 命令将的daysToExpiration控制参数恢复ACM.1为其在指定配置策略中的默认值。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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"}}}]}}'
```

在一个账户和区域中恢复为默认参数值

如果您不使用中心配置或拥有自行管理账户，则可以恢复为每次在一个区域中使用账户的默认参数值。

选择您的首选方法，然后按照以下步骤在单个区域中将您的账户恢复为默认参数值。要在其他区域中恢复为默认参数值，请在每个其他区域中重复这些步骤。

> **Note**
>
> 如果您禁用 Security Hub CSPM，则您的自定义控制参数将被重置。如果您将来再次启用 Security Hub CSPM，则所有控件最开始都将使用默认参数值。

Security Hub CSPM console

在一个账户和区域中恢复默认控件参数值（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择控件。选择要恢复为默认值的参数。

3. 在 Parameters 选项卡上，选择控制参数旁边的自定义。然后，选择删除自定义。此参数现在使用默认 Security Hub CSPM 值，并会跟踪未来的默认值更新。
4. 对要恢复的每个参数值重复上述步骤。

Security Hub CSPM API

在一个账户和区域中恢复默认控件参数值（API）

1. 调用 UpdateSecurityControl API。
2. 对于 SecurityControlId，请提供要恢复其参数的控件的 ARN 或 ID。
3. 在 Parameters 对象中，为要恢复的每个参数提供 DEFAULT 作为 ValueType 字段的值。当 ValueType 设置为 DEFAULT 时，无需为该 Value 字段提供值。如果您的请求中包含了值，Security Hub CSPM 会将其忽略。
4. （可选）对于 LastUpdateReason，提供恢复为默认参数值的原因。

例如，以下 AWS CLI 命令将的daysToExpiration控制参数恢复ACM.1为其默认值。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

检查控件参数更改的状态

尝试自定义控件参数或恢复为默认值时，可以验证所需的更改是否已生效。这有助于确保控件按预期运行，并达到预期的安全值。如果参数更新失败，Security Hub CSPM 会保留该参数的当前值。

要验证参数更新是否成功，您可以在 Security Hub CSPM 控制台上查看控件的详细信息。在控制台中，选择导航窗格中的控件。然后，选择一个控件以显示其详细信息。参数选项卡将显示参数更改的状态。

以编程方式执行操作时，如果您更新参数的请求有效，则作为对 BatchGetSecurityControls 操作的响应，字段 UpdateStatus 的值将为 UPDATING。这意味着更新有效，但可能并非所有调查发现都包含

更新后的参数值。当 UpdateState 的值更改为 READY 时，Security Hub CSPM 在对控件运行安全检查时使用更新后的控件参数值。调查发现包含更新后的参数值。

该 UpdateSecurityControl 操作返回无效参数值的 InvalidInputException 响应。该响应提供关于失败原因的其他详细信息。例如，您指定的值可能超出了参数的有效范围。或者，您指定的值可能没有使用正确的数据类型。请使用有效的输入再次提交您的请求。

如果您尝试更新参数值时出现内部故障，如果您已启用，Security Hub CSPM 会自动重试。 AWS Config 有关更多信息，请参阅 启用和配置前的注意事项 AWS Config。

在 Security Hub CSPM 中查看和管理控件调查发现

控件详细信息页面显示控件的活动调查发现列表。该列表不包括已存档的调查发现。

控件详细信息页面支持跨区域聚合。如果您设置了聚合区域，则控件详细信息页面上的控件状态和安全检查列表将包括来自所有链接的 AWS 区域检查。

该列表提供了对结果进行筛选和排序的工具，这样您就可以先将注意力集中在更紧急的发现上。调查发现可能包含指向相关服务控制台中资源详细信息的链接。对于基于 AWS Config 规则的控件，您可以查看有关规则的详细信息。

您还可以使用 S AWS ecurity Hub CSPM API 来检索发现结果列表并查找详细信息。

有关更多信息，请参阅 查看调查发现的详细信息和历史记录。

为了反映对控件调查发现的调查的当前状态，您可以设置工作流状态。有关更多信息，请参阅 the section called “设置调查发现的工作流状态”。

您也可以将选定的 Security Hub CSPM 调查结果发送到亚马逊的自定义操作。 EventBridge有关更多信息，请参阅 the section called “将结果发送到自定义操作”。

主题

- 对控件调查发现进行筛选和排序
- 控件调查发现示例

对控件调查发现进行筛选和排序

从 Sec AWS urity Hub CSPM 控制台的 “控件” 页面或标准的详细信息页面中选择控件将进入控件详细信息页面。

控件详细信息页面显示控件的名称和描述、总体控件状态以及过去 24 小时内该控件的安全检查明细。

使用控件检查列表旁边筛选依据选项，可以快速关注具有特定工作流状态或合规性状态的调查发现。

除了“筛选依据”选项外，您还可以使用添加筛选器框按其他字段（例如 AWS 账户 ID 或资源 ID）筛选检查列表。

默认情况下，合规性状态为通过的调查发现列在最前面。您可以通过在列标题中选择其他选项更改默认排序方式。

在控件详细信息页面上，您可以选择下载，将控件调查发现的当前页面下载为 .csv 文件。

如果您筛选调查发现列表，则下载内容仅包含与筛选条件匹配的控件。如果您从列表中选择特定的调查发现，则下载内容仅包含选定的调查发现。

有关筛选调查发现的更多信息，请参阅 在 Security Hub CSPM 中筛选调查发现。

控件调查发现示例

以下示例以 AWS 安全调查结果格式 (ASFF) 提供了 Security Hub CSPM 控制结果的 AWS 示例。控件调查发现的内容会有所不同，具体取决于您是否启用了整合的控件调查发现。

如果您启用整合的控件调查发现，则即使该控件适用于多个启用的标准，Security Hub CSPM 也会为该控件生成一个调查发现。如果不启用此功能，Security Hub CSPM 会为控件适用的每个已启用标准生成单独的控件调查发现。例如，如果启用了两个标准，并且一个控件适用于这两个标准，则您会收到两个针对该控件的单独调查发现，每个标准一个。如果启用整合的控件调查发现，则只会收到控件的一个调查发现。有关更多信息，请参阅 整合的控件调查发现。

本页上的示例提供了这两个场景的示例。示例包括：禁用整合的控件调查发现时各个 Security Hub CSPM 标准的控件调查发现，以及启用整合的控件调查发现时多个 Security Hub CSPM 标准的控件调查发现。

控件调查发现示例

- AWS 基础安全最佳实践标准的调查结果示例
- CIS AWS 基金会基准测试 v5.0.0 的样本发现
- CIS AWS 基金会基准测试 v3.0.0 的样本发现
- CIS AWS 基金会基准测试 v1.4.0 的样本发现
- CIS AWS 基金会基准测试 v1.2.0 的样本发现
- NIST SP 800-53 修订版 5 标准的调查发现示例
- NIST SP 800-171 修订版 2 标准的调查发现示例
- 支付卡行业数据安全标准 v3.2.1 的调查发现示例

- AWS 资源标签标准的调查结果示例
- AWS Control Tower 服务托管标准的调查结果示例
- 多个标准的整合的控件调查发现示例

> **Note**
>
> 控件调查发现将参考中国地区和 AWS GovCloud (US) 区域的不同字段和值。有关更多信息，请参阅 合并对 ASFF 字段和值的影响。

AWS 基础安全最佳实践标准的调查结果示例

以下示例提供了适用于 AWS 基础安全最佳实践（FSBP）标准的控件的调查发现示例。在此示例中，整合的控件调查发现处于禁用状态。


```
{
  "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": "This AWS control checks whether AWS CloudTrail is 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 the AWS Security
 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",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources: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/AWS MacieTrail-
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/AWS MacieTrail-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"
    ]
  }
}
```

CIS AWS 基金会基准测试 v5.0.0 的样本发现

以下示例提供了一个适用于 CIS AWS 基金会基准 v5.0.0 的控件的发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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/CIS AWS
 Foundations Benchmark"
  ],
  "UpdatedAt": "2025-10-14T05:22:38.671Z",
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW"
}
```


CIS AWS 基金会基准测试 v3.0.0 的样本发现

以下示例提供了一个适用于 CIS AWS 基金会基准 v3.0.0 的控件的发现示例。在此示例中，整合的控件调查发现处于禁用状态。


```
{
  "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/CIS AWS
 Foundations 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 the AWS Security
 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/CIS AWS
 Foundations Benchmark"
    ]
```

```
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

CIS AWS 基金会基准测试 v1.4.0 的样本发现

以下示例提供了一个适用于CIS AWS 基金会基准测试v1.4.0的控件的发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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/CIS AWS
 Foundations 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 CloudTrail is a web service that records AWS API 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) and AWS 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 the AWS Security
 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/AWS MacieTrail-
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/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations 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/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

CIS AWS 基金会基准测试 v1.2.0 的样本发现

以下示例提供了一个适用于CIS AWS 基金会基准测试v1.2.0的控件的发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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/CIS AWS
 Foundations 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 the AWS Security
 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",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources: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/AWS MacieTrail-
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/AWS MacieTrail-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/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

NIST SP 800-53 修订版 5 标准的调查发现示例

以下示例提供了一个适用于 NIST SP 800-53 修订版 5 标准的控件的调查发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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": "This AWS control checks whether AWS CloudTrail is 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 the AWS Security 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/AWS MacieTrail-
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/AWS MacieTrail-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"
}
```

NIST SP 800-171 修订版 2 标准的调查发现示例

以下示例提供了一个适用于 NIST SP 800-171 修订版 2 标准的控件的调查发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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 whether AWS CloudTrail is 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 the AWS Security
 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"
}
```

支付卡行业数据安全标准 v3.2.1 的调查发现示例

以下示例提供了一个适用于支付卡行业数据安全标准（PCI DSS）v3.2.1 的控件的调查发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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 using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is 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 the AWS Security
 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",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources: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/AWS MacieTrail-
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/AWS MacieTrail-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"
    ]
  }
}
```

AWS 资源标签标准的调查结果示例

以下示例提供了一个适用于 AWS 资源标注标准的控件的调查发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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 the AWS Security
 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"
}
```

AWS Control Tower 服务托管标准的调查结果示例

以下示例提供了一个适用于 AWS Control Tower 服务托管标准的控件的调查发现示例。在此示例中，整合的控件调查发现处于禁用状态。

```
{
  "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": "This AWS control checks whether AWS CloudTrail is 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 the AWS Security
 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"
    ]
  }
}
```

多个标准的整合的控件调查发现示例

以下示例提供了一个适用于多个已启用标准的控件的调查发现示例。在此示例中，整合的控件调查发现处于启用状态。

```
{
  "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 whether AWS CloudTrail is 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 the AWS Security
 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"
}
```


了解 Security Hub CSPM 中的集成

AWS Security Hub CSPM 可以从多个 AWS 服务 受支持的第三方 AWS Partner Network 安全解决方案中提取安全发现。这些集成可以帮助您全面了解整个 AWS 环境的安全性和合规性。Security Hub CSPM 从集成解决方案中提取调查结果，并将其转换为 AWS 安全调查结果格式 (ASFF)。

> **Important**
>
> 对于受支持的产品 AWS 和第三方产品集成，Security Hub CSPM 会接收并整合只有在您为自己启用 Security Hub CSPM 后才生成的调查结果。 AWS 账户该服务不会以追溯方式接收和整合在您启用 Security Hub CSPM 之前生成的安全调查发现。

Security Hub CSPM 控制台的集成页面提供对可用 AWS 和第三方产品集成的访问权限。Security Hub CSPM API 还包含用于管理集成的操作。

可能并非所有集成都可用 AWS 区域。如果某项集成在您当前登录到 Security Hub CSPM 控制台的区域中不受支持，则不会显示在控制台的集成页面上。有关在中国和地区可用的集成列表 AWS GovCloud (US) Regions，请参阅。按区域划分的集成可用性

除了内置的第三方集成外，您还可以将自定义安全产品与 Security Hub CSPM 集成。 AWS 服务 然后，您可以使用 Security Hub CSPM API 将这些产品的调查发现发送到 Security Hub CSPM。您还可以使用 API 更新 Security Hub CSPM 从自定义安全产品收到的现有调查发现。

主题

- 查看 Security Hub CSPM 集成列表
- 启用来自 Security Hub CSPM 集成的调查发现流
- 禁用来自 Security Hub CSPM 集成的调查发现流
- 查看来自 Security Hub CSPM 集成的调查发现
- AWS 服务 与 Security Hub CSPM 集成
- Third-party 与 Security Hub CSPM 的产品集成
- 将 Security Hub CSPM 与自定义产品集成

查看 Security Hub CSPM 集成列表

选择您喜欢的方法，然后按照以下步骤在 AWS Security Hub CSPM 中查看集成列表或有关特定集成的详细信息。

Security Hub CSPM console

查看集成选项和详细信息（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在 Security Hub CSPM 导航窗格中，选择集成。

在集成页面上，先列出与其他 AWS 服务 的集成，后面列出与第三方产品的集成。

对于每个集成，集成页面提供了以下信息：

- 公司的名称
- 产品的名称
- 集成的描述
- 集成适用于的类别
- 启用集成的方式
- 集成的当前状态

您可以通过在以下字段中输入文本来筛选列表。

- 公司名称
- Product name
- 集成描述
- 类别

Security Hub CSPM API

查看集成选项和详细信息（API）

要获取集成列表，请使用 DescribeProducts 操作。如果您使用的是 AWS CLI，请运行describe-products命令。

要检索特定产品集成的详细信息，请使用 `ProductArn` 参数指定集成的 Amazon 资源名称（ARN）。

例如，以下 AWS CLI 命令检索有关 Security Hub CSPM 与 3CoreSec 集成的详细信息。

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

启用来自 Security Hub CSPM 集成的调查发现流

在 Sec AWS urity Hub CSPM 控制台的集成页面上，您可以看到启用每个集成所需的步骤。

对于与其他服务的大部分集成 AWS 服务，启用集成的唯一步骤就是启用其他服务。集成信息包含指向其他服务主页的链接。在启用另一项服务时，将自动创建并应用资源级权限，从而使 Security Hub CSPM 能够收到来自服务的调查发现。

对于第三方产品集成，您可能需要从购买集成 AWS Marketplace，然后配置集成。集成信息提供了用于完成这些任务的链接。

如果产品有多个版本可供选择 AWS Marketplace，请选择要订阅的版本，然后选择 “继续订阅”。例如，有些产品提供标准版本和 AWS GovCloud (US) 版本。

启用产品集成时，将向该产品订阅自动附加资源策略。此资源策略定义 Security Hub CSPM 从该产品接收调查发现所需的权限。

在完成启用集成的任何初步步骤后，您可以禁用并重新启用来自该集成的调查发现流。在集成页面上，对于发送调查发现的集成，状态信息指示您当前是否正在接受调查发现。

Security Hub CSPM console

启用来自集成的调查发现流（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在 Security Hub CSPM 导航窗格中，选择集成。
3. 对于发送调查发现的集成，状态信息指示 Security Hub CSPM 当前是否正在接受来自该集成的调查发现。
4. 选择接受调查发现。

Security Hub CSPM API

使用 EnableImportFindingsForProduct 操作。如果您使用的是 AWS CLI，请运行enable-import-findings-for-product命令。要允许 Security Hub 接收来自集成的调查发现，您需要产品 ARN。要获

取可用集成的 ARN，请使用 DescribeProducts 操作。如果你使用的是 AWS CLI，请运行describe-products。

例如，以下 AWS CLI 命令使 Security Hub CSPM 能够接收来自 CrowdStrike Falcon 集成的调查结果。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

禁用来自 Security Hub CSPM 集成的调查发现流

选择您的首选方法，然后按照以下步骤禁用 Sec AWS urity Hub CSPM 集成的发现流。

Security Hub CSPM console

禁用来自集成的调查发现流（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在 Security Hub CSPM 导航窗格中，选择集成。
3. 对于发送调查发现的集成，状态信息指示 Security Hub CSPM 当前是否正在接受来自该集成的调查发现。
4. 选择停止接受调查发现。

Security Hub CSPM API

使用 DisableImportFindingsForProduct 操作。如果您使用的是 AWS CLI，请运行disable-import-findings-for-product命令。要禁用来自集成的调查发现流，您需要使用已启用的集成的订阅 ARN。要获取订阅 ARN，请使用 ListEnabledProductsForImport 操作。如果你使用的是 AWS CLI，请运行list-enabled-products-for-import。

例如，以下 AWS CLI 命令禁止将结果从 Falcon 集成流向 Security Hub CSPM。 CrowdStrike 此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

查看来自 Security Hub CSPM 集成的调查发现

当你开始接受 Sec AWS urity Hub CSPM 集成的结果时，Security Hub CSPM 控制台的 “集成” 页面会将集成的状态显示为 “正在接受调查结果”。要查看来自集成的调查发现列表，请选择查看调查发现。

结果列表显示了工作流状态为 `NEW` 或 `NOTIFIED` 的所选集成的活动结果。

如果您启用跨区域聚合，则在聚合区域中，列表将包括来自聚合区域和启用集成的关联区域的调查发现。Security Hub 不会根据跨区域聚合配置自动启用集成。

在其他区域，集成的查找调查发现列表仅包含来自当前区域的调查发现。

有关如何配置跨区域聚合的信息，请参阅 the section called “跨区域聚合数据”。

从调查结果列表中，您可以执行以下操作。

- 更改列表的筛选条件和分组
- 查看单个结果的详细信息
- 更新调查发现的工作流状态
- 将结果发送到自定义操作

AWS 服务 与 Security Hub CSPM 集成

AWS Security Hub CSPM 支持与其他几个集成。 AWS 服务这些集成可以帮助您全面了解整个 AWS 环境的安全性和合规性。

除非下文另有说明，否则在您启 AWS 服务 用 Security Hub CSPM 和其他服务后，将自动激活将结果发送到 Security Hub CSPM 的集成。接收 Security Hub CSPM 调查发现的集成可能需要额外的激活步骤。查看有关每个集成的信息以了解更多信息。

有些集成并非全部 AWS 区域可用。在 Security Hub CSPM 控制台中，如果当前区域不支持某个集成，则该集成不会显示在集成页面上。有关在中国和地区可用的集成列表 AWS GovCloud (US) Regions，请参阅。按区域划分的集成可用性

的概述 AWS 与 Security Hub CSPM 的服务集成

下表概述了将调查结果发送到 Security Hub CSPM 或从 Security Hub CSPM 接收调查结果的 AWS 服务。

综合 AWS 服务	方向
AWS Config	发送调查发现
AWS Firewall Manager	发送调查发现
Amazon GuardDuty	发送调查发现
AWS Health	发送调查发现
AWS Identity and Access Management Access Analyzer	发送调查发现
Amazon Inspector	发送调查发现
AWS IoT Device Defender	发送调查发现
Amazon Macie	发送调查发现
Amazon Route 53 Resolver 域名防火墙	发送调查发现
AWS Systems Manager Patch Manager	发送调查发现
AWS Audit Manager	接收调查发现
聊天应用程序中的 Amazon Q 开发者版	接收调查发现
Amazon Detective	接收调查发现
Amazon Security Lake	接收调查发现
AWS Systems Manager 探险家和 OpsCenter	接收和更新调查发现
AWS Trusted Advisor	接收调查发现

AWS 服务 将调查结果发送给 Security Hub CSPM

以下内容 AWS 服务 与 Security Hub CSPM 集成并可以将发现结果发送到 Security Hub CSPM。Security Hub CSPM 会将调查发现转换为 AWS 安全调查发现格式。

AWS Config （发送调查结果）

AWS Config 是一项允许您评估、审核和评估 AWS 资源配置的服务。 AWS Config 持续监控和记录您的 AWS 资源配置，并允许您根据所需的配置自动评估记录的配置。

通过与集成 AWS Config，您可以在 Security Hub CSPM 中将 AWS Config 托管和自定义规则评估的结果作为发现结果进行查看。这些调查发现可与其他 Security Hub CSPM 调查发现一起查看，提供您的安全态势的全面概述。

AWS Config 使用亚马逊向 S EventBridge ecurity Hub CSPM 发送 AWS Config 规则评估。Security Hub CSPM 将规则评估转换成遵循 AWS 安全调查发现格式的调查发现。然后，Security Hub CSPM 通过获取有关受影响资源的更多信息（例如 Amazon 资源名称（ARN）、资源标签和创建日期），尽最大努力丰富调查发现。

有关此集成的更多信息，请参阅以下部分：

操作方法 AWS Config 将调查结果发送到 Security Hub CSPM

Security Hub CSPM 中的所有调查发现都使用 ASFF 的标准 JSON 格式。ASFF 包括有关发现的来源、受影响的资源以及发现的当前状态的详细信息。 AWS Config 通过向 Security Hub CSPM 发送托管和自定义规则评估。 EventBridgeSecurity Hub CSPM 将规则评估转化为遵循 ASFF 的调查发现，并尽最大努力丰富调查发现。

发现的类型 AWS Config 发送到 Security Hub CSPM

激活集成后， AWS Config 将所有 AWS Config 托管规则和自定义规则的评估发送到 Security Hub CSPM。仅会发送启用 Security Hub CSPM 后执行的评估。例如，假设 AWS Config 规则评估显示五个失败的资源。如果在该评估之后启用 Security Hub CSPM，并且该规则随后显示第六个失败的资源，则 AWS Config 仅会向 Security Hub CSPM 发送第六个资源评估。

不包括来自服务相关 AWS Config 规则的评估，例如用于检查 Security Hub CSPM 控件的评估。例外情况是通过在中 AWS Control Tower AWS Config创建和管理的服务相关规则生成的调查结果。包括这些规则的调查结果有助于确保您的调查结果数据包括由执行的主动检查的结果 AWS Control Tower。

正在发送 AWS Config Security Hub CSPM 的调查结果

激活集成后，Security Hub CSPM 将自动分配从 AWS Config中接收调查发现所需的权限。Security Hub CSPM 使用服务到服务级别的权限，为你提供了一种安全的方式来激活此集成并通过亚马逊导入调查结果。 AWS Config EventBridge

发送调查发现的延迟

AWS Config 创建新发现时，您通常可以在五分钟内在 Security Hub CSPM 中查看该发现结果。

Security Hub CSPM 不可用时重试

AWS Config 尽最大努力将调查结果发送给 Security Hub CSPM。 EventBridge如果事件未成功传送到 Security Hub CSPM，则 EventBridge 会重试投递最多 24 小时或 185 次，以先到者为准。

更新现有的 AWS Config Security Hub CSPM 中的调查结果

将调查结果 AWS Config 发送到 Security Hub CSPM 后，它可以向 Security Hub CSPM 发送同一发现的更新，以反映对发现活动的其他观察结果。仅针对 `ComplianceChangeNotification` 事件发送更新。如果没有发生合规性变化，则不会向 Security Hub CSPM 发送更新。Security Hub CSPM 会在最近一次更新后的 90 天或（如果没有更新）创建后的 90 天删除结果。

AWS Config 即使您删除了关联的资源，Security Hub CSPM 也不会存档从中发送的结果。

其中的地区 AWS Config 发现是存在的

AWS Config 调查结果以区域为基础出现。 AWS Config 将发现结果发送到发现结果所在的一个或多个区域的 Security Hub CSPM。

查看 AWS Config Security Hub CSPM 中的调查结果

要查看您的 AWS Config 发现，请从 Security Hub CSPM 导航窗格中选择调查结果。要筛选搜索结果以仅显示搜索 AWS Config 结果，请在搜索栏下拉列表中选择产品名称。输入Config，然后选择应用。

口译 AWS Config 在 Security Hub CSPM 中查找名字

Security Hub CSPM 将 AWS Config 规则评估转化为遵循以下内容的结果。AWS 安全调查结果格式 (ASFF) AWS Config 与 ASFF 相比，规则评估使用不同的事件模式。下表将 AWS Config 规则评估字段与 Security Hub CSPM 中出现的 ASFF 对应字段进行了映射。

Config 规则评估调查发现类型	ASFF 结果类型	硬编码值
detail.awsAccountId	AwsAccountId	

Config 规则评估调查发现类型	ASFF 结果类型	硬编码值
detail.newEvaluationResult.resultRecordedTime	CreatedAt	
detail.newEvaluationResult.resultRecordedTime	UpdatedAt	
	ProductArn	<region>“arn:: securityhub::: / confi <partition>g” product/aws
	ProductName	"Config"
	CompanyName	"AWS"
	Region	"eu-central-1"
配置 RuleArn	GeneratorId, ProductFields	
细节。 ConfigRuleARN/finding/hash	Id	
详情配置 RuleName	标题 ， ProductFields	
详情配置 RuleName	说明	“此调查发现是针对配置规则的资源合规性更改而创建的：${detail.ConfigRuleName} ”
配置项“ARN”或 Security Hub CSPM 计算的 ARN	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	"eu-central-1"
配置项目“配置”	Resources[i].Details	
	SchemaVersion	"2018-10-08"

Config 规则评估调查发现类型	ASFF 结果类型	硬编码值
	Severity.Label	请参阅下面的“解释严重性标签”
	类型	[“软件和配置检查”]
详情.new EvaluationResult.complianceType	Compliance.Status	"FAILED", "NOT_AVAILABLE", "PASSED", or "WARNING"
	Workflow.Status	如果生成 AWS Config 结果的结果为 “已通过”，或者结果从 “失败” Compliance.Status 变为 “通过”，则为 “已解决”。Compliance.Status 否则，Workflow.Status 将是 “全新”。您可以通过 BatchUpdateFindingsAPI 操作更改此值。

解释严重性标签

AWS Config 规则评估的所有发现在 ASFF 中都有一个默认的严重性标签为 MEDIUM。您可以通过 `BatchUpdateFindings` API 操作更新调查发现的严重性标签。

来自的典型发现 AWS Config

Security Hub CSPM 将 AWS Config 规则评估转化为遵循 ASFF 的调查结果。以下是ASFF中典型发现 AWS Config 的示例。

> **Note**
>
> 如果描述超过 1,024 个字符，则它将被截断为 1,024 个字符，并在结尾处显示 “（截断）”。

```
{
 "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"
  ]
 }
}
```

启用和配置集成

启用 Security Hub CSPM 后，此集成将自动激活。 AWS Config 立即开始将调查发现发送到 Security Hub CSPM。

停止向 Security Hub CSPM 发布调查发现

要停止向 Security Hub CSPM 发送调查发现，您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。

有关停止调查发现流的说明，请参阅启用来自 Security Hub CSPM 集成的调查发现流。

AWS Firewall Manager （发送调查结果）

当 Web 应用程序防火墙（WAF）资源策略或 Web 访问控制列表（Web ACL）规则不合规时，Firewall Manager 会将调查发现发送到 Security Hub CSPM。F AWS Shield Advanced irewall Manager 还会在未保护资源或发现攻击时发送调查结果。

启用 Security Hub CSPM 后，此集成将自动激活。Firewall Manager 会立即开始向 Security Hub CSPM 发送调查发现。

要了解有关集成的更多信息，请查看 Security Hub CSPM 控制台中的集成页面。

要了解有关 Firewall Manager 的更多信息，请参阅 AWS WAF 开发人员指南。

亚马逊 GuardDuty （发送调查结果）

GuardDuty 将其生成的所有查找结果类型发送到 Security Hub CSPM。某些调查发现类型具有先决条件、启用要求或区域限制。有关更多信息，请参阅 Amazon GuardDuty 用户指南中的GuardDuty 查找类型。

来自 GuardDuty 的新发现将在五分钟内发送给 Security Hub CSPM。调查结果的更新是根据设置 EventBridge 中亚马逊的 “更新调查结果 GuardDuty ” 设置发送的。

当您使用 GuardDuty “设置” 页面生成 GuardDuty 示例查找结果时，Security Hub CSPM 会收到样本查找结果并省略查找结果类型`[Sample]`中的前缀。例如，中的样本查找结果类型显示 GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions`为 `Recon:IAMUser/ResourcePermissions` Security Hub CSPM。

启用 Security Hub CSPM 后，此集成将自动激活。 GuardDuty 立即开始将调查发现发送到 Security Hub CSPM。

有关集成的更多信息，请参阅亚马逊 GuardDuty 用户指南中的与 Sec AWS urity Hub CSPM 集 GuardDuty 成。

AWS Health （发送调查结果）

AWS Health 提供对您的资源性能以及和可用性的持续可见 AWS 服务 性 AWS 账户。您可以使用 AWS Health 事件来了解服务和资源更改会如何影响正在 AWS运行的应用程序。

与的集成 AWS Health 不起作用`BatchImportFindings`。而是 AWS Health 使用服务到服务事件消息将发现结果发送到 Security Hub CSPM。

有关此集成的更多信息，请参阅以下部分：

操作方法 AWS Health 将调查结果发送到 Security Hub CSPM

在 Security Hub CSPM 中，安全问题按调查发现进行跟踪。一些发现来自其他 AWS 服务或第三方合作伙伴检测到的问题。Security Hub CSPM 还有一套用于检测安全问题和生成调查发现的规则。

Security Hub CSPM 提供了用于管理来自所有这些来源的调查发现的工具。您可以查看和筛选调查发现列表，并查看调查发现的详细信息。请参阅在 Security Hub CSPM 中查看调查发现详细信息和历史记录。您还可以跟踪调查发现的调查状态。请参阅在 Security Hub CSPM 中设置调查发现的工作流状态。

Security Hub CSPM 中的所有调查发现都使用标准的 JSON 格式（称为 AWS 安全调查结果格式 (ASFF)）。ASFF 包括有关问题根源、受影响资源以及调查发现当前状态的详细信息。

AWS Health 是向 Security Hub CSPM 发送调查结果的 AWS 服务之一。

发现的类型 AWS Health 发送到 Security Hub CSPM

启用集成后，AWS Health 将符合列出的一项或多项规范的发现结果发送给 Security Hub CSPM。Security Hub CSPM 会以 AWS 安全调查结果格式 (ASFF) 提取调查发现。

- 包含 AWS 服务的以下任何值的调查发现：
  - 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

- 带有securityabuse、或字样certificate在 AWS Health typeCode现场的调查结果
- 发现 AWS Health 服务所在位置risk或 abuse

正在发送 AWS Health Security Hub CSPM 的调查结果

当您选择接受来自的调查结果时 AWS Health，Security Hub CSPM 将自动分配从中接收调查结果所需的权限。 AWS Health Security Hub CSPM 使用服务到服务级别的权限，为您提供一种安全、简便的方法来启用此集成并代表您通过 AWS Health 亚马逊 EventBridge 导入调查结果。选择接受调查发现会授予 Security Hub CSPM 使用 AWS Health中的调查发现的权限。

发送调查发现的延迟

AWS Health 创建新发现时，通常会在五分钟内将其发送到 Security Hub CSPM。

Security Hub CSPM 不可用时重试

AWS Health 尽最大努力将调查结果发送给 Security Hub CSPM。 EventBridge如果事件未成功传送到 Security Hub CSPM，则会在 24 小时内 EventBridge重试发送该事件。

更新 Security Hub CSPM 中的现有调查发现

将调查结果 AWS Health 发送到 Security Hub CSPM 后，它可以向 Security Hub CSPM 发送同一发现的更新，以反映对发现活动的其他观察结果。

存在调查发现的区域

对于全球事件，以 us-east-1（分区）、cn-northwest-1（中国分区）和 gov-us-west-1（分区AWS ）AWS Health 将调查结果发送给 Security Hub CSPM。GovCloud AWS Health 将 Region-specific 事件发送到事件发生地相同的一个或多个区域的 Security Hub CSPM。

查看 AWS Health Security Hub CSPM 中的调查结果

要在 Security Hub CSPM 中查看您的 AWS Health 发现，请从导航面板中选择调查结果。要筛选结果以仅显示搜索 AWS Health 结果，请从 “产品名称” 字段中选择 “Heal th”。

口译 AWS Health 在 Security Hub CSPM 中查找名字

AWS Health 使用将发现结果发送到 Security Hub CSPM。AWS 安全调查结果格式 (ASFF) AWS Health 与 Security Hub CSPM ASFF 格式相比，finding 使用了不同的事件模式。下表详细列出了所有 AWS Health 查找字段及其在 Security Hub CSPM 中显示的 ASFF 对应字段。

健康调查发现类型	ASFF 结果类型	硬编码值
账户	AwsAccountId	
detail.startTime	CreatedAt	
细节。事件 Description.latest Description	说明	
细节。事件 TypeCode	GeneratorId	
detail.eventArn（包括账户）+ detail.startTime 的 hash	Id	
<region>“arn: aws: securityh ub::: /health” product/aws	ProductArn	
账户或 resourceId	Resources[i].id	
	Resources[i].Type	“其他”
	SchemaVersion	"2018-10-08"
	Severity.Label	请参阅下面的“解释严重性标签”

健康调查发现类型	ASFF 结果类型	硬编码值
“AWS Health -” 详情。事件 TypeCode	标题	
-	类型	[“软件和配置检查”]
event.time	UpdatedAt	
Health 控制台上事件的 URL	SourceUrl	

解释严重性标签

ASFF 调查发现中的严重性标签是使用以下逻辑确定的：

- 如果满足以下条件，则严重性为危急。
  - AWS Health 调查发现中的 `service` 字段具有值 `Risk`
  - AWS Health 调查发现中的 `typeCode` 字段具有值 `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - AWS Health 调查发现中的 `typeCode` 字段具有值 `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - AWS Health 调查发现中的 `typeCode` 字段具有值 `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  严重性为高，如果：
  - AWS Health 调查发现中的 `service` 字段具有值 `Abuse`
  - AWS Health 调查发现中的 `typeCode` 字段包含值 `SECURITY_NOTIFICATION`
  - AWS Health 调查发现中的 `typeCode` 字段包含值 `ABUSE_DETECTION`

  如果满足以下条件，则严重性为中。
  - 调查发现中的 `service` 字段为以下任意字段：`ACM`、`ARTIFACT`、`AUDITMANAGER`、`BACKUP`、`CLOUDENDURE`、`CLOUDHSM`、`CLOUDTRAIL`、`CLOU` 或 `WAF`
  - AWS Health 调查发现中的typeCode字段包含值 `CERTIFICATE`
  - AWS Health 调查发现中的typeCode字段包含值 `END_OF_SUPPORT`

来自的典型发现 AWS Health

AWS Health 使用将发现结果发送到 Security Hub CSPM。AWS 安全调查结果格式 (ASFF)以下是来自的典型发现的示例 AWS Health。

> **Note**
>
> 如果描述超过 1024 个字符，则它将被截断至 1024 个字符，并在结尾处显示（截断）。


```
{
            "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"
                ]
            }
        }
    ]
}
```

启用和配置集成

启用 Security Hub CSPM 后，此集成将自动激活。 AWS Health 立即开始将调查发现发送到 Security Hub CSPM。

停止向 Security Hub CSPM 发布调查发现

要停止向 Security Hub CSPM 发送调查发现，您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。

有关停止调查发现流的说明，请参阅启用来自 Security Hub CSPM 集成的调查发现流。

AWS Identity and Access Management Access Analyzer（发送调查结果）

借助 IAM Access Analyzer，所有调查发现都会发送到 Security Hub CSPM。

IAM Access Analyzer 使用基于逻辑的推理来分析应用于您账户中受支持资源的基于资源的策略。IAM Access Analyzer 在检测到允许外部主体访问您账户中资源的策略语句时生成一个调查发现。

在 IAM Access Analyzer 中，只有管理员账户才能看到适用于组织的分析器的调查发现。对于组织分析器，`AwsAccountId` ASFF 字段反映管理员账户 ID。在 `ProductFields` 下方，`ResourceOwnerAccount` 字段表示调查发现被发现的账户。如果您为每个账户单独启用分析器，Security Hub CSPM 会生成多个调查发现：一个用于标识管理员账户 ID，另一个用于标识资源账户 ID。

有关更多信息，请参阅 IAM 用户指南中的与 Sec AWS urity Hub CSPM 集成。

Amazon Inspector（发送调查发现）

Amazon Inspector 是一项漏洞管理服务，可持续扫描您的 AWS 工作负载中是否存在漏洞。Amazon Inspector 可以自动发现并扫描驻留在 Amazon 弹性容器注册表中的 Amazon EC2 实例和容器映像。扫描会查找软件漏洞和意外网络暴露。

启用 Security Hub CSPM 后，此集成将自动激活。Amazon Inspector 立即开始将其生成的所有调查发现发送到 Security Hub CSPM。

有关集成的更多信息，请参阅《Amazon Inspector 用户指南》中的与 AWS Security Hub CSPM 集成。

Security Hub CSPM 还可以接收来自 Amazon Inspector Classic 的调查发现。Amazon Inspector Classic 会将通过所有受支持规则包的评测运行生成的调查发现发送到 Security Hub CSPM。

有关集成的更多信息，请参阅 Amazon Inspector Classic 用户指南中的与 Sec AWS urity Hub CSPM 集成。

Amazon Inspector 和 Amazon Inspector Classic 的调查发现使用相同的产品 ARN。Amazon Inspector 的调查发现在 `ProductFields` 中有以下条目：

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Amazon Inspector Code Security 生成的安全调查发现不适用于此集成。但是，您可以在 Amazon Inspector 控制台中和通过 Amazon Inspector API 访问这些特定调查发现。

AWS IoT Device Defender （发送调查结果）

AWS IoT Device Defender 是一项安全服务，可审核您的物联网设备的配置，监控连接的设备以检测异常行为，并帮助降低安全风险。

同时启用两者 AWS IoT Device Defender 和 Security Hub CSPM 后，请访问 Sec urity Hub CSPM 控制台的 “集成” 页面，然后选择 “接受审计”、“检测” 或 “两者” 的调查结果。 AWS IoT Device Defender 审计和检测开始将所有发现结果发送到 Security Hub CSPM。

AWS IoT Device Defender 审计向 Security Hub CSPM 发送支票摘要，其中包含特定审计检查类型和审计任务的一般信息。 AWS IoT Device Defender 检测将机器学习 (ML)、统计和静态行为的违规发现发送到 Security Hub CSPM。“审计”还会将调查发现更新发送到 Security Hub CSPM。

有关此集成的更多信息，请参阅《AWS IoT 开发者指南》中的与 AWS Security Hub CSPM 集成。

Amazon Macie（发送调查发现）

Amazon Macie 是一项数据安全服务，该服务使用机器学习和模式匹配来发现敏感数据，提供对数据安全风险的可见性，并实现针对这些风险的自动防护。Macie 的调查发现可能表明 Amazon S3 数据资产中存在潜在的策略违规行为或敏感数据。

启用 Security Hub CSPM 后，Macie 会自动开始向 Security Hub CSPM 发送策略调查发现。您可以对集成进行配置，将敏感数据调查发现也发送到 Security Hub CSPM。

在 Security Hub CSPM 中，策略或敏感数据调查发现的调查发现类型更改为与 ASFF 兼容的值。例如，Macie 中的 `Policy:IAMUser/S3BucketPublic` 调查发现类型在 Security Hub CSPM 中显示为 `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`。

Macie 还会将生成的调查发现样本发送到 Security Hub CSPM。对于调查发现样本，受影响资源的名称为 `macie-sample-finding-bucket`，`Sample` 字段的值为 `true`。

有关更多信息，请参阅《Amazon Macie 用户指南》中的使用 Security Hub 评估 Macie 调查发现。

Amazon Route 53 Resolver DNS 防火墙（发送调查结果）

借助 Amazon Route 53 Resolver DNS 防火墙，您可以筛选和监管虚拟私有云 (VPC) 的出站 DNS 流量。为此，请在 DNS Firewall 规则组中创建可重复使用的筛选规则集合，将规则组与您的 VPC 关联，然后监控 DNS Firewall 日志和指标中的活动。根据活动，您可以调整 DNS Firewall 行为。DNS Firewall 是 Route 53 Resolver 的一项功能。

Route 53 Resolver DNS Firewall 可以将多种类型的调查发现发送到 Security Hub CSPM：

- 与托管域列表（ AWS 管理的域名列表）关联的域名被屏蔽或提醒的查询相关的发现。 AWS
- 对于与您定义的自定义域列表关联的域，与被阻止或发出警报的查询相关的调查发现。
- 与 DNS Firewall Advanced 阻止或发出警报的查询相关的调查发现，这是一项 Route 53 Resolver 功能，可以检测与高级 DNS 威胁（例如域生成算法（DGA）和 DNS 隧道）相关的查询。

启用 Security Hub CSPM 和 Route 53 Resolver DNS 防火墙后，DNS Firewall 会自动开始向 Security Hub CSPM 发送 AWS 托管域列表和 DNS 防火墙高级版的搜索结果。要同时将自定义域列表的调查发现发送到 Security Hub CSPM，请在 Security Hub CSPM 中手动启用集成。

在 Security Hub CSPM 中，Route 53 Resolver DNS Firewall 的所有调查发现都具有以下类型：`TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`。

有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的将来自 Route 53 Resolver DNS Firewall 的调查发现发送到 Security Hub。

AWS Systems Manager 补丁管理器（发送调查结果）

AWS Systems Manager 当客户队列中的实例不符合其补丁合规性标准时，补丁管理器会将发现结果发送给 Security Hub CSPM。

补丁管理器能够使用安全相关更新及其他更新类型自动执行修补托管实例的过程。

启用 Security Hub CSPM 后，此集成将自动激活。Systems Manager 补丁管理器立即开始将调查发现发送到 Security Hub CSPM。

有关使用 Patch Manager 的更多信息，请参阅 AWS Systems Manager 用户指南中的 AWS Systems Manager Patch Manager。

AWS 接收来自 Security Hub CSPM 的调查结果的服务

以下 AWS 服务与 Security Hub CSPM 集成并接收来自 Security Hub CSPM 的调查结果。如有注明，集成服务也可能更新调查发现。在这种情况下，您在集成服务中进行的调查发现更新也将反映在 Security Hub CSPM 中。

AWS Audit Manager（接收调查结果）

AWS Audit Manager 收到 Security Hub CSPM 的调查结果。这些调查发现有助于 Audit Manager 用户为审计做好准备。

要了解有关 Audit Manager 的更多信息，请参阅 Au AWS dit Manager 用户指南。AWSAWS Audit Manager支持的 Security Hub CSPM 检查列出了 Security Hub CSPM 向 Audit Manager 发送调查发现的控件。

聊天应用程序中的 Amazon Q 开发者版（接收调查发现）

聊天应用程序中的 Amazon Q 开发者版是一种交互式代理，可帮助您监控 Slack 频道和 Amazon Chime 聊天室中的 AWS 资源并与之交互。

聊天应用程序中的 Amazon Q 开发者版会收到来自 Security Hub CSPM 的调查发现。

要详细了解聊天应用程序中的 Amazon Q 开发者版如何与 Security Hub CSPM 集成，请参阅《聊天应用程序中的 Amazon Q 开发者版管理员指南》中的 Security Hub CSPM 集成概述。

Amazon Detective（接收调查发现）

Detective 会自动从您的 AWS 资源中收集日志数据，并使用机器学习、统计分析和图论来帮助您实现可视化，并更快、更高效地进行安全调查。

Security Hub CSPM 与 Detective 的集成允许你从亚马逊在 Security Hub CSPM 中的 GuardDuty 发现转向侦探。然后，您可以使用 Detective 工具和可视化功能调查它们。该集成不需要在 Security Hub CSPM 或 Detective 中进行任何其他配置。

对于从其他人那里收到的调查结果 AWS 服务，Security Hub CSPM控制台上的调查结果详细信息面板包括侦探调查小节。该小节包含指向 Detective 的链接，您可以在其中进一步调查调查发现所标记的安全问题。您还可以根据 Security Hub CSPM 调查发现在 Detective 中构建行为图，以进行更有效的调查。要了解更多信息，请参阅《Amazon Detective 管理指南》中的AWS 安全调查发现。

如果启用了跨区域聚合，则当您从聚合区域进行转向时，Detective 将在调查发现的来源区域中打开。

如果链接无效，请参阅对转换进行故障排除以了解故障排除建议。

Amazon Security Lake（接收调查发现）

Security Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 自动将来自云、本地和自定义源的安全数据集中到存储在您账户中的数据湖中。订阅用户可以使用 Security Lake 中的数据进行调查和分析用例。

要激活此集成，您必须启用这两项服务，并在 Security Lake 控制台、Security Lake API 或中将 Security Hub CSPM 添加为来源。 AWS CLI完成这些步骤后，Security Hub CSPM 开始将所有调查发现发送到 Security Lake。

Security Lake 会自动对 Security Hub CSPM 调查发现进行标准化，并将其转换为名为开放网络安全架构框架（OCSF）的标准化开源架构。在 Security Lake 中，您可以添加一个或多个订阅用户来使用 Security Hub CSPM 调查发现。

有关此集成的更多信息，包括有关添加 Security Hub CSPM 作为来源和创建订阅者的说明，请参阅 Amazon Sec AWS urity Lake 用户指南中的与 Sec urity Hub CSPM 集成。

AWS Systems Manager Explorer 和 OpsCenter （接收和更新调查结果）

AWS Systems Manager 浏览并 OpsCenter 接收来自 Security Hub CSPM 的调查结果，然后在 Security Hub CSPM 中更新这些发现。

Explorer 为您提供可自定义的控制面板，提供有关您 AWS 环境运营状况和性能的关键见解和分析。

OpsCenter 为您提供查看、调查和解决操作工作项的中心位置。

有关 Explorer 和的更多信息 OpsCenter，请参阅《AWS Systems Manager 用户指南》中的操作管理。

AWS Trusted Advisor （接收调查结果）

Trusted Advisor 借鉴了从为成千上万的 AWS 客户提供服务中学到的最佳实践。 Trusted Advisor 检查您的 AWS 环境，然后在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。

当你同时启用两者 Trusted Advisor 并启用 Security Hub CSPM 时，集成会自动更新。

Security Hub CSPM 将其 AWS 基础安全最佳实践检查结果发送给。 Trusted Advisor

有关 Security Hub CSPM 与集成的更多信息 Trusted Advisor，请参阅《支持AWS 用户指南》中的 “查看 Sec AWS urity Hub CSPM 控件 AWS Trusted Advisor”。

Third-party 与 Security Hub CSPM 的产品集成

AWS Security Hub CSPM 与多个第三方合作伙伴产品集成。集成可以执行以下一项或多项操作：

- 将生成的调查发现发送到 Security Hub CSPM
- 从 Security Hub CSPM 接收调查发现
- 在 Security Hub CSPM 中更新调查发现

将调查发现发送到 Security Hub CSPM 的集成具有 Amazon 资源名称（ARN）。

可能并非所有集成都可用 AWS 区域。如果某项集成在您当前登录到 Security Hub CSPM 控制台的区域中不受支持，则不会显示在控制台的集成页面上。有关在中国和地区可用的集成列表 AWS GovCloud (US) Regions，请参阅。按区域划分的集成可用性

如果您有安全解决方案并有兴趣成为 Security Hub CSPM 合作伙伴，请发送电子邮件至 <securityhub-partners@amazon.com>。有关更多信息，请参阅合作伙伴集成指南。

第三方与 Security Hub CSPM 的集成概述

下表概述了可以向 Security Hub CSPM 发送调查发现或从 Security Hub CSPM 接收调查发现的第三方集成。

集成	方向	ARN（如果适用）
3CORESec – 3CORESec NTA	发送调查发现	arn:aws:securityhub: *<REGION>*::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	发送调查发现	arn:aws:securityhub: *<REGION>*:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	发送调查发现	arn:aws:securityhub: *<REGION>*::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	发送调查发现	arn:aws:securityhub: *<REGION>*::product/

集成	方向	ARN（如果适用）
		aqua-security/kube-bench
Armor – Armor Anywhere	发送调查发现	arn:aws:securityhub: *<REGION>*:679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	发送调查发现	arn:aws:securityhub: *<REGION>*::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	发送调查发现	arn:aws:securityhub: *<REGION>*:151784055945:product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	发送调查发现	arn:aws:securityhub: *<REGION>*::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	发送调查发现	arn:aws:securityhub: *<REGION>*::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	发送调查发现	arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas

集成	方向	ARN（如果适用）
Check Point – CloudGuard Posture Management	发送调查发现	arn:aws:securityhub: *<REGION>*:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	发送调查发现	arn:aws:securityhub: *<REGION>*::product/claroty/xdome
Cloud Storage Security – Antivirus for Amazon S3	发送调查发现	arn:aws:securityhub: *<REGION>*::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	发送调查发现	arn:aws:securityhub: *<REGION>*::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	发送调查发现	arn:aws:securityhub: *<REGION>*:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	发送调查发现	arn:aws:securityhub: *<REGION>*:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	发送调查发现	arn:aws:securityhub: *<REGION>*::product/data-theorem/api-cloud-web-secure

集成	方向	ARN（如果适用）
Drata	发送调查发现	arn:aws:securityhub: *<REGION>*::product/drata/drata-integration
Forcepoint – Forcepoint CASB	发送调查发现	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	发送调查发现	arn:aws:securityhub: *<REGION>*::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	发送调查发现	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	发送调查发现	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	发送调查发现	arn:aws:securityhub: *<REGION>*::product/fugue/fugue

集成	方向	ARN（如果适用）
Guardicore – Centra 4.0	发送调查发现	arn:aws:securityhub: *<REGION>*::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	发送调查发现	arn:aws:securityhub: *<REGION>*::product/hackerone/vulnerability-intelligence
JFrog – Xray	发送调查发现	arn:aws:securityhub: *<REGION>*::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	发送调查发现	arn:aws:securityhub: *<REGION>*::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	发送调查发现	arn:aws:securityhub: *<REGION>*::product/k9-security/access-analyzer
Lacework – Lacework	发送调查发现	arn:aws:securityhub: *<REGION>*::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	发送调查发现	arn:aws:securityhub: *<REGION>*::product/mcafee-skyhigh/mcafee-mvision-cloud-aws

集成	方向	ARN（如果适用）
NETSCOUT – NETSCOUT Cyber Investigator	发送调查发现	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Orca Cloud Security Platform	发送调查发现	arn:aws:securityhub: *<REGION>*::product/orca-security/orca-security
Palo Alto Networks – Prisma Cloud Compute	发送调查发现	arn:aws:securityhub: *<REGION>*:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	发送调查发现	arn:aws:securityhub: *<REGION>*:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	发送调查发现	arn:aws:securityhub: *<REGION>*::product/plerion/cloud-security-platform
Prowler – Prowler	发送调查发现	arn:aws:securityhub: *<REGION>*::product/prowler/prowler
Qualys – Vulnerability Management	发送调查发现	arn:aws:securityhub: *<REGION>*:805950163170:product/qualys/qualys-vm

集成	方向	ARN（如果适用）
Rapid7 – InsightVM	发送调查发现	arn:aws:securityhub: *<REGION>*:336818582268:product/rapid7/insightvm
SentinelOne – SentinelOne	发送调查发现	arn:aws:securityhub: *<REGION>*::product/sentinelone/endpoint-protection
Snyk	发送调查发现	arn:aws:securityhub: *<region>*::product/snyk/snyk
Sonrai Security – Sonrai Dig	发送调查发现	arn:aws:securityhub: *<REGION>*::product/sonrai-security/sonrai-dig
Sophos – Server Protection	发送调查发现	arn:aws:securityhub: *<REGION>*:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	发送调查发现	arn:aws:securityhub: *<REGION>*::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	发送调查发现	arn:aws:securityhub: *<REGION>*:956882708938:product/sumologicinc/sumologic-mda

集成	方向	ARN（如果适用）
Symantec – Cloud Workload Protection	发送调查发现	arn:aws:securityhub: *<REGION>*:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	发送调查发现	arn:aws:securityhub: *<REGION>*:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	发送调查发现	arn:aws:securityhub: *<REGION>*::product/trend-micro/cloud-one
Vectra – Cognito Detect	发送调查发现	arn:aws:securityhub: *<REGION>*:978576646331:product/vectra-ai/cognito-detect
Wiz	发送调查发现	arn:aws:securityhub: *<REGION>*::product/wiz-security/wiz-security
Atlassian - Jira Service Management	接收和更新调查发现	不适用
Atlassian - Jira Service Management Cloud	接收和更新调查发现	不适用
Atlassian – Opsgenie	接收调查发现	不适用
Dynatrace	接收调查发现	不适用
Elastic	接收调查发现	不适用

集成	方向	ARN（如果适用）
Fortinet – FortiCNP	接收调查发现	不适用
IBM – QRadar	接收调查发现	不适用
Logz.io Cloud SIEM	接收调查发现	不适用
MetricStream	接收调查发现	不适用
MicroFocus – MicroFocus Arcsight	接收调查发现	不适用
New Relic Vulnerability Management	接收调查发现	不适用
PagerDuty – PagerDuty	接收调查发现	不适用
Palo Alto Networks – Cortex XSOAR	接收调查发现	不适用
Palo Alto Networks – VM-Series	接收调查发现	不适用
Rackspace Technology – Cloud Native Security	接收调查发现	不适用
Rapid7 – InsightConnect	接收调查发现	不适用
RSA – RSA Archer	接收调查发现	不适用
ServiceNow – ITSM	接收和更新调查发现	不适用
Slack – Slack	接收调查发现	不适用
Splunk – Splunk Enterprise	接收调查发现	不适用
Splunk – Splunk Phantom	接收调查发现	不适用
ThreatModeler	接收调查发现	不适用

集成	方向	ARN（如果适用）
Trellix – Trellix Helix	接收调查发现	不适用
Caveonix – Caveonix Cloud	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/disruptops-inc/disruptops
Kion	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/cloudtamerio/cloudtamerio
Turbot – Turbot	发送和接收调查发现	arn:aws:securityhub: *<REGION>*:453761072151:product/turbot/turbot

Third-party 将调查结果发送到 Security Hub CSPM 的集成

以下第三方合作伙伴产品集成可以将调查发现发送到 Security Hub CSPM。Security Hub CSPM 将调查发现转换为 AWS 安全调查发现格式。

3CoreSec – 3CoreSec NTA

集成类型：发送

产品 ARN：arn:aws:securityhub:*<REGION>*::product/3coresec/3coresec

3CORESec 为本地和 AWS 系统提供托管检测服务。它们与 Security Hub CSPM 的集成允许查看恶意软件、权限升级、横向移动和不当网络分段等威胁。

产品链接

合作伙伴文档

Alert Logic – Siemless 威胁管理

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

获得适当的覆盖级别：漏洞和资产可见性、威胁检测和事件管理 AWS WAF，以及分配的 SOC 分析师选项。

产品链接

合作伙伴文档

Aqua 安全性 – Aqua 云原生安全平台

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)为基于容器和无服务器的应用程序（从您的 CI/CD 管道到运行时生产环境）提供完整的生命周期安全性。

产品链接

合作伙伴文档

Aqua 安全性 – Kube-bench

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench 是一款开源工具，可针对您的环境运行 Center for Internet Security（CIS）Kubernetes 基准。

产品链接

合作伙伴文档

Armor – Armor Anywhere

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere为。提供托管的安全性和合规性 AWS。

产品链接

合作伙伴文档

AttackIQ – AttackIQ

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform 模拟与 MITRE ATT&CK 框架一致的真实对抗行为，以帮助验证和改善您的整体安全状况。

产品链接

合作伙伴文档

Barracuda Networks – Cloud Security Guardian

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry 帮助组织在公共云中构建应用程序并将工作负载迁移到公共云时保持安全。

AWS 商城链接

产品链接

BigID – BigID Enterprise

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform 帮助公司管理和保护其所有系统中的敏感数据（PII）。

产品链接

合作伙伴文档

蓝色六边形 – 蓝色六边形 适合 AWS

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon 是一个实时威胁检测平台。它使用深度学习原理来检测已知和未知威胁，包括恶意软件和网络异常。

AWS 商城链接

合作伙伴文档

检查点 – CloudGuard IaaS

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard轻松将全面的威胁防御安全扩展到，AWS 同时保护云中的资产。

产品链接

合作伙伴文档

检查点 – CloudGuard 姿势管理

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

一个 SaaS 平台，提供可验证的云网络安全、高级 IAM 保护以及全面的合规性和治理。

产品链接

合作伙伴文档

Claroty – xDome

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome 帮助组织在工业（OT）、医疗保健（IoMT）和企业（IoT）环境中通过扩展物联网（XioT）保护其网络物理系统。

产品链接

合作伙伴文档

Cloud Storage Security – 的防病毒软件 Amazon S3

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security为 Amazon S3 对象提供云原生防恶意软件和防病毒扫描。

Antivirus for Amazon S3 提供对 Amazon S3 中对象和文件的实时和计划扫描，以发现恶意软件和威胁。它为问题文件和受感染文件提供了可见性和补救措施。

产品链接

合作伙伴文档

对比安全 — 对比度评估

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess 是一款 IAST 工具，可在 Web 应用、API 和微服务中提供实时漏洞检测。Contrast Assess 与 Security Hub CSPM 集成，有助于为所有工作负载提供集中可见性和响应能力。

产品链接

合作伙伴文档

CrowdStrike – CrowdStrike 猎鹰

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

这款轻巧的CrowdStrike Falcon单一传感器统一了下一代防病毒、端点检测和响应以及通过云端进行24/7 托管搜寻。

AWS 商城链接

合作伙伴文档

CyberArk – Privileged Threat Analytics

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics 收集、检测、警报和响应特权账户的高风险活动和行为，以遏制正在进行的攻击。

产品链接

合作伙伴文档

数据定理 – 数据定理

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem持续扫描 Web 应用程序、API 和云资源，寻找安全漏洞和数据隐私漏洞，防止 AppSec 数据泄露。

产品链接

合作伙伴文档

德拉塔

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata 是一个合规性自动化平台，可帮助您实现和保持与各种框架（例如 SOC2、ISO 和 GDPR）的合规性。Drata 和 Security Hub CSPM 之间的集成可帮助您将安全调查发现集中在一个位置。

AWS 商城链接

合作伙伴文档

Forcepoint – Forcepoint CASB

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB 允许您发现云应用程序的使用情况、分析风险并对 SaaS 和自定义应用程序实施适当的控制。

产品链接

合作伙伴文档

Forcepoint – 原力点云安全网关

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway 是一项融合云安全服务，无论用户身在何处，都能为用户和数据提供可见性、控件和威胁防护。

产品链接

合作伙伴文档

Forcepoint – Forcepoint DLP

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP 通过员工工作的任何地方和数据所在的任何地方的可见性和控制来解决以人为中心的风险。

产品链接

合作伙伴文档

Forcepoint – Forcepoint NGFW

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW允许您将 AWS 环境连接到企业网络，提供管理网络和应对威胁所需的可扩展性、保护和洞察力。

产品链接

合作伙伴文档

赋格曲 – 赋格曲

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue 是一个无需代理、可扩展的云原生平台，可使用相同的策略自动持续验证基础架构即代码和云运行时环境。

产品链接

合作伙伴文档

Guardicore – Centra 4.0

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra 为现代数据中心和云中的工作负载提供流量可视化、微分段和违规检测。

产品链接

合作伙伴文档

HackerOne – 漏洞情报

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOne 平台与全球黑客社区合作，发现最相关的安全问题。Vulnerability Intelligence 让您的组织能够超越自动扫描的局限。它共享 HackerOne 道德黑客已经验证的漏洞，并提供了重现步骤。

AWS 市场链接

合作伙伴文档

jFrog – X 射线

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray 是一款通用的应用程序安全软件组成分析（SCA）工具，可持续扫描二进制文件中的许可证合规性和安全漏洞，以便您可以运行安全的软件供应链。

AWS 商城链接

合作伙伴文档

瞻博网络 – vSRX 下一代防火墙

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'vSRX Virtual Next Generation Firewall 提供基于云的完整虚拟防火墙，具有高级安全性 SD-WAN、安全、强大的网络和内置的自动化功能。

AWS 商城链接

合作伙伴文档

产品链接

k9 安全性 – 访问分析器

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

当您的 AWS Identity and Access Management 账户发生重要的访问权限更改时，k9 Security 会通知您。借k9 Security助，您可以了解用户和 IAM 角色对关键数据 AWS 服务 和您的数据的访问权限。

k9 Security 专为持续交付而设计，允许您通过可操作的访问审计和针对 AWS CDK 和 Terraform 的简单策略自动化来实施 IAM。

产品链接

合作伙伴文档

蕾丝工艺 – 蕾丝工艺

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework 是数据驱动的云安全平台。Lacework Cloud Security Platform 可实现大规模云安全自动化，因此您可以快速、安全地进行创新。

产品链接

合作伙伴文档

McAfee – MVISION 云原生应用程序保护平台 (CNAPP)

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)为您的环境提供云安全状态管理 (CSPM) 和云工作负载保护平台 (CWPP)。 AWS

产品链接

合作伙伴文档

NETSCOUT – NETSCOUT 网络调查员

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator 是一个企业范围的网络威胁、风险调查和取证分析平台，有助于减少网络威胁对企业的影响。

产品链接

合作伙伴文档

Orca 云安全平台

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Orca Cloud Security Platform它可以识别整个云资产中的风险和合规性问题，确定其优先顺序并进行修复。 Orca's无代理优先，该 AI-driven 平台提供全面的覆盖范围，可检测漏洞、错误配置、横向移动、API 风险、敏感数据、异常事件和行为以及过于宽松的身份。

Orca 与 Security Hub CSPM 集成，将深度云安全遥测数据引入 Security Hub CSPM。Orca 利用其 SideScanning 技术优先处理云基础设施、工作负载、应用程序、数据、API、身份等方面的风险。

产品链接

合作伙伴文档

Palo Alto Networks – Prisma 云计算

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute 是一种云原生网络安全平台，可为虚拟机、容器和无服务器平台提供保护。

产品链接

合作伙伴文档

Palo Alto Networks – Prisma 云企业版

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

通过云安全分析、高级威胁检测和合规性监控来保护您的 AWS 部署。

产品链接

合作伙伴文档

Plerion – 云安全平台

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion 是一个云安全平台，采用以威胁为导向、以风险驱动的独特方法，可针对您的工作负载提供预防、检测和纠正措施。Plerion 与 Security Hub CSPM 的集成使客户能够将其安全调查发现集中到一个地方，并据此采取行动。

AWS 商城链接

合作伙伴文档

徘徊者 – 徘徊者

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler是一种开源安全工具，用于执行与安全最佳实践、强化和持续监控相关的 AWS 检查。

产品链接

合作伙伴文档

Qualys – 漏洞管理

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) 持续扫描和识别漏洞，保护您的资产。

产品链接

合作伙伴文档

Rapid7 – InsightVM

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM 为现代环境提供漏洞管理，使您能够有效地查找、优先处理和修复漏洞。

产品链接

合作伙伴文档

SentinelOne – SentinelOne

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne是一个自主扩展检测和响应 (XDR) 平台，包括跨端点、容器、云工作负载和物联网设备的 AI-powered 预防、检测、响应和搜寻。

AWS 商城链接

产品链接

Snyk

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk 提供了一个安全平台，用于扫描在 AWS上运行的工作负载中应用组件的安全风险。这些风险作为调查发现发送到 Security Hub CSPM，帮助开发人员和安全团队可视化和优先处理它们以及其余 AWS 安全调查发现。

AWS 商城链接

合作伙伴文档

Sonrai 安全 – Sonrai Dig

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig 监控和修复云端错误配置和策略违规行为，因此您可以改善安全性和合规性。

产品链接

合作伙伴文档

Sophos – Server Protection

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection 使用全面的纵深防御技术保护处于组织核心的关键应用程序和数据。

产品链接

StackRox – StackRox Kubernetes 安全

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox 通过在整个容器生命周期（构建、部署和运行）中强制执行合规性和安全策略，帮助企业大规模保护其容器和 Kubernetes 部署。

产品链接

合作伙伴文档

Sumo Logic – Machine Data Analytics

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic 是一个安全的机器数据分析平台，使开发和安全运营团队能够构建、运行和保护其 AWS 应用程序。

产品链接

合作伙伴文档

Symantec – Cloud Workload Protection

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection 通过反恶意软件、入侵防御和文件完整性监控为您的 Amazon EC2 实例提供全面的保护。

产品链接

合作伙伴文档

Tenable – Tenable.io

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

准确识别、调查漏洞并确定其优先级。托管在云中。

产品链接

合作伙伴文档

Trend Micro – 一号云

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One 在正确的时间和地点为团队提供正确的安全信息。这种集成可将安全发现实时发送到 Security Hub CSPM，从而增强了 Security Hub CSPM 中 AWS 资源和Trend Micro Cloud One 事件详细信息的可见性。

AWS 商城链接

合作伙伴文档

Vectra – Cognito 检测

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra 正在改变网络安全领域，它通过应用先进的 AI 检测和应对隐藏的网络攻击者，以防止其窃取信息或造成损害。

AWS 商城链接

合作伙伴文档

Wiz – Wiz Security

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz持续分析您 AWS 账户的、用户和工作负载中的配置、漏洞、网络、IAM 设置、密钥等，以发现构成实际风险的关键问题。将 Wiz 与 Security Hub CSPM 集成，可视化并响应 Wiz 从 Security Hub CSPM 控制台检测到的问题。

AWS 商城链接

合作伙伴文档

Third-party 接收来自 Security Hub CSPM 调查结果的集成

以下第三方合作伙伴产品集成可以从 Security Hub CSPM 接收调查发现。如有说明，产品还可能更新调查发现。在这种情况下，您对合作伙伴产品中的调查发现所做的更新也会反映在 Security Hub CSPM 中。

Atlassian - Jira Service Management

集成类型：接收和更新

f AWS 服务管理连接器 or 将来自 Security Hub CSPM 的发现结果Jira发送到。Jira Jira问题是根据调查结果创建的。当 Jira 问题更新时，Security Hub CSPM 中的相应调查发现也会更新。

该集成仅支持 Jira 服务器和 Jira 数据中心。

有关集成及其工作原理的概述，请观看视频 AWS Security Hub CSPM - 与 Atlassian Jira Service Management 的双向集成。

产品链接

合作伙伴文档

Atlassian - Jira 服务管理云

集成类型：接收和更新

Jira Service Management Cloud 是 Jira 服务管理的云组件。

f AWS 服务管理连接器 or 将来自 Security Hub CSPM 的发现结果Jira发送到。Jira这些结果引发 Jira Service Management Cloud 中的问题产生。当您在 Jira Service Management Cloud 中更新这些问题时，Security Hub CSPM 中也会更新相应的调查发现。

产品链接

合作伙伴文档

Atlassian – Opsgenie

集成类型：接收

Opsgenie 是一种现代事件管理解决方案，用于运营始终在线的服务，使开发和运营团队能够规划服务中断并在事件期间保持控制。

与 Security Hub CSPM 集成可确保将与安全相关的关键任务事件路由到适当的团队以立即解决。

产品链接

合作伙伴文档

Dynatrace

集成类型：接收

与 Security Hub CSPM 的 Dynatrace 集成有助于统一、可视化和自动执行跨工具和环境的安全发现。在安全调查结果中添加Dynatrace运行时上下文可以更明智地确定优先级，有助于减少警报产生的噪音，并使您的 DevSecOps 团队集中精力有效地解决影响生产环境和应用程序的关键问题。

产品链接

合作伙伴文档

弹性

集成类型：接收

Elastic 为安全、可观测性和搜索构建基于搜索的解决方案。借助 Security Hub CSPM 集成，Elastic 可以编程方式从 Security Hub CSPM 中提取调查发现和见解，对其进行规范化以进行关联和分析，并在 Elastic Security 中呈现统一的控制面板和检测，从而无需部署代理即可更快地进行分类和调查。

产品链接

合作伙伴文档

Fortinet – ForticNP

集成类型：接收

FortiCNP 是一款云原生防护产品，可将安全调查发现汇总为切实可行的见解，并根据风险评分确定安全见解的优先级，以减少警报疲劳并加快补救速度。

AWS Marketplace 链接

合作伙伴文档

IBM – QRadar

集成类型：接收

IBM QRadar SIEM 让安全团队能够快速、准确地检测威胁并确定其优先级，然后调查和响应威胁。

产品链接

合作伙伴文档

Logz.io 云 SIEM

集成类型：接收

Logz.io 是一家提供 Cloud SIEM 的提供商，它提供日志和事件数据高级关联，可帮助安全团队实时检测、分析和应对安全威胁。

产品链接

合作伙伴文档

MetricStream – CyberGRC

集成类型：接收

MetricStream CyberGRC 帮助您管理、衡量和降低网络安全风险。通过接收 Security Hub CSPM 调查发现，CyberGRC 让您可以更清楚地了解这些风险，因此您可以优先考虑网络安全投资并遵守 IT 策略。

AWS 商城链接

产品链接

MicroFocus – MicroFocus 弧视网

集成类型：接收

ArcSight 实时加速有效的威胁检测和响应，将事件关联以及受监督和无监督的分析与响应自动化和编排相结合。

产品链接

合作伙伴文档

全新 Relic 漏洞管理

集成类型：接收

New Relic Vulnerability Management 接收来自 Security Hub CSPM 的安全调查发现，因此您可以集中查看整个堆栈中情境的安全情况以及性能遥测数据。

AWS 商城链接

合作伙伴文档

PagerDuty – PagerDuty

集成类型：接收

PagerDuty 的数字运营管理平台让团队能够自动将任何信号转化为适当的见解和操作，从而主动缓解影响客户的问题。

AWS 用户可以放心地使用这PagerDuty组 AWS 集成来扩展其 AWS 和混合环境。

与 Security Hub CSPM 聚合和组织的安全警报结合使用时，PagerDuty 让团队自动化威胁响应流程并快速设置自定义操作以防止潜在问题。

正在进行云迁移项目的 PagerDuty 用户可以快速迁移，同时减少整个迁移生命周期中发生的问题的影响。

产品链接

合作伙伴文档

Palo Alto Networks – Cortex XSOAR

集成类型：接收

Cortex XSOAR 是一种安全编排、自动化和响应（SOAR）平台，可与您的整个安全产品堆栈集成，以加快事件响应和安全操作。

产品链接

合作伙伴文档

Palo Alto Networks – VM-Series

集成类型：接收

Palo Alto VM-Series 与 Security Hub CSPM 集成可收集威胁情报，并将其作为自动安全策略更新发送到 VM-Series 下一代防火墙，从而阻止恶意 IP 地址活动。

产品链接

合作伙伴文档

机架空间技术 – 原生云安全性

集成类型：接收

Rackspace Technology 在本机 AWS 安全产品之上提供托管安全服务，通过 Rackspace SOC 进行 24x7x365 监控、高级分析和威胁修复。

产品链接

Rapid7 – InsightConnect

集成类型：接收

Rapid7 InsightConnect 是一种安全编排和自动化解决方案，使您的团队无需编写代码即可优化 SOC 操作。

产品链接

合作伙伴文档

RSA – RSA Archer

集成类型：接收

RSA Archer IT 和安全风险管理让您可以确定哪些资产对您的业务至关重要，制定和传达安全策略和标准，检测和应对攻击，识别和修复安全缺陷，并建立明确的 IT 风险管理最佳实践。

产品链接

合作伙伴文档

ServiceNow – ITSM

集成类型：接收和更新

ServiceNow 与 Security Hub CSPM 集成允许在 ServiceNow ITSM 内部查看 Security Hub CSPM 的安全调查发现。您也可以配置 ServiceNow 以在收到来自 Security Hub CSPM 的调查发现时自动创建事件或问题。

对这些事件和问题的任何更新都会导致 Security Hub CSPM 中的调查发现更新。

有关集成及其工作原理的概述，请观看视频 AWS Security Hub CSPM - 与 ServiceNow ITSM 的双向集成。

产品链接

合作伙伴文档

Slack – Slack

集成类型：接收

Slack 是业务技术堆栈中的一层，它将人员、数据和应用程序组合在一起。它可让人员有效地协同工作、查找重要信息和访问数十万种关键应用程序和服务，以取得最佳的工作成果。

产品链接

合作伙伴文档

Splunk – Splunk Enterprise

集成类型：接收

Splunk使用 Amazon E CloudWatch vents 作为 Security Hub CSPM 调查结果的使用者。将您的数据发送到 Splunk 以进行高级安全分析和 SIEM。

产品链接

合作伙伴文档

Splunk – Splunk Phantom

集成类型：接收

使用 Sec AWS urity Hub CSPM Splunk Phantom 应用程序，可以将发现结果发送到，Phantom以便使用额外的威胁情报信息自动丰富上下文，或者执行自动响应操作。

产品链接

合作伙伴文档

ThreatModeler

集成类型：接收

ThreatModeler 是一种自动威胁建模解决方案，可保护和扩展企业软件和云开发生命周期。

产品链接

合作伙伴文档

Trellix – Trellix Helix

集成类型：接收

Trellix Helix 是一个云托管的安全操作平台，可让组织控制从警报到修复的任何事件。

产品链接

合作伙伴文档

Third-party 将调查结果发送到 Security Hub CSPM 并从中接收调查结果的集成

以下第三方合作伙伴产品集成可以向 Security Hub CSPM 发送调查发现并从中接收调查发现。

Caveonix – Caveonix Cloud

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

该Caveonix AI-powered 平台可自动实现混合云中的可见性、评估和缓解措施，涵盖云原生服务、虚拟机和容器。与 Securit AWS y Hub CSPM 集成，可Caveonix合并 AWS 数据和高级分析，以深入了解安全警报和合规性。

AWS 商城链接

合作伙伴文档

Cloud Custodian – Cloud Custodian

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian 使用户能够在云端得到良好的管理。简单的 YAML DSL 允许轻松定义规则，以实现安全且成本优化的管理良好的云基础设施。

产品链接

合作伙伴文档

DisruptOps, Inc. – DisruptOPS

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps 的安全运营平台通过使用自动化护栏，帮助企业在云中维护最佳安全实践。

产品链接

合作伙伴文档

Kion

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion（前身为 cloudtamer.io）是一款针对 AWS的全套云治理解决方案。Kion 让利益相关者了解云运营情况，帮助云用户管理账户、控件预算和成本，并确保持续合规。

产品链接

合作伙伴文档

Turbot – Turbot

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot 可确保您的云基础设施安全、合规、可扩展且保持最优成本。

产品链接

合作伙伴文档

将 Security Hub CSPM 与自定义产品集成

除了集成 AWS 服务和第三方产品生成的调查结果外，Sec AWS urity Hub CSPM 还可以使用其他定制安全产品生成的调查结果。

您可以使用 Security Hub CSPM API 的 BatchImportFindings 操作将这些调查发现发送到 Security Hub CSPM。您可以使用相同的操作来更新自定义产品中已发送到 Security Hub CSPM 的调查发现。

设置自定义集成时，请使用《Security Hub CSPM 合作伙伴集成指南》中提供的指南和清单。

自定义产品集成的要求和建议

在成功调用 `BatchImportFindings` API 操作之前，您必须启用 Security Hub CSPM。

您还必须使用 the section called “调查发现格式：ASFF” 提供自定义产品的调查发现详细信息。查看自定义产品集成的以下要求和建议：

设置产品 ARN

启用 Security Hub CSPM 时，会在当前账户中为 Security Hub CSPM 生成默认产品 Amazon 资源名称（ARN）。

该产品 ARN 具有以下格式：`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`。例如 `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`。

调用 `BatchImportFindings` API 操作时，请使用此产品 ARN 作为 `ProductArn` 属性的值。

设置公司名称和产品名称

您可以使用 `BatchImportFindings` 为将调查发现发送到 Security Hub CSPM 的自定义集成设置首选公司名称和产品名称。

您指定的名称将替换预先配置的公司名称和产品名称（分别称为个人名称和默认名称），并显示在 Security Hub CSPM 控制台和每个调查发现的 JSON 中。请参阅BatchImportFindings 用于寻找提供者。

设置结果 ID

您必须使用 `Id` 属性提供、管理和增加您自己的结果 ID。

每个新调查发现应具有唯一的调查发现 ID。如果自定义产品发送了多个具有相同调查发现 ID 的调查发现，则 Security Hub CSPM 仅会处理第一个调查发现。

设置账户 ID

您必须使用 `AwsAccountId` 属性指定您自己的账户 ID。

设置创建日期和更新日期

您必须为 `CreatedAt` 和 `UpdatedAt` 属性提供您自己的时间戳。

更新来自自定义产品的结果

除了从自定义产品发送新结果以外，您还可以使用 `BatchImportFindings` API 操作更新来自自定义产品的现有结果。

要更新现有结果，请使用现有结果 ID（通过 `Id` 属性）。使用请求中更新的相应信息（包括修改后的 `UpdatedAt` 时间戳）重新发送完整的结果。

示例自定义集成

您可以使用以下示例自定义产品集成作为指南来创建您自己的自定义解决方案：

将 Chef InSpec 扫描的调查发现发送到 Security Hub CSPM

您可以创建一个 CloudFormation 模板来运行Chef InSpec合规性扫描，然后将结果发送到 Security Hub CSPM。

有关更多详细信息，请参阅 Continuous compliance monitoring with Chef InSpec and AWS Security Hub CSPM。

将 Trivy 检测到的容器漏洞发送到 Security Hub CSPM

您可以创建一个用于扫描容器中是否存在漏洞的 CloudFormation 模板，然后将这些漏洞发现发送到 Security Hub CSPM。AquaSecurity Trivy

有关更多详细信息，请参阅如何使用Trivy和 Sec AWS urity Hub CSPM 构建容器漏洞扫描 CI/CD 管道。

在 Security Hub CSPM 中创建和更新调查发现

在 Sec AWS urity Hub CSPM 中，发现是安全检查或安全相关检测的可观察记录。调查发现可能来自以下来源之一：

- Security Hub CSPM 中控件的安全检查。
- 与他人的集成 AWS 服务。
- 与第三方产品的集成。
- 自定义集成。

Security Hub CSPM 将所有来源中的调查发现标准化为一种标准语法和格式，称为 AWS 安全调查发现格式（ASFF）。有关此格式的详细信息，包括各个 ASFF 字段的描述，请参阅 AWS 安全调查结果格式 (ASFF)。如果启用跨区域聚合，Security Hub CSPM 还会自动将所有关联区域中新增和更新的调查发现聚合到您指定的聚合区域中。有关更多信息，请参阅 了解 Security Hub CSPM 中的跨区域聚合。

创建调查发现后，可以按如下方式进行更新：

- 调查发现提供者可以使用 Security Hub CSPM API 的 BatchImportFindings 操作更新有关调查发现的一般信息。结果提供商只能更新他们创建的结果。
- 客户可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API 的 BatchUpdateFindings 操作来更新对调查发现的调查状态。SIEM、票证、事件管理、SOAR 或其他类型的工具也可以代表客户使用 `BatchUpdateFindings` 操作。

为了减少调查发现噪音并简化对单个调查发现的跟踪和分析，Security Hub CSPM 会自动删除最近未更新的调查发现。Security Hub CSPM 执行此操作的时间取决于调查发现是处于活跃状态还是已存档：

- 活跃调查发现是指其记录状态（`RecordState`）为 `ACTIVE` 的调查发现。Security Hub CSPM 会将活跃调查发现存储 90 天。如果某活跃调查发现已 90 天未更新，则其将过期，并且 Security Hub CSPM 会将其永久删除。
- 存档的调查发现是指其记录状态（`RecordState`）为 `ARCHIVED` 的调查发现。Security Hub CSPM 会将存档的调查发现存储 30 天。如果某存档的调查发现已 30 天未更新，则其将过期，并且 Security Hub CSPM 会将其永久删除。

对于控件调查发现（即 Security Hub CSPM 从控件的安全检查生成的调查发现），Security Hub CSPM 会根据调查发现的 `UpdatedAt` 字段的值来确定调查发现是否已过期。如果活跃调查发现的此值已超过 90 天，则 Security Hub CSPM 将永久删除该调查发现。如果存档的调查发现的此值已超过 30 天，则 Security Hub CSPM 将永久删除该调查发现。

对于所有其他类型的调查发现，Security Hub CSPM 会根据调查发现的 `ProcessedAt` 和 `UpdatedAt` 字段的值来确定调查发现是否已过期。Security Hub CSPM 会比较这些字段的值，并确定哪个值是最新的。如果活跃调查发现的最新值已超过 90 天，则 Security Hub CSPM 将永久删除该调查发现。如果存档的调查发现的最新值已超过 30 天，则 Security Hub CSPM 将永久删除该调查发现。调查发现提供者可以使用 Security Hub CSPM API 的 BatchImportFindings 操作来更改一个或多个调查发现的 `UpdatedAt` 字段的值。

为了长期保留调查发现，您可以将调查发现导出到 S3 存储桶。您可以通过使用带有 Amazon EventBridge 规则的自定义操作来实现此目的。有关更多信息，请参阅 EventBridge 用于自动响应和补救。

主题

- BatchImportFindings 用于寻找提供者
- BatchUpdateFindings 为顾客服务

- 在 Security Hub CSPM 中查看调查发现详细信息和历史记录
- 在 Security Hub CSPM 中筛选调查发现
- 在 Security Hub CSPM 中对调查发现进行分组
- 在 Security Hub CSPM 中设置调查发现的工作流状态
- 将调查发现发送到自定义 Security Hub CSPM 操作
- AWS 安全调查结果格式 (ASFF)

BatchImportFindings 用于寻找提供者

调查发现提供者可以使用 BatchImportFindings 操作在 AWS Security Hub CSPM 中创建新的调查发现。他们还可以使用此操作来更新自己创建的调查发现。调查发现提供者无法更新他们未创建的调查发现。

客户、SIEMS、票证、SOAR 和其他类型的工具必须使用 BatchUpdateFindings 操作进行与来自调查发现提供者的调查发现的调查相关的更新。有关更多信息，请参阅 the section called “BatchUpdateFindings 为顾客服务”。

当 Security Hub CSPM 收到创建或更新调查结果的`BatchImportFindings`请求时，它会自动在亚马逊中生成一个Security Hub Findings - Imported事件。 EventBridge您可以对该事件执行自动操作。有关更多信息，请参阅 the section called “自动响应和补救”。

使用 `BatchImportFindings` 的先决条件

`BatchImportFindings` 必须由以下之一调用：

- 与调查发现关联的账户。相关账户的标识符必须与调查发现的 `AwsAccountId` 属性值相匹配。
- 列入官方 Security Hub CSPM 合作伙伴集成允许列表的账户。

Security Hub CSPM 只能接受已启用 Security Hub CSPM 的账户的调查发现更新。还必须启用结果提供商。如果禁用 Security Hub CSPM，或者未启用调查发现提供者集成，则会在 `FailedFindings` 列表中返回调查发现，并显示 `InvalidAccess` 错误。

确定是创建还是更新结果

要确定是创建还是更新调查发现，Security Hub CSPM 需要检查 `ID` 字段。如果 `ID` 的值与现有调查发现不匹配，则 Security Hub CSPM 会创建新的调查发现。

如果 ID 与现有调查发现匹配，则 Security Hub CSPM 会检查 UpdatedAt 字段是否有更新，并按如下方式继续：

- 如果更新的 UpdatedAt 匹配或出现在现有调查发现的 UpdatedAt 之前，则 Security Hub CSPM 会忽略更新请求。
- 如果更新的 UpdatedAt 出现在现有结果的 UpdatedAt 之后，则 Security Hub CSPM 会更新现有调查发现。

使用 **BatchImportFindings** 对调查发现进行更新的限制

调查发现提供者无法使用 BatchImportFindings 更新现有调查发现的以下属性：

- Note
- UserDefinedFields
- VerificationState
- Workflow

Security Hub CSPM 会忽略在 BatchImportFindings 请求这些属性时提供的任何内容。客户或代表他们行事的实体（例如票证工具）可以使用 BatchUpdateFindings 更新这些属性。

使用更新调查结果 FindingProviderFields

查找提供者也不应使用BatchImportFindings来更新 AWS 安全调查结果格式 (ASFF) 中的以下顶级属性：

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

相反，调查发现提供者应使用 FindingProviderFields 对象为这些属性提供值。

示例

```
"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" ]
}
```

对于 BatchImportFindings 请求，Security Hub CSPM 按如下方式处理顶级属性和 FindingProviderFields 中的值。

（首选）**BatchImportFindings** 为 **FindingProviderFields** 中的属性提供值，但并未为相应的顶级属性提供值。

例如，BatchImportFindings 提供 FindingProviderFields.Confidence，但不提供 Confidence。这是 BatchImportFindings 请求的首选选项。

Security Hub CSPM 更新 FindingProviderFields 中属性的值。

仅当属性尚未由 BatchUpdateFindings 更新时，它才会将该值复制到顶级属性。

BatchImportFindings 为顶级属性提供值，但不为 **FindingProviderFields** 中的相应属性提供值。

例如，BatchImportFindings 提供 Confidence，但不提供 FindingProviderFields.Confidence。

Security Hub CSPM 使用该值来更新 FindingProviderFields 中的属性。它会覆盖任何现有值。

只有当顶级属性尚未由 BatchUpdateFindings 更新时，Security Hub CSPM 才会更新该属性。

BatchImportFindings 为顶级属性和 **FindingProviderFields** 中的相应属性提供了一个值。

例如，BatchImportFindings 同时提供 Confidence 和 FindingProviderFields.Confidence。

对于新调查发现，Security Hub CSPM 使用 FindingProviderFields 中的值填充顶级属性和 FindingProviderFields 中的相应属性。它不使用提供的顶级属性值。

对于现有调查发现，Security Hub CSPM 使用这两个值。但是，只有当属性尚未由 BatchUpdateFindings 更新时，它才会更新顶级属性值。

BatchUpdateFindings 为顾客服务

AWS Security Hub CSPM客户和代表他们行事的实体可以使用该BatchUpdateFindings操作来更新与处理Security Hub CSPM调查结果相关的信息，这些信息来自寻找提供商。作为客户，您可以直接使用此操作。SIEM、票证、事件管理和 SOAR 工具也可以代表客户使用此操作。

您不能使用 BatchUpdateFindings 操作来创建新的调查发现。但是，您可以使用它一次性更新多达 100 个现有调查发现。在BatchUpdateFindings请求中，您可以指定要更新的调查结果、要为查找结果更新哪些 AWS 安全结果格式 (ASFF) 字段，以及这些字段的新值。Security Hub CSPM 随后会按照您的请求指定的内容更新调查发现。此过程可能耗时数分钟。如果您使用 BatchUpdateFindings 操作更新调查发现，则更新不会影响调查发现 UpdatedAt 字段的现有值。

当 Security Hub CSPM 收到更新调查结果的BatchUpdateFindings请求时，它会自动在亚马逊中生成一个Security Hub Findings – Imported事件。 EventBridge您还可以选择使用此事件对指定的调查发现执行自动操作。有关更多信息，请参阅 the section called “自动响应和补救”。

的可用字段 BatchUpdateFindings

如果您已登录 Security Hub CSPM 管理员账户，则可以使用 BatchUpdateFindings 更新该管理员账户或成员账户生成的调查发现。成员账户仅可以使用 BatchUpdateFindings 更新其账户的调查发现。

客户可以使用 BatchUpdateFindings 更新以下字段和对象：

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields

- VerificationState
- Workflow

配置访问权限 BatchUpdateFindings

您可以配置 AWS Identity and Access Management (IAM) 策略以限制访问权限，使用BatchUpdateFindings来更新查找字段和字段值。

在限制访问 BatchUpdateFindings 的语句中，使用以下值：

- Action 是 securityhub:BatchUpdateFindings
- Effect 是 Deny
- 对于 Condition，您可以根据以下条件拒绝 BatchUpdateFindings 请求：
  - 调查发现包括一个特定的字段。
  - 调查发现包括一个特定的字段值。

条件键

这些是限制访问 BatchUpdateFindings 的条件键。

ASFF 字段

ASFF 字段的条件键如下所示：

```
securityhub:ASFFSyntaxPath/<fieldName>
```

<fieldName> 替换为 ASFF 字段。配置访问 BatchUpdateFindings 权限时，请在 IAM policy 中包含一个或多个特定的 ASFF 字段，而不是父级字段。例如，要限制对 Workflow.Status 字段的访问权限，您必须在策略中包含 securityhub:ASFFSyntaxPath/Workflow.Status 而不是 Workflow 父级字段。

禁止对某个字段进行所有更新

要防止用户对特定字段进行任何更新，请使用如下条件：

```
"Condition": {
               "Null": {
                   "securityhub:ASFFSyntaxPath/<fieldName>": "false"
```

```
                }
}
```

例如，以下语句表示 BatchUpdateFindings 不能用于更新调查发现的 Workflow.Status 字段。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

禁用特定的字段值

要防止用户将字段设置为特定值，请使用如下条件：

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
               }
}
```

例如，以下语句表示 BatchUpdateFindings 不能用于把 Workflow.Status 设置为 SUPPRESSED。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

您还可以提供不允许的值的列表。

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

例如，以下语句表示BatchUpdateFindings 不能用于把 Workflow.Status 设置为 RESOLVED 或 SUPPRESSED。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

在 Security Hub CSPM 中查看调查发现详细信息和历史记录

在 Sec AWS urity Hub CSPM 中，发现是安全检查或安全相关检测的可观察记录。在完成对控件的安全检查以及从集成 AWS 服务 或第三方产品中提取调查发现时，Security Hub CSPM 会生成调查发现。每项调查发现都包括更改历史记录和其他详细信息，例如严重性评级和有关受影响资源的信息。

您可以在 Security Hub CSPM 控制台上查看各个调查发现的历史记录和其他详细信息，也可以使用 Security Hub CSPM API 或 AWS CLI以编程方式查看。

为了帮助您简化分析，Security Hub CSPM 控制台会在您选择特定调查发现时显示调查发现面板。该面板包含不同的菜单和选项卡，用于查看调查发现的具体详细信息。

操作菜单

在此菜单中，您可以查看调查发现的完整 JSON 或添加注释。一项调查发现一次只能附上一个注释。此菜单还提供了用于设置查找结果的工作流程状态或将调查结果发送到 Amazon 中的自定义操作的选项 EventBridge。

调查菜单

在这个菜单中，您可以在 Amazon Detective 中对调查发现进行调查。Detective 从调查结果中提取实体，例如 IP 地址和 AWS 用户，并可视化他们的活动。您可以使用实体活动作为起点对调查发现的原因和影响进行调查。

“概述”选项卡

此选项卡提供调查发现的摘要。例如，您可以确定调查发现的创建时间和上次更新时间、调查发现所在的账户以及调查发现的来源。对于控件调查发现，此选项卡还会显示关联的 AWS Config 规则的名称以及指向 Security Hub CSPM 文档中补救指导的链接。

在概述选项卡上的资源快照中，您可以获得调查发现中涉及的资源的简要概述。对于某些资源，这包括打开资源选项，该选项直接链接到相关 AWS 服务 控制台上受影响的资源。历史记录快照最多会显示在所跟踪历史记录的最近日期对调查发现所做的两次更改。例如，如果您昨天进行了更改，今天又进行了另一个更改，则快照会显示今天的更改。要查看之前的条目，请切换到历史记录选项卡。

展开合规行将显示更多详细信息。例如，如果某个控件包含参数，您可以查看 Security Hub CSPM 在对该控件进行安全检查时当前使用的参数值。

“资源”选项卡

此选项卡提供有关调查发现中涉及的资源的详细信息。如果您登录的是拥有资源的账户，则可以在相应的 AWS 服务 控制台中查看该资源。如果您不是资源的所有者，则此选项卡会显示所有者的 AWS 账户 ID。

详细信息行显示调查发现中特定于资源的详细信息。它以 JSON 格式显示调查发现的 ResourceDetails 部分。

标签行显示分配给调查发现中涉及的资源的标签键和值。可以标记 AWS Resource Groups 标记 API 的 GetResources 操作支持的资源。Security Hub CSPM 在处理新的或更新的调查发现时，会使用服务相关角色调用此操作，并且如果 AWS 安全调查发现格式（ASFF）`Resource.Id` 字段填充了资源的 ARN，则会检索资源标签。Security Hub CSPM 会忽略无效的资源 ID。有关在调查发现中包含资源标签的更多信息，请参阅 标签。

“历史记录”选项卡

此选项卡跟踪调查发现的历史记录。调查发现的历史记录适用于活动和已归档的调查发现。它提供随着时间推移对调查发现所做的更改的不可改变跟踪，包括 ASFF 字段更改的内容、更改发生的时间以及由哪个用户所做的更改。选项卡上的每个页面最多显示 20 个更改。最近的更改优先显示。

对于活跃调查发现，调查发现历史记录最多可保留 90 天。对于存档的调查发现，调查发现历史记录最多可保留 30 天。调查发现历史记录包括手动进行的更改或通过 Security Hub CSPM 自动化规则自动进行的更改。它不包括对顶级时间戳字段的更改，例如 `CreatedAt` 和 `UpdatedAt` 字段。

如果您登录了 Security Hub CSPM 管理员账户，则显示该管理员账户和所有成员账户的调查发现历史记录。

“威胁”选项卡

此选项卡包括 ASFF 的 Action、Malware 和 ProcessDetails 对象的数据，包括威胁类型以及资源是目标还是角色。这些详细信息通常适用于源自 Amazon GuardDuty 的调查结果。

“漏洞”选项卡

此选项卡显示 ASFF 的 Vulnerability 对象的数据，包括是否存在与调查发现关联的漏洞或可用的修复程序。这些详细信息通常适用于源自 Amazon Inspector 的调查发现。

每个选项卡上的行都包含复制或筛选选项。例如，如果您打开了工作流状态为已通知的调查发现的面板，则可以选择工作流状态行旁边的筛选选项。如果选择显示包含此值的所有调查发现，则 Security Hub CSPM 会筛选调查发现表格，仅显示具有相同工作流状态的调查发现。

查看调查发现的详细信息和历史记录

选择您喜欢的方法，然后按照以下步骤在 Security Hub CSPM 中查看调查发现详细信息。

如果您启用了跨区域聚合并登录了聚合区域，则调查发现将包括来自聚合区域和关联区域的数据。在其他区域，调查发现数据仅特定于当前区域。有关跨区域聚合的更多信息，请参阅 the section called “跨区域聚合数据”。

Security Hub CSPM console

查看调查发现的详细信息和历史记录

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 要显示调查发现列表，请执行以下操作之一：
   - 在导航窗格中，选择 调查发现。根据需要添加搜索筛选条件以缩小调查发现列表的范围。
   - 在导航窗格中，选择 Insights。选择见解。然后在结果列表中，选择一个见解结果。
   - 在导航窗格中，选择集成。选择查看集成的调查发现。
   - 在导航窗格中，选择控件。

3. 选择一个调查发现。调查发现面板显示调查发现的详细信息。
4. 在调查发现面板中，执行以下任一操作：

   - 要查看调查发现的特定详细信息，请选择一个选项卡。
   - 要对调查发现采取行动，请从操作菜单中选择一个选项。
   - 要在 Amazon Detective 中调查调查发现，请选择调查选项。

> **Note**
>
> 如果您集成 AWS Organizations 并登录了成员账户，则搜索面板中会包含账户名称。对于手动邀请而非通过 Organizations 邀请的成员账户，调查发现面板仅包括账户 ID。

Security Hub CSPM API

使用 Security Hub CSPM API 的GetFindings操作，或者如果你使用的是 AWS CLI，则运行命令。get-findings您可以为 `Filters` 参数提供一个或多个值，以缩小要检索的调查发现的范围。

如果调查发现的数量过大，则可以使用 `MaxResults` 参数将调查发现限制为指定数量，并使用 `NextToken` 参数对调查发现进行分页。使用 `SortCriteria` 参数以按特定字段对调查发现进行排序。

例如，以下 AWS CLI 命令检索符合指定筛选条件的结果，并按字段降序对结果进行排序。`LastObservedAt`此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

```
$ 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
```

要查看调查发现的历史记录，请使用 GetFindingHistory 操作。如果您使用的是 AWS CLI，请运行get-finding-history命令。使用 `ProductArn` 和 `Id` 字段确定要获取历史记录的调查发现。有关这些字段的信息，请参阅 AwsSecurityFindingIdentifier。每个请求只能检索一个调查发现的历史记录。

例如，以下 AWS CLI 命令检索指定查找结果的历史记录。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

```
$ 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

使用 `Get-SHUBFinding` cmdlet。或者，填充 `Filter` 参数以缩小要检索的调查发现的范围。

例如，以下 cmdlet 将检索与指定的筛选条件匹配的调查发现

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> 如果按 `CompanyName` 或 `ProductName` 筛选调查发现，Security Hub 会使用属于 `ProductFields` ASFF 对象一部分的值。Security Hub CSPM 不使用顶级 `CompanyName` 和 `ProductName` 字段。

在 Security Hub CSPM 中筛选调查发现

AWS Security Hub CSPM 通过安全检查生成自己的调查结果，并从集成产品中接收调查结果。您可以在 Security Hub CSPM 控制台的调查发现、集成和见解页面上显示调查发现列表。您可以添加筛选条件来缩小调查发现列表的范围，使列表与您的组织或使用案例相关。

有关筛选特定安全控件的调查发现的信息，请参阅the section called “对控件调查发现进行筛选和排序”。本页上的信息适用于调查发现、见解和集成页面。

调查发现列表上的默认筛选条件

默认情况下，Security Hub CSPM 控制台上的调查发现列表是根据 AWS 安全调查发现格式（ASFF）的 `RecordState` 和 `Workflow.Status` 字段进行筛选的。这是特定见解或集成的筛选条件的补充。

记录状态指示调查发现处于活动状态还是存档状态。默认情况下，结果列表仅显示活动结果。如果调查发现不再处于活动状态或不再重要，则调查发现提供者可以将其归档。如果关联的资源被删除，Security Hub CSPM 还会自动归档控件调查发现。

工作流状态指示对调查发现进行的调查的状态。默认情况下，调查发现列表仅显示工作流状态为 NEW 或 NOTIFIED 的调查发现。您可以更新调查发现的工作流状态。

添加筛选条件的说明

您最多可以按十个属性筛选调查发现列表。对于每个属性，您最多可以提供 20 个筛选值。

筛选调查发现列表时，Security Hub CSPM 会将 AND 逻辑应用于筛选条件集。仅在调查发现符合所有提供的筛选条件时才被视为匹配的调查发现。例如，如果您添加GuardDuty 为产品名称的筛选器，并AwsS3Bucket添加为资源类型的筛选器，Security Hub CSPM 会显示符合这两个条件的搜索结果。

Security Hub CSPM 会对使用的属性相同但值不同的筛选条件应用 OR 逻辑。例如，如果您同时添加两者 GuardDuty 和 Amazon Inspector 作为商品名称的筛选值，Security Hub CSPM 会显示由任一方 GuardDuty 或亚马逊检查员生成的结果。

向调查发现列表添加筛选条件（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 要显示调查发现列表，请从导航窗格执行以下操作之一：
   - 选择调查发现。
   - 选择 Insights。选择见解。然后在结果列表上，选择一个见解结果。
   - 选择集成。选择查看集成的调查发现。
3. 在添加筛选条件框中，选择一个或多个要筛选的字段。

   当您按公司名称或产品名称筛选时，控制台将使用 AWS 安全调查结果格式 (ASFF) 的顶层CompanyName和ProductName字段。API 使用嵌套在 ProductFields 下的值。
4. 选择筛选器匹配类型。

   对于字符串筛选条件，您可以从以下选项中进行选择：
   - 是——查找与筛选值完全匹配的值。
   - 以...开头——查找以筛选值开头的值。
   - 不是——查找与筛选值不匹配的值。
   - 不以...开头——查找不以筛选值开头的值。

对于资源标签字段，您可以基于特定键或值进行筛选。

对于数值筛选条件，您可以选择是提供单个数字简单还是数值范围范围。

对于日期或时间筛选条件，您可以选择是提供从当前日期时间开始的时间长度滚动窗口还是提供具体日期范围固定范围。

添加多个筛选条件具有以下交互作用：

- 是和以...开头筛选条件由“或”连接。如果一个值包含任何筛选条件值，则该值匹配。例如，如果您将“严重性”标签指定为“重大”，“严重性”标签为“高”，则结果将包括重大和高严重性结果。
- 不是，不以...开头筛选条件由“和”连接的。仅当值不包含任何这些筛选条件值时才匹配。例如，如果您指定“严重性”标签不为“低”，“严重性”标签不为“中”，则结果不包括低或中等严重性调查发现。

如果在某个字段上有是的筛选条件，则不能在同一个字段上使用不是或不以.....开头的筛选条件。

5. 指定筛选器值。对于字符串筛选条件，筛选条件值区分大小写。
6. 选择应用。

对于现有筛选条件，您可以更改筛选条件匹配类型或值。在筛选后的调查发现列表中，选择筛选条件。在编辑筛选条件框中，选择新的匹配类型或值，然后选择应用。

要删除筛选条件，请选择 x 图标。列表会自动更新以反映更改。

在 Security Hub CSPM 中对调查发现进行分组

您可以根据所选属性的值对 Sec AWS urity Hub CSPM 中的发现结果进行分组。

对调查发现进行分组时，调查发现列表将替换为匹配调查发现中选定属性的值列表。对于每个值，列表会显示匹配调查发现的数量。

例如，如果您按 AWS 账户 ID 对发现结果进行分组，则会看到账户标识符列表，其中包含每个账户的匹配结果数量。

Security Hub CSPM 可以为选定的属性显示多达 100 个值。如果值超过 100 个，则只能看到前 100 个。

当您选择一个属性值时，Security Hub CSPM 会显示与该值匹配的调查发现列表。

将调查发现分组到调查发现列表中（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 要显示调查发现列表，请从导航窗格执行以下操作之一：
   - 选择调查发现。
   - 选择 Insights。选择见解。然后在结果列表上，选择一个见解结果。
   - 选择集成。选择查看集成的调查发现。
3. 在分组依据下拉列表中，选择要用于分组的属性。

   要删除分组属性，请选择 x 图标。删除分组属性时，列表将从属性值列表更改为调查发现列表。

在 Security Hub CSPM 中设置调查发现的工作流状态

工作流状态跟踪对调查发现的调查进度。工作流状态特定于单个调查发现，不会影响新调查发现的生成。例如，如果将调查发现的工作流状态更改为 SUPPRESSED 或 RESOLVED，则您的更改不会阻止 Security Hub CSPM 针对同一问题生成新的调查发现。

调查发现的工作流状态可以是以下值之一。

新

调查发现在被审查前的初始状态。

从集成 AWS 服务（例如）中提取的发现以 AWS Config其初始状态NEW为初始状态。

在以下情况下，Security Hub CSPM 还会将工作流状态从 NOTIFIED 或 RESOLVED 重置为 NEW：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status 从 PASSED 变为 FAILED、WARNING 或 NOT_AVAILABLE。

这些变化表明需要进一步调查。

NOTIFIED

表示您已将安全问题告知资源拥有者。如果您不是资源拥有者，并且需要资源拥有者的干预才能解决安全问题，则可以使用此状态。

如果出现以下情况之一，则工作流状态将自动从 NOTIFIED 更改为 NEW：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status 从 PASSED 变为 FAILED、WARNING 或 NOT_AVAILABLE。

SUPPRESSED

表示您已查看调查发现，但认为不需要采取任何操作。

如果 RecordState 从 ARCHIVED 变为 ACTIVE，则 SUPPRESSED 调查发现的工作流状态不会改变。

RESOLVED

已对结果进行审查并采取了补救措施，现在被视为已解决。

除非出现下列情况之一，否则调查发现将保持为 RESOLVED：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status 从 PASSED 变为 FAILED、WARNING 或 NOT_AVAILABLE。

在这种情况下，工作流状态会自动重置为 NEW。

对于来自控件的调查发现，如果 Compliance.Status 是 PASSED，则 Security Hub CSPM 会自动将工作流状态设置为 RESOLVED。

设置调查发现的工作流状态

要更改一个或多个调查发现的工作流状态，您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。如果您更改了调查发现的工作流状态，请注意，Security Hub CSPM 可能需要几分钟时间来处理您的请求并更新调查发现。

> **Tip**
>
> 您还可以使用自动化规则自动更改调查发现的工作流状态。通过自动化规则，您可以配置 Security Hub CSPM，使其根据您指定的条件自动更新调查发现的工作流状态。有关更多信息，请参阅 了解 Security Hub CSPM 中的自动化规则。

要更改一个或多个调查发现的工作流状态，请选择您喜欢的方法并按照步骤进行操作。

Security Hub CSPM console

更改调查发现的工作流状态

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

2. 在导航窗格中，执行以下操作之一以显示调查发现表格：

   - 选择调查发现。
   - 选择 Insights。然后选择一个见解。在见解结果中，选择一个结果。
   - 选择集成。然后，在集成的部分中，选择查看调查发现。
   - 选择安全标准。然后，在标准的部分中，选择查看结果。在控件表格中，选择一个控件以显示控件的调查发现。

3. 在调查发现表格中，选中要更改工作流状态的每个调查发现对应的复选框。
4. 在页面顶部，选择工作流状态，然后为所选调查发现选择新的工作流状态。
5. 在设置工作流状态对话框中，选择输入注释，以详细说明更改工作流状态的原因。然后选择设置状态。

Security Hub CSPM API

使用 BatchUpdateFindings 操作。提供用于生成调查发现的产品调查发现 ID 和 ARN。您可以使用GetFindings操作获取这些详细信息。

AWS CLI

运行 batch-update-findings 命令。提供用于生成调查发现的产品调查发现 ID 和 ARN。您可以通过运行 get-findings 命令来获取这些详细信息。

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

示例

```
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"
```

将调查发现发送到自定义 Security Hub CSPM 操作

你可以创建 S AWS ecurity Hub CSPM 自定义操作，通过亚马逊自动执行 Security Hub CSPM。EventBridge对于自定义操作，事件类型为 Security Hub Findings - Custom Action。设置自定义操作

后，您可以向其发送结果。有关创建自定义操作的更多信息和详细步骤，请参阅 the section called “自动响应和补救”。

将结果发送到自定义操作（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 要显示调查发现列表，请执行以下操作之一：
   - 在 Security Hub CSPM 导航窗格中，选择调查发现。
   - 在 Security Hub CSPM 导航窗格中，选择见解。选择见解。然后在结果列表上，选择一个见解结果。
   - 在 Security Hub CSPM 导航窗格中，选择集成。选择查看集成的调查发现。
   - 在 Security Hub CSPM 导航窗格中，选择安全标准。选择查看结果以显示控件列表。然后选择控件名称。
3. 在调查发现列表中，选中要发送到自定义操作的每个调查发现的复选框。

   您一次最多可以发送 20 个结果。
4. 对于操作，选择自定义操作。

AWS 安全调查结果格式 (ASFF)

AWS Security Hub CSPM 使用和汇总来自集成 AWS 服务 和第三方产品的发现。Security Hub CSPM 使用一种称为 AWS 安全调查发现格式（ASFF）的标准调查发现格式来处理这些调查发现，无需进行耗时的数据转换工作。

本页提供了 AWS 安全调查结果格式 (ASFF) 中查找结果的 JSON 的完整概述。该格式源自 JSON 架构。选择链接对象的名称，以查看该对象的调查发现示例。将 Security Hub CSPM 调查发现与此处显示的资源和示例进行比较，以帮助您解释调查发现。

有关各个 ASFF 属性的描述，请参阅the section called “必需的顶级 ASFF 属性”和the section called “可选顶级 ASFF 属性”。

```
"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"
     }
]
```

合并对 ASFF 字段和值的影响

AWS Security Hub CSPM 为控制提供了两种类型的整合：

- 整合控件视图 – 通过这种类型的整合，每个控件在所有标准中都有一个标识符。此外，在 Security Hub CSPM 控制台上，控件页面显示所有标准的所有控件。
- 整合的控件调查发现 – 通过这种整合，Security Hub CSPM 可以为控件生成一个调查发现，即使该控件适用于多个已启用标准也是如此。这样可以减少调查发现噪音。

您无法启用或禁用整合控件视图。如果您在 2023 年 2 月 23 日当天或之后启用 Security Hub CSPM，则默认情况下会启用整合的控件调查发现。否则，默认情况下禁用。但是，对于组织，只有当为管理员账户启用整合的控件调查发现时，Security Hub CSPM 成员帐户才能启用该功能。要了解有关整合的控件调查发现的更多信息，请参阅生成和更新控件调查发现。

这两种类型的整合都会影响 AWS 安全调查结果格式 (ASFF) 安全调查发现格式（ASFF）中控件调查发现的字段和值。

主题

- 整合的控件视图——ASFF 变更
- 整合的控件调查发现——ASFF 的变化
- 启用整合的控件调查发现之前和之后的生成器 ID
- 整合如何影响控件 ID 和标题
- 更新工作流以进行整合。

整合的控件视图——ASFF 变更

整合的控件视图功能对 ASFF 中的控件调查发现的字段和值进行了以下更改。如果您的工作流不依赖于这些 ASFF 字段的值，则无需执行任何操作。如果有工作流依赖于这些字段的特定值，请更新工作流以使用当前值。

ASFF 字段	整合的控件视图之前的样本值	整合的控件视图后的样本值以及更改描述
Compliance.SecurityControlId	不适用（新字段）	EC2.2 引入各类标准的单一控件 ID。`ProductFields.Rule`

ASFF 字段	整合的控件视图之前的样本值	整合的控件视图后的样本值以及更改描述
		`Id` 仍然为 CIS v1.2.0 控件提供基于标准的控件 ID。`ProductFields.ControlId` 仍然为其他标准中的控件提供基于标准的控件 ID。
Compliance.AssociatedStandards	不适用（新字段）	[{" StandardsId ":"-f standards /aws oundational-security-best-/1.0.0 "}] practices/v 显示启用控件的标准。
ProductFields.ArchivalReasons:0/Description	不适用（新字段）	"调查发现处于已存档状态，因为整合的控件调查发现已开启或关闭。这会导致在生成新调查发现时存档先前状态的调查发现。" 描述 Security Hub CSPM 为何对现有调查发现进行存档。
ProductFields.ArchivalReasons:0/ReasonCode	不适用（新字段）	"CONSOLIDATED_CONTROL_FINDINGS_UPDATE" 提供 Security Hub CSPM 存档现有调查发现的原因。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此字段不再引用标准。

ASFF 字段	整合的控件视图之前的样本值	整合的控件视图后的样本值以及更改描述
Remediation.Recommendation.Text	“有关如何解决此问题的说明，请查阅 Sec AWS urity Hub CSPM PCI DSS 文档。”	“有关如何更正此问题的说明，请参阅 Sec AWS urity Hub CSPM 控制文档。” 此字段不再引用标准。
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此字段不再引用标准。

整合的控件调查发现——ASFF 的变化

如果您启用整合的控件调查发现，则可能会受到 ASFF 中的控件调查发现的字段和值的以下更改影响。这些更改是对整合的控件视图功能引入的更改的补充。如果您的工作流不依赖于这些 ASFF 字段的值，则无需执行任何操作。如果有工作流依赖于这些字段的特定值，请更新工作流以使用当前值。

> **Tip**
>
> 如果您在 AWS v2.0.0 上使用自动安全响应解决方案，请注意它支持整合的控制结果。这意味着，如果您启用整合的控件调查发现，则可以保持当前的工作流。

ASFF 字段	启用整合的控件调查发现之前的示例值	启用整合的控件调查发现后的示例值和更改的描述
GeneratorId	aws-foundational-security-best-/1.practices/v 0/Config.1	安全性-control/Config .1 此字段不再引用标准。
标题	PCI.Config.1 AWS Config 应该启用	AWS Config 应该启用 该字段将不再引用特定于标准的信息。

ASFF 字段	启用整合的控件调查发现之前的示例值	启用整合的控件调查发现后的示例值和更改的描述
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 此字段不再引用标准。
ProductFields.ControlId	PCI.EC2.2	已删除。请改而参阅 `Compliance.SecurityControlId` 。 该字段已被删除，取而代之的是单一的、与标准无关的控制 ID。
ProductFields.RuleId	1.3	已删除。请改而参阅 `Compliance.SecurityControlId` 。 该字段已被删除，取而代之的是单一的、与标准无关的控制 ID。
说明	此 PCI DSS 控件检查当前账户和地区 AWS Config 是否已启用。	此 AWS 控件检查当前账户和区域中 AWS Config 是否已启用。 此字段不再引用标准。

严重性	"Severity": {
	
	“产品”：90，
	
	“标签”：“重大”，
	
	“标准化”：90，
	
	“原始”：“重大”
	
	}
		"Severity": {
		
		“标签”：“重大”，
		
		“标准化”：90，
		
		“原始”：“重大”
		
		}
		
		Security Hub CSPM 将不再使用“产品”字段描述调查发现的严重性。

ASFF 字段	启用整合的控件调查发现之前的示例值	启用整合的控件调查发现后的示例值和更改的描述
类型	[“软件、配置 Checks/Industry 和监管 Standards/PCI-DSS”]	[“软件和配置 Checks/Industry 及监管标准”] 此字段不再引用标准。
Compliance.Related Requirements	["PCI DSS 10.5.2", "PCI DSS 11.5", “CIS AWS 基金会 2.5"]	[” PCI DSS v3.2。 1/10.5.2 英寸， “PCI DSS v3.2。 1/11.5 英寸， “CIS AWS 基金会基准测试版本 1.2。 0/2.5"] 该字段将显示所有启用标准中的相关要求。
CreatedAt	2022-05-05 T08:18:13.138Z	2022-09-25 T08:18:13.138Z 格式将保持不变，但是当您打开整合的控件调查发现时，值将重置。
FirstObservedAt	2022-05-07 T08:18:13.138Z	2022-09-28 T08:18:13.138Z 格式将保持不变，但是当您打开整合的控件调查发现时，值将重置。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	已删除。请改而参阅 `Remediation.Recommendation.Url` 。
ProductFields.StandardsArn	arn: aws: securityhub:::-foundational-security-best-/standards/aws practices/v	已删除。请改而参阅 `Compliance.AssociatedStandards` 。

ASFF 字段	启用整合的控件调查发现之前的示例值	启用整合的控件调查发现后的示例值和更改的描述
ProductFields.StandardsControlArn	arn: aws: securityhub: us-east-1 :123456789012:-foundational-security-best-/1.0。control/aws practices/v 0/Config.1	已删除。Security Hub CSPM 针对各标准的安全检查生成调查发现。
ProductFields.StandardsGuideArn	arn: aws: securityhub:::-aws -foundations-/ ruleset/cis benchmark/v	已删除。请改而参阅 `Compliance.AssociatedStandards` 。
ProductFields.StandardsGuideSubscriptionArn	arn: aws: securityhub: us-east-2 :123456789012:-aws-foundations-/1.2.0 subscription/cis benchmark/v	已删除。Security Hub CSPM 针对各标准的安全检查生成调查发现。
ProductFields.StandardsSubscriptionArn	arn: aws: securityhub: us-east-1 :123456789012:-foundational-security-best-/1.0.0 subscription/aws practices/v	已删除。Security Hub CSPM 针对各标准的安全检查生成调查发现。
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-a5 210dfb1d67	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 此字段不再引用标准。

启用整合的控件调查发现后，客户提供的 ASFF 字段的值

如果您启用整合的控件调查发现，Security Hub CSPM 会生成一个各类标准的调查发现并存档原始调查发现（每个标准都有单独的调查发现）。

使用 Security Hub CSPM 控制台或 BatchUpdateFindings 操作对原始调查发现所做的更新将不会保留在新调查发现中。如有必要，您可以参考存档的调查发现来恢复此数据。要查看已存档的调查发现，您

可以使用 Security Hub CSPM 控制台上的调查发现页面，并将记录状态筛选条件设置为 ARCHIVED。或者，您可以使用 Security Hub CSPM API 的 GetFindings 操作。

Customer-provided ASFF 字段	启用整合的控件调查发现后的更改的描述
置信度	重置为空状态。
严重性	重置为空状态。
备注	重置为空状态。
RelatedFindings	重置为空状态。
严重性	调查发现的默认严重性（与控件的严重性相匹配）。
类型	重置为与标准无关的值。
UserDefinedFields	重置为空状态。
VerificationState	重置为空状态。
工作流	新的失败调查发现的默认值为 NEW。新通过的调查发现的默认值为 RESOLVED。

启用整合的控件调查发现之前和之后的生成器 ID

下表列出了启用整合的控件调查发现时控件的生成器 ID 值的变化。这些更改适用于自 2023 年 2 月 15 日起 Security Hub CSPM 支持的控件。

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
arn: aws: securityhub:::-aws-foundations-/ruleset/cis benchmark/v 0/rule/1.1	安全性-control/CloudWatch .1
arn: aws: securityhub:::-aws-foundations-/ruleset/cis benchmark/v 0/rule/1.10	secur control/IAM ity-.16

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.11	secur control/IAM ity-.17
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.12	安全-control/IAM .4
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.13	安全-control/IAM .9
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.14	安全-control/IAM .6
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.16	安全性-control/IAM .2
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.2	安全-control/IAM .5
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.20	secur control/IAM ity-.18
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.22	安全性-control/IAM .1
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.3	安全-control/IAM .8
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.4	安全-control/IAM .3
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.5	secur control/IAM ity-.11
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.6	secur control/IAM ity-.12
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.7	secur control/IAM ity-.13

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.8	secur control/IAM ity-.14
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/1.9	secur control/IAM ity-.15
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.1	安全性-control/CloudTrail .1
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.2	安全-control/CloudTrail .4
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.3	安全-control/CloudTrail .6
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.4	安全-control/CloudTrail .5
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.5	安全性-control/Config .1
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.6	安全-control/CloudTrail .7
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.7	安全性-control/CloudTrail .2
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.8	安全-control/KMS .4
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/2.9	安全-control/EC2 .6
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.1	安全性-control/CloudWatch .2
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.2	安全性-control/CloudWatch .3

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.3	安全性-control/CloudWatch .1
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.4	安全-control/CloudWatch .4
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.5	安全-control/CloudWatch .5
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.6	安全-control/CloudWatch .6
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.7	安全-control/CloudWatch .7
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.8	安全-control/CloudWatch .8
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.9	安全-control/CloudWatch .9
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.10	secur control/CloudWatch ity-.10
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.11	安全性-control/CloudWatch .11
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.12	secur control/CloudWatch ity-.12
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.13	secur control/CloudWatch ity-.13
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/3.14	secur control/CloudWatch ity-.14
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/4.1	secur control/EC2 ity-.13

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/4.2	secur control/EC2 ity-.14
arn: aws: securityhub:::-aws-foundations-/ ruleset/cis benchmark/v 0/rule/4.3	安全性-control/EC2 .2
cis-aws-foundations-/1.4 benchmark/v 0/1.10	安全-control/IAM .5
cis-aws-foundations-/1.4 benchmark/v 0/1.14	安全性-control/IAM .3
cis-aws-foundations-/1.4 benchmark/v 0/1.16	安全性-control/IAM .1
cis-aws-foundations-/1.4 benchmark/v 0/1.17	secur control/IAM ity-.18
cis-aws-foundations-/1.4 benchmark/v 0/1.4	安全-control/IAM .4
cis-aws-foundations-/1.4 benchmark/v 0/1.5	安全-control/IAM .9
cis-aws-foundations-/1.4 benchmark/v 0/1.6	安全-control/IAM .6
cis-aws-foundations-/1.4 benchmark/v 0/1.7	安全性-control/CloudWatch .1
cis-aws-foundations-/1.4 benchmark/v 0/1.8	secur control/IAM ity-.15
cis-aws-foundations-/1.4 benchmark/v 0/1.9	secur control/IAM ity-.16
cis-aws-foundations-/1.4 benchmark/v 0/2.1.2	安全-control/S3 .5
cis-aws-foundations-/1.4 benchmark/v 0/2.1.5.1	安全性-control/S3 .1
cis-aws-foundations-/1.4 benchmark/v 0/2.1.5.2	安全-control/S3 .8
cis-aws-foundations-/1.4 benchmark/v 0/2.2.1	安全-control/EC2 .7
cis-aws-foundations-/1.4 benchmark/v 0/2.3.1	安全性-control/RDS .3
cis-aws-foundations-/1.4 benchmark/v 0/3.1	安全性-control/CloudTrail .1
cis-aws-foundations-/1.4 benchmark/v 0/3.2	安全-control/CloudTrail .4

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
cis-aws-foundations-/1.4 benchmark/v 0/3.4	安全-control/CloudTrail .5
cis-aws-foundations-/1.4 benchmark/v 0/3.5	安全性-control/Config .1
cis-aws-foundations-/1.4 benchmark/v 0/3.6	安全-control/S3 .9
cis-aws-foundations-/1.4 benchmark/v 0/3.7	安全性-control/CloudTrail .2
cis-aws-foundations-/1.4 benchmark/v 0/3.8	安全-control/KMS .4
cis-aws-foundations-/1.4 benchmark/v 0/3.9	安全-control/EC2 .6
cis-aws-foundations-/1.4 benchmark/v 0/4.3	安全性-control/CloudWatch .1
cis-aws-foundations-/1.4 benchmark/v 0/4.4	安全-control/CloudWatch .4
cis-aws-foundations-/1.4 benchmark/v 0/4.5	安全-control/CloudWatch .5
cis-aws-foundations-/1.4 benchmark/v 0/4.6	安全-control/CloudWatch .6
cis-aws-foundations-/1.4 benchmark/v 0/4.7	安全-control/CloudWatch .7
cis-aws-foundations-/1.4 benchmark/v 0/4.8	安全-control/CloudWatch .8
cis-aws-foundations-/1.4 benchmark/v 0/4.9	安全-control/CloudWatch .9
cis-aws-foundations-/1.4 benchmark/v 0/4.10	secur control/CloudWatch ity-.10
cis-aws-foundations-/1.4 benchmark/v 0/4.11	安全性-control/CloudWatch .11
cis-aws-foundations-/1.4 benchmark/v 0/4.12	secur control/CloudWatch ity-.12
cis-aws-foundations-/1.4 benchmark/v 0/4.13	secur control/CloudWatch ity-.13
cis-aws-foundations-/1.4 benchmark/v 0/4.14	secur control/CloudWatch ity-.14
cis-aws-foundations-/1.4 benchmark/v 0/5.1	secur control/EC2 ity-.21
cis-aws-foundations-/1.4 benchmark/v 0/5.3	安全性-control/EC2 .2

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ Account.1	安全性-control/Account .1
aws-foundational-security-best-/1. practices/v 0/ ACM.1	安全性-control/ACM .1
aws-foundational-security-best-/1. practices/v 0/ APIGateway.1	安全性-control/APIGateway .1
aws-foundational-security-best-/1. practices/v 0/ APIGateway.2	安全性-control/APIGateway .2
aws-foundational-security-best-/1. practices/v 0/ APIGateway.3	安全性-control/APIGateway .3
aws-foundational-security-best-/1. practices/v 0/ APIGateway.4	安全-control/APIGateway .4
aws-foundational-security-best-/1. practices/v 0/ APIGateway.5	安全-control/APIGateway .5
aws-foundational-security-best-/1. practices/v 0/ APIGateway.8	安全-control/APIGateway .8
aws-foundational-security-best-/1. practices/v 0/ APIGateway.9	安全-control/APIGateway .9
aws-foundational-security-best-/1. practices/v 0/ AutoScaling.1	安全性-control/AutoScaling .1
aws-foundational-security-best-/1. practices/v 0/ AutoScaling.2	安全性-control/AutoScaling .2
aws-foundational-security-best-/1. practices/v 0/ AutoScaling.3	安全性-control/AutoScaling .3
aws-foundational-security-best-/1. practices/v 0/ Autoscaling.5	安全-control/Autoscaling .5

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/AutoScaling.6	安全-control/AutoScaling .6
aws-foundational-security-best-/1. practices/v 0/AutoScaling.9	安全-control/AutoScaling .9
aws-foundational-security-best-/1. practices/v 0/CloudFront.1	安全性-control/CloudFront .1
aws-foundational-security-best-/1. practices/v 0/CloudFront.3	安全性-control/CloudFront .3
aws-foundational-security-best-/1. practices/v 0/CloudFront.4	安全-control/CloudFront .4
aws-foundational-security-best-/1. practices/v 0/CloudFront.5	安全-control/CloudFront .5
aws-foundational-security-best-/1. practices/v 0/CloudFront.6	安全-control/CloudFront .6
aws-foundational-security-best-/1. practices/v 0/CloudFront.7	安全-control/CloudFront .7
aws-foundational-security-best-/1. practices/v 0/CloudFront.8	安全-control/CloudFront .8
aws-foundational-security-best-/1. practices/v 0/CloudFront.9	安全-control/CloudFront .9
aws-foundational-security-best-/1. practices/v 0/CloudFront.10	secur control/CloudFront ity-.10
aws-foundational-security-best-/1. practices/v 0/CloudFront.12	secur control/CloudFront ity-.12
aws-foundational-security-best-/1. practices/v 0/CloudTrail.1	安全性-control/CloudTrail .1

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/CloudTrail.2	安全性-control/CloudTrail .2
aws-foundational-security-best-/1. practices/v 0/CloudTrail.4	安全-control/CloudTrail .4
aws-foundational-security-best-/1. practices/v 0/CloudTrail.5	安全-control/CloudTrail .5
aws-foundational-security-best-/1. practices/v 0/CodeBuild.1	安全性-control/CodeBuild .1
aws-foundational-security-best-/1. practices/v 0/CodeBuild.2	安全性-control/CodeBuild .2
aws-foundational-security-best-/1. practices/v 0/CodeBuild.3	安全性-control/CodeBuild .3
aws-foundational-security-best-/1. practices/v 0/CodeBuild.4	安全-control/CodeBuild .4
aws-foundational-security-best-/1. practices/v 0/Config.1	安全性-control/Config .1
aws-foundational-security-best-/1. practices/v 0/DMS.1	安全性-control/DMS .1
aws-foundational-security-best-/1. practices/v 0/DynamoDB.1	安全性-control/DynamoDB .1
aws-foundational-security-best-/1. practices/v 0/DynamoDB.2	安全性-control/DynamoDB .2
aws-foundational-security-best-/1. practices/v 0/DynamoDB.3	安全性-control/DynamoDB .3
aws-foundational-security-best-/1. practices/v 0/EC2.1	安全性-control/EC2 .1

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/EC2.3	安全性-control/EC2 .3
aws-foundational-security-best-/1. practices/v 0/EC2.4	安全-control/EC2 .4
aws-foundational-security-best-/1. practices/v 0/EC2.6	安全-control/EC2 .6
aws-foundational-security-best-/1. practices/v 0/EC2.7	安全-control/EC2 .7
aws-foundational-security-best-/1. practices/v 0/EC2.8	安全-control/EC2 .8
aws-foundational-security-best-/1. practices/v 0/EC2.9	安全-control/EC2 .9
aws-foundational-security-best-/1. practices/v 0/EC2.10	secur control/EC2 ity-.10
aws-foundational-security-best-/1. practices/v 0/EC2.15	secur control/EC2 ity-.15
aws-foundational-security-best-/1. practices/v 0/EC2.16	secur control/EC2 ity-.16
aws-foundational-security-best-/1. practices/v 0/EC2.17	secur control/EC2 ity-.17
aws-foundational-security-best-/1. practices/v 0/EC2.18	secur control/EC2 ity-.18
aws-foundational-security-best-/1. practices/v 0/EC2.19	secur control/EC2 ity-.19
aws-foundational-security-best-/1. practices/v 0/EC2.2	安全性-control/EC2 .2

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ EC2.20	secur control/EC2 ity-.20
aws-foundational-security-best-/1. practices/v 0/ EC2.21	secur control/EC2 ity-.21
aws-foundational-security-best-/1. practices/v 0/ EC2.23	secur control/EC2 ity-.23
aws-foundational-security-best-/1. practices/v 0/ EC2.24	secur control/EC2 ity-.24
aws-foundational-security-best-/1. practices/v 0/ EC2.25	secur control/EC2 ity-.25
aws-foundational-security-best-/1. practices/v 0/ ECR.1	安全性-control/ECR .1
aws-foundational-security-best-/1. practices/v 0/ ECR.2	安全性-control/ECR .2
aws-foundational-security-best-/1. practices/v 0/ ECR.3	安全性-control/ECR .3
aws-foundational-security-best-/1. practices/v 0/ ECS.10	secur control/ECS ity-.10
aws-foundational-security-best-/1. practices/v 0/ ECS.12	secur control/ECS ity-.12
aws-foundational-security-best-/1. practices/v 0/ ECS.2	安全性-control/ECS .2
aws-foundational-security-best-/1. practices/v 0/ ECS.3	安全性-control/ECS .3
aws-foundational-security-best-/1. practices/v 0/ ECS.4	安全-control/ECS .4

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ ECS.5	安全-control/ECS .5
aws-foundational-security-best-/1. practices/v 0/ ECS.8	安全-control/ECS .8
aws-foundational-security-best-/1. practices/v 0/ EFS.1	安全性-control/EFS .1
aws-foundational-security-best-/1. practices/v 0/ EFS.2	安全性-control/EFS .2
aws-foundational-security-best-/1. practices/v 0/ EFS.3	安全性-control/EFS .3
aws-foundational-security-best-/1. practices/v 0/ EFS.4	安全-control/EFS .4
aws-foundational-security-best-/1. practices/v 0/ EKS.2	安全性-control/EKS .2
aws-foundational-security-best-/1. practices/v 0/ ElasticBeanstalk.1	安全性-control/ElasticBeanstalk .1
aws-foundational-security-best-/1. practices/v 0/ ElasticBeanstalk.2	安全性-control/ElasticBeanstalk .2
aws-foundational-security-best-/1. practices/v 0/ ELBv2.1	安全性-control/ELB .1
aws-foundational-security-best-/1. practices/v 0/ ELB.2	安全性-control/ELB .2
aws-foundational-security-best-/1. practices/v 0/ ELB.3	安全性-control/ELB .3
aws-foundational-security-best-/1. practices/v 0/ ELB.4	安全-control/ELB .4

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ ELB.5	安全-control/ELB .5
aws-foundational-security-best-/1. practices/v 0/ ELB.6	安全-control/ELB .6
aws-foundational-security-best-/1. practices/v 0/ ELB.7	安全-control/ELB .7
aws-foundational-security-best-/1. practices/v 0/ ELB.8	安全-control/ELB .8
aws-foundational-security-best-/1. practices/v 0/ ELB.9	安全-control/ELB .9
aws-foundational-security-best-/1. practices/v 0/ ELB.10	secur control/ELB ity-.10
aws-foundational-security-best-/1. practices/v 0/ ELB.11	安全性-control/ELB .11
aws-foundational-security-best-/1. practices/v 0/ ELB.12	secur control/ELB ity-.12
aws-foundational-security-best-/1. practices/v 0/ ELB.13	secur control/ELB ity-.13
aws-foundational-security-best-/1. practices/v 0/ ELB.14	secur control/ELB ity-.14
aws-foundational-security-best-/1. practices/v 0/ EMR.1	安全性-control/EMR .1
aws-foundational-security-best-/1. practices/v 0/ ES.1	安全性-control/ES .1
aws-foundational-security-best-/1. practices/v 0/ ES.2	安全性-control/ES .2

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ ES.3	安全性-control/ES .3
aws-foundational-security-best-/1. practices/v 0/ ES.4	安全-control/ES .4
aws-foundational-security-best-/1. practices/v 0/ ES.5	安全-control/ES .5
aws-foundational-security-best-/1. practices/v 0/ ES.6	安全-control/ES .6
aws-foundational-security-best-/1. practices/v 0/ ES.7	安全-control/ES .7
aws-foundational-security-best-/1. practices/v 0/ ES.8	安全-control/ES .8
aws-foundational-security-best-/1. practices/v 0/ GuardDuty.1	安全性-control/GuardDuty .1
aws-foundational-security-best-/1. practices/v 0/ IAM.1	安全性-control/IAM .1
aws-foundational-security-best-/1. practices/v 0/ IAM.2	安全性-control/IAM .2
aws-foundational-security-best-/1. practices/v 0/ IAM.21	secur control/IAM ity-.21
aws-foundational-security-best-/1. practices/v 0/ IAM.3	安全性-control/IAM .3
aws-foundational-security-best-/1. practices/v 0/ IAM.4	安全-control/IAM .4
aws-foundational-security-best-/1. practices/v 0/ IAM.5	安全-control/IAM .5

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/IAM.6	安全-control/IAM .6
aws-foundational-security-best-/1. practices/v 0/IAM.7	安全-control/IAM .7
aws-foundational-security-best-/1. practices/v 0/IAM.8	安全-control/IAM .8
aws-foundational-security-best-/1. practices/v 0/Kinesis.1	安全性-control/Kinesis .1
aws-foundational-security-best-/1. practices/v 0/KMS.1	安全性-control/KMS .1
aws-foundational-security-best-/1. practices/v 0/KMS.2	安全性-control/KMS .2
aws-foundational-security-best-/1. practices/v 0/KMS.3	安全性-control/KMS .3
aws-foundational-security-best-/1. practices/v 0/Lambda.1	安全性-control/Lambda .1
aws-foundational-security-best-/1. practices/v 0/Lambda.2	安全性-control/Lambda .2
aws-foundational-security-best-/1. practices/v 0/Lambda.5	安全-control/Lambda .5
aws-foundational-security-best-/1. practices/v 0/NetworkFirewall.3	安全性-control/NetworkFirewall .3
aws-foundational-security-best-/1. practices/v 0/NetworkFirewall.4	安全-control/NetworkFirewall .4
aws-foundational-security-best-/1. practices/v 0/NetworkFirewall.5	安全-control/NetworkFirewall .5

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ NetworkFirewall.6	安全-control/NetworkFirewall .6
aws-foundational-security-best-/1. practices/v 0/ Opensearch.1	安全性-control/Opensearch .1
aws-foundational-security-best-/1. practices/v 0/ Opensearch.2	安全性-control/Opensearch .2
aws-foundational-security-best-/1. practices/v 0/ Opensearch.3	安全性-control/Opensearch .3
aws-foundational-security-best-/1. practices/v 0/ Opensearch.4	安全-control/Opensearch .4
aws-foundational-security-best-/1. practices/v 0/ Opensearch.5	安全-control/Opensearch .5
aws-foundational-security-best-/1. practices/v 0/ Opensearch.6	安全-control/Opensearch .6
aws-foundational-security-best-/1. practices/v 0/ Opensearch.7	安全-control/Opensearch .7
aws-foundational-security-best-/1. practices/v 0/ Opensearch.8	安全-control/Opensearch .8
aws-foundational-security-best-/1. practices/v 0/ RDS.1	安全性-control/RDS .1
aws-foundational-security-best-/1. practices/v 0/ RDS.10	secur control/RDS ity-.10
aws-foundational-security-best-/1. practices/v 0/ RDS.11	安全性-control/RDS .11
aws-foundational-security-best-/1. practices/v 0/ RDS.12	secur control/RDS ity-.12

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ RDS.13	secur control/RDS ity-.13
aws-foundational-security-best-/1. practices/v 0/ RDS.14	secur control/RDS ity-.14
aws-foundational-security-best-/1. practices/v 0/ RDS.15	secur control/RDS ity-.15
aws-foundational-security-best-/1. practices/v 0/ RDS.16	secur control/RDS ity-.16
aws-foundational-security-best-/1. practices/v 0/ RDS.17	secur control/RDS ity-.17
aws-foundational-security-best-/1. practices/v 0/ RDS.19	secur control/RDS ity-.19
aws-foundational-security-best-/1. practices/v 0/ RDS.2	安全性-control/RDS .2
aws-foundational-security-best-/1. practices/v 0/ RDS.20	secur control/RDS ity-.20
aws-foundational-security-best-/1. practices/v 0/ RDS.21	secur control/RDS ity-.21
aws-foundational-security-best-/1. practices/v 0/ RDS.22	secur control/RDS ity-.22
aws-foundational-security-best-/1. practices/v 0/ RDS.23	secur control/RDS ity-.23
aws-foundational-security-best-/1. practices/v 0/ RDS.24	secur control/RDS ity-.24
aws-foundational-security-best-/1. practices/v 0/ RDS.25	secur control/RDS ity-.25

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/RDS.3	安全性-control/RDS .3
aws-foundational-security-best-/1. practices/v 0/RDS.4	安全-control/RDS .4
aws-foundational-security-best-/1. practices/v 0/RDS.5	安全-control/RDS .5
aws-foundational-security-best-/1. practices/v 0/RDS.6	安全-control/RDS .6
aws-foundational-security-best-/1. practices/v 0/RDS.7	安全-control/RDS .7
aws-foundational-security-best-/1. practices/v 0/RDS.8	安全-control/RDS .8
aws-foundational-security-best-/1. practices/v 0/RDS.9	安全-control/RDS .9
aws-foundational-security-best-/1. practices/v 0/Redshift.1	安全性-control/Redshift .1
aws-foundational-security-best-/1. practices/v 0/Redshift.2	安全性-control/Redshift .2
aws-foundational-security-best-/1. practices/v 0/Redshift.3	安全性-control/Redshift .3
aws-foundational-security-best-/1. practices/v 0/Redshift.4	安全-control/Redshift .4
aws-foundational-security-best-/1. practices/v 0/Redshift.6	安全-control/Redshift .6
aws-foundational-security-best-/1. practices/v 0/Redshift.7	安全-control/Redshift .7

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ Redshift.8	安全-control/Redshift .8
aws-foundational-security-best-/1. practices/v 0/ S3.1	安全性-control/S3 .1
aws-foundational-security-best-/1. practices/v 0/ S3.12	secur control/S3 ity-.12
aws-foundational-security-best-/1. practices/v 0/ S3.13	secur control/S3 ity-.13
aws-foundational-security-best-/1. practices/v 0/ S3.2	安全性-control/S3 .2
aws-foundational-security-best-/1. practices/v 0/ S3.3	安全性-control/S3 .3
aws-foundational-security-best-/1. practices/v 0/ S3.5	安全-control/S3 .5
aws-foundational-security-best-/1. practices/v 0/ S3.6	安全-control/S3 .6
aws-foundational-security-best-/1. practices/v 0/ S3.8	安全-control/S3 .8
aws-foundational-security-best-/1. practices/v 0/ S3.9	安全-control/S3 .9
aws-foundational-security-best-/1. practices/v 0/ SageMaker.1	安全性-control/SageMaker .1
aws-foundational-security-best-/1. practices/v 0/ SageMaker.2	安全性-control/SageMaker .2
aws-foundational-security-best-/1. practices/v 0/ SageMaker.3	安全性-control/SageMaker .3

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/ SecretsManager.1	安全性-control/SecretsManager .1
aws-foundational-security-best-/1. practices/v 0/ SecretsManager.2	安全性-control/SecretsManager .2
aws-foundational-security-best-/1. practices/v 0/ SecretsManager.3	安全性-control/SecretsManager .3
aws-foundational-security-best-/1. practices/v 0/ SecretsManager.4	安全-control/SecretsManager .4
aws-foundational-security-best-/1. practices/v 0/ SQS.1	安全性-control/SQS .1
aws-foundational-security-best-/1. practices/v 0/ SSM.1	安全性-control/SSM .1
aws-foundational-security-best-/1. practices/v 0/ SSM.2	安全性-control/SSM .2
aws-foundational-security-best-/1. practices/v 0/ SSM.3	安全性-control/SSM .3
aws-foundational-security-best-/1. practices/v 0/ SSM.4	安全-control/SSM .4
aws-foundational-security-best-/1. practices/v 0/ WAF.1	安全性-control/WAF .1
aws-foundational-security-best-/1. practices/v 0/ WAF.2	安全性-control/WAF .2
aws-foundational-security-best-/1. practices/v 0/ WAF.3	安全性-control/WAF .3
aws-foundational-security-best-/1. practices/v 0/ WAF.4	安全-control/WAF .4

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
aws-foundational-security-best-/1. practices/v 0/WAF.6	安全-control/WAF .6
aws-foundational-security-best-/1. practices/v 0/WAF.7	安全-control/WAF .7
aws-foundational-security-best-/1. practices/v 0/WAF.8	安全-control/WAF .8
aws-foundational-security-best-/1. practices/v 0/WAF.10	secur control/WAF ity-.10
pci-dss/v /3.2. 1/PCI。 AutoScaling.1	安全性-control/AutoScaling .1
pci-dss/v /3.2. 1/PCI。 CloudTrail.1	安全性-control/CloudTrail .2
pci-dss/v /3.2. 1/PCI。 CloudTrail.2	安全性-control/CloudTrail .3
pci-dss/v /3.2. 1/PCI。 CloudTrail.3	安全-control/CloudTrail .4
pci-dss/v /3.2. 1/PCI。 CloudTrail.4	安全-control/CloudTrail .5
pci-dss/v /3.2. 1/PCI。 CodeBuild.1	安全性-control/CodeBuild .1
pci-dss/v /3.2. 1/PCI。 CodeBuild.2	安全性-control/CodeBuild .2
pci-dss/v /3.2. 1/PCI。 Config.1	安全性-control/Config .1
pci-dss/v /3.2. 1/PCI。 CW.1	安全性-control/CloudWatch .1
pci-dss/v /3.2. 1/PCI。 DMS.1	安全性-control/DMS .1
pci-dss/v /3.2. 1/PCI。 EC2.1	安全性-control/EC2 .1
pci-dss/v /3.2. 1/PCI。 EC2.2	安全性-control/EC2 .2
pci-dss/v /3.2. 1/PCI。 EC2.4	secur control/EC2 ity-.12
pci-dss/v /3.2. 1/PCI。 EC2.5	secur control/EC2 ity-.13

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
pci-dss/v /3.2. 1/PCI。 EC2.6	安全-control/EC2 .6
pci-dss/v /3.2. 1/PCI。 ELBv2.1	安全性-control/ELB .1
pci-dss/v /3.2. 1/PCI。 ES.1	安全性-control/ES .2
pci-dss/v /3.2. 1/PCI。 ES.2	安全性-control/ES .1
pci-dss/v /3.2. 1/PCI。 GuardDuty.1	安全性-control/GuardDuty .1
pci-dss/v /3.2. 1/PCI。 IAM.1	安全-control/IAM .4
pci-dss/v /3.2. 1/PCI。 IAM.2	安全性-control/IAM .2
pci-dss/v /3.2. 1/PCI。 IAM.3	安全性-control/IAM .1
pci-dss/v /3.2. 1/PCI。 IAM.4	安全-control/IAM .6
pci-dss/v /3.2. 1/PCI。 IAM.5	安全-control/IAM .9
pci-dss/v /3.2. 1/PCI。 IAM.6	secur control/IAM ity-.19
pci-dss/v /3.2. 1/PCI。 IAM.7	安全-control/IAM .8
pci-dss/v /3.2. 1/PCI。 IAM.8	secur control/IAM ity-.10
pci-dss/v /3.2. 1/PCI。 KMS.1	安全-control/KMS .4
pci-dss/v /3.2. 1/PCI。 Lambda.1	安全性-control/Lambda .1
pci-dss/v /3.2. 1/PCI。 Lambda.2	安全性-control/Lambda .3
pci-dss/v /3.2. 1/PCI。 Opensearch.1	安全性-control/Opensearch .2
pci-dss/v /3.2. 1/PCI。 Opensearch.2	安全性-control/Opensearch .1
pci-dss/v /3.2. 1/PCI。 RDS.1	安全性-control/RDS .1
pci-dss/v /3.2. 1/PCI。 RDS.2	安全性-control/RDS .2

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
pci-dss/v /3.2. 1/PCI。 Redshift.1	安全性-control/Redshift .1
pci-dss/v /3.2. 1/PCI。 S3.1	安全性-control/S3 .3
pci-dss/v /3.2. 1/PCI。 S3.2	安全性-control/S3 .2
pci-dss/v /3.2. 1/PCI。 S3.3	安全-control/S3 .7
pci-dss/v /3.2. 1/PCI。 S3.5	安全-control/S3 .5
pci-dss/v /3.2. 1/PCI。 S3.6	安全性-control/S3 .1
pci-dss/v /3.2. 1/PCI。 SageMaker.1	安全性-control/SageMaker .1
pci-dss/v /3.2. 1/PCI。 SSM.1	安全性-control/SSM .2
pci-dss/v /3.2. 1/PCI。 SSM.2	安全性-control/SSM .3
pci-dss/v /3.2. 1/PCI。 SSM.3	安全性-control/SSM .1
服务管理-aws-control-/1.0。tower/v 0/ACM.1	安全性-control/ACM .1
服务管理-aws-control-/1.0。tower/v 0/APIGateway.1	安全性-control/APIGateway .1
服务管理-aws-control-/1.0。tower/v 0/APIGateway.2	安全性-control/APIGateway .2
服务管理-aws-control-/1.0。tower/v 0/APIGateway.3	安全性-control/APIGateway .3
服务管理-aws-control-/1.0。tower/v 0/APIGateway.4	安全-control/APIGateway .4
服务管理-aws-control-/1.0。tower/v 0/APIGateway.5	安全-control/APIGateway .5
服务管理-aws-control-/1.0。tower/v 0/AutoScaling.1	安全性-control/AutoScaling .1

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/AutoScaling.2	安全性-control/AutoScaling .2
服务管理-aws-control-/1.0。tower/v 0/AutoScaling.3	安全性-control/AutoScaling .3
服务管理-aws-control-/1.0。tower/v 0/AutoScaling.4	安全-control/AutoScaling .4
服务管理-aws-control-/1.0。tower/v 0/Autoscaling.5	安全-control/Autoscaling .5
服务管理-aws-control-/1.0。tower/v 0/AutoScaling.6	安全-control/AutoScaling .6
服务管理-aws-control-/1.0。tower/v 0/AutoScaling.9	安全-control/AutoScaling .9
服务管理-aws-control-/1.0。tower/v 0/CloudTrail.1	安全性-control/CloudTrail .1
服务管理-aws-control-/1.0。tower/v 0/CloudTrail.2	安全性-control/CloudTrail .2
服务管理-aws-control-/1.0。tower/v 0/CloudTrail.4	安全-control/CloudTrail .4
服务管理-aws-control-/1.0。tower/v 0/CloudTrail.5	安全-control/CloudTrail .5
服务管理-aws-control-/1.0。tower/v 0/CodeBuild.1	安全性-control/CodeBuild .1
服务管理-aws-control-/1.0。tower/v 0/CodeBuild.2	安全性-control/CodeBuild .2
服务管理-aws-control-/1.0。tower/v 0/CodeBuild.4	安全-control/CodeBuild .4

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/CodeBuild.5	安全-control/CodeBuild .5
服务管理-aws-control-/1.0。tower/v 0/DMS.1	安全性-control/DMS .1
服务管理-aws-control-/1.0。tower/v 0/DynamoDB.1	安全性-control/DynamoDB .1
服务管理-aws-control-/1.0。tower/v 0/DynamoDB.2	安全性-control/DynamoDB .2
服务管理-aws-control-/1.0。tower/v 0/EC2.1	安全性-control/EC2 .1
服务管理-aws-control-/1.0。tower/v 0/EC2.2	安全性-control/EC2 .2
服务管理-aws-control-/1.0。tower/v 0/EC2.3	安全性-control/EC2 .3
服务管理-aws-control-/1.0。tower/v 0/EC2.4	安全-control/EC2 .4
服务管理-aws-control-/1.0。tower/v 0/EC2.6	安全-control/EC2 .6
服务管理-aws-control-/1.0。tower/v 0/EC2.7	安全-control/EC2 .7
服务管理-aws-control-/1.0。tower/v 0/EC2.8	安全-control/EC2 .8
服务管理-aws-control-/1.0。tower/v 0/EC2.9	安全-control/EC2 .9
服务管理-aws-control-/1.0。tower/v 0/EC2.10	secur control/EC2 ity-.10
服务管理-aws-control-/1.0。tower/v 0/EC2.15	secur control/EC2 ity-.15
服务管理-aws-control-/1.0。tower/v 0/EC2.16	secur control/EC2 ity-.16
服务管理-aws-control-/1.0。tower/v 0/EC2.17	secur control/EC2 ity-.17
服务管理-aws-control-/1.0。tower/v 0/EC2.18	secur control/EC2 ity-.18
服务管理-aws-control-/1.0。tower/v 0/EC2.19	secur control/EC2 ity-.19
服务管理-aws-control-/1.0。tower/v 0/EC2.20	secur control/EC2 ity-.20

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/EC2.21	secur control/EC2 ity-.21
服务管理-aws-control-/1.0。tower/v 0/EC2.22	secur control/EC2 ity-.22
服务管理-aws-control-/1.0。tower/v 0/ECR.1	安全性-control/ECR .1
服务管理-aws-control-/1.0。tower/v 0/ECR.2	安全性-control/ECR .2
服务管理-aws-control-/1.0。tower/v 0/ECR.3	安全性-control/ECR .3
服务管理-aws-control-/1.0。tower/v 0/ECS.2	安全性-control/ECS .2
服务管理-aws-control-/1.0。tower/v 0/ECS.3	安全性-control/ECS .3
服务管理-aws-control-/1.0。tower/v 0/ECS.4	安全-control/ECS .4
服务管理-aws-control-/1.0。tower/v 0/ECS.5	安全-control/ECS .5
服务管理-aws-control-/1.0。tower/v 0/ECS.8	安全-control/ECS .8
服务管理-aws-control-/1.0。tower/v 0/ECS.10	secur control/ECS ity-.10
服务管理-aws-control-/1.0。tower/v 0/ECS.12	secur control/ECS ity-.12
服务管理-aws-control-/1.0。tower/v 0/EFS.1	安全性-control/EFS .1
服务管理-aws-control-/1.0。tower/v 0/EFS.2	安全性-control/EFS .2
服务管理-aws-control-/1.0。tower/v 0/EFS.3	安全性-control/EFS .3
服务管理-aws-control-/1.0。tower/v 0/EFS.4	安全-control/EFS .4
服务管理-aws-control-/1.0。tower/v 0/EKS.2	安全性-control/EKS .2
服务管理-aws-control-/1.0。tower/v 0/ELB.2	安全性-control/ELB .2
服务管理-aws-control-/1.0。tower/v 0/ELB.3	安全性-control/ELB .3
服务管理-aws-control-/1.0。tower/v 0/ELB.4	安全-control/ELB .4

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/ELB.5	安全-control/ELB .5
服务管理-aws-control-/1.0。tower/v 0/ELB.6	安全-control/ELB .6
服务管理-aws-control-/1.0。tower/v 0/ELB.7	安全-control/ELB .7
服务管理-aws-control-/1.0。tower/v 0/ELB.8	安全-control/ELB .8
服务管理-aws-control-/1.0。tower/v 0/ELB.9	安全-control/ELB .9
服务管理-aws-control-/1.0。tower/v 0/ELB.10	secur control/ELB ity-.10
服务管理-aws-control-/1.0。tower/v 0/ELB.12	secur control/ELB ity-.12
服务管理-aws-control-/1.0。tower/v 0/ELB.13	secur control/ELB ity-.13
服务管理-aws-control-/1.0。tower/v 0/ELB.14	secur control/ELB ity-.14
服务管理-aws-control-/1.0。tower/v 0/ELBv2.1	安全性-control/ELBv2 .1
服务管理-aws-control-/1.0。tower/v 0/EMR.1	安全性-control/EMR .1
服务管理-aws-control-/1.0。tower/v 0/ES.1	安全性-control/ES .1
服务管理-aws-control-/1.0。tower/v 0/ES.2	安全性-control/ES .2
服务管理-aws-control-/1.0。tower/v 0/ES.3	安全性-control/ES .3
服务管理-aws-control-/1.0。tower/v 0/ES.4	安全-control/ES .4
服务管理-aws-control-/1.0。tower/v 0/ES.5	安全-control/ES .5
服务管理-aws-control-/1.0。tower/v 0/ES.6	安全-control/ES .6
服务管理-aws-control-/1.0。tower/v 0/ES.7	安全-control/ES .7
服务管理-aws-control-/1.0。tower/v 0/ES.8	安全-control/ES .8
服务管理-aws-control-/1.0。tower/v 0/Elastic Beanstalk.1	安全性-control/ElasticBeanstalk .1

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/Elastic Beanstalk.2	安全性-control/ElasticBeanstalk .2
服务管理-aws-control-/1.0。tower/v 0/GuardDuty.1	安全性-control/GuardDuty .1
服务管理-aws-control-/1.0。tower/v 0/IAM.1	安全性-control/IAM .1
服务管理-aws-control-/1.0。tower/v 0/IAM.2	安全性-control/IAM .2
服务管理-aws-control-/1.0。tower/v 0/IAM.3	安全性-control/IAM .3
服务管理-aws-control-/1.0。tower/v 0/IAM.4	安全-control/IAM .4
服务管理-aws-control-/1.0。tower/v 0/IAM.5	安全-control/IAM .5
服务管理-aws-control-/1.0。tower/v 0/IAM.6	安全-control/IAM .6
服务管理-aws-control-/1.0。tower/v 0/IAM.7	安全-control/IAM .7
服务管理-aws-control-/1.0。tower/v 0/IAM.8	安全-control/IAM .8
服务管理-aws-control-/1.0。tower/v 0/IAM.21	secur control/IAM ity-.21
服务管理-aws-control-/1.0。tower/v 0/Kinesis.1	安全性-control/Kinesis .1
服务管理-aws-control-/1.0。tower/v 0/KMS.1	安全性-control/KMS .1
服务管理-aws-control-/1.0。tower/v 0/KMS.2	安全性-control/KMS .2
服务管理-aws-control-/1.0。tower/v 0/KMS.3	安全性-control/KMS .3
服务管理-aws-control-/1.0。tower/v 0/Lambda.1	安全性-control/Lambda .1
服务管理-aws-control-/1.0。tower/v 0/Lambda.2	安全性-control/Lambda .2

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/Lambda.5	安全-control/Lambda .5
服务管理-aws-control-/1.0。tower/v 0/NetworkFirewall.3	安全性-control/NetworkFirewall .3
服务管理-aws-control-/1.0。tower/v 0/NetworkFirewall.4	安全-control/NetworkFirewall .4
服务管理-aws-control-/1.0。tower/v 0/NetworkFirewall.5	安全-control/NetworkFirewall .5
服务管理-aws-control-/1.0。tower/v 0/NetworkFirewall.6	安全-control/NetworkFirewall .6
服务管理-aws-control-/1.0。tower/v 0/Opensearch.1	安全性-control/Opensearch .1
服务管理-aws-control-/1.0。tower/v 0/Opensearch.2	安全性-control/Opensearch .2
服务管理-aws-control-/1.0。tower/v 0/Opensearch.3	安全性-control/Opensearch .3
服务管理-aws-control-/1.0。tower/v 0/Opensearch.4	安全-control/Opensearch .4
服务管理-aws-control-/1.0。tower/v 0/Opensearch.5	安全-control/Opensearch .5
服务管理-aws-control-/1.0。tower/v 0/Opensearch.6	安全-control/Opensearch .6
服务管理-aws-control-/1.0。tower/v 0/Opensearch.7	安全-control/Opensearch .7
服务管理-aws-control-/1.0。tower/v 0/Opensearch.8	安全-control/Opensearch .8

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/RDS.1	安全性-control/RDS .1
服务管理-aws-control-/1.0。tower/v 0/RDS.2	安全性-control/RDS .2
服务管理-aws-control-/1.0。tower/v 0/RDS.3	安全性-control/RDS .3
服务管理-aws-control-/1.0。tower/v 0/RDS.4	安全-control/RDS .4
服务管理-aws-control-/1.0。tower/v 0/RDS.5	安全-control/RDS .5
服务管理-aws-control-/1.0。tower/v 0/RDS.6	安全-control/RDS .6
服务管理-aws-control-/1.0。tower/v 0/RDS.8	安全-control/RDS .8
服务管理-aws-control-/1.0。tower/v 0/RDS.9	安全-control/RDS .9
服务管理-aws-control-/1.0。tower/v 0/RDS.10	secur control/RDS ity-.10
服务管理-aws-control-/1.0。tower/v 0/RDS.11	secur control/RDS ity-.11
服务管理-aws-control-/1.0。tower/v 0/RDS.13	secur control/RDS ity-.13
服务管理-aws-control-/1.0。tower/v 0/RDS.17	secur control/RDS ity-.17
服务管理-aws-control-/1.0。tower/v 0/RDS.19	secur control/RDS ity-.19
服务管理-aws-control-/1.0。tower/v 0/RDS.20	secur control/RDS ity-.20
服务管理-aws-control-/1.0。tower/v 0/RDS.21	secur control/RDS ity-.21
服务管理-aws-control-/1.0。tower/v 0/RDS.22	secur control/RDS ity-.22
服务管理-aws-control-/1.0。tower/v 0/RDS.23	secur control/RDS ity-.23
服务管理-aws-control-/1.0。tower/v 0/RDS.25	secur control/RDS ity-.25
服务管理-aws-control-/1.0。tower/v 0/Redshif t.1	安全性-control/Redshift .1

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/Redshift.2	安全性-control/Redshift .2
服务管理-aws-control-/1.0。tower/v 0/Redshift.4	安全-control/Redshift .4
服务管理-aws-control-/1.0。tower/v 0/Redshift.6	安全-control/Redshift .6
服务管理-aws-control-/1.0。tower/v 0/Redshift.7	安全-control/Redshift .7
服务管理-aws-control-/1.0。tower/v 0/Redshift.8	安全-control/Redshift .8
服务管理-aws-control-/1.0。tower/v 0/S3.1	安全性-control/S3 .1
服务管理-aws-control-/1.0。tower/v 0/S3.2	安全性-control/S3 .2
服务管理-aws-control-/1.0。tower/v 0/S3.3	安全性-control/S3 .3
服务管理-aws-control-/1.0。tower/v 0/S3.5	安全-control/S3 .5
服务管理-aws-control-/1.0。tower/v 0/S3.6	安全-control/S3 .6
服务管理-aws-control-/1.0。tower/v 0/S3.8	安全-control/S3 .8
服务管理-aws-control-/1.0。tower/v 0/S3.9	安全-control/S3 .9
服务管理-aws-control-/1.0。tower/v 0/S3.12	secur control/S3 ity-.12
服务管理-aws-control-/1.0。tower/v 0/S3.13	secur control/S3 ity-.13
服务管理-aws-control-/1.0。tower/v 0/SageMaker.1	安全性-control/SageMaker .1
服务管理-aws-control-/1.0。tower/v 0/SecretsManager.1	安全性-control/SecretsManager .1

启用整合的控件调查发现之前的生成器 ID	启用整合的控件调查发现之后的生成器 ID
服务管理-aws-control-/1.0。tower/v 0/Secrets Manager.2	安全性-control/SecretsManager .2
服务管理-aws-control-/1.0。tower/v 0/Secrets Manager.3	安全性-control/SecretsManager .3
服务管理-aws-control-/1.0。tower/v 0/Secrets Manager.4	安全-control/SecretsManager .4
服务管理-aws-control-/1.0。tower/v 0/SQS.1	安全性-control/SQS .1
服务管理-aws-control-/1.0。tower/v 0/SSM.1	安全性-control/SSM .1
服务管理-aws-control-/1.0。tower/v 0/SSM.2	安全性-control/SSM .2
服务管理-aws-control-/1.0。tower/v 0/SSM.3	安全性-control/SSM .3
服务管理-aws-control-/1.0。tower/v 0/SSM.4	安全-control/SSM .4
服务管理-aws-control-/1.0。tower/v 0/WAF.2	安全性-control/WAF .2
服务管理-aws-control-/1.0。tower/v 0/WAF.3	安全性-control/WAF .3
服务管理-aws-control-/1.0。tower/v 0/WAF.4	安全-control/WAF .4

整合如何影响控件 ID 和标题

整合的控件视图和整合的控件调查发现标准化了各类标准的控件 ID 和标题。安全控件 ID 和安全控件标题这两个术语是指这些与标准无关的值。

无论您的账户启用还是禁用了整合的控件调查发现，Security Hub CSPM 控制台都会显示与标准无关的安全控件 ID 和安全控件标题。但是，如果您的账户禁用了整合的控件调查发现，则 Security Hub CSPM 调查发现包含针对 PCI DSS 和 CIS v1.2.0 的特定于标准的控件标题。此外，Security Hub CSPM 调查发现包含特定于标准的控件 ID 和安全控件 ID。有关整合如何影响控件调查发现的示例，请参阅控件调查发现示例。

对于属于 AWS Control Tower 服务托管标准一部分的控件，启用整合的控件调查发现后，将从调查发现的控件 ID 和标题中删除前缀 CT.。

要在 Security Hub CSPM 中禁用安全控件，必须禁用与该安全控件对应的所有标准控件。下表显示了安全控件 ID 和标题与特定标准的控件 ID 和标题的映射。属于 AWS 基础安全最佳实践 (FSBP) 标准的控件的 ID 和标题已经与标准无关。有关控件与 Center for Internet Security（CIS）v3.0.0 要求的映射，请参阅 将控件映射到每个版本中的 CIS 要求。要在此表上运行您自己的脚本，您可以将其下载为 .csv 文件。

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.2.0	1.1 避免使用根用户	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
CIS v1.2.0	1.10 确保 IAM 密码策略阻止重复使用密码	[IAM.16] 确保 IAM 密码策略阻止重复使用密码
CIS v1.2.0	1.11 确保 IAM 密码策略使密码在 90 天或更短时间内失效	[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
CIS v1.2.0	1.12 确保不存在根用户访问密钥	[IAM.4] 不应存在 IAM 根用户访问密钥
CIS v1.2.0	1.13 确保为根用户启用 MFA	[IAM.9] 应为根用户启用 MFA
CIS v1.2.0	1.14 确保为根用户启用硬件 MFA	[IAM.6] 应该为根用户启用硬件 MFA
CIS v1.2.0	1.16 确保 IAM policy 仅附加到组或角色	[IAM.2] IAM 用户不应附加 IAM policy
CIS v1.2.0	1.2 确保为拥有控制台密码的所有 IAM 用户启用多重身份验证（MFA）	[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
CIS v1.2.0	1.20 确保创建支持角色来管理涉及 支持的事务	[IAM.18] 确保已创建支持角色来管理事件 AWS 支持
CIS v1.2.0	1.22 确保未创建允许完全“*.*”管理权限的 IAM policy	[IAM.1] IAM policy 不应允许完整的“*”管理权限
CIS v1.2.0	1.3 确保禁用 90 天或更长时间未使用的凭证	[IAM.8] 应移除未使用的 IAM 用户凭证

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.2.0	1.4 确保访问密钥每 90 天或更短时间轮换一次	[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
CIS v1.2.0	1.5 确保 IAM 密码策略要求包含至少一个大写字母	[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
CIS v1.2.0	1.6 确保 IAM 密码策略要求包含至少一个小写字母	[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
CIS v1.2.0	1.7 确保 IAM 密码策略要求包含至少一个符号	[IAM.13] 确保 IAM 密码策略要求包含至少一个符号
CIS v1.2.0	1.8 确保 IAM 密码策略要求包含至少一个数字	[IAM.14] 确保 IAM 密码策略要求包含至少一个数字
CIS v1.2.0	1.9 确保 IAM 密码策略要求最短密码长度不低于 14	[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
CIS v1.2.0	2.1 确保 CloudTrail 在所有地区都已启用	[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
CIS v1.2.0	2.2 确保已启用 CloudTrail 日志文件验证	[CloudTrail.4] 应启用 CloudTrail 日志文件验证
CIS v1.2.0	2.3 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
CIS v1.2.0	2.4 确保 CloudTrail 跟踪与 CloudWatch 日志集成	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
CIS v1.2.0	2.5 确保 AWS Config 已启用	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.2.0	2.6 确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
CIS v1.2.0	2.7 确保使用 KMS CMK 对 CloudTrail 日志进行静态加密	[CloudTrail.2] CloudTrail 应该启用静态加密
CIS v1.2.0	2.8 确保为客户创建的 CMK 启用轮换	[KMS.4] 应启用 AWS KMS 密钥轮换
CIS v1.2.0	2.9 确保在所有 VPC 中启用 VPC 流日志记录	[EC2.6] 应在所有 VPC 中启用 VPC 流量记录
CIS v1.2.0	3.1 确保存在关于未经授权的 API 调用的日志指标筛选条件和警报	[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报
CIS v1.2.0	3.10 确保存在关于安全组更改的日志指标筛选条件和警报	[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
CIS v1.2.0	3.11 确保存在关于网络访问控制列表（NACL）更改的日志指标筛选条件和警报	[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
CIS v1.2.0	3.12 确保存在关于网络网关更改的日志指标筛选条件和警报	[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
CIS v1.2.0	3.13 确保存在关于路由表更改的日志指标筛选条件和警报	[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
CIS v1.2.0	3.14 确保存在关于 VPC 更改的日志指标筛选条件和警报	[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报
CIS v1.2.0	3.2 确保存在关于无 MFA 的管理控制台登录的日志指标筛选条件和警报	[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.2.0	3.3 确保存在关于使用根用户的日志指标筛选条件和警报	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
CIS v1.2.0	3.4 确保存在关于 IAM policy 更改的日志指标筛选条件和警报	[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报
CIS v1.2.0	3.5 确保存在针对 CloudTrail 配置更改的日志指标筛选器和警报	[CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报
CIS v1.2.0	3.6 确保存在针对 AWS 管理控制台身份验证失败的日志指标筛选器和警报	[CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报
CIS v1.2.0	3.7 确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
CIS v1.2.0	3.8 确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报
CIS v1.2.0	3.9 确保存在 AWS Config 配置更改的日志指标筛选器和警报	[CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报
CIS v1.2.0	4.1 确保没有安全组允许从 0.0.0 开始进入。 0/0 到端口 22	[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22
CIS v1.2.0	4.2 确保没有安全组允许从 0.0.0 开始进入。 0/0 到端口 3389	[EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
CIS v1.2.0	4.3 确保每个 VPC 的默认安全组限制所有流量	[EC2.2] VPC 默认安全组不应允许入站或出站流量
CIS v1.4.0	1.10 确保为拥有控制台密码的所有 IAM 用户启用多重身份验证（MFA）	[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.4.0	1.14 确保访问密钥每 90 天或更短时间轮换一次	[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
CIS v1.4.0	1.16 确保未附加的允许完全“*.*”管理权限的 IAM policy	[IAM.1] IAM policy 不应允许完整的“*”管理权限
CIS v1.4.0	1.17 确保创建支持角色来管理涉及 支持的事务	[IAM.18] 确保已创建支持角色来管理事件 AWS 支持
CIS v1.4.0	1.4 确保不存在根用户账户访问密钥	[IAM.4] 不应存在 IAM 根用户访问密钥
CIS v1.4.0	1.5 确保为根用户账户启用 MFA	[IAM.9] 应为根用户启用 MFA
CIS v1.4.0	1.6 确保为根用户账户启用硬件 MFA	[IAM.6] 应该为根用户启用硬件 MFA
CIS v1.4.0	1.7 避免使用根用户执行管理和日常任务	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
CIS v1.4.0	1.8 确保 IAM 密码策略要求最短长度不低于 14	[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
CIS v1.4.0	1.9 确保 IAM 密码策略阻止重复使用密码	[IAM.16] 确保 IAM 密码策略阻止重复使用密码
CIS v1.4.0	2.1.2 确保 S3 存储桶策略设置为拒绝 HTTP 请求	[S3.5] S3 通用存储桶应需要请求才能使用 SSL
CIS v1.4.0	2.1.5.1 应启用 S3 阻止公有访问设置	[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置
CIS v1.4.0	2.1.5.2 应在存储桶级别启用 S3 阻止公有访问设置	[S3.8] S3 通用存储桶应屏蔽公共访问权限
CIS v1.4.0	2.2.1 确保启用 EBS 卷加密	[EC2.7] 应启用 EBS 默认加密
CIS v1.4.0	2.3.1 确保已为 RDS 实例启用加密	[RDS.3] RDS 数据库实例应启用静态加密

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.4.0	3.1 确保 CloudTrail 在所有地区都已启用	[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
CIS v1.4.0	3.2 确保已启用 CloudTrail 日志文件验证	[CloudTrail.4] 应启用 CloudTrail 日志文件验证
CIS v1.4.0	3.4 确保 CloudTrail 跟踪与 CloudWatch 日志集成	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
CIS v1.4.0	3.5 确保 AWS Config 在所有地区都已启用	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录
CIS v1.4.0	3.6 确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
CIS v1.4.0	3.7 确保使用 KMS CMK 对 CloudTrail 日志进行静态加密	[CloudTrail.2] CloudTrail 应该启用静态加密
CIS v1.4.0	3.8 确保为客户创建的 CMK 启用轮换	[KMS.4] 应启用 AWS KMS 密钥轮换
CIS v1.4.0	3.9 确保在所有 VPC 中启用 VPC 流日志记录	[EC2.6] 应在所有 VPC 中启用 VPC 流量记录
CIS v1.4.0	4.4 确保存在关于 IAM policy 更改的日志指标筛选条件和警报	[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报
CIS v1.4.0	4.5 确保存在针对 CloudTrail 配置更改的日志指标筛选器和警报	[CloudWatch.5] 确保存在 CloudTrail 配置更改的日志指标筛选器和警报
CIS v1.4.0	4.6 确保存在针对 AWS 管理控制台身份验证失败的日志指标筛选器和警报	[CloudWatch.6] 确保存在针对 AWS 管理控制台 身份验证失败的日志指标筛选器和警报

标准	标准控件 ID 和标题	安全控件 ID 和标题
CIS v1.4.0	4.7 确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
CIS v1.4.0	4.8 确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报
CIS v1.4.0	4.9 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报	[CloudWatch.9] 确保存在 AWS Config 配置更改的日志指标筛选器和警报
CIS v1.4.0	4.10 确保存在关于安全组更改的日志指标筛选条件和警报	[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
CIS v1.4.0	4.11 确保存在关于网络访问控制列表（NACL）更改的日志指标筛选条件和警报	[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
CIS v1.4.0	4.12 确保存在关于网络网关更改的日志指标筛选条件和警报	[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
CIS v1.4.0	4.13 确保存在关于路由表更改的日志指标筛选条件和警报	[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
CIS v1.4.0	4.14 确保存在关于 VPC 更改的日志指标筛选条件和警报	[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报
CIS v1.4.0	5.1 确保没有网络 ACL 允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口	[EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
CIS v1.4.0	5.3 确保每个 VPC 的默认安全组限制所有流量	[EC2.2] VPC 默认安全组不应允许入站或出站流量

标准	标准控件 ID 和标题	安全控件 ID 和标题
PCI DSS v3.2.1	PCI.AutoScaling.1 与负载均衡器关联的 Auto Scaling 组应使用负载均衡器运行状况检查	[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail 应使用 AWS KMS CMK 对日志进行静态加密	[CloudTrail.2] CloudTrail 应该启用静态加密
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail 应该启用	[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail 应启用日志文件验证	[CloudTrail.4] 应启用 CloudTrail 日志文件验证
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail 跟踪应与 Amazon CloudWatch 日志集成	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub 或者 Bitbucket 源存储库网址应使用 OAuth	[CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild 项目环境变量不应包含明文凭证	[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
PCI DSS v3.2.1	PCI.Config.1 AWS Config 应该启用	[Config.1] AWS Config 应该启用并使用服务相关角色进行资源记录
PCI DSS v3.2.1	PCI.CW.1 “root” 用户应使用日志指标筛选器和警报	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service 的复制实例不应是公共的	[DMS.1] Database Migration Service 复制实例不应公开
PCI DSS v3.2.1	PCI.EC2.1 EBS 快照不应公开恢复	[EC2.1] 不应将 Amazon EBS 快照配置为可公开还原
PCI DSS v3.2.1	PCI.EC2.2 VPC 默认安全组应禁止入站和出站流量	[EC2.2] VPC 默认安全组不应允许入站或出站流量

标准	标准控件 ID 和标题	安全控件 ID 和标题
PCI DSS v3.2.1	PCI.EC2.4 应移除未使用的 EC2 EIP	[EC2.12] 应移除未使用的 Amazon EC2 EIP
PCI DSS v3.2.1	PCI.EC2.5 安全组不应允许从 0.0.0 开始的入口。 0/0 到端口 22	[EC2.13] 安全组不应允许从 0.0.0 开始的入口。 0/0 或:: /0 到端口 22
PCI DSS v3.2.1	PCI.EC2.6 应在所有 VPC 中启用 VPC 流量记录	[EC2.6] 应在所有 VPC 中启用 VPC 流量记录
PCI DSS v3.2.1	PCI.ELBv2.1 Application Load Balancer 应配置为将所有 HTTP 请求重定向到 HTTPS	[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch 域名应位于 VPC 中	[ES.2] Elasticsearch 域名不应公开访问
PCI DSS v3.2.1	PCI.ES.2 Elasticsearch 域名应启用静态加密	[ES.1] Elasticsearch 域应启用静态加密
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty 应该启用	[GuardDuty.1] GuardDuty 应该启用
PCI DSS v3.2.1	PCI.IAM.1 IAM 根用户访问密钥不应存在	[IAM.4] 不应存在 IAM 根用户访问密钥
PCI DSS v3.2.1	PCI.IAM.2 IAM 用户不应附加 IAM 策略	[IAM.2] IAM 用户不应附加 IAM policy
PCI DSS v3.2.1	PCI.IAM.3 IAM 策略不应允许完全的“*” 管理权限	[IAM.1] IAM policy 不应允许完整的“*”管理权限
PCI DSS v3.2.1	PCI.IAM.4 应为根用户启用硬件 MFA	[IAM.6] 应该为根用户启用硬件 MFA
PCI DSS v3.2.1	PCI.IAM.5 应为根用户启用虚拟 MFA	[IAM.9] 应为根用户启用 MFA
PCI DSS v3.2.1	PCI.IAM.6 应为所有 IAM 用户启用 MFA	[IAM.19] 应为所有 IAM 用户启用 MFA

标准	标准控件 ID 和标题	安全控件 ID 和标题
PCI DSS v3.2.1	PCI.IAM.7 如果未在预定义的天数内使用 IAM 用户证书，则应禁用	[IAM.8] 应移除未使用的 IAM 用户凭证
PCI DSS v3.2.1	PCI.IAM.8 IAM 用户的密码策略应具有强大的配置	[IAM.10] IAM 用户的密码策略应具有很强的配置
PCI DSS v3.2.1	PCI.KMS.1 应启用客户主密钥 (CMK) 轮换	[KMS.4] 应启用 AWS KMS 密钥轮换
PCI DSS v3.2.1	PCI.Lambda.1 Lambda 函数应禁止公众访问	[Lambda.1] Lambda 函数策略应禁止公众访问
PCI DSS v3.2.1	PCI.Lambda.2 Lambda 函数应位于 VPC 中	[Lambda.3] Lambda 函数应位于 VPC 中
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch 域名应该在 VPC 中	[Opensearch.2] OpenSearch 域名不应向公众开放
PCI DSS v3.2.1	PCI.Opensearch.2 EBS 快照不应公开恢复	[Opensearch.1] OpenSearch 域名应启用静态加密
PCI DSS v3.2.1	PCI.RDS.1 RDS 快照应该是私有的	[RDS.1] RDS 快照应该是私有的
PCI DSS v3.2.1	PCI.RDS.2 RDS 数据库实例应禁止公共访问	[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置
PCI DSS v3.2.1	PCI.Redshift.1 亚马逊 Redshift 集群应禁止公众访问	[Redshift.1] Amazon Redshift 集群应禁止公共访问
PCI DSS v3.2.1	PCI.S3.1 S3 存储桶应禁止公共写入权限	[S3.3] S3 通用存储桶应阻止公共写入访问权限
PCI DSS v3.2.1	PCI.S3.2 S3 存储桶应禁止公共读取权限	[S3.2] S3 通用存储桶应阻止公共读取访问权限
PCI DSS v3.2.1	PCI.S3.3 S3 存储桶应启用跨区域复制	[S3.7] S3 通用存储桶应使用跨区域复制

标准	标准控件 ID 和标题	安全控件 ID 和标题
PCI DSS v3.2.1	PCI.S3.5 S3 存储桶应要求请求才能使用安全套接字层	[S3.5] S3 通用存储桶应需要请求才能使用 SSL
PCI DSS v3.2.1	PCI.S3.6 应启用 S3 阻止公共访问设置	[S3.1] S3 通用存储桶应启用屏蔽公共访问权限设置
PCI DSS v3.2.1	PCI.SageMaker.1 Amazon SageMaker 笔记本实例不应直接访问互联网	[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
PCI DSS v3.2.1	PCI.SSM.1 安装补丁后，由 Systems Manager 管理的 EC2 实例的补丁合规性状态应为 “合规”	[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
PCI DSS v3.2.1	PCI.SSM.2 由 Systems Manager 管理的 EC2 实例的关联合规状态应为 “合规”	[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
PCI DSS v3.2.1	PCI.SSM.3 EC2 实例应由以下人员管理 AWS Systems Manager	[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

更新工作流以进行整合。

如果工作流不依赖于控件调查发现中任何字段的特定格式，则无需执行任何操作。

如果工作流依赖于控件调查发现中一个或多个字段的特定格式，则应更新工作流。例如，如果您创建的 Amazon EventBridge 规则触发了针对特定控件 ID 的操作，例如在控件 ID 等于 CIS 2.7 时调用 AWS Lambda 函数，请更新要使用的规则 CloudTrail.2，即该控件`Compliance.SecurityControlId`字段的值。

如果您创建了使用任何已更改字段或值的自定义见解，请更新这些见解以使用新字段或值。

必需的顶级 ASFF 属性

Security Hub CSPM 中的所有搜索结果都需要 AWS 安全调查结果格式 (ASFF) 中的以下顶级属性。有关这些属性的更多信息，请参阅《AWS Security Hub API 参考》中的 AwsSecurityFinding。

AwsAccountId

调查结果适用的 AWS 账户 ID。

示例

```
"AwsAccountId": "111111111111"
```

CreatedAt

表示调查发现捕获到的潜在安全问题或事件的创建时间。

示例

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

说明

结果说明。该字段可以是非特定的样板文本，也可以是特定于结果实例的详细信息。

对于 Security Hub CSPM 生成的控件调查发现，此字段提供控件的描述。

如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

生成结果的特定于解决方案的组件（离散的逻辑单元）的标识符。

对于 Security Hub CSPM 生成的控件调查发现，如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"GeneratorId": "security-control/Config.1"
```

Id

结果的特定于产品的标识符。对于 Security Hub CSPM 生成的控件调查发现，此字段提供调查发现的 Amazon 资源名称（ARN）。

如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

由 Security Hub CSPM 生成的 Amazon 资源名称（ARN），用于在产品注册到 Security Hub CSPM 后唯一标识第三方调查发现产品。

此字段的格式为 `arn:partition:securityhub:region:account-id:product/company-id/product-id`。

- 为了 AWS 服务 与 Security Hub CSPM 集成，`company-id`必须`aws`是 “”，并且`product-id`必须是 AWS 公共服务名称。由于 AWS 产品和服务未与账户关联，所以 ARN 的`account-id`部分为空。 AWS 服务 尚未与 Security Hub CSPM 集成的产品被视为第三方产品。
- 对于公共产品，`company-id` 和 `product-id` 必须为注册时指定的 ID 值。
- 对于私有产品，`company-id` 必须为账户 ID。`product-id` 必须为保留字“default”或注册时指定的 ID。

示例

```
// 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"
```

资源

对象Resources数组提供了一组资源数据类型，这些数据类型描述了调查结果所指的 AWS 资源。有关 Resources 对象可能包含的字段的详细信息（包括哪些字段是必需的），请参阅《AWS Security Hub API 参考》中的 Resource。有关特定Resources对象的示例 AWS 服务，请参见资源 ASFF 对象。

示例

```
"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

格式化结果的架构版本。该字段的值必须为 AWS确定的官方发布版本之一。在当前版本中， AWS 安全调查结果格式架构版本为2018-10-08。

示例

```
"SchemaVersion": "2018-10-08"
```

严重性

定义调查发现的重要性。有关此对象的详细信息，请参阅 AWS Security Hub API 参考中的 Severity。

Severity 既是调查发现中的顶级对象，又嵌套在 FindingProviderFields 对象之下。

只能使用 BatchUpdateFindings API 来更新调查发现的顶级 Severity 对象的值。

要提供严重性信息，调查发现提供商在进行 BatchImportFindings API 请求时应更新 FindingProviderFields 下的 Severity 对象。
如果对新调查发现的 BatchImportFindings 请求仅提供 Label 或仅提供 Normalized，则 Security Hub CSPM 会自动填充其他字段的值。可能还会填充 Product 和 Original 字段。

如果顶级 Finding.Severity 对象存在但 Finding.FindingProviderFields 不存在，Security Hub CSPM 会创建 FindingProviderFields.Severity 对象并将整个 Finding.Severity object 复制到其中。这样可以确保即使顶级 Severity 对象被覆盖，提供者提供的原始详细信息也会保留在 FindingProviderFields.Severity 结构中。

结果严重性不考虑涉及的资产或底层资源的严重性。严重性将定义为与结果关联的资源的重要性级别。例如，与任务关键型应用程序关联的资源比与非生产测试关联的资源具有更高的关键性。要捕获有关资源严重性的信息，请使用 Criticality 字段。

我们建议在将调查发现的本机严重性评分转换为 ASFF 中的 Severity.Label 值时使用以下指南。

- INFORMATIONAL——此类别可能包括 PASSED、WARNING、NOT AVAILABLE 的调查发现或敏感数据标识。
- LOW——可能导致未来受损的调查发现。例如，此类别可能包括漏洞、配置隐患和泄露密码。
- MEDIUM——结果表明遭受活动攻击，但未指示攻击者已达成其目标 例如，此类别可能包括恶意软件活动、黑客活动和异常行为检测。
- HIGH 或 CRITICAL——指示攻击者达成目标（例如主动数据丢失或泄露、拒绝服务）的调查发现。

示例

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

标题

结果的标题。该字段可以包含非特定的样板文本，也可以包含特定于结果实例的详细信息。

对于控件调查发现，此字段提供控件的标题。如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"Title": "AWS Config should be enabled"
```

类型

一个或多个 *namespace*/*category*/*classifier* 格式的结果类型，用于对结果进行分类。如果您启用整合的控件调查发现，则此字段不会引用标准。

只能使用 BatchUpdateFindings API 来更新 Types。

调查发现提供商想要为 Types 提供值，应使用 FindingProviderFields 下面的 Types 属性。

在下面的列表中，顶级项目符号是命名空间，二级项目符号是类别，三级项目符号是分类器。我们建议调查发现提供商使用定义的命名空间来帮助对调查发现进行排序和分组。也可以使用定义的类别和分类器，但不是必需的。仅软件和配置检查命名空间定义了分类器。

你可以为 namespace/category /classifier 定义一个部分路径。例如，以下调查发现类型均有效：

- TTP
- TTPs/Defense 逃避
- TTPs/Defense Evasion/CloudTrailStopped

以下列表中的策略、技术和程序（TTP）类别与 MITRE ATT&CK MatrixTM 一致。Unusual Behaviours 命名空间反映一般异常行为，例如一般统计异常，并且与特定 TTP 不一致。但是，您可以使用 Unusual Behaviors 和 TTP 结果类型对结果进行分类。

命名空间、类别和分类器列表：

- Software and Configuration Checks
  - 漏洞
    - CVE
  - AWS 安全最佳实践
    - 网络可到达性
    - 运行时行为分析
  - 行业和法规标准
    - AWS 基础安全最佳实践
    - CIS 主机强化基准
    - CIS AWS 基金会基准
    - PCI-DSS
    - 云安全联盟控制
    - ISO 90001 控制
    - ISO 27001 控制
    - ISO 27017 控制
    - ISO 27018 控制
    - SOC 1
    - SOC 2

    - HIPAA 控制（美国）
    - NIST 800-53 控制（美国）
    - NIST CSF 控制（美国）
    - IRAP 控制（澳大利亚）
    - K-ISMS 控制（韩国）
    - MTCS 控制（新加坡）
    - FISC 控制（日本）
    - My Number Act 控制（日本）
    - ENS 控制（西班牙）
    - Cyber Essentials Plus 控制（英国）
    - G-Cloud 控制（英国）
    - C5 控制（德国）
    - IT-Grundschutz 控制（德国）
    - GDP 控制（欧洲）
    - TISAX 控制（欧洲）
  - 补丁管理
- TTP
  - 首次访问
  - Execution
  - Persistence
  - 权限提升
  - 躲避防御系统
  - 凭证访问
  - Discovery
  - 横向移动
  - 集合
  - 命令和控制
- 影响
  - 数据公开
  - 数据泄露

  - 数据销毁
  - 拒绝服务
  - 资源消耗
- 不寻常的行为
  - 应用程序
  - 网络流量
  - IP 地址
  - 用户
  - VM
  - Container
  - Serverless（无服务器）
  - 流程
  - 数据库
  - 数据
- 敏感数据识别
  - PII
  - 密码
  - 法律条款
  - 财务
  - 安全性
  - 商业

示例

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

表示调查发现提供商上次更新查找记录的时间。

此时间戳反映了上次或最近一次更新的调查发现记录的时间。因此，它可能与 LastObservedAt 时间戳不同，后者反映的是上次或最近观察到事件或漏洞的时间。

更新结果记录时，必须将该时间戳更新为当前时间戳。创建调查发现记录后，CreatedAt 和 UpdatedAt 时间戳必须相同。更新调查发现记录后，该字段的值必须比它包含的所有先前值更新。

请注意，UpdatedAt 无法使用 BatchUpdateFindings 操作进行更新。您只能使用 BatchImportFindings 操作更新它。

示例

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

可选顶级 ASFF 属性

在 Security Hub CSPM 中查找结果时， AWS 安全调查结果格式 (ASFF) 中的以下顶级属性是可选的。有关这些属性的更多信息，请参阅《AWS Security Hub API 参考》中的 AwsSecurityFinding。

处理建议

Action 对象提供有关影响资源或已对资源采取的操作的详细信息。

示例

```
"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

调查结果适用的 AWS 账户 名称。

示例

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

生成调查发现的产品的公司名称。对于基于控制的调查结果，该公司是。 AWS

Security Hub CSPM 会为每个调查发现自动填充此属性。您无法使用 `BatchImportFindings` 或 `BatchUpdateFindings` 对其进行更新。使用自定义集成是此规则的例外。请参阅the section called “自定义产品集成”。

当您使用 Security Hub CSPM 控制台按公司名称筛选调查发现时，请使用此属性。当您使用 Security Hub CSPM API 按公司名称筛选调查发现时，请使用 `ProductFields` 下的 `aws/securityhub/CompanyName` 属性。Security Hub CSPM 不会同步这两个属性。

示例

```
"CompanyName": "AWS"
```

合规

Compliance 对象通常会提供有关控件调查发现的详细信息，例如适用的标准和控件检查的状态。

示例

```
"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."
```

```
        }
    ]
}
```

置信度

调查发现能够准确识别其理应识别的行为或问题的可能性。

Confidence 只能使用 BatchUpdateFindings 进行更新。

调查发现提供商想要为 Confidence 提供值，应使用 FindingProviderFields 下面的 Confidence 属性。请参阅the section called “使用更新调查结果 FindingProviderFields”。

使用比例刻度按 0-100 分对 Confidence 进行评分。 0 表示置信度为 0%，100 表示置信度为 100%。例如，基于网络流量统计偏差的数据泄露检测的置信度较低，因为实际的泄露尚未得到验证。

示例

```
"Confidence": 42
```

严重性

分配给与调查发现关联的资源的重要性级别。

Criticality 只能通过调用 BatchUpdateFindings API 操作进行更新。不要使用 BatchImportFindings 更新此对象。

调查发现提供商想要为 Criticality 提供值，应使用 FindingProviderFields 下面的 Criticality 属性。请参阅the section called “使用更新调查结果 FindingProviderFields”。

使用仅支持全整型的比例刻度以 0-100 为基础对 Criticality 进行评分。评分为 0 意味着底层资源不关键，对于最关键的资源，评分为 100。

对于每种资源，在分配 Criticality 时请考虑以下几点：

- 受影响的资源是否包含敏感数据（例如，具有 PII 的 S3 存储桶）？
- 受影响的资源是否使攻击者能够加深访问或扩展其能力以执行其他恶意活动（例如，受损的系统管理员账户）？
- 资源是否为业务关键型资产（例如，在受到攻击时可能会对收入造成重大影响的关键业务系统）？

您可以使用以下准则：

- 对于支持关键任务型系统或包含高度敏感数据的资源，评分范围为 75–100。
- 对于支持重要（但非关键）系统或包含中等重要程度数据的资源，评分范围为 25–74。
- 对于支持非重要系统或包含非敏感数据的资源，评分范围应 为 0–24。

示例

```
"Criticality": 99
```

检测

该Detection对象提供有关从 Amazon GuardDuty 扩展威胁检测中发现的攻击序列的详细信息。GuardDuty 当多个事件与潜在可疑活动对应时，生成攻击序列查找结果。要在 Sec AWS urity Hub CSPM 中接收 GuardDuty 攻击序列结果，你必须已在 GuardDuty 账户中启用。有关更多信息，请参阅《亚马逊 GuardDuty 用户指南》中的 “亚马逊 GuardDuty 扩展威胁检测”。

示例

```
"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 包括以下属性：

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

前面的字段都嵌套在 FindingProviderFields 对象下，但具有与顶级 ASFF 字段相同的名称。当调查发现提供者将新调查发现发送到 Security Hub CSPM 时，如果 FindingProviderFields 对象为空，Security Hub CSPM 会根据相应的顶级字段自动填充该对象。

调查发现提供者可以通过使用 Security Hub CSPM API 的 BatchImportFindings 操作更新 FindingProviderFields。调查发现提供者无法使用 BatchUpdateFindings 更新此对象。

有关 Security Hub CSPM 如何处理由 BatchImportFindings 到 FindingProviderFields，再到相应顶级属性的更新的详细信息，请参阅the section called “使用更新调查结果 FindingProviderFields”。

客户可以使用 BatchUpdateFindings 操作更新顶级字段。客户无法更新 FindingProviderFields。

示例

```
"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

表示调查发现捕获到的潜在安全问题或事件的首次观察时间。

此时间戳指定首次观察到事件或漏洞的时间。因此，它可能与 `CreatedAt` 时间戳不同，后者反映了此调查发现记录的创建时间。

对于 Security Hub CSPM 生成和更新的控件调查发现，此时间戳还可以指示资源的合规性状态最近发生更改的时间。对于其他类型的调查发现，此时间戳在调查发现记录的更新之间应该是不可变的，但如果确定了更准确的时间戳，则可以更新。

示例

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

表示安全调查发现产品最近一次观察到由调查发现捕获的潜在安全问题或事件的时间。

此时间戳指定上次或最近观察到事件或漏洞的时间。因此，它可能与 `UpdatedAt` 时间戳不同，后者反映了该调查发现记录的最后一次更新时间或最近更新的时间。

您可以提供此时间戳，但在首次观察时不需要此时间戳。如果您在首次观察时填充此字段，则时间戳应与 `FirstObservedAt` 时间戳相同。每次观察到结果时，您应该更新该字段，以反映上次或最近一次观察的时间戳。

示例

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

恶意软件

`Malware` 对象提供与调查发现相关的恶意软件列表。

示例

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
```

```
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

网络（已停用）

Network 对象提供有关调查发现的网络相关信息。

此对象已停用。要提供此数据，您可以将数据映射到 Resources 中的资源，也可以使用 Action 对象。

示例

```
"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

NetworkPath 对象提供与调查发现相关的网络路径的相关信息。NetworkPath 中的每个条目都代表路径的一个组成部分。

示例

```
"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" ]
            }
        }
    }
]
```

备注

Note 对象指定了用户定义的注释，您可以将其添加到调查发现中。

结果提供商可以为结果提供初始注释，但不能在此之后添加注释。您只能使用 BatchUpdateFindings 更新注释。

示例

```
"Note": {
```

```
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

PatchSummary 对象根据所选合规性标准提供实例的补丁合规性状态摘要。

示例

```
"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"
}
```

流程

Process 对象提供有关调查发现的过程相关详细信息。

示例：

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

指示 Security Hub CSPM 何时收到调查发现并开始对其进行处理。

与 CreatedAt 和 UpdatedAt 不同，这二者是必需的时间戳，与调查发现提供者与安全问题和调查发现的交互有关。ProcessedAt 时间戳指示 Security Hub CSPM 何时开始处理调查发现。处理完成后，调查发现会出现在用户的账户中。

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

一种数据类型，其中安全调查结果产品可以包含其他特定于解决方案的详细信息，这些详细信息不是定义 AWS 的安全调查结果格式的一部分。

有关由 Security Hub CSPM 控件生成的调查发现，ProductFields 包括有关控件的信息。请参阅the section called “生成和更新控件调查发现”。

此字段不应包含冗余数据，也不得包含与 AWS 安全调查结果格式字段冲突的数据。

“aws/” 前缀仅代表为 AWS 产品和服务保留的命名空间，不得与第三方集成的发现一起提交。

虽然不是必需的，但产品应将字段名称格式化为 company-id/product-id/field-name，其中 company-id 和 product-id 与结果的 ProductArn 中提供的名称匹配。

当 Security Hub CSPM 存档现有调查发现时，将使用引用 Archival 的字段。例如，当您禁用控件或标准以及打开或关闭整合的控件调查发现时，Security Hub CSPM 会存档现有调查发现。

此字段还可能包含有关标准的信息，标准中包括产生调查发现的控件。

示例

```
"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

提供生成调查发现的产品的名称。对于基于控件的调查发现，产品名称为 Security Hub CSPM。

Security Hub CSPM 会为每个调查发现自动填充此属性。您无法使用 BatchImportFindings 或 BatchUpdateFindings 对其进行更新。使用自定义集成是此规则的例外。请参阅the section called “自定义产品集成”。

当您使用 Security Hub CSPM 控制台按产品名称筛选调查发现时，请使用此属性。

当您使用 Security Hub CSPM API 按产品名称筛选调查发现时，请使用 ProductFields 下面的 aws/securityhub/ProductName 属性。

Security Hub CSPM 不会同步这两个属性。

RecordState

提供调查发现的记录状态。

默认情况下，在最初由服务生成时，结果被视为 ACTIVE。

ARCHIVED 状态表示应从视图中隐藏结果。存档的调查发现不会立即删除。您可以搜索、查看和报告这些结果。如果关联的资源被删除、资源不存在或控件被禁用，Security Hub CSPM 会自动存档基于控件的调查发现。

RecordState 适用于调查发现提供者，并且只能使用 BatchImportFindings 操作进行更新。您不能使用 BatchUpdateFindings 操作进行更新。

要跟踪调查发现的状态，请使用 Workflow 而不是 RecordState。

如果记录状态从 ARCHIVED 变为 ACTIVE，并且调查发现的工作流状态为 NOTIFIED 或 RESOLVED，则 Security Hub CSPM 会自动将工作流状态更改为 NEW。

示例

```
"RecordState": "ACTIVE"
```

Region

指定生成查找结果 AWS 区域 的依据。

Security Hub CSPM 会为每个调查发现自动填充此属性。您无法使用 BatchImportFindings 或 BatchUpdateFindings 对其进行更新。

示例

```
"Region": "us-west-2"
```

RelatedFindings

提供与当前发现相关的调查发现列表。

`RelatedFindings` 只能使用 `BatchUpdateFindings` API 操作进行更新。您不应使用 `BatchImportFindings` 更新此对象。

对于 `BatchImportFindings` 请求，调查发现提供商应使用 `FindingProviderFields` 下面的 `RelatedFindings` 对象。

要查看 `RelatedFindings` 属性的描述，请参阅 AWS Security Hub API 参考中的 `RelatedFinding`。

示例

```
"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

示例

```
"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"
                    }
                ]
            }
        ]
    }
}
```

修复

Remediation 对象提供有关为解决调查发现问题而建议的修复步骤的信息。

示例

```
"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"
    }
}
```

样本

指定调查发现是否为调查发现样本。

```
"Sample": true
```

SourceUrl

SourceUrl 对象提供一个 URL，指向有关调查发现产品中当前调查发现的页面

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

ThreatIntelIndicator 对象提供与调查发现相关的威胁情报详细信息。

示例

```
"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",
  }
]
```

威胁

Threats 对象提供调查发现所检测到的威胁的详细信息。

示例

```
"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

提供与调查发现关联的名称/值字符串对的列表。这些是添加到结果的自定义用户定义字段。这些字段可以通过特定配置自动生成。

调查发现提供商不应将此字段用于产品生成的数据。相反，查找提供者可以将该ProductFields字段用于未映射到任何标准 AWS 安全查找格式字段的数据。

这些字段只能使用 BatchUpdateFindings 进行更新。

示例

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

提供调查发现的准确性。结果产品可以提供 UNKNOWN 作为该字段的值。如果在结果产品的系统中存在有意义的类比，则结果产品应该为该字段提供值。该字段通常由用户在对调查发现进行调查后做出的决定或操作填充。

结果提供商可以为此属性提供初始值，但在此之后无法更新它。您只能使用 BatchUpdateFindings 来更新此属性。

```
"VerificationState": "Confirmed"
```

漏洞

Vulnerabilities 对象提供与调查发现相关的漏洞列表。

示例

```
"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"
            }
        ]
    }
]
```

工作流

`Workflow` 对象提供有关调查发现调查状态的信息。

此字段专供客户与修复、编排和票务工具配合使用。它不适用于结果提供商。

您只能使用 `BatchUpdateFindings` 更新 `Workflow` 字段。客户还可以从控制台更新它。请参阅the section called “设置调查发现的工作流状态”。

示例

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState （已退休）

此对象已停用，已被 `Workflow` 对象的 `Status` 字段所取代。

此字段提供调查发现的工作流程状态。结果产品可以提供 `NEW` 作为该字段的值。如果在结果产品的系统中存在有意义的类比，则结果产品可以为该字段提供值。

示例

```
"WorkflowState": "NEW"
```

资源 ASFF 对象

在 AWS 安全调查结果格式 (ASFF) 中，Resources对象提供有关查找结果中涉及的资源的信息。它包含最多 32 个资源对象的数组。要确定资源名称的格式，请参阅 AWS 安全调查结果格式 (ASFF)。有关每个资源对象的示例，请从以下列表中选择资源。

主题

- ASFF 中的资源属性
- AwsAmazonMQ ASFF 中的资源
- AwsApiGateway ASFF 中的资源
- AwsAppSync ASFF 中的资源
- AwsAthena ASFF 中的资源
- AwsAutoScaling ASFF 中的资源
- AwsBackup ASFF 中的资源
- AwsCertificateManager ASFF 中的资源
- AwsCloudFormation ASFF 中的资源
- AwsCloudFront ASFF 中的资源
- AwsCloudTrail ASFF 中的资源
- AwsCloudWatch ASFF 中的资源
- AwsCodeBuild ASFF 中的资源
- AwsDms ASFF 中的资源
- AwsDynamo数据库 ASFF 中的资源
- AwsEc2 ASFF 中的资源
- AwsEcr ASFF 中的资源
- AwsEcs ASFF 中的资源
- AwsEfs ASFF 中的资源
- AwsEks ASFF 中的资源
- AwsElasticBeanstalk ASFF 中的资源

- AwsElasticSearch ASFF 中的资源
- AwsElb ASFF 中的资源
- AwsEventBridge ASFF 中的资源
- AwsGuardDuty ASFF 中的资源
- AwsIam ASFF 中的资源
- AwsKinesis ASFF 中的资源
- AwsKms ASFF 中的资源
- AwsLambda
- AwsMsk ASFF 中的资源
- AwsNetworkFirewall ASFF 中的资源
- AwsOpenSearchService ASFF 中的资源
- AwsRds ASFF 中的资源
- AwsRedshift ASFF 中的资源
- AwsRoute53 ASFF 中的资源
- awss3 ASFF 中的资源
- AwsSageMaker ASFF 中的资源
- AwsSecretsManager ASFF 中的资源
- AwsSns ASFF 中的资源
- AwsSqs ASFF 中的资源
- AwsSsm ASFF 中的资源
- AwsStepFunctions ASFF 中的资源
- AwsWaf ASFF 中的资源
- AwsXray ASFF 中的资源
- CodeRepository ASFF 中的对象
- Container ASFF 中的对象
- 其他 ASFF 中的对象

ASFF 中的资源属性

以下是 AWS 安全调查结果格式 (ASFF) 中该`Resources`对象的描述和示例。有关这些字段的更多信息，请参阅资源。

ApplicationArn

确定调查发现中涉及的应用程序的 Amazon 资源名称（ARN）。

示例

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

确定调查发现中涉及的应用程序的名称。

示例

```
"ApplicationName": "SampleApp"
```

DataClassification

DataClassification 字段提供有关在资源上检测到的敏感数据的信息。

示例

```
"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
    }
  }
}
```

说明

Details 字段使用相应对象提供有关单个资源的更多信息。必须在 Resources 对象中的单独资源对象中提供每个资源。

请注意，如果调查发现大小超过最大值 240 KB，则 Details 对象将从调查发现中移除。对于使用 AWS Config 规则的控制结果，您可以在 AWS Config 控制台上查看资源详细信息。

Security Hub CSPM 为其支持的资源类型提供了一组可用的资源详细信息。这些细节对应于 Type 对象的值。尽可能使用提供的类型。

例如，如果资源是 S3 存储桶，则将资源 Type 设置为 AwsS3Bucket 并在 AwsS3Bucket 对象中提供资源详细信息。

Other 对象允许您提供自定义字段和值。您在以下情况下使用 Other 对象：

- 资源类型（资源 Type 的值）没有对应的详细信息对象。要提供资源的详细信息，您可以使用 Other 对象。
- 资源类型的对象不包括您要填充的所有字段。在这种情况下，请使用资源类型的详细信息对象来填充可用字段。使用 Other 对象填充不在特定于类型的对象中的字段。
- 资源类型不是提供的类型之一。在此情况下，将 Resource.Type 设置为 Other，并使用 Other 对象填充详细信息。

示例

```
"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

给定资源类型的标识符。

对于 AWS 由 Amazon 资源名称 (ARN) 标识的资源，这是 ARN。

对于缺少 ARN 的 AWS 资源，这是创建资源的 AWS 服务所定义的标识符。

对于非AWS 资源，这是与资源关联的唯一标识符。

示例

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

分区

资源所在的分区。分区是一组 AWS 区域。每个分区的作用域 AWS 账户 仅限于一个分区。

支持以下分区：

- aws – AWS 区域
- aws-cn – 中国区域
- aws-us-gov – AWS GovCloud (US) Region

示例

```
"Partition": "aws"
```

Region

此资源 AWS 区域 所在位置的代码。有关区域代码的列表，请参阅区域端点。

示例

```
"Region": "us-west-2"
```

ResourceRole

标识资源在调查发现中的作用。资源要么是调查发现活动的目标，要么是执行该活动的行为者。

示例

```
"ResourceRole": "target"
```

标签

此字段会提供调查发现中涉及的资源的标签的键值信息。您可以为标记 API `GetResources` 操作支持的资源 AWS Resource Groups 添加标签。Security Hub CSPM 通过服务相关角色调用此操作，如果 AWS 安全调查结果格式 (ASFF) `Resource.Id` 字段填充了资源 ARN，则会检索资源标签。 AWS 将忽略无效资源 ID。

您可以向 Security Hub CSPM 提取的调查结果（包括来自集成产品 AWS 服务 和第三方产品的发现）添加资源标签。

添加标签会指明在处理调查发现时与资源关联的标签的列表。您仅可以包含具有关联标签的资源的 `Tags` 属性。如果资源没有关联的标签，请不要在结果中包含 `Tags` 属性。

在调查发现中包含资源标签后，无需构建数据扩充管线或手动扩充调查发现的元数据。您还可以使用标签搜索或筛选调查发现和见解，并创建自动化规则。

有关适用于标签的限制的信息，请参阅 Tag naming limits and requirements。

您只能在此字段中提供 AWS 资源上存在的标签。要提供未在 AWS 安全调查结果格式中定义的数据，请使用`Other`详细信息子字段。

示例

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Type

要为其提供详细信息的资源的类型。

如果可能，使用提供的资源类型之一，例如 `AwsEc2Instance` 或 `AwsS3Bucket`。

如果资源类型与提供的任何资源类型不匹配，则将资源 Type 设置为 Other，并使用 Other 详细信息子字段填写详细信息。

支持的值列在资源下。

示例

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ ASFF 中的资源

以下是AwsAmazonMQ资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsAmazonMQBroker

AwsAmazonMQBroker 提供有关 Amazon MQ 代理的信息，该代理是运行在 Amazon MQ 上的消息代理环境。

以下示例显示了 AwsAmazonMQBroker 对象的 ASFF。要查看 AwsAmazonMQBroker 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsAmazonMQBroker。

示例

```
"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 ASFF 中的资源

以下是AwsApiGateway资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsApiGatewayRestApi

AwsApiGatewayRestApi 对象包含有关 Amazon API Gateway 版本 1 中的 REST API 的信息。

以下是 AWS 安全调查发现格式（ASFF）中的 AwsApiGatewayRestApi 调查发现示例。要查看 AwsApiGatewayRestApi 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsApiGatewayRestApiDetails。

示例

```
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

`AwsApiGatewayStage` 对象提供有关版本 1 的 Amazon API Gateway 阶段的信息。

以下是 AWS 安全调查发现格式（ASFF）中的 `AwsApiGatewayStage` 调查发现示例。要查看 `AwsApiGatewayStage` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsApiGatewayStageDetails。

示例

```
"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

`AwsApiGatewayV2Api` 对象包含有关 Amazon API Gateway 中版本 2 API 的信息。

以下是 AWS 安全调查发现格式（ASFF）中的 `AwsApiGatewayV2Api` 调查发现示例。要查看 `AwsApiGatewayV2Api` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsApiGatewayV2ApiDetails。

示例

```
"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` 包含有关 Amazon API Gateway 的版本 2 阶段的信息。

以下是 AWS 安全调查发现格式（ASFF）中的 `AwsApiGatewayV2Stage` 调查发现示例。要查看 `AwsApiGatewayV2Stage` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsApiGatewayV2StageDetails。

示例

```
"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 ASFF 中的资源

以下是AwsAppSync资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi提供有关 AWS AppSync GraphQL API 的信息，该API是您的应用程序的顶级结构。

以下示例显示了 AwsAppSyncGraphQLApi 对象的 ASFF。要查看 AwsAppSyncGraphQLApi 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsAppSyncGraphQLApi。

示例

```
"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 ASFF 中的资源

以下是AwsAthena资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsAthenaWorkGroup

AwsAthenaWorkGroup 提供了有关 Amazon Athena 工作组的信息。工作组可帮助您分离用户、团队、应用程序或工作负载。它还可以帮助您设置数据处理限制并跟踪成本。

以下示例显示了 AwsAthenaWorkGroup 对象的 ASFF。要查看 AwsAthenaWorkGroup 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsAthenaWorkGroup。

示例

```
"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 ASFF 中的资源

以下是AwsAutoScaling资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsAutoScalingAutoScalingGroup

AwsAutoScalingAutoScalingGroup 对象提供有关自动扩展组的详细信息。

以下是 AWS 安全调查发现格式（ASFF）中的 AwsAutoScalingAutoScalingGroup 调查发现示例。要查看 AwsAutoScalingAutoScalingGroup 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsAutoScalingAutoScalingGroupDetails。

示例

```
"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

AwsAutoScalingLaunchConfiguration 对象提供有关启动配置的详细信息。

以下是 AWS 安全AwsAutoScalingLaunchConfiguration调查结果格式 (ASFF) 中的示例发现。

要查看 AwsAutoScalingLaunchConfiguration 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsAutoScalingLaunchConfigurationDetails。

示例

```
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 ASFF 中的资源

以下是AwsBackup资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsBackupBackupPlan

AwsBackupBackupPlan 对象提供有关 AWS Backup 备份计划的信息。 AWS Backup 备份计划是一种策略表达式，用于定义何时以及如何备份 AWS 资源。

以下示例显示了AwsBackupBackupPlan对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsBackupBackupPlan 属性的描述，请参阅 AWS Security Hub API 参考中的AwsBackupBackupPlan。

示例

```
"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

`AwsBackupBackupVault` 对象提供有关 AWS Backup 备份文件库的信息。 AWS Backup 备份保管库是一个用于存储和组织备份的容器。

以下示例显示了`AwsBackupBackupVault`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsBackupBackupVault` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsBackupBackupVault。

示例

```
"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

`AwsBackupRecoveryPoint` 对象提供有关 AWS Backup 备份的信息，也称为恢复点。 AWS Backup 恢复点代表资源在指定时间的内容。

以下示例显示了`AwsBackupRecoveryPoint`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsBackupBackupVault` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsBackupRecoveryPoint。

示例

```
"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 ASFF 中的资源

以下是AwsCertificateManager资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsCertificateManagerCertificate

AwsCertificateManagerCertificate 对象提供有关 AWS Certificate Manager （ ACM ）证书的详细信息。

以下是 AWS 安全AwsCertificateManagerCertificate调查结果格式 (ASFF) 中的示例发现。要查看 AwsCertificateManagerCertificate 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsCertificateManagerCertificateDetails。

示例

```
"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 ASFF 中的资源

以下是`AwsCloudFormation`资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsCloudFormationStack

`AwsCloudFormationStack` 对象提供有关在顶级模板中作为资源进行嵌套的 AWS CloudFormation 堆栈的详细信息。

以下示例显示了AwsCloudFormationStack对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsCloudFormationStack 属性的描述，请参阅 AWS Security Hub API 参考中的AwsCloudFormationStackDetails。

示例

```
"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 ASFF 中的资源

以下是AwsCloudFront资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsCloudFrontDistribution

该AwsCloudFrontDistribution对象提供有关 Amazon CloudFront 分配配置的详细信息。

以下是 AWS 安全调查发现格式（ASFF）中的 AwsCloudFrontDistribution 调查发现示例。要查看 AwsCloudFrontDistribution 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsCloudFrontDistributionDetails。

示例

```
"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 ASFF 中的资源

以下是AwsCloudTrail资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsCloudTrailTrail

AwsCloudTrailTrail 对象提供有关 AWS CloudTrail 路径的详细信息。

以下是 AWS 安全调查发现格式（ASFF）中的 AwsCloudTrailTrail 调查发现示例。要查看 AwsCloudTrailTrail 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsCloudTrailTrailDetails。

示例

```
"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 ASFF 中的资源

以下是AwsCloudWatch资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsCloudWatchAlarm

该AwsCloudWatchAlarm对象提供有关 Amazon CloudWatch 警报的详细信息，这些警报会监视指标或在警报状态发生变化时执行操作。

以下示例显示了AwsCloudWatchAlarm对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsCloudWatchAlarm 属性的描述，请参阅 AWS Security Hub API 参考中的AwsCloudWatchAlarmDetails。

示例

```
"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 ASFF 中的资源

以下是AwsCodeBuild资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsCodeBuildProject

AwsCodeBuildProject 对象提供有关 AWS CodeBuild 项目的信息。

以下是 AWS 安全调查发现格式（ASFF）中的 AwsCodeBuildProject 调查发现示例。要查看 AwsCodeBuildProject 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsCodeBuildProjectDetails。

示例

```
"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 ASFF 中的资源

以下是AwsDms资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsDmsEndpoint

该AwsDmsEndpoint对象提供有关 AWS Database Migration Service (AWS DMS) 端点的信息。端点提供有关数据存储的连接、数据存储类型和位置信息。

以下示例显示了AwsDmsEndpoint对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsDmsEndpoint 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsDmsEndpointDetails。

示例

```
"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

该AwsDmsReplicationInstance对象提供有关 AWS Database Migration Service (AWS DMS) 复制实例的信息。DMS 使用复制实例连接到源数据存储，读取源数据并设置数据格式以供目标数据存储使用。

以下示例显示了AwsDmsReplicationInstance对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsDmsReplicationInstance 属性的描述，请参阅 AWS Security Hub API 参考中的AwsDmsReplicationInstanceDetails。

示例

```
"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

该AwsDmsReplicationTask对象提供有关 AWS Database Migration Service (AWS DMS) 复制任务的信息。复制任务将一组数据从源端点移动到目标端点。

以下示例显示了AwsDmsReplicationInstance对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsDmsReplicationInstance 属性的描述，请参阅 AWS Security Hub API 参考中的AwsDmsReplicationInstance。

示例

```
"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"
}
```

AwsDynamo数据库 ASFF 中的资源

以下是AwsDynamoDB资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsDynamoDbTable

AwsDynamoDbTable 对象提供有关 Amazon DynamoDB 表的详细信息。

以下是 AWS 安全调查发现格式（ASFF）中的 AwsDynamoDbTable 调查发现示例。要查看 AwsDynamoDbTable 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsDynamoDbTableDetails。

示例

```
"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 ASFF 中的资源

以下是AwsEc2资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsEc2ClientVpnEndpoint

该AwsEc2ClientVpnEndpoint对象提供有关 AWS Client VPN 端点的信息。客户端 VPN 端点是您创建并配置以用于启用和管理客户端 VPN 会话的资源。这是所有 Client VPN 会话的终止点。

以下示例显示了AwsEc2ClientVpnEndpoint对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEc2ClientVpnEndpoint 属性的描述，请参阅 AWS Security Hub API 参考中的AwsEc2ClientVpnEndpointDetails。

示例

```
"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

`AwsEc2Eip` 对象提供有关弹性 IP 地址的信息。

以下示例显示了`AwsEc2Eip`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2Eip` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2EipDetails。

示例

```
"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

`AwsEc2Instance` 对象提供有关 Amazon EC2 实例的详细信息。

以下示例显示了`AwsEc2Instance`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2Instance` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2InstanceDetails。

示例

```
"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

`AwsEc2LaunchTemplate` 对象包含有关指定实例配置信息的 Amazon Elastic Compute Cloud 启动模板的详细信息。

以下示例显示了`AwsEc2LaunchTemplate`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2LaunchTemplate` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2LaunchTemplateDetails。

示例

```
"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

`AwsEc2NetworkAcl` 对象包含有关 Amazon EC2 网络访问控制列表（ACL）的详细信息。

以下示例显示了`AwsEc2NetworkAcl`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2NetworkAcl` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2NetworkAclDetails。

示例

```
"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

`AwsEc2NetworkInterface` 对象提供有关 Amazon EC2 网络接口的信息。

以下示例显示了`AwsEc2NetworkInterface`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2NetworkInterface` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2NetworkInterfaceDetails。

示例

```
"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

`AwsEc2RouteTable` 对象提供有关 Amazon EC2 路由表的信息。

以下示例显示了`AwsEc2RouteTable`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2RouteTable` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2RouteTableDetails。

示例

```
"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

`AwsEc2SecurityGroup` 对象描述 Amazon EC2 安全组。

以下示例显示了`AwsEc2SecurityGroup`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2SecurityGroup` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2SecurityGroupDetails。

示例

```
"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

AwsEc2Subnet 对象提供有关 Amazon EC2 中子网的信息。

以下示例显示了AwsEc2Subnet对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEc2Subnet 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2SubnetDetails。

示例

```
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

AwsEc2TransitGateway 对象提供有关互连虚拟私有云（VPC）和本地网络的 Amazon EC2 中转网关的详细信息。

以下是 AWS 安全AwsEc2TransitGateway调查结果格式 (ASFF) 中的示例发现。要查看 AwsEc2TransitGateway 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2TransitGatewayDetails。

示例

```
"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

`AwsEc2Volume` 对象提供有关 Amazon EC2 卷的详细信息。

以下示例显示了`AwsEc2Volume`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2Volume` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2VolumeDetails。

示例

```
"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

`AwsEc2Vpc` 对象提供有关 Amazon EC2 VPC 的详细信息。

以下示例显示了AwsEc2Vpc对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEc2Vpc 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2VpcDetails。

示例

```
"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

AwsEc2VpcEndpointService 对象包含有关 VPC 端点服务的服务配置的详细信息。

以下示例显示了AwsEc2VpcEndpointService对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEc2VpcEndpointService 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2VpcEndpointServiceDetails。

示例

```
"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

`AwsEc2VpcPeeringConnection` 对象提供有关两个 VPC 之间网络连接的详细信息。

以下示例显示了`AwsEc2VpcPeeringConnection`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEc2VpcPeeringConnection` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEc2VpcPeeringConnectionDetails。

示例

```
"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 ASFF 中的资源

以下是AwsEcr资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsEcrContainerImage

AwsEcrContainerImage 对象提供 Amazon ECR 镜像的信息。

以下示例显示了AwsEcrContainerImage对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEcrContainerImage 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcrContainerImageDetails。

示例

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

`AwsEcrRepository` 对象提供有关 Amazon Elastic Container Registry 存储库的信息。

以下示例显示了`AwsEcrRepository`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEcrRepository` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcrRepositoryDetails。

示例

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs ASFF 中的资源

以下是`AwsEcs`资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsEcsCluster

`AwsEcsCluster` 对象提供有关 Amazon Elastic Container Service 集群的详细信息。

以下示例显示了AwsEcsCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEcsCluster 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcsClusterDetails。

示例

```
    "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

AwsEcsContainer 对象包含有关 Amazon ECS 容器的详细信息。

以下示例显示了AwsEcsContainer对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEcsContainer 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcsContainerDetails。

示例

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

`AwsEcsService` 对象提供有关 Amazon ECS 集群内的服务的详细信息。

以下示例显示了`AwsEcsService`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsEcsService` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcsServiceDetails。

示例

```
"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

AwsEcsTask 对象提供有关 Amazon ECS 任务的详细信息。

以下示例显示了AwsEcsTask对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEcsTask 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcsTask。

示例

```
"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

AwsEcsTaskDefinition 对象包含有关任务定义的详细信息。任务定义描述 Amazon Elastic Container Service 任务的容器和卷定义。

以下示例显示了AwsEcsTaskDefinition对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEcsTaskDefinition 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEcsTaskDefinitionDetails。

示例

```
    "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 ASFF 中的资源

以下是AwsEfs资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsEfsAccessPoint

AwsEfsAccessPoint 对象提供有关存储在 Amazon Elastic File System 中的文件的详细信息。

以下示例显示了AwsEfsAccessPoint对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEfsAccessPoint 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEfsAccessPointDetails。

示例

```
"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 ASFF 中的资源

以下是AwsEks资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsEksCluster

AwsEksCluster 对象提供有关 Amazon EKS 集群的详细信息。

以下示例显示了AwsEksCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEksCluster 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEksClusterDetails。

示例

```
{
  "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 ASFF 中的资源

以下是`AwsElasticBeanstalk`资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsElasticBeanstalkEnvironment

`AwsElasticBeanstalkEnvironment` 对象包含有关 AWS Elastic Beanstalk 环境的详细信息。

以下示例显示了`AwsElasticBeanstalkEnvironment`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsElasticBeanstalkEnvironment` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsElasticBeanstalkEnvironmentDetails。

示例

```
"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 ASFF 中的资源

以下是AwsElasticSearch资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsElasticSearchDomain

该AwsElasticSearchDomain对象提供有关亚马逊 OpenSearch 服务域的详细信息。

以下示例显示了AwsElasticSearchDomain对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsElasticSearchDomain 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsElasticSearchDomainDetails。

示例

```
"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 ASFF 中的资源

以下是AwsElb资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsElbLoadBalancer

AwsElbLoadBalancer 对象包含有关经典负载均衡器的详细信息。

以下示例显示了AwsElbLoadBalancer对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsElbLoadBalancer 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsElbLoadBalancerDetails。

示例

```
"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

`AwsElbv2LoadBalancer` 对象提供有关负载均衡器的信息。

以下示例显示了`AwsElbv2LoadBalancer`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsElbv2LoadBalancer` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsElbv2LoadBalancerDetails。

示例

```
"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 ASFF 中的资源

以下是AwsEventBridge资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsEventSchemasRegistry

该AwsEventSchemasRegistry对象提供有关 Amazon EventBridge 架构注册表的信息。架构定义了发送到的事件的结构 EventBridge。架构注册表是收集架构并对其进行逻辑分组的容器。

以下示例显示了AwsEventSchemasRegistry对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEventSchemasRegistry 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEventSchemasRegistry。

示例

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
```

```
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

该AwsEventsEndpoint对象提供有关 Amazon EventBridge 全局终端节点的信息。终端节点可以通过设置 Regional-fault 容忍度来提高应用程序的可用性。

以下示例显示了AwsEventsEndpoint对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEventsEndpoint 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsEventsEndpointDetails。

示例

```
"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

该AwsEventsEventbus对象提供有关 Amazon EventBridge 全局终端节点的信息。终端节点可以通过设置 Regional-fault 容忍度来提高应用程序的可用性。

以下示例显示了AwsEventsEventbus对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsEventsEventbus 属性的描述，请参阅 AWS Security Hub API 参考中的AwsEventsEventbusDetails。

示例

```
"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 ASFF 中的资源

以下是AwsGuardDuty资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsGuardDutyDetector

该AwsGuardDutyDetector对象提供有关 Amazon GuardDuty 探测器的信息。探测器是代表 GuardDuty 服务的对象。需要探测器 GuardDuty 才能运行。

以下示例显示了AwsGuardDutyDetector对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsGuardDutyDetector 属性的描述，请参阅 AWS Security Hub API 参考中的AwsGuardDutyDetector。

示例

```
"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 ASFF 中的资源

以下是AwsIam资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsIamAccessKey

AwsIamAccessKey 对象包含与调查发现相关的 IAM 访问密钥的详细信息。

以下示例显示了AwsIamAccessKey对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsIamAccessKey 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsIamAccessKeyDetails。

示例

```
"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

AwsIamGroup 对象包含有关 IAM 组的详细信息。

以下示例显示了AwsIamGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsIamGroup 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsIamGroupDetails。

示例

```
"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

AwsIamPolicy 对象代表一个 IAM 权限策略。

以下示例显示了AwsIamPolicy对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsIamPolicy 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsIamPolicyDetails。

示例

```
"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

`AwsIamRole` 对象包含有关 IAM 角色的信息，包括该角色的所有策略。

以下示例显示了`AwsIamRole`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsIamRole` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsIamRoleDetails。

示例

```
"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

`AwsIamUser` 对象提供有关用户的信息。

以下示例显示了`AwsIamUser`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsIamUser` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsIamUserDetails。

示例

```
"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 ASFF 中的资源

以下是AwsKinesis资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsKinesisStream

AwsKinesisStream 对象提供有关 Amazon Kinesis Data Streams 的详细信息。

以下示例显示了AwsKinesisStream对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsKinesisStream 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsKinesisStreamDetails。

示例

```
"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 ASFF 中的资源

以下是AwsKms资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsKmsKey

该AwsKmsKey对象提供有关一个的详细信息 AWS KMS key。

以下示例显示了AwsKmsKey对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsKmsKey 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsKmsKeyDetails。

示例

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

以下是AwsLambda资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsLambdaFunction

AwsLambdaFunction 对象提供有关 Lambda 函数配置的详细信息。

以下示例显示了AwsLambdaFunction对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsLambdaFunction 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsLambdaFunctionDetails。

示例

```
"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

AwsLambdaLayerVersion 对象提供有关 Lambda 层版本的详细信息。

以下示例显示了AwsLambdaLayerVersion对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsLambdaLayerVersion 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsLambdaLayerVersionDetails。

示例

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk ASFF 中的资源

以下是AwsMsk资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsMskCluster

AwsMskCluster 对象提供有关 Amazon Managed Streaming for Apache Kafka（Amazon MSK）集群的信息。

以下示例显示了AwsMskCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsMskCluster 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsMskClusterDetails。

示例

```
"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 ASFF 中的资源

以下是AwsNetworkFirewall资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsNetworkFirewallFirewall

AwsNetworkFirewallFirewall 对象包含有关 AWS Network Firewall 防火墙的详细信息。

以下示例显示了AwsNetworkFirewallFirewall对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsNetworkFirewallFirewall 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsNetworkFirewallFirewallDetails。

示例

```
"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

AwsNetworkFirewallFirewallPolicy 对象提供有关防火墙策略的详细信息。防火墙策略定义网络防火墙的行为。

以下示例显示了AwsNetworkFirewallFirewallPolicy对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsNetworkFirewallFirewallPolicy 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsNetworkFirewallFirewallPolicyDetails。

示例

```
"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

AwsNetworkFirewallRuleGroup 对象提供有关 AWS Network Firewall 规则组的详细信息。规则组用于检查和控制网络流量。无状态规则组适用于各个数据包。有状态规则组适用于其流量上下文中的数据包。

规则组在防火墙策略中引用。

以下示例显示了AwsNetworkFirewallRuleGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsNetworkFirewallRuleGroup 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsNetworkFirewallRuleGroupDetails。

示例——无状态规则组

```
"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"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

示例——有状态规则组

```
"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"
                        }
                    ]
                }
            ]
         }
    }
}
```

以下是 AwsNetworkFirewallRuleGroup 属性的有效值示例列表：

- Action

  有效值：PASS |DROP |ALERT

- Protocol

  有效值：IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

有效值：FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

有效值：FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService ASFF 中的资源

以下是AwsOpenSearchService资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsOpenSearchServiceDomain

该AwsOpenSearchServiceDomain对象包含有关亚马逊 OpenSearch 服务域的信息。

以下示例显示了AwsOpenSearchServiceDomain对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsOpenSearchServiceDomain 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsOpenSearchServiceDomainDetails。

示例

```
"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 ASFF 中的资源

以下是AwsRds资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsRdsDbCluster

AwsRdsDbCluster 对象提供有关 Amazon RDS 数据库集群的详细信息。

以下示例显示了AwsRdsDbCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsRdsDbCluster 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRdsDbClusterDetails。

示例

```
"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

AwsRdsDbClusterSnapshot 对象包含有关 Amazon RDS DS集群快照的信息。

以下示例显示了AwsRdsDbClusterSnapshot对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsRdsDbClusterSnapshot 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRdsDbClusterSnapshotDetails。

示例

```
"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

`AwsRdsDbInstance` 对象提供有关 Amazon RDS 数据库实例的详细信息。

以下示例显示了`AwsRdsDbInstance`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsRdsDbInstance` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRdsDbInstanceDetails。

示例

```
"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

`AwsRdsDbSecurityGroup` 对象包含有关 Amazon Relational Database Service 的信息

以下示例显示了`AwsRdsDbSecurityGroup`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsRdsDbSecurityGroup` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRdsDbSecurityGroupDetails。

示例

```
"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

AwsRdsDbSnapshot 对象包含有关 Amazon RDS DS集群快照的详细信息。

以下示例显示了AwsRdsDbSnapshot对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsRdsDbSnapshot 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRdsDbSnapshotDetails。

示例

```
"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 包含有关 RDS 事件通知订阅的详细信息。订阅允许 RDS 将事件发布到 SNS 主题。

以下示例显示了AwsRdsEventSubscription对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsRdsEventSubscription 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRdsEventSubscriptionDetails。

示例

```
"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 ASFF 中的资源

以下是AwsRedshift资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsRedshiftCluster

AwsRedshiftCluster 对象包含有关 Amazon Redshift 集群的详细信息。

以下示例显示了AwsRedshiftCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsRedshiftCluster 属性的描述，请参阅 AWS Security Hub API 参考中的AwsRedshiftClusterDetails。

示例

```
"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 ASFF 中的资源

以下是AwsRoute53资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsRoute53HostedZone

AwsRoute53HostedZone 对象提供有关 Amazon Route 53 托管区域的信息，包括分配给托管区域的四个名称服务器。托管区域表示可统一管理的一组记录，属于单一父域名。

以下示例显示了AwsRoute53HostedZone对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsRoute53HostedZone 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsRoute53HostedZoneDetails。

示例

```
"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"
        }
    ]
}
```

awss3 ASFF 中的资源

以下是AwsS3资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsS3AccessPoint

AwsS3AccessPoint 提供有关 Amazon S3 接入点的信息。S3 接入点是附加到 S3 存储桶的具名网络端点，您可以使用这些存储桶执行 S3 对象操作。

以下示例显示了AwsS3AccessPoint对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsS3AccessPoint 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsS3AccessPointDetails。

示例

```
"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` 提供了有关账户的 Amazon S3 公共访问屏蔽配置的信息。

以下示例显示了`AwsS3AccountPublicAccessBlock`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsS3AccountPublicAccessBlock` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsS3AccountPublicAccessBlockDetails。

示例

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

`AwsS3Bucket` 对象提供有关 Amazon S3 存储桶的详细信息。

以下示例显示了`AwsS3Bucket`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsS3Bucket` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsS3BucketDetails。

示例

```
"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"
```

```
                }
            }
        ]
    }
}
```

AWSS3Object

`AwsS3Object` 对象提供有关 Amazon S3 对象的信息。

以下示例显示了`AwsS3Object`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsS3Object` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsS3ObjectDetails。

示例

```
"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 ASFF 中的资源

以下是`AwsSageMaker`资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsSageMakerNotebookInstance

该`AwsSageMakerNotebookInstance`对象提供有关 Amazon A SageMaker I 笔记本实例的信息，该实例是运行 Jupyter Notebook 应用程序的机器学习计算实例。

以下示例显示了`AwsSageMakerNotebookInstance`对象 AWS 的安全调查结果格式 (ASFF)。要查看 `AwsSageMakerNotebookInstance` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsSageMakerNotebookInstanceDetails。

示例

```
"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 ASFF 中的资源

以下是AwsSecretsManager资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsSecretsManagerSecret

AwsSecretsManagerSecret 对象提供有关 Secrets Manager 密钥的详细信息。

以下示例显示了AwsSecretsManagerSecret对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsSecretsManagerSecret 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsSecretsManagerSecretDetails。

示例

```
"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 ASFF 中的资源

以下是AwsSns资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsSnsTopic

AwsSnsTopic 对象包含有关 Amazon Simple Notification Service 主题。

以下示例显示了AwsSnsTopic对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsSnsTopic 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsSnsTopicDetails。

示例

```
"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 ASFF 中的资源

以下是AwsSqs资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsSqsQueue

AwsSqsQueue 对象包含有关 Amazon Simple Queue Service 队列的信息。

以下示例显示了AwsSqsQueue对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsSqsQueue 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsSqsQueueDetails。

示例

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm ASFF 中的资源

以下是AwsSsm资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsSsmPatchCompliance

AwsSsmPatchCompliance 对象根据用于修补实例的补丁基准提供有关实例补丁状态的信息。

以下示例显示了AwsSsmPatchCompliance对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsSsmPatchCompliance 属性的描述，请参阅 AWS Security Hub API 参考中的AwsSsmPatchComplianceDetails。

示例

```
"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 ASFF 中的资源

以下是AwsStepFunctions资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsStepFunctionStateMachine

AwsStepFunctionStateMachine 对象提供有关 AWS Step Functions 状态机的信息，状态机是一个由一系列事件驱动步骤组成的工作流程。

以下示例显示了AwsStepFunctionStateMachine对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsStepFunctionStateMachine 属性的描述，请参阅 AWS Security Hub API 参考中的AwsStepFunctionStateMachine。

示例

```
"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 ASFF 中的资源

以下是AwsWaf资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsWafRateBasedRule

AwsWafRateBasedRule 对象包含有关 AWS WAF 基于速率的全局资源规则的详细信息。 AWS WAF 基于速率的规则提供设置，以指示何时允许、阻止或计算请求。 Rate-based 规则包括在指定时间段内到达的请求数量。

以下示例显示了AwsWafRateBasedRule对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafRateBasedRule 属性的描述，请参阅 AWS Security Hub API 参考中的AwsWafRateBasedRuleDetails。

示例

```
"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

AwsWafRegionalRateBasedRule 对象包含有关基于速率的区域性资源规则的详细信息。基于速率的规则提供设置，以指示何时允许、阻止或计算请求。 Rate-based 规则包括在指定时间段内到达的请求数量。

以下示例显示了AwsWafRegionalRateBasedRule对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafRegionalRateBasedRule 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsWafRegionalRateBasedRuleDetails。

示例

```
"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

该AwsWafRegionalRule对象提供有关 AWS WAF 区域规则的详细信息。此规则标识您想要允许、阻止或计数的 Web 请求。

以下示例显示了AwsWafRegionalRule对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafRegionalRule 属性的描述，请参阅 AWS Security Hub API 参考中的AwsWafRegionalRuleDetails。

示例

```
"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

AwsWafRegionalRuleGroup 对象提供有关 AWS WAF 区域规则组的详细信息。规则组是添加到 Web 访问控制列表（Web ACL）的预定义规则的集合。

以下示例显示了AwsWafRegionalRuleGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafRegionalRuleGroup 属性的描述，请参阅 AWS Security Hub API 参考中的AwsWafRegionalRuleGroupDetails。

示例

```
"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`提供了有关 AWS WAF 区域 Web 访问控制列表 (Web ACL) 的详细信息。Web ACL 包含用于标识您要允许、阻止或计数的请求的规则。

以下是 AWS 安全调查发现格式（ASFF）中的 `AwsWafRegionalWebAcl` 调查发现示例。要查看 `AwsApiGatewayV2Stage` 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsWafRegionalWebAclDetails。

示例

```
"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`提供有关 AWS WAF 规则的信息。 AWS WAF 规则用于标识您想要允许、阻止或计数的 Web 请求。

以下是 AWS 安全AwsWafRule调查结果格式 (ASFF) 中的示例发现。要查看AwsApiGatewayV2Stage属性的描述，请参阅 AWS Security Hub API 参考中的AwsWafRuleDetails。

示例

```
"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提供了有关 AWS WAF 规则组的信息。 AWS WAF 规则组是您添加到 Web 访问控制列表（Web ACL）中的预定义规则的集合。

以下是 AWS 安全AwsWafRuleGroup调查结果格式 (ASFF) 中的示例发现。要查看AwsApiGatewayV2Stage属性的描述，请参阅 AWS Security Hub API 参考中的AwsWafRuleGroupDetails。

示例

```
"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

该AwsWafv2RuleGroup对象提供有关 AWS WAF V2 规则组的详细信息。

以下示例显示了AwsWafv2RuleGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafv2RuleGroup 属性的描述，请参阅 AWS Security Hub API 参考中的AwsWafv2RuleGroupDetails。

示例

```
"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

该AwsWafWebAcl对象提供有关 AWS WAF Web ACL 的详细信息。

以下示例显示了AwsWafWebAcl对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafWebAcl 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsWafWebAclDetails。

示例

```
"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

该AwsWafv2WebAcl对象提供有关 AWS WAF V2 Web ACL 的详细信息。

以下示例显示了AwsWafv2WebAcl对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsWafv2WebAcl 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsWafv2WebAclDetails。

示例

```
"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 ASFF 中的资源

以下是AwsXray资源 AWS 的安全调查结果格式 (ASFF) 语法的示例。

AWS Security Hub CSPM 将各种来源的发现标准化为 ASFF。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

AwsXrayEncryptionConfig

该AwsXrayEncryptionConfig对象包含有关加密配置的信息 AWS X-Ray。

以下示例显示了AwsXrayEncryptionConfig对象 AWS 的安全调查结果格式 (ASFF)。要查看 AwsXrayEncryptionConfig 属性的描述，请参阅 AWS Security Hub API 参考中的 AwsXrayEncryptionConfigDetails。

示例

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository ASFF 中的对象

该CodeRepository对象提供有关外部代码存储库的信息，您已将该代码存储库连接到 AWS 资源并将 Amazon Inspector 配置为扫描漏洞。

以下示例显示了该CodeRepository对象 AWS 的安全调查结果格式 (ASFF) 语法。要查看 CodeRepository 属性的描述，请参阅 AWS Security Hub API 参考中的 CodeRepositoryDetails。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

示例

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Container ASFF 中的对象

以下示例显示了该Container对象 AWS 的安全调查结果格式 (ASFF) 语法。要查看 Container 属性的描述，请参阅 AWS Security Hub API 参考中的 ContainerDetails。有关 ASFF 的背景信息，请参阅 AWS 安全调查结果格式 (ASFF)。

示例

```
"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"
    }]
}
```

其他 ASFF 中的对象

在 AWS 安全调查结果格式 (ASFF) 中，Other对象指定自定义字段和值。有关 ASFF 的更多信息，请参阅 AWS 安全调查结果格式 (ASFF)。

通过使用 Other 对象，您可以为资源指定自定义字段和值。您可以在以下情况下使用 Other 对象：

- 该资源类型没有对应的 Details 对象。要指定资源的详细信息，请使用 Other 对象。
- 资源类型的 Details 对象不包括要指定的所有属性。在这种情况下，请使用资源类型的 Details 对象来指定可用属性。使用 Other 对象指定不在特定于类型的 Details 对象中的属性。
- 资源类型不是提供的类型之一。在这种情况下，请将 Resource.Type 设置为 Other，并使用 Other 对象指定详细信息。

类型：最多 50 个键/值对的映射

每个键-值对必须满足以下要求。

- 密钥包含的字符数必须少于 128 个。
- 该值包含的字符数必须少于 1024 个。

在 Security Hub CSPM 中查看见解

在 S AWS ecurity Hub CSPM 中，见解是相关发现的集合。见解可以确定需要注意和干预的特定安全领域。例如，见解可能会指出发现不良安全做法的调查结果所针对的实 EC2 例。见解汇集了来自各个调查发现提供商的结果。

每个见解由一个分组依据语句和多个可选的筛选条件定义。分组依据语句指示如何对匹配的调查发现进行分组，并确定见解应用于的项目的类型。例如，如果见解按资源标识符分组，则该见解会生成资源标识符列表。可选的筛选条件用于识别与见解匹配的调查发现。例如，您可能希望仅查看来自特定提供商的调查发现或与特定类型的资源相关的调查发现。

Security Hub CSPM 提供了多个内置的托管见解。您无法修改或删除托管见解。要跟踪您的 AWS 环境和使用情况所特有的安全问题，您可以创建自定义见解。

Sec AWS urity Hub CSPM 控制台上的 “见解” 页面显示可用见解列表。

默认情况下，该列表同时显示托管和自定义见解。要根据见解类型筛选见解列表，请从筛选字段旁边的下拉菜单中选择见解类型。

- 要显示所有可用的见解，请选择所有见解。这是默认选项。
- 要仅显示托管见解，请选择 Security Hub CSPM 托管见解。
- 要仅显示自定义见解，请选择自定义见解。

您还可以根据见解名称筛选见解列表。为此，在筛选字段中，键入用于筛选列表的文本。筛选不区分大小写。筛选器会查找在见解名称中任意位置包含文本的见解。

仅在启用了集成或标准来生成匹配的调查发现时，见解才返回结果。例如，托管见解 29. 仅当您启用 Center for Internet Security（CIS） AWS 基金会基准标准版本时，失败的 CIS 检查次数排在首位的资源才会返回结果。

查看 Security Hub CSPM 中的见解并对其采取行动

对于每个见解，S AWS ecurity Hub CSPM 首先确定与筛选条件匹配的结果，然后使用分组属性对匹配的结果进行分组。

在控制台上的见解页面中，您可以查看结果和调查发现并执行相应操作。

如果您启用跨区域聚合，则托管见解的结果（在您登录到聚合区域后）包括聚合区域和关联区域的调查发现。如果见解未按区域筛选，则自定义见解的结果还会包括聚合区域和关联区域的调查发现（在您登录到聚合区域后）。在其他区域，见解结果仅适用于本区域。

有关配置跨区域聚合的信息，请参阅the section called “跨区域聚合数据”。

查看见解结果并执行相应操作

见解结果由见解结果的分组列表组成。例如，如果见解按资源标识符进行分组，则见解结果是资源标识符的列表。结果列表中的每个项均指示该项的匹配调查发现数。

如果调查发现按资源标识符或资源类型分组，则结果会包括匹配调查发现中的所有资源。这包括与筛选条件中指定的资源类型不同的资源。例如，一个见解识别与 S3 存储桶相关联的调查发现。如果匹配的调查发现同时包含 S3 存储桶资源和 IAM 访问密钥资源，则洞察结果会包括这两种资源。

在 Security Hub CSPM 控制台上，结果列表从匹配率最高的调查发现到匹配率最低的调查发现排序。Security Hub CSPM 只能显示 100 个结果。如果分组值超过 100 个，则只能看到前 100 个。

除了结果列表之外，见解结果还显示一组图表，其中汇总了以下属性的匹配调查发现数。

- 严重性标签——每个严重性标签的调查发现数
- AWS 账户 ID — 匹配结果的前五个原因 IDs
- 资源类型——匹配调查发现的前 5 个资源类型
- 资源 ID-匹配结果的前五个资源 IDs
- 产品名称——匹配的调查发现的前 5 个调查发现提供商

如果您已配置自定义操作，则可以将选定结果发送到自定义操作。该操作必须与`Security Hub Insight Results`事件类型的 Amazon CloudWatch 规则相关联。有关更多信息，请参阅 the section called “自动响应和补救”。如果您尚未配置自定义操作，则操作菜单处于禁用状态。

Security Hub CSPM console

查看见解结果并执行相应操作（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 要显示见解结果列表，请选择见解名称。
4. 选中要发送到自定义操作的每个结果的复选框。
5. 从操作菜单中，选择自定义操作。

Security Hub CSPM API, AWS CLI

要查看洞察结果并对其采取行动（API， AWS CLI）

要查看见解结果，请使用 Security Hub CSPM API 的 >GetInsightResults 操作。如果您使用 AWS CLI，请运行该get-insight-results命令。

要确定要返回结果的见解，您需要见解 ARN。要获取自定义见解 ARNs 的见解，请使用 GetInsightsAPI 操作或get-insight-results命令。

以下示例会检索指定见解的结果。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

有关如何以编程方式创建自定义操作的信息，请参阅使用自定义操作将调查结果和见解结果发送到 EventBridge。

查看见解结果调查发现并执行相应操作（控制台）

从 Security Hub CSPM 控制台上的见解结果列表中，您可以显示每个结果的调查发现列表。

显示见解调查发现并执行相应操作（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 要显示见解结果列表，请选择见解名称。
4. 要显示见解结果的调查结果列表，请从结果列表中选择项目。调查发现结果列表显示了工作流状态为 NEW 或 NOTIFIED 的所选见解结果的活动调查发现。

从调查发现列表中，您可以执行以下操作：

- 在 Security Hub CSPM 中筛选调查发现
- 查看调查发现的详细信息和历史记录
- 在 Security Hub CSPM 中设置调查发现的工作流状态

- 将调查发现发送到自定义 Security Hub CSPM 操作

Security Hub CSPM 中的托管见解

AWS Security Hub CSPM 提供了多种托管见解。

您无法编辑或删除 Security Hub CSPM 托管见解。您可以查看见解结果和调查发现并采取措施。您还可以将托管见解用作新的自定义见解的基础。

与所有见解一样，仅在启用了产品集成或安全标准来生成匹配的调查发现时，托管见解才返回结果。

对于按资源标识符分组的见解，结果包括匹配调查发现中所有资源的标识符。这包括与筛选条件中的资源类型不同的资源。例如，以下列表中的见解 2 识别与 Amazon S3 存储桶关联的调查发现。如果匹配的调查发现同时包含 S3 存储桶资源和 IAM 访问密钥资源，则见解结果会包括这两种资源。

Security Hub CSPM 目前提供了以下托管见解：

1。 AWS 发现最多的资源

ARN：`arn:aws:securityhub:::insight/securityhub/default/1`

分组依据：资源标识符

调查发现筛选条件：

- 记录状态为 `ACTIVE`
- 工作流状态为 `NEW` 或 `NOTIFIED`

2. 具有公共写入或读取权限的 S3 存储桶

ARN：`arn:aws:securityhub:::insight/securityhub/default/10`

分组依据：资源标识符

调查发现筛选条件：

- 类型以 `Effects/Data Exposure` 开头
- 资源类型为 `AwsS3Bucket`
- 记录状态为 `ACTIVE`
- 工作流状态为 `NEW` 或 `NOTIFIED`

3。 AMIs 得出的发现最多

ARN：arn:aws:securityhub:::insight/securityhub/default/3

分组依据： EC2 实例镜像 ID

调查发现筛选条件：

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

4。 EC2 已知战术、技术和程序中涉及的实例 (TTPs)

ARN：arn:aws:securityhub:::insight/securityhub/default/14

分组依据：资源 ID

调查发现筛选条件：

- 类型以 TTPs 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

5。 AWS 访问密钥活动可疑的校长

ARN：arn:aws:securityhub:::insight/securityhub/default/9

分组依据：IAM 访问密钥主体名称

调查发现筛选条件：

- 资源类型为 AwsIamAccessKey
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

6。 AWS 不符合安全标准/最佳实践的资源实例

ARN：arn:aws:securityhub:::insight/securityhub/default/6

分组依据：资源 ID

调查发现筛选条件：

- 类型为 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

7。 AWS 与潜在数据泄露相关的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/7

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Effects/Data Exfiltration/ 开头
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

8。 AWS 与未经授权的资源消耗相关的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/8

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Effects/Resource Consumption 开头
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

9. 不符合安全标准/最佳实践的 S3 存储桶

ARN：arn:aws:securityhub:::insight/securityhub/default/11

分组依据：资源 ID

调查发现筛选条件：

- 资源类型为 AwsS3Bucket
- 类型为 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- 记录状态为 ACTIVE

- 工作流状态为 NEW 或 NOTIFIED

10. 具有敏感数据的 S3 存储桶

ARN：arn:aws:securityhub:::insight/securityhub/default/12

分组依据：资源 ID

调查发现筛选条件：

- 资源类型为 AwsS3Bucket
- 类型以 Sensitive Data Identifications/ 开头
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

11. 可能泄露的凭证

ARN：arn:aws:securityhub:::insight/securityhub/default/13

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Sensitive Data Identifications/Passwords/ 开头
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

12。 EC2 缺少针对重要漏洞的安全补丁的实例

ARN：arn:aws:securityhub:::insight/securityhub/default/16

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Software and Configuration Checks/Vulnerabilities/CVE 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

13。 EC2 具有一般异常行为的实例

ARN：arn:aws:securityhub:::insight/securityhub/default/17

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Unusual Behaviors 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

14。 EC2 具有可从互联网访问端口的实例

ARN：arn:aws:securityhub:::insight/securityhub/default/18

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Software and Configuration Checks/AWS Security Best Practices/Network Reachability 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

15。 EC2 不符合安全标准/最佳实践的实例

ARN：arn:aws:securityhub:::insight/securityhub/default/19

分组依据：资源 ID

调查发现筛选条件：

- 类型以下列某个项开头：
  - Software and Configuration Checks/Industry and Regulatory Standards/
  - Software and Configuration Checks/AWS Security Best Practices
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

16。 EC2 向互联网开放的实例

ARN：arn:aws:securityhub:::insight/securityhub/default/21

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Software and Configuration Checks/AWS Security Best Practices/Network Reachability 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

17。 EC2 与对手侦察相关的实例

ARN：arn:aws:securityhub:::insight/securityhub/default/22

分组依据：资源 ID

调查发现筛选条件：

- 类型以 /Discovery TTPs /Recon 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

18。 AWS 与恶意软件关联的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/23

分组依据：资源 ID

调查发现筛选条件：

- 类型以下列某个项开头：
  - 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
- 记录状态为 ACTIVE

- 工作流状态为 NEW 或 NOTIFIED

19。 AWS 与加密货币问题相关的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/24

分组依据：资源 ID

调查发现筛选条件：

- 类型以下列某个项开头：
  - Effects/Resource Consumption/Cryptocurrency
  - TTPs/Command and Control/CryptoCurrency
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

20。 AWS 尝试未经授权访问的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/25

分组依据：资源 ID

调查发现筛选条件：

- 类型以下列某个项开头：
  - TTPs/Command and Control/UnauthorizedAccess
  - TTPs/Initial Access/UnauthorizedAccess
  - Effects/Data Exfiltration/UnauthorizedAccess
  - Unusual Behaviors/User/UnauthorizedAccess
  - Effects/Resource Consumption/UnauthorizedAccess
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

21. 上周命中次数最多的威胁情报指标

ARN：arn:aws:securityhub:::insight/securityhub/default/26

调查发现筛选条件：

- 已在过去 7 天内创建

22. 按调查发现数排列的顶级账户

    ARN：arn:aws:securityhub:::insight/securityhub/default/27

    分组依据： AWS 账户 ID

    调查发现筛选条件：

    - 记录状态为 ACTIVE
    - 工作流状态为 NEW 或 NOTIFIED

23. 按调查发现数排列的顶级产品

    ARN：arn:aws:securityhub:::insight/securityhub/default/28

    分组依据：产品名称

    调查发现筛选条件：

    - 记录状态为 ACTIVE
    - 工作流状态为 NEW 或 NOTIFIED

24. 按调查发现数排列的严重性

    ARN：arn:aws:securityhub:::insight/securityhub/default/29

    分组依据：严重性标签

    调查发现筛选条件：

    - 记录状态为 ACTIVE
    - 工作流状态为 NEW 或 NOTIFIED

25. 按调查发现数排列的顶级 S3 存储桶

    ARN：arn:aws:securityhub:::insight/securityhub/default/30

    分组依据：资源 ID

    调查发现筛选条件：

    - 资源类型为 AwsS3Bucket
    - 记录状态为 ACTIVE
    - 工作流状态为 NEW 或 NOTIFIED

26. 按发现次数排列的热门 EC2 实例

ARN：arn:aws:securityhub:::insight/securityhub/default/31

分组依据：资源 ID

调查发现筛选条件：

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

27. AMIs 按发现次数排在首位

ARN：arn:aws:securityhub:::insight/securityhub/default/32

分组依据： EC2 实例镜像 ID

调查发现筛选条件：

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

28. 按调查发现数排列的顶级 IAM 用户

ARN：arn:aws:securityhub:::insight/securityhub/default/33

分组依据：IAM 访问密钥 ID

调查发现筛选条件：

- 资源类型为 AwsIamAccessKey
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

29. 按失败 CIS 检查数排列的顶级资源

ARN：arn:aws:securityhub:::insight/securityhub/default/34

分组依据：资源 ID

调查发现筛选条件：

- 生成器 ID 以 arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule 开头
- 已在最后一天更新
- 合规性状态为 FAILED
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

30. 按调查发现数排列的顶级集成

ARN：arn:aws:securityhub:::insight/securityhub/default/35

分组依据：产品 ARN

调查发现筛选条件：

- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

31. 安全检查失败最多的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/36

分组依据：资源 ID

调查发现筛选条件：

- 已在最后一天更新
- 合规性状态为 FAILED
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

32。有可疑活动的 IAM 用户

ARN：arn:aws:securityhub:::insight/securityhub/default/37

分组依据：IAM 用户

调查发现筛选条件：

- 资源类型为 AwsIamUser
- 记录状态为 ACTIVE
- 工作流状态为 NEW 或 NOTIFIED

33。 AWS Health 发现最多的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/38

分组依据：资源 ID

调查发现筛选条件：

- ProductName 等于 Health

34。 AWS Config 发现最多的资源

ARN：arn:aws:securityhub:::insight/securityhub/default/39

分组依据：资源 ID

调查发现筛选条件：

- ProductName 等于 Config

35。调查发现最多的应用程序

ARN：arn:aws:securityhub:::insight/securityhub/default/40

分组依据: ResourceApplicationArn

调查发现筛选条件：

- RecordState 等于 ACTIVE
- Workflow.Status 等于 NEW 或 NOTIFIED

了解 Security Hub CSPM 中的自定义见解

除了 S AWS ecurity Hub CSPM 托管见解外，您还可以在 Security Hub CSPM 中创建自定义见解，以跟踪特定于您的环境的问题。自定义见解可帮助您跟踪一部分精选问题。

以下是一些可能有助于设置的自定义见解示例：

- 如果您拥有管理员账户，则可以设置自定义见解来跟踪影响成员账户的关键和高严重性调查发现。
- 如果您依赖特定的集成 AWS 服务，则可以设置自定义洞察来跟踪该服务的关键和高严重性发现。
- 如果您依赖第三方集成，您可以设置一个自定义见解来跟踪来自该集成产品的关键和高严重性调查发现。

您可以创建全新的自定义见解，也可以从现有的自定义见解或托管见解开始。

每个见解都可以配置以下选项：

- 分组属性——分组属性确定了在见解结果列表中显示哪些项目。例如，如果分组属性是产品名称，则见解结果会显示与每个调查发现提供者关联的调查发现数量。
- 可选筛选条件——筛选条件将缩小见解的匹配调查发现的范围。

  只有当调查发现符合所有提供的筛选条件时，它才会包含在见解结果中。例如，如果筛选条件为 “产品名称为 GuardDuty”，“资源类型为`AwsS3Bucket`”，则匹配的结果必须符合这两个条件。

  但是，Security Hub CSPM 会对使用相同属性但不同值的筛选条件应用布尔值 OR 逻辑。例如，如果筛选条件为 “商品名称为”，“商品名称为 Amazon In GuardDuty spector”，则如果搜索结果由亚马逊 GuardDuty 或亚马逊检查员生成，则结果与之匹配。

如果您使用资源标识符或资源类型作为分组属性，则见解结果会包括匹配调查发现中的所有资源。该列表不限于与资源类型筛选条件匹配的资源。例如，见解可以识别与 S3 存储桶关联的调查发现，并按资源标识符对这些调查发现进行分组。匹配的调查发现同时包含 S3 存储桶资源和 IAM 访问密钥资源。见解结果包括这两种资源。

如果您启用了跨区域聚合，然后创建自定义见解，则该见解会应用于聚合区域和关联区域中的匹配调查发现。例外情况是见解包含区域筛选条件。

创建自定义见解

在 S AWS ecurity Hub CSPM 中，可以使用自定义见解来收集一组特定的调查结果并跟踪您的环境所特有的问题。有关自定义见解的背景信息，请参阅了解 Security Hub CSPM 中的自定义见解。

选择您喜欢的方法，然后按照以下步骤在 Security Hub CSPM 中创建自定义见解

Security Hub CSPM console

创建自定义见解（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 选择创建见解。
4. 要为见解选择分组属性，请执行以下操作：

   a. 选择搜索框以显示筛选选项。

b. 选择分组依据。

c. 选择要用于对与该见解关联的调查发现进行分组的属性。

d. 选择应用。

5. （可选）选择要用于此见解的任何其他筛选条件。为每个筛选条件定义筛选标准，然后选择应用。
6. 选择创建见解。
7. 输入见解名称，然后选择创建见解。

Security Hub CSPM API

创建自定义见解（API）

1. 要创建自定义见解，请使用 Security Hub CSPM API 的 CreateInsight 操作。如果您使用 AWS CLI，请运行该create-insight命令。
2. 为自定义见解输入 `Name` 参数名称。
3. 填充 `Filters` 参数以指定要在见解中包含哪些调查发现。
4. 填充 `GroupByAttribute` 参数以指定使用哪个属性对包含在见解中的调查发现进行分组。
5. 或者，填充 `SortCriteria` 参数以按特定字段对调查发现进行排序。

以下示例会创建一个自定义见解，其中包括具有 `AwsIamRole` 资源类型的重要调查发现。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

创建自定义见解 (PowerShell)

1. 使用 `New-SHUBInsight` cmdlet。
2. 为自定义见解输入 `Name` 参数名称。
3. 填充 `Filter` 参数以指定要在见解中包含哪些调查发现。
4. 填充 `GroupByAttribute` 参数以指定使用哪个属性对包含在见解中的调查发现进行分组。

如果您已启用跨区域聚合并使用聚合区域中的此 cmdlet，则该见解将应用于聚合和关联区域的匹配调查发现。

示例

```
$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
```

从托管见解创建自定义见解（仅限控制台）

您无法保存对托管见解的更改，也无法删除托管见解。但是，您可以将托管见解用作自定义见解的基础。这仅是 Security Hub CSPM 控制台中的一个选项。

从托管见解创建自定义见解（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 选择要使用的托管见解。
4. 根据需要编辑见解配置。
   - 要更改用于对见解中的调查发现进行分组的属性，请执行以下操作：
     a. 要删除现有分组，请选择分组设置旁边的 X。
     b. 选择搜索框。
     c. 选择要用于分组的属性。
     d. 选择应用。
   - 要从见解中删除筛选条件，请选择筛选条件旁边带圆圈的 X。
   - 要将筛选条件添加到见解，请执行以下操作：
     a. 选择搜索框。

b. 选择要用作筛选条件的属性和值。

c. 选择应用。

5. 更新完成后，请选择创建见解。
6. 在出现提示时，输入见解名称，然后选择创建见解。

编辑自定义见解

您可以编辑现有的自定义见解来更改分组值和筛选条件。进行更改后，您可以保存对原始见解的更新，或将更新后的版本另存为新见解。

在 S AWS ecurity Hub CSPM 中，可以使用自定义见解来收集一组特定的调查结果并跟踪您的环境所特有的问题。有关自定义见解的背景信息，请参阅了解 Security Hub CSPM 中的自定义见解。

要编辑自定义见解，请选择您的首选方法，然后按照说明操作。

Security Hub CSPM console

编辑自定义见解（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 选择要修改的自定义见解。
4. 根据需要编辑见解配置。
   - 要更改用于对见解中的调查发现进行分组的属性，请执行以下操作：
     a. 要删除现有分组，请选择分组设置旁边的 X。
     b. 选择搜索框。
     c. 选择要用于分组的属性。
     d. 选择应用。
   - 要从见解中删除筛选条件，请选择筛选条件旁边带圆圈的 X。
   - 要将筛选条件添加到见解，请执行以下操作：
     a. 选择搜索框。
     b. 选择要用作筛选条件的属性和值。
     c. 选择应用。

5. 完成更新后，请选择保存见解。
6. 在出现提示时，执行下列操作之一：
   - 要更新现有洞察以反映您的更改，请选择 “更新”，*<Insight_Name>*然后选择 “保存见解”。
   - 要使用更新创建新的见解，请选择保存新见解。输入见解名称，然后选择保存见解。

Security Hub CSPM API

编辑自定义见解（API）

1. 使用 Security Hub CSPM API 的 UpdateInsight 操作。如果你使用，请 AWS CLI 运行update-insight命令。
2. 要识别您要更新的自定义见解，请提供该见解的 Amazon 资源名称（ARN）。要获取自定义见解的 ARN，请使用 GetInsights 操作或 get-insights 命令。
3. 根据需要更新参数 Name、Filters 和 GroupByAttribute。

以下示例会更新指定的见解。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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

编辑自定义见解 (PowerShell)

1. 使用 Update-SHUBInsight cmdlet。
2. 要识别自定义见解，请提供见解的 Amazon 资源名称（ARN）。要获取自定义见解的 ARN，请使用 Get-SHUBInsight cmdlet。
3. 根据需要更新参数 Name、Filter 和 GroupByAttribute。

示例

```
$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"
```

删除自定义见解

在 S AWS ecurity Hub CSPM 中，可以使用自定义见解来收集一组特定的调查结果并跟踪您的环境所特有的问题。有关自定义见解的背景信息，请参阅了解 Security Hub CSPM 中的自定义见解。

要删除自定义见解，请选择您的首选方法，然后按照说明操作。您无法删除托管见解。

Security Hub CSPM console

删除自定义见解（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 找到要删除的自定义见解。
4. 对于该见解，请选择更多选项图标（卡右上角的三个点）。
5. 选择删除。

Security Hub CSPM API

删除自定义见解（API）

1. 使用 Security Hub CSPM API 的 `DeleteInsight` 操作。如果你使用，请 AWS CLI 运行delete-insight命令。

2. 要识别删除的自定义见解，请提供见解的 ARN。要获取自定义见解的 ARN，请使用 `GetInsights` 操作或 get-insights 命令。

以下示例会删除指定的见解。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

删除自定义见解 (PowerShell)

1. 使用 `Remove-SHUBInsight` cmdlet。
2. 要识别自定义见解，请提供该见解的 ARN。要获取自定义见解的 ARN，请使用 `Get-SHUBInsight` cmdlet。

示例

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

自动修改 Security Hub CSPM 中的调查发现并对其采取行动

AWS Security Hub CSPM 具有根据您的规格自动修改发现结果并对其采取措施的功能。

Security Hub CSPM 目前支持两种类型的自动化：

- 自动化规则：根据您定义的标准，近乎实时地自动更新和隐藏调查发现。
- 自动响应和补救 — 创建自定义 Amazon EventBridge 规则，定义针对特定发现和见解采取的自动操作。

当您想要自动更新 AWS 安全查找结果格式 (ASFF) 中的查找字段时，自动化规则会很有用。例如，您可以使用自动化规则更新来自特定第三方集成的发现的严重性级别或工作流状态。使用自动化规则，无需手动更新该第三方产品中每个调查发现的严重性级别或工作流状态。

EventBridge 当你想在 Security Hub CSPM 之外就特定发现采取措施或将特定发现发送给第三方工具进行补救或进行额外调查时，规则会很有用。这些规则可用于触发支持的操作，例如调用 AWS Lambda 函数或将特定发现通知亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题。

自动化规则在应用 EventBridge 规则之前生效。也就是说，在EventBridge 收到查找结果之前，会触发自动化规则并更新结果。 EventBridge 然后，规则适用于更新的调查结果。

在为安全控件设置自动化时，我们建议根据控件 ID 而不是标题或描述进行筛选。虽然 Security Hub CSPM 偶尔会更新控件标题和描述，但控制 IDs 保持不变。

主题

- 了解 Security Hub CSPM 中的自动化规则
- EventBridge 用于自动响应和补救

了解 Security Hub CSPM 中的自动化规则

您可以使用自动化规则自动更新 Security Hub CSP AWS M 中的搜索结果。提取调查发现时，Security Hub CSPM 可以应用各种规则操作，例如隐藏调查发现、更改其严重性以及添加注释。此类规则操作会修改符合您指定的条件的调查发现。

自动化规则用例的示例如下：

- 如果调查发现的资源 ID 指的是业务关键型资源，则将调查发现的严重性提升为 `CRITICAL`。
- 如果调查发现影响特定生产账户中的资源，则将调查发现的严重性从 `HIGH` 提升到 `CRITICAL`。
- 分配具有 `SUPPRESSED` 工作流状态 `INFORMATIONAL` 严重性的特定调查发现。

您只能通过 Security Hub CSPM 管理员账户创建和管理自动化规则。

规则适用于新的和更新后的调查发现。您可以从头开始创建自定义规则，也可以使用 Security Hub CSPM 提供的规则模板。您也可以从模板开始创建规则，然后根据需要对其进行修改。

定义规则条件和规则操作

通过 Security Hub CSPM 管理员账户，您可以通过定义一个或多个规则条件以及一个或多个规则操作来创建自动化规则。当调查发现与定义的条件相匹配时，Security Hub CSPM 会对其应用规则操作。有关可用条件和操作的更多信息，请参阅 可用的规则条件和规则操作。

对于每个管理员账户，Security Hub CSPM 目前最多支持 100 条自动化规则。

Security Hub CSPM 管理员账户还可以编辑、查看和删除自动化规则。规则适用于管理员账户及其所有成员账户中的匹配调查发现。通过提供成员帐户 IDs 作为规则标准，Security Hub CSPM 管理员还可以使用自动化规则来更新或隐藏特定成员帐户中的搜索结果。

自动化规则仅适用于其创建时 AWS 区域 所在的。要在多个区域中应用规则，管理员必须在每个区域中创建规则。这可以通过 Security Hub CSPM 控制台、Security Hub CSPM API 或 AWS CloudFormation 完成。您也可以使用多区域部署脚本。

可用的规则条件和规则操作

目前支持以下 AWS 安全查找格式 (ASFF) 字段作为自动化规则的标准：

规则标准	筛选条件运算符	字段类型
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串

规则标准	筛选条件运算符	字段类型
ComplianceStatus	Is, Is Not	选择：[FAILED、NOT_AVAILABLE 、PASSED、WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数字
CreatedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数字
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
FirstObservedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
LastObservedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）

规则标准	筛选条件运算符	字段类型
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
NoteUpdatedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串

规则标准	筛选条件运算符	字段类型
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串

规则标准	筛选条件运算符	字段类型
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceType	Is, Is Not	选择（请参阅 ASFF 支持的资源）
SeverityLabel	Is, Is Not	选择：[CRITICAL、HIGH、MEDIUM、LOW、I ONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	字符串
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	字符串
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	字符串
UpdatedAt	Start, End, DateRange	日期（格式为 2022-12-0 1T21:47:39.269Z）
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map

规则标准	筛选条件运算符	字段类型
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
WorkflowStatus	Is, Is Not	选择：[NEW、NOTIFIED、RESOLVED、SUPPRESSED]

对于标记为字符串字段的条件，在同一字段上使用不同的筛选运算符会影响评估逻辑。有关更多信息，请参阅《AWS Security Hub CSPM API 参考》中的 StringFilter。

每个标准都支持可用于筛选匹配调查发现的最大值数。有关每个标准的限制，请参阅《AWS Security Hub CSPM API 参考》中的 AutomationRulesFindingFilters。

目前支持以下 ASFF 字段作为自动化规则的操作：

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

有关特定 ASFF 字段的更多信息，请参阅 AWS 安全调查发现格式（ASFF）语法。

> **Tip**
>
> 如果您希望 Security Hub CSPM 停止为特定控件生成调查发现，我们建议您禁用该控件，而不是使用自动化规则。当您禁用某个控件时，Security Hub CSPM 会停止对其运行安全检查，并停止为其生成调查发现，因此您不会为该控件支付费用。对于符合定义条件的调查发现，

我们建议使用自动化规则来更改特定 ASFF 字段的值。有关禁用控件的详细信息，请参阅 在 Security Hub CSPM 中禁用控件。

自动化规则评估的调查发现

在您创建规则后，自动化规则会评估 Security Hub CSPM 通过 BatchImportFindings 操作生成或提取的新调查发现和更新的调查发现。Security Hub CSPM 每 12 至 24 小时或在关联资源状态发生变化时更新控件调查发现。有关更多信息，请参阅 有关运行安全检查的计划。

自动化规则会评估提供者提供的原始调查发现。提供者可以使用 Security Hub CSPM API 的 `BatchImportFindings` 操作来提供新的调查发现并更新现有调查发现。如果原始调查发现中不存在以下字段，Security Hub CSPM 会自动填充这些字段，然后在自动化规则的评估中使用填充的值：

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

创建了一个或多个自动化规则后，如果您使用 BatchUpdateFindings 操作更新调查发现字段，则不会触发这些规则。如果您创建的自动化规则和进行的 `BatchUpdateFindings` 更新都会影响同一个调查发现字段，则上次更新会设置该字段的值。请参见以下示例：

1. 您可以使用 `BatchUpdateFindings` 操作将调查发现 `Workflow.Status` 字段的值从 `NEW` 更改为 `NOTIFIED`。
2. 如果您调用了 `GetFindings`，则 `Workflow.Status` 字段现在的值为 `NOTIFIED`。
3. 您创建了一条自动化规则，该规则会将调查发现的 `Workflow.Status` 字段从 `NEW` 更改为 `SUPPRESSED`。（请记住，规则会忽略使用 `BatchUpdateFindings` 操作所做的更新。）
4. 调查发现提供者使用 `BatchImportFindings` 操作来更新调查发现，并将调查发现 `Workflow.Status` 字段的值更改为 `NEW`。
5. 如果您调用了 `GetFindings`，则 `Workflow.Status` 字段现在的值为 `SUPPRESSED`。这是因为应用了自动化规则，而该规则是针对调查发现采取的最后一个操作。

在 Security Hub CSPM 控制台中创建或编辑规则时，控制台会显示与规则条件匹配的调查发现的测试版。虽然自动化规则会评估调查发现提供者发送的原始调查发现，但控制台测试版会反映最终状态的调

查发现，就像它们在响应 GetFindings 操作时所显示的那样（即在对调查发现应用规则操作或其他更新之后）。

规则顺序的工作原理

创建自动化规则时，您可以为每条规则分配一个顺序。这决定了 Security Hub CSPM 应用您的自动化规则的顺序，当多个规则与同一个调查发现或调查发现字段相关时，这变得非常重要。

当多个规则操作与同一个调查发现或调查发现字段相关时，规则顺序数值最高的规则将应用于最后并产生最终效果。

在 Security Hub CSPM 控制台中创建规则时，Security Hub CSPM 会根据规则的创建顺序自动分配规则顺序。最近创建的规则具有最低的规则顺序数值，因此首先适用。Security Hub CSPM 按升序应用后续规则。

当你通过 Security Hub CSPM API 创建规则时 AWS CLI，Security Hub CSPM 会首先应用数值最低的规则。`RuleOrder`然后它按升序应用后续规则。如果多个调查发现具有相同的 `RuleOrder`，则 Security Hub CSPM 会先为 `UpdatedAt` 字段应用具有较早值的规则（也就是说，最近编辑的规则应用在最后）。

您可以随时修改规则顺序。

规则顺序示例：

规则 A（规则顺序为 **1**）：

- 规则 A 条件
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` 是 `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` 是 `NEW`
  - `Workflow.Status` = `ACTIVE`
- 规则 A 操作
  - `Confidence` 更新为 `95`
  - `Severity` 更新为 `CRITICAL`

规则 B（规则顺序为 **2**）：

- 规则 B 条件
  - `AwsAccountId = 123456789012`
- 规则 B 操作
  - `Severity` 更新为 `INFORMATIONAL`

规则 A 操作首先应用于符合规则 A 条件的 Security Hub CSPM 调查发现。接下来，规则 B 操作将应用于具有指定账户 ID 的 Security Hub CSPM 调查发现。在此示例中，由于规则 B 最后适用，因此调查发现中来自指定账户 ID 的 `Severity` 的最终值为 `INFORMATIONAL`。根据规则 A 操作，在匹配调查发现中 `Confidence` 的最终值为 `95`。

创建自动化规则

自动化规则可用于自动更新 Security Hub CSP AWS M 中的搜索结果。您可以从头开始创建自动化规则，也可以在 Security Hub CSPM 控制台中使用预先填充的规则模板。有关自动化规则的工作原理的背景信息，请参阅了解 Security Hub CSPM 中的自动化规则。

您一次只能创建一条自动化规则。要创建多个自动化规则，请多次遵循控制台过程，或者使用所需的参数多次调用 API 或命令。

您必须在您希望规则应用于调查发现的每个区域和账户中创建自动化规则。

当您在 Security Hub CSPM 控制台中创建自动化规则时，Security Hub CSPM 会显示您的规则所适用的调查发现测试版。如果您的规则条件包含 CONTAINS 或 NOT_CONTAINS 筛选条件，则当前不支持测试版。您可以为映射和字符串字段类型选择这些筛选条件。

> **Important**
>
> AWS 建议您不要在规则名称、描述或其他字段中包含个人身份、机密或敏感信息。

创建自定义自动化规则

选择您的首选方式，完成以下步骤以创建自定义自动化规则。

Console

创建自定义自动化规则（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/

2. 在导航窗格中，选择 自动化。
3. 选择 Create rule（创建规则）。对于规则类型，选择创建自定义规则。
4. 在规则部分，为您的规则提供唯一的规则名称和描述。
5. 对于条件，使用键、运算符和值下拉菜单来指定您的规则条件。您必须至少指定一项规则标准。

   如果您的选定条件支持，则控制台会显示符合您条件的调查发现测试版。
6. 对于自动操作，请使用下拉菜单，指定在调查发现符合规则条件时要更新的调查发现字段。您必须指定至少一个规则操作。
7. 对于规则状态，请选择在规则创建后将其设置为启用或是禁用。
8. （可选）展开附加设置部分。如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请选择忽略符合这些条件的调查发现后续规则。
9. （可选）对于标签，请以键-值对的形式添加标签以帮助您轻松识别规则。
10. 选择 Create rule（创建规则）。

API

创建自定义自动化规则（API）

1. 从 Security Hub CSPM 管理员账户运行 `CreateAutomationRule`。此 API 使用特定的 Amazon 资源名称（ARN）创建规则。
2. 提供规则的名称和描述。
3. 如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请将 `IsTerminal` 参数设置为 `true`。
4. 对于 `RuleOrder` 参数，请提供规则的顺序。Security Hub CSPM 首先对此参数应用数值较小的规则。
5. 对于 `RuleStatus` 参数，请指定是否希望 Security Hub CSPM 启用该规则，并在创建后开始将规则应用于调查发现。如果未指定值，则默认值为 `ENABLED`。值为 `DISABLED` 表示规则在创建后暂停。
6. 对于 `Criteria` 参数，请提供您希望 Security Hub CSPM 用来筛选调查发现的条件。规则操作将适用于符合条件的调查发现。有关支持的标准的列表，请参阅 可用的规则条件和规则操作。
7. 对于 `Actions` 参数，请提供您希望 Security Hub CSPM 在调查发现与您定义的条件相匹配时采取的操作。有关受支持操作的列表，请参阅 可用的规则条件和规则操作。

以下示例 AWS CLI 命令创建了一条自动化规则，用于更新工作流程状态和匹配结果的注释。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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
```

使用模版创建自动化规则（仅限控制台）

规则模板反映了自动化规则的常见用例。目前，只有 Security Hub CSPM 控制台支持规则模板。完成以下步骤以在控制台中的模板创建自动化规则。

使用模板创建自动化规则（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 自动化。
3. 选择 Create rule（创建规则）。在规则类型中，选择从模板创建规则。

4. 从下拉菜单中选择规则模板。
5. （可选）如果您的用例有需要，请修改规则、条件和自动操作部分。您必须指定至少一个规则条件和一个规则操作。

   如果您的选定条件支持，则控制台会显示符合您条件的调查发现测试版。
6. 对于规则状态，请选择在规则创建后将其设置为启用或是禁用。
7. （可选）展开附加设置部分。如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请选择忽略符合这些条件的调查发现后续规则。
8. （可选）对于标签，请以键-值对的形式添加标签以帮助您轻松识别规则。
9. 选择 Create rule（创建规则）。

查看自动化规则

自动化规则可用于自动更新 Security Hub CSP AWS M 中的搜索结果。有关自动化规则的工作原理的背景信息，请参阅[了解 Security Hub CSPM 中的自动化规则]。

选择您的首选方法，然后按照步骤查看您的现有自动化规则和每条规则的详细信息。

要查看自动化规则改变您的调查发现的历史记录，请参阅 [在 Security Hub CSPM 中查看调查发现详细信息和历史记录]。

Console

查看自动化规则（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 自动化。
3. 选择规则名称。或者，选择一条规则。
4. 选择操作和视图。

API

查看自动化规则（API）

1. 要查看您的账户的自动化规则，请从 Security Hub CSPM 管理员账户运行 `ListAutomationRules`。此 API 会返回规则 ARNs 和其他规则的元数据。此 API 不需

要输入参数，但您可以选择提供 MaxResults 以限制结果数量和 NextToken 作为分页参数。NextToken 的初始值应为 NULL。

2. 有关其他规则详细信息，包括规则的条件和操作，请从 Security Hub CSPM 管理员账户运行 BatchGetAutomationRules。提供您想要详细了解的自动化规则。 ARNs

   以下示例将检索指定自动化规则的详细信息。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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
```

编辑自动化规则

自动化规则可用于自动更新 Security Hub CSP AWS M 中的搜索结果。有关自动化规则的工作原理的背景信息，请参阅了解 Security Hub CSPM 中的自动化规则。

创建自动化规则后，委派的 Security Hub CSPM 管理员可以编辑该规则。当您编辑自动化规则时，更改将应用于规则编辑后 Security Hub CSPM 生成或提取的新增或更新后的调查发现。

选择您的首选方式，按照步骤编辑自动化规则的内容。您只需一个请求即可编辑一条或多条规则。有关编辑规则顺序的说明，请参阅 编辑自动化规则顺序。

Console

编辑自动化规则（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 自动化。
3. 选择您要编辑的规则。选择操作和编辑。
4. 根据需要更改规则，然后选择保存更改。

API

编辑自动化规则（API）

1. 从 Security Hub CSPM 管理员账户运行 BatchUpdateAutomationRules。
2. 对于 RuleArn 参数，请提供要编辑的规则的 ARN。
3. 为要编辑的参数提供新值。除 RuleArn 之外，您可以编辑任何参数。

以下示例将更新指定自动化规则。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\ ) 行继续符来提高可读性。

```
$ 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
```

编辑自动化规则顺序

自动化规则可用于自动更新 Security Hub CSP AWS M 中的搜索结果。有关自动化规则的工作原理的背景信息，请参阅了解 Security Hub CSPM 中的自动化规则。

创建自动化规则后，委派的 Security Hub CSPM 管理员可以编辑该规则。

如果您希望保持规则条件和操作不变，但要更改 Security Hub CSPM 应用自动化规则的顺序，可以编辑规则顺序。选择您喜欢的方法，然后按照步骤编辑规则顺序。

有关编辑自动化规则的条件或操作的说明，请参阅编辑自动化规则。

Console

编辑自动化规则顺序（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 自动化。
3. 选择要更改其顺序的规则。选择编辑优先级。
4. 选择向上移动可将规则的优先级提高一个单位。选择下移可将规则优先级降低一个单位。选择移至顶部，将规则的顺序分配为 1（这使规则优先于其他现有规则）。

> **Note**
>
> 在 Security Hub CSPM 控制台中创建规则时，Security Hub CSPM 会根据规则的创建顺序自动分配规则顺序。最近创建的规则具有最低的规则顺序数值，因此首先适用。

API

编辑自动化规则顺序（API）

1. 从 Security Hub CSPM 管理员账户使用 `BatchUpdateAutomationRules` 操作。
2. 对于 `RuleArn` 参数，请提供要编辑其顺序的规则的 ARN。
3. 修改 `RuleOrder` 字段的值。

> **Note**
>
> 如果多个规则具有相同的 `RuleOrder`，Security Hub CSPM 会先为 `UpdatedAt` 字段应用具有较早值的规则（也就是说，最后应用最近编辑的规则）。

删除或禁用自动化规则

自动化规则可用于自动更新 Security Hub CSP AWS M 中的搜索结果。有关自动化规则的工作原理的背景信息，请参阅了解 Security Hub CSPM 中的自动化规则。

当您删除自动化规则时，Security Hub CSPM 会将其从您的账户中移除，并且不再将该规则应用于调查发现。除了删除之外，您还可以禁用规则。这会保留该规则以备将来使用，但是在您启用该规则之前，Security Hub CSPM 不会将该规则应用于任何匹配的调查发现。

选择您的首选方法，然后按照步骤删除自动化规则。您可以在单个请求中删除一个或多个规则。

Console

删除或禁用自动化规则（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 自动化。
3. 选择您要删除的规则。选择操作和删除（要保留规则，但暂时将其禁用，请选择禁用）。
4. 确认您的选择，然后选择删除。

API

删除或禁用自动化规则（API）

1. 从 Security Hub CSPM 管理员账户使用 `BatchDeleteAutomationRules` 操作。
2. 对于 `AutomationRulesArns` 参数，请提供要删除的规则的 ARN（要保留规则，但暂时将其禁用，请提供 `RuleStatus` 参数的 `DISABLED`）。

以下示例将删除指定自动化规则。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ 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
```

自动化规则示例

本部分提供了常见 Security Hub CSPM 使用案例的自动化规则示例。这些示例对应于 Security Hub CSPM 控制台上提供的规则模板。

当特定资源（例如 S3 存储桶）面临风险时，将严重性提升为“严重”

在本示例中，当 `ResourceId` 在调查发现中的对象是特定的 Amazon Simple Storage Service（Amazon S3）存储桶时，匹配规则条件。规则操作是将匹配调查发现的严重性更改为 `CRITICAL`。您可以修改此模板以应用于其他资源。

API 请求示例：

```
{
    "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"
            }
        }
    }]
}
```

示例 CLI 命令：

```
$
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
```

提高与生产账户中资源相关调查发现的严重性

在此示例中，当在特定的生产账户中生成 HIGH 严重级别的调查发现时，匹配规则条件。规则操作是将匹配调查发现的严重性更改为 CRITICAL。

API 请求示例：

```
{
    "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"
            }
        }
    }]
}
```

示例 CLI 命令：

```
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
```

隐藏信息性调查发现

在此示例中，与从亚马逊发送到 Security Hub CSPM 的INFORMATIONAL严重性调查结果的规则标准相匹配。 GuardDuty规则操作是将匹配调查发现的工作流状态更改为 SUPPRESSED。

API 请求示例：

```
{
    "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"
            }
        }
    }]
}
```

示例 CLI 命令：

```
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
```

EventBridge 用于自动响应和补救

通过在亚马逊中创建规则 EventBridge，您可以自动响应 Sec AWS urity Hub CSPM 的调查结果。Security Hub CSPM 近乎实时地将发现结果作为事件发送给。 EventBridge 您可以编写简单的规则来指示您对哪些事件感兴趣，以及当事件与规则匹配时要采取哪些自动操作。可自动触发的操作包括：

- 调用函数 AWS Lambda
- 调用 Amazon EC2 运行命令
- 将事件中继到 Amazon Kinesis Data Streams
- 激活 AWS Step Functions 状态机
- 通知 Amazon SNS 主题或 Amazon SQS 队列
- 将结果发送到第三方票证、聊天、SIEM 或事件响应和管理工具

Security Hub CSPM 会自动将所有新发现和现有发现的所有更新 EventBridge 作为 EventBridge 事件发送到。您还可以创建自定义操作，允许您将选定的调查结果和见解结果发送到 EventBridge。

然后，您可以配置 EventBridge 规则以响应每种类型的事件。

有关使用的更多信息 EventBridge，请参阅 Amazon EventBridge 用户指南。

> **Note**
>
> 作为最佳实践，请确保授予用户的访问权限 EventBridge 使用仅授予所需权限的最低权限 AWS Identity and Access Management (IAM) 策略。
> 有关更多信息，请参阅 Amazon 中的身份和访问管理 EventBridge。

AWS 解决方案中还提供了一组用于跨账户自动响应和补救的模板。这些模板利用了 EventBridge 事件规则和 Lambda 函数。您可以使用 CloudFormation 和部署解决方案 AWS Systems Manager。该解决方案可以创建完全自动化的响应和补救措施操作。它还可以使用 Security Hub CSPM 自定义操作来创建用户触发的响应和修复操作。有关如何配置和使用解决方案的详细信息，请参阅 AWS解决方案页面上的自动安全响应。

主题

- 中的 Security Hub CSPM 事件类型 EventBridge
- EventBridge Security Hub CSPM 的事件格式
- 为 Security Hub CSPM 发现配置 EventBridge 规则
- 使用自定义操作将调查结果和见解结果发送到 EventBridge

中的 Security Hub CSPM 事件类型 EventBridge

Security Hub CSPM 使用以下亚马逊 EventBridge 事件类型进行集成。 EventBridge

在 Security Hub CSPM 的 EventBridge 控制面板上，“所有事件” 包括所有这些事件类型。

所有调查发现（Security Hub Findings - Imported）

Security Hub CSPM 会自动将所有新发现和现有发现的所有更新 EventBridge 作为Security Hub Findings - Imported事件发送到。每个 Security Hub Findings - Imported 事件都包含一个调查发现。

每个 `BatchImportFindings` 和 `BatchUpdateFindings` 请求都会触发一个 Security Hub Findings - Imported 事件。

对于管理员账户，中的事件源 EventBridge 包括来自其账户和成员账户的调查结果的事件。

在聚合区域中，事件源包括来自聚合区域和关联区域的调查发现的事件。跨区域调查发现几乎实时地包含在事件源中。有关如何配置调查发现聚合的信息，请参阅 the section called “跨区域聚合数据”。

您可以在中定义规则 EventBridge ，自动将发现结果传送到修复工作流程、第三方工具或其他支持的 EventBridge 目标。这些规则可以包括筛选条件，使仅在调查发现具有特定属性值时才应用规则。

您可以使用此方法自动将所有调查发现或具有特定特征的所有调查发现发送到响应或补救工作流。

请参阅the section called “配置 EventBridge 规则”。

自定义操作的调查发现（Security Hub Findings - Custom Action）

Security Hub CSPM 还会将与自定义操作相关的结果 EventBridge 作为Security Hub Findings - Custom Action事件发送给事件。

这对于使用 Security Hub CSPM 控制台且想要将特定调查发现或一小组调查发现发送到响应或修复工作流的分析师非常有用。您可以每次为最多 20 个调查发现选择自定义操作。每个发现都 EventBridge 作为一个单独 EventBridge 的事件发送到。

创建自定义操作时，您可以为其分配一个自定义操作 ID。您可以使用此 ID 来创建 EventBridge 规则，该规则在收到与该自定义操作 ID 关联的发现后采取指定操作。

请参阅the section called “配置和使用自定义操作”。

例如，您可以在 Security Hub CSPM 中创建名为 `send_to_ticketing` 的自定义操作。然后在中 EventBridge，您创建一条规则，该规则在 EventBridge 收到包含`send_to_ticketing`自定义操作 ID 的调查结果时触发。该规则包括将调查发现发送到票证系统的逻辑。然后，您可以在 Security Hub CSPM 中选择调查发现，并在 Security Hub CSPM 中使用自定义操作将调查发现手动发送到票证系统。

有关如何将 Security Hub CSPM 调查结果发送给进一步处理的示例，请参阅 AWS 合作伙伴网络 (APN) 博客上的 “如何将 Sec AWS urity Hub CSPM 自定义操作与 Security Hub CSPM 集成 PagerDuty以及如何在 Sec AWS urity Hub CSPM 中启用自定义操作”。 EventBridge

自定义操作的见解结果（Security Hub Insight Results）

您还可以使用自定义操作将一组见解结果 EventBridge 作为Security Hub Insight Results事件发送到。见解结果是与见解相匹配的资源。请注意，当您将洞察结果发送到时 EventBridge，您不会将调查结果发送给 EventBridge。您仅发送与见解结果关联的资源标识符。您每次最多可以发送 100 个资源标识符。

与查找结果的自定义操作类似，您首先要在 Security Hub CSPM 中创建自定义操作，然后在中创建规则。 EventBridge

请参阅the section called “配置和使用自定义操作”。

例如，假设您看到了一个您感兴趣的特定见解结果，想与同事分享。在这种情况下，您可以使用自定义操作通过聊天或票务系统将见解结果发送给同事。

EventBridge Security Hub CSPM 的事件格式

Security Hub Findings - Imported、Security Findings - Custom Action 和 Security Hub Insight Results 事件类型使用以下事件格式。

事件格式是 Security Hub CSPM 向发送事件时使用的格式。 EventBridge

Security Hub Findings - Imported

Security Hub Findings - Imported从 Security Hub CSPM 发送的事件 EventBridge 使用以下格式。

```
{
   "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> 是事件发送的调查发现的内容，采用 JSON 格式。每个事件都会发送一项调查发现。

有关调查发现属性的完整列表，请参阅 AWS 安全调查结果格式 (ASFF)。

有关如何配置由这些事件触发的 EventBridge 规则的信息，请参阅the section called “配置 EventBridge 规则”。

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action从 Security Hub CSPM 发送的事件 EventBridge 使用以下格式。每项调查发现均在单独的事件中发送。

```
{
  "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> 是事件发送的调查发现的内容，采用 JSON 格式。每个事件都会发送一项调查发现。

有关调查发现属性的完整列表，请参阅 AWS 安全调查结果格式 (ASFF)。

有关如何配置由这些事件触发的 EventBridge 规则的信息，请参阅the section called “配置和使用自定义操作”。

Security Hub Insight Results

Security Hub Insight Results从 Security Hub CSPM 发送的事件 EventBridge 使用以下格式。

```
{
  "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}
    ]
  }
}
```

有关如何创建由这些事件触发的 EventBridge 规则的信息，请参阅the section called “配置和使用自定义操作”。

为 Security Hub CSPM 发现配置 EventBridge 规则

您可以在 Amazon 中创建规则 EventBridge ，定义在收到Security Hub Findings - Imported事件时要采取的操作。 Security Hub Findings - Imported事件由`BatchImportFindings`和`BatchUpdateFindings`操作的更新触发。

每条规则都包含一个事件模式，用于标识触发规则的事件。事件模式始终包含事件源（`aws.securityhub`）和事件类型（Security Hub 调查发现 - 已导入）。事件模式还可以指定筛选条件来识别规则适用的调查发现。

然后，该事件规则用于确定规则目标。目标是在 EventBridge 收到 Sec urity Hub Findings-Imported 事件并且发现结果与筛选器匹配时要采取的操作。

此处提供的说明使用 EventBridge 控制台。当您使用控制台时， EventBridge会自动创建所需的基于资源的策略， EventBridge 以允许写入 Amazon CloudWatch Logs。

您也可以使用 EventBridge API 的`PutRule`操作。但是，如果您使用 EventBridge API，则必须创建基于资源的策略。有关所需策略的信息，请参阅 Amazon EventBridge 用户指南中的CloudWatch 日志权限。

事件模式的格式

Security Hub 调查发现 - 已导入事件的事件模式格式如下：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` 将 Security Hub CSPM 标识为生成事件的服务。
- `detail-type` 标识事件的类型。
- `detail` 是可选的，它提供了事件模式的筛选条件值。如果事件模式不包含 `detail` 字段，则所有调查发现都会触发规则。

您可以根据任何调查发现属性筛选调查发现。您可以为每个属性提供一个或多个值的逗号分隔的数组。

```
"<attribute name>": [ "<value1>", "<value2>"]
```

如果您为一个属性提供多个值，则这些值将通过 OR 连接在一起。如果调查发现包含任何列出的值，则该调查发现与单个属性的筛选条件相匹配。例如，如果您同时提供 `INFORMATIONAL` 和 `LOW` 作为 `Severity.Label` 的值，则如果调查发现的严重性标签为 `INFORMATIONAL` 或 `LOW`，则调查发现将匹配。

属性的连接方式为 AND。如果调查发现与所有提供的属性的筛选条件相匹配，则该调查发现与之匹配。

提供属性值时，它必须反映该属性在 AWS 安全调查结果格式 (ASFF) 结构中的位置。

> **Tip**
>
> 筛选控件调查发现时，我们建议使用 `SecurityControlId` 或 `SecurityControlArn` ASFF 字段作为筛选条件，而不是 `Title` 或 `Description`。后面的字段偶尔会发生变化，而控件 ID 和 ARN 是静态标识符。

在以下示例中，事件模式为 ProductArn 和 Severity.Label 提供了筛选值，因此，如调查发现由 Amazon Inspector 生成，并且其严重性标签为 INFORMATIONAL 或 LOW，则调查发现与之匹配。

```
{
    "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"]
            }
        }
    }
}
```

创建事件规则

您可以使用预定义的事件模式或自定义的事件模式在中创建规则 EventBridge。如果您选择预定义的图案，则 EventBridge 会自动填充source和detail-type。 EventBridge 还提供了用于为以下查找结果属性指定筛选值的字段：

- AwsAccountId
- Compliance.Status
- Criticality
- ProductArn
- RecordState
- ResourceId
- ResourceType
- Severity.Label
- Types
- Workflow.Status

创建 EventBridge 规则（控制台）

1. 打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 使用以下值创建监控查找事件的 EventBridge 规则：

   - 对于规则类型，选择具有事件模式的规则。
   - 选择如何构建事件模式。

使用...构建事件模式	请执行此操作...
一个模板	在事件模式部分中，选择以下选项： • 对于事件源，选择AWS 服务。 • 对于AWS 服务，选择 Security Hub。 • 对于事件类型，选择 Security Hub 调查发现 - 已导入。 • （可选）要使规则更具体，请添加筛选条件值。例如，要将规则限制为具有活动记录状态的调查发现，请在特定记录状态下选择活动。
自定义事件模式 （如果要根据 EventBridge 控制台中未显示的属性筛选结果，请使用自定义模式。）	• 在事件模式部分中，选择自定义模式（JSON 编辑器），然后将以下事件模式粘贴到文本区域中： `{ "source": [ "aws.securityhub" ], "detail-type": [`

使用...构建事件模式	请执行此操作...
	<pre>"Security Hub Findings - Imported"], "detail": { "findings": { "<attribute name>": ["<value1>", "<value2>"] } } }</pre> • 更新事件模式以包含要用作筛选器的属性和属性值。 例如，要将规则应用于验证状态为 TRUE_POSITIVE 的调查发现，请使用以下模式示例： <pre>{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } }</pre>

使用...构建事件模式	请执行此操作...
	}

- 对于目标类型，选择AWS 服务，在选择目标中，选择目标，例如 Amazon SNS 主题或 AWS Lambda 函数。在收到与规则中定义的事件模式匹配的事件时将触发目标。

有关创建规则的详细信息，请参阅《亚马逊 EventBridge 用户指南 EventBridge》中的创建对事件做出反应的 Amazon 规则。

使用自定义操作将调查结果和见解结果发送到 EventBridge

要使用 Sec AWS urity Hub CSPM 自定义操作向亚马逊发送调查结果或洞察结果 EventBridge，请先在 Security Hub CSPM 中创建自定义操作。然后，您可以在中 EventBridge 定义适用于您的自定义操作的规则。

您最多可以创建 50 个自定义操作。

如果您启用跨区域聚合并在聚合区域中管理调查发现，则需要在聚合区域中创建自定义操作。

中的规则 EventBridge 使用自定义操作中的 Amazon 资源名称 (ARN)。

创建自定义操作

在 Sec AWS urity Hub CSPM 中创建自定义操作时，需要指定其名称、描述和唯一标识符。

自定义操作指定当 EventBridge 事件与 EventBridge 规则匹配时要采取的操作。Security Hub CSPM 将每项发现都 EventBridge 作为事件发送到。

选择您的首选方式，然后按照以下步骤创建自定义操作。

Console

在 Security Hub CSPM 中创建自定义操作（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择设置，然后选择自定义操作。
3. 选择创建自定义操作。
4. 为操作提供名称、描述和自定义操作 ID。

名称的长度必须少于 20 个字符。

每个 AWS 账户的自定义操作 ID 必须是唯一的。

5. 选择创建自定义操作。
6. 记下自定义操作 ARN。在 EventBridge 中创建与该操作关联的规则时，您需要使用 ARN。

API

创建自定义操作（API）

使用 CreateActionTarget 操作。如果您使用的是 AWS CLI，请运行create-action-target命令。

以下示例会创建一个自定义操作，将调查发现发送到修复工具。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠（\）行继续符来提高可读性。

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

在中定义规则 EventBridge

要在 Amazon 中触发自定义操作 EventBridge，您必须在中创建相应的规则 EventBridge。规则定义包括自定义操作的 Amazon 资源名称（ARN）。

Security Hub 调查发现 - 自定义操作事件的事件模式采用以下格式：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub 见解结果事件的事件模式采用以下格式：

```
{
  "source": [
```

```
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

在这两种模式中，*<custom action ARN>* 都是自定义操作的 ARN。您可以配置适用于多个自定义操作的规则。

此处提供的说明适用于 EventBridge 控制台。使用控制台时， EventBridge 会自动创建所需的基于资源的策略， EventBridge 以允许写入 CloudWatch 日志。

您也可以使用 PutRuleAPI 的 AP EventBridge I 操作。但是，如果您使用 EventBridge API，则必须创建基于资源的策略。有关所需策略的详细信息，请参阅 Amazon EventBridge 用户指南中的CloudWatch 日志权限。

在 EventBridge （ EventBridge 控制台）中定义规则

1. 打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。
5. 对于事件总线，请选择要与此规则关联的事件总线。如果您希望此规则对来自您自己的账户的匹配事件触发，请选择默认。当您账户中的某个 AWS 服务发出一个事件时，它始终会发送到您账户的默认事件总线。
6. 对于规则类型，选择具有事件模式的规则。
7. 选择下一步。
8. 对于事件源，选择 AWS 事件。
9. 对于事件模式，选择事件模式表。
10. 对于事件源，选择AWS 服务。
11. 要获得AWS 服务，请选择 Security Hub。
12. 对于事件类型，执行以下操作之一：

    - 要创建在将调查发现发送到自定义操作时要应用的规则，请选择 Security Hub 调查发现 - 自定义操作。

- 要创建在向自定义操作发送见解结果时要应用的规则，请选择 Security Hub 见解结果。

13. 选择特定自定义操作 ARNs，添加自定义操作 ARN。

    如果该规则适用于多个自定义操作，请选择 “添加” 以添加更多自定义操作 ARNs。

14. 选择下一步。
15. 在选择目标下，选择并配置匹配此规则时要调用的目标。
16. 选择下一步。
17. （可选）为规则输入一个或多个标签。有关更多信息，请参阅《亚马逊 EventBridge 用户指南》中的亚马逊 EventBridge 标签。
18. 选择下一步。
19. 查看规则详细信息并选择创建规则。

    当您对账户中的发现或洞察结果执行自定义操作时，将在中生成事件 EventBridge。

为调查发现和见解结果选择自定义操作

创建 Sec AWS urity Hub CSPM 自定义操作和 Amazon EventBridge 规则后，您可以将调查结果和见解结果发送到以 EventBridge 进行自动管理和处理。

EventBridge 只有在查看事件的账户中才会发送到事件。如果您使用管理员帐户查看调查结果，则该事件将 EventBridge 以管理员帐户发送到。

要 AWS 使 API 调用生效，目标代码的实现必须将角色切换到成员账户。这也意味着您切换到的角色必须部署到需要采取行动的每个成员。

将调查结果发送到 EventBridge（控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 显示调查发现列表：

   - 在调查发现中，您可以查看所有已启用的产品集成和控件的调查发现。
   - 在安全标准中，您可以导航到通过特定控件生成的调查发现列表。有关更多信息，请参阅 查看 Security Hub CSPM 中的控件的详细信息。
   - 从集成中，您可以导航到已启用的集成生成的调查发现列表。有关更多信息，请参阅 查看来自 Security Hub CSPM 集成的调查发现。
   - 从见解中，您可以导航到见解结果的调查发现列表。有关更多信息，请参阅 查看 Security Hub CSPM 中的见解并对其采取行动。

3. 选择要发送到的调查结果 EventBridge。您一次最多可选择 20 个调查发现。
4. 在操作中，选择与要应用的 EventBridge 规则一致的自定义操作。

   Security Hub CSPM 会为每个调查发现单独发送一个 Security Hub 调查发现 - 自定义操作事件。

将分析结果发送到 EventBridge （控制台）

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择 Insights。
3. 在 Insights 页面上，选择包含要发送到的结果的见解 EventBridge。
4. 选择要发送到的洞察结果 EventBridge。您一次最多可以选择 20 个结果。
5. 在操作中，选择与要应用的 EventBridge 规则一致的自定义操作。

使用 Security Hub CSPM 中的控制面板

在 Security Hub CSPM 控制台上，摘要控制面板显示您的风险、攻击序列和安全覆盖范围的摘要。此控制面板可帮助您根据不同安全功能的严重性和账户覆盖范围识别风险和攻击序列。每次打开控制面板时，它都会自动刷新。但请注意，安全分数和控件状态每 24 小时刷新一次。

您可以通过在摘要控制面板中添加和删除不同的安全小组件来对其进行自定义。您也可以指定筛选条件来检索和显示特定类型的数据。如果自定义控制面板，Security Hub 会保存您的自定义设置。如果您的账户的其他用户自定义了控制面板，则其更改将独立于您的自定义设置进行保存。

如果您在 Security Hub CSPM 中配置了跨区域聚合，则摘要控制面板会显示聚合数据。如果您的账户是某组织的委派管理员账户，则数据包括您的账户和成员帐户的调查发现。如果您的账户是成员账户或独立账户，则数据仅包含您的账户的调查发现。

主题

- 摘要控制面板的可用小组件
- 在 Security Hub CSPM 中筛选摘要控制面板
- 在 Security Hub CSPM 中自定义摘要控制面板

摘要控制面板的可用小组件

摘要仪表板包括反映现代云安全威胁形势的小部件，以 AWS 客户的安全运营和体验为指导。有些小组件是默认显示的，而另一些则不是。您可以通过添加或删除小组件来自定义控制面板视图。

要添加小组件，请选择控制面板顶部的添加小组件。然后，您可以浏览可用小组件列表，也可以在搜索栏中输入小组件的标题。找到要添加的小组件后，请将其拖动到希望它在控制面板上显示的位置。有关更多信息，请参阅 自定义 控制面板。

默认显示的小组件

默认情况下，摘要控制面板包含以下小组件。

主要威胁序列

显示严重性最高的威胁序列。威胁序列发现（在 Amazon 中称为攻击序列发现）将多个事件关联起来 GuardDuty，以识别您的 AWS 环境面临的潜在威胁。威胁序列可能包括您的环境中正在进行或最近发生的攻击行为（在 24 小时时间范围内），这反过来可能导致进一步危害。您必须启用 GuardDuty 并启用 GuardDuty S3 防护才能在 Security Hub CSPM 中接收威胁序列发现。

主要风险

显示您的环境中的主要风险摘要。小组件顶部显示每个严重性级别的风险计数。您可以选择一个严重性级别来前往风险页面，并将风险筛选到所选严重性级别。在您的环境中发生频率最高的风险会首先显示。此小组件可帮助您优先处理要缓解的风险。

安全覆盖范围

根据覆盖范围控件调查发现，总结您的安全覆盖范围。覆盖范围控制检查是否启用了特定 AWS 服务 及其功能（例如，[Macie.1] 应启用 Amazon Macie）。此小组件可帮助您拥有覆盖范围控件的 PASSED 调查发现。Security Hub CSPM 控制台通过此小组件提供链接，帮助您启用缺失的安全功能。我们建议使用集中配置来启用多个 AWS 账户 和中缺少的安全功能 AWS 区域。有关更多信息，请参阅 了解 Security Hub CSPM 中的中心配置。

安全标准

显示您最新的摘要安全分数以及每项 Security Hub CSPM 标准的安全分数。安全分数（介于 0-100% 之间）表示已通过控件与所有已启用控件的比例。有关这些资源的更多信息，请参阅计算安全分数的方法。此小组件可帮助您了解自己的整体安全状况。

具有最多调查发现的资产

概述具有最多调查发现的资源、账户和应用程序。该列表按调查发现的数量降序排序。在小组件中，按严重性和资源类型分组，每个选项卡显示该类别中排名前六的项目。如果您在调查发现总数列中选择一个数字，Security Hub CSPM 会打开一个页面显示资产的调查发现。此小组件可帮助您快速识别哪些核心资产存在潜在的安全威胁。

按地区划分的调查发现

按严重性分组，显示每个启用了 Security Hub CSPM 的 AWS 区域 中的调查发现总数。此小组件可帮助您识别可能影响特定区域的安全问题。如果您在聚合区域中打开控制面板，则此小组件可帮助您监控每个关联区域中的潜在安全问题。

最常见的威胁类型

详细列出您的 AWS 环境中最常见的 10 种威胁类型。包括权限升级、使用公开的凭证或与恶意 IP 地址通信等威胁。

要查看这些数据， GuardDuty必须启用 Amazon。如果是，请在此小组件中选择一种威胁类型以打开 GuardDuty 控制台并查看与此威胁相关的发现。此小组件可帮助您评估其他安全问题背景下的潜在威胁。

已被利用的软件漏洞

提供您的 AWS 环境中存在且已知漏洞利用的软件漏洞的摘要。您还可以查看有可用修复程序和没有可用修复程序的漏洞明细。

要查看这些数据，必须启用 Amazon Inspector。如果已启用，请在此小组件中选择一项统计数据，打开 Amazon Inspector 控制台并查看有关该漏洞的更多详细信息。此小组件可帮助您在其他安全问题背景下评估软件漏洞。

随着时间推移而出现的新调查发现

显示过去 90 天内每日新调查发现数量的趋势。您可以按严重性或按提供程序对数据进行细分，以获取更多背景信息。此小组件可帮助您了解在过去 90 天中的特定时间内，调查发现数量是激增还是下降。

具有最多调查发现的资源

提供生成最多发现结果的资源摘要，按以下资源类型细分：亚马逊简单存储服务 (Amazon S3) Service 存储桶、亚马逊弹性计算云 (Amazon EC2) Elastic Compute Cloud (Amazon EC2) 实例和函数。 AWS Lambda

在小组件中，每个选项卡都侧重于上述某个资源类型，列出了调查发现最多的 10 个资源实例。要查看特定资源的调查发现，请选择该资源实例。此小组件可帮助您对与公共 AWS 资源相关的安全发现进行分类。

默认隐藏的小组件

以下小组件也可用于摘要控制面板，但默认情况下处于隐藏状态。

具有最多调查发现的 AMI

提供生成调查发现最多的 10 个亚马逊机器映像（AMI）的列表。仅当您的账户启用了 Amazon EC2 时，此数据才可用。它可以帮助您识别哪些 AMI 会带来潜在的安全风险。

调查发现最多的 IAM 主体

提供生成调查结果最多的 10 个 AWS Identity and Access Management (IAM) 用户的列表。此小组件可帮助您执行管理和计费任务。它会显示那些使用 Security Hub CSPM 最多的用户。

调查发现最多的账户（按严重性分类）

显示生成调查发现最多的 10 个账户的图表，并按严重性分组。此小组件可帮助您确定要重点分析和修复哪些账户。

调查发现最多的账户（按资源类型分类）

显示生成调查发现最多的 10 个账户的图表，并按资源类型分组。此小组件可帮助您确定要优先分析和修复哪些账户和资源类型。

见解

列出五个 Security Hub CSPM 托管见解及其生成的调查发现数量。见解力确定了需要关注的特定安全领域。

AWS 集成的最新发现

显示您在 Security Hub CSPM 中从集成 AWS 服务 中收到的调查发现数量。它还会显示您最近一次从每项集成服务中收到调查发现的时间。此小组件提供来自多个的合并结果数据 AWS 服务。要深入了解，请选择集成服务。然后，Security Hub CSPM 会打开该服务的控制台。

在 Security Hub CSPM 中筛选摘要控制面板

您可以整理 Security Hub CSPM 控制台的摘要控制面板，使其仅包含与自己最相关的安全数据。例如，如果您是某个应用程序团队的成员，则可以为生产环境中的关键应用程序创建专用视图。如果您是某个安全团队的成员，则可以创建一个专用视图，帮助自己专注于高严重性的调查发现。

要创建这些精选视图，请在控制面板上方的筛选框中输入筛选条件。如果应用了筛选条件，则该条件会应用于控制面板上的所有数据和小组件，但见解和安全标准小组件中的数据除外。有关控制面板上可用的小组件列表，请参阅摘要控制面板的可用小组件。

您可以使用以下字段筛选数据。

- 帐户名称
- 账户 ID
- 应用程序 ARN
- 应用程序名称
- 产品名称（适用于将调查结果发送到 S AWS 服务 ecurity Hub CSPM 的第三方产品）
- Record state
- Region
- 资源标签
- 严重性
- 工作流状态

默认情况下，使用以下条件筛选控制面板数据：`Workflow.Status` 为 `NOTIFIED` 或 `NEW`、以及 `RecordState` 为 `ACTIVE`。这些条件显示在控制面板上方，筛选框下方。要删除这些条件，请在要删除的条件筛选令牌中选择 X。

如果您应用了想再次使用的筛选条件，则可以将其另存为筛选器集。筛选器集是一组筛选标准，您可以创建并保存这些筛选标准，以便您在摘要控制面板上查看数据时重新应用。您可以创建并保存一个筛选条件集，该筛选条件集可以使用除以下字段之外的任何可用字段：应用程序 ARN、应用程序名称和资源标签。

创建和保存筛选器集

要创建和保存筛选器集，请执行下列步骤。

要创建和保存筛选器集

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择摘要。
3. 在摘要控制面板上方的筛选框中，为筛选器集输入筛选条件。
4. 在清除筛选条件菜单上，选择保存新筛选器集。
5. 在保存筛选器集对话框中，输入筛选器集的名称。
6. （可选）要在每次打开摘要页面时使用默认设置的筛选器集，请选择将其设置为默认视图的选项。
7. 选择保存。

要在已创建和保存的筛选器集之间切换，请使用摘要控制面板上方的选择筛选器集菜单。当您选择筛选条件集时，Security Hub CSPM 会将该筛选条件集的条件应用于控制面板上的数据。

更新或删除筛选器集

请按照以下步骤更新或删除现有筛选器集。如果您删除当前设置为摘要控制面板默认视图的筛选条件集，则默认视图将重置为默认 Security Hub CSPM 视图。

要更新或删除筛选器集

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择摘要。
3. 在摘要页面上方的选择筛选器集菜单中，选择筛选器集。
4. 在清除筛选条件菜单上，执行以下操作之一：
   - 要更新筛选器集，请选择更新当前筛选器集。然后在出现的对话框中输入您的更改。
   - 要删除筛选器集，请选择删除当前筛选器集。然后在出现的对话框中选择删除。

在 Security Hub CSPM 中自定义摘要控制面板

您可以通过多种方式自定义 Security Hub CSPM 控制台上的摘要控制面板。例如，您可以在控制面板中添加和移除小组件。您还可以在控制面板上重新排列小组件并调整其大小。有关可用小组件列表以及每个小组件的描述，请参阅摘要控制面板的可用小组件。

如果您自定义控制面板，Security Hub CSPM 会立即应用您的更改并保存新的控制面板设置。您的更改将应用于您在所有浏览器 AWS 区域 和浏览器中对仪表板的视图。

要自定义 Summary 控制面板

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中，选择摘要。
3. 执行以下任一操作：
   - 要添加小组件，请选择页面右上角的添加小组件。在搜索栏中，输入要添加的小组件的标题。然后，将小组件拖到所需位置。
   - 要删除小组件，请选择小组件右上角的三个点。
   - 要移动小组件，请选择小组件左上角的图柄，然后将小组件拖到所需位置。

- 要更改小组件的大小，请选择小组件右下角的大小调整图柄。拖动小组件的边缘，使其达到您想要的大小。

要随后恢复原始设置，请选择页面顶部的重置为默认布局。

Security Hub CSPM 的区域限制

某些 S AWS ecurity Hub CSPM 功能仅在某些情况下可用。 AWS 区域以下各节详细说明了这些区域限制。有关 Security Hub CSPM 当前可用的所有区域的完整列表，请参阅 AWS 一般参考 中的 AWS Security Hub 端点和配额。

Cross-Region 聚合限制

在中 AWS GovCloud (US) Regions，跨区域聚合 AWS GovCloud (US) Regions 仅适用于调查结果、查找更新和见解。具体而言，您只能在 () 和 AWS GovCloud AWS GovCloud (US-EastUS-West) 区域之间汇总调查结果、查找结果更新和见解。

在中国区域，跨区域聚合仅可用于在中国区域的调查发现、调查发现更新和见解。具体而言，您只能聚合中国（北京）和中国（宁夏）区域之间的调查发现、调查发现更新和见解。

您不能使用默认禁用的区域作为聚合区域。有关默认禁用的区域列表，请参阅AWS 账户管理 参考指南 AWS 区域 中的在您的账户中启用或禁用。

按区域划分的集成可用性

有些集成并非全部 AWS 区域可用。在 Security Hub CSPM 控制台中，如果某个集成在您当前登录的区域中不可用，则该集成不会显示在集成页面上。

中国（北京）和中国（宁夏）区域支持的集成

在中国（北京）和中国（宁夏）区域，Security Hub CSPM 仅支持以下 AWS 服务集成：

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager 补丁管理器

在中国（北京）和中国（宁夏）区域，Security Hub CSPM 仅支持以下第三方集成：

- 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

中支持的集成 AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions

在 AWS GovCloud (US-East) 和 AWS GovCloud (US-West) 区域中，Security Hub CSPM 仅支持以下集成： AWS 服务

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM 访问分析器
- Amazon Inspector
- AWS IoT Device Defender

在 AWS GovCloud (US-East) 和 AWS GovCloud (US-West) 区域中，Security Hub CSPM 仅支持以下第三方集成：

- 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（仅在 AWS GovCloud (US-West) 中可用）
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

按区域划分的标准的可用性

AWS Control Tower 服务管理标准仅在 AWS Control Tower 支持的版本中 AWS 区域 可用。有关 AWS Control Tower 当前支持的区域列表，请参阅《AWS Control Tower 用户指南》 AWS Control Tower中的 “如何 AWS 区域 使用”。

AWS 资源标签标准不在亚太地区（台北）区域提供。

在 Security Hub CSPM 目前可用的所有区域，均可使用其他安全标准。

按地区划分的控件可用性

某些 Security Hub CSPM 控件并非全部可用。 AWS 区域有关每个区域不可用的控件列表，请参阅对 Security Hub CSPM 控件的区域限制。

在 Security Hub CSPM 控制台上，如果某个控件在您当前登录的区域中不可用，则该控件不会出现在控件列表中。聚合区域除外。如果您设置了某个聚合区域并登录到该区域，控制台将显示聚合区域或者一个或多个关联区域中可用的控件。

对 Security Hub CSPM 控件的区域限制

某些 S AWS ecurity Hub CSPM 控件并非全部可用。 AWS 区域此页面指定了哪些控件在特定区域不可用。

在 Security Hub CSPM 控制台上，如果某个控件在您当前登录的区域中不可用，则该控件不会出现在控件列表中。聚合区域除外。如果您设置了某个聚合区域并登录到该区域，控制台将显示聚合区域或者一个或多个关联区域中可用的控件。

AWS 区域

- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（北加利福尼亚）
- 美国西部（俄勒冈州）
- 非洲（开普敦）
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）

- 亚太地区（马来西亚）
- 亚太地区（墨尔本）
- 亚太地区（孟买）
- 亚太地区（新西兰）
- 亚太地区（大阪）
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（台北）
- 亚太地区（泰国）
- 亚太地区（东京）
- 加拿大（中部）
- 加拿大西部（卡尔加里）
- 中国（北京）
- 中国（宁夏）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（米兰）
- 欧洲地区（巴黎）
- 欧洲（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 墨西哥（中部）
- 中东（巴林）
- 中东（阿联酋）：
- 南美洲（圣保罗）
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

美国东部（弗吉尼亚州北部）

美国东部（弗吉尼亚州北部）区域不支持以下控件。

- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置

美国东部（俄亥俄州）

美国东部（俄亥俄州）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型

- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [RDS.31] 应标记 RDS 数据库安全组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

美国西部（北加利福尼亚）

美国西部（北加利福尼亚）区域不支持以下控件。

- [AppRunner.1] 应标记 App Runner 服务

- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密

- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对

- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [Redshift.18] Redshift 集群应启用多可用区部署
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

美国西部（俄勒冈州）

美国西部（俄勒冈州）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

非洲（开普敦）

非洲（开普敦）区域不支持以下控件。

- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式

- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例

- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [ECR.4] 应标记 ECR 公有存储库
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板

- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [RDS.1] RDS 快照应该是私有的
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密

- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

亚太地区（香港）

亚太地区（香港）区域不支持以下控件。

- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描

- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集

- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（海得拉巴）

亚太地区（海得拉巴）区域不支持以下控件。

- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制

- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例

- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.175] 应标记 EC2 启动模板
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中

- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户

- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道

- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制

- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离

- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（雅加达）

亚太地区（雅加达）区域不支持以下控件。

- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制

- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密

- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描

- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密

- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.11] S3 通用存储桶应启用事件通知
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SQS.1] 应对 Amazon SQS 队列进行静态加密

- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（马来西亚）

亚太地区（马来西亚）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录

- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Athena.4] Athena 工作组应启用日志记录
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.2] AWS Backup 应标记恢复点
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.1] DataSync 任务应启用日志记录
- [DataSync.2] 应标记 DataSync 任务

- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷

- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限

- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [ECS.19] ECS 容量提供商应启用托管终止保护
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EFS.7] EFS 文件系统应启用自动备份
- [EFS.8] 应对 EFS 文件系统进行静态加密
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组

- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护

- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器

- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪

- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密

- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密
- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志

- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网
- [Redshift.17] 应标记 Redshift 集群参数组
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（墨尔本）

亚太地区（墨尔本）区域不支持以下控件。

- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密

- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Batch.1] 应标记批处理作业队列
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联

- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.175] 应标记 EC2 启动模板
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果

- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描

- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应该是私有的
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch

- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表

- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.4] SSM 文档不应公开
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（孟买）

亚太地区（孟买）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [RDS.31] 应标记 RDS 数据库安全组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件

- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

亚太地区（新西兰）

亚太地区（新西兰）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 跟踪
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.5] API Gateway REST API 缓存数据应进行静态加密
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync Gr APIs aphQL

- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [Athena.4] Athena 工作组应启用日志记录
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.2] AWS Backup 应标记恢复点
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密

- [DataSync.1] DataSync 任务应启用日志记录
- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.172] EC2 VPC 阻止公共访问设置应阻止互联网网关流量
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库

- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.16] ECS 任务集不应自动分配公有 IP 地址
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [ECS.18] ECS 任务定义应对 EFS 卷使用传输中加密
- [ECS.19] ECS 容量提供商应启用托管终止保护
- [ECS.20] ECS 任务定义应在 Linux 容器定义中配置非 root 用户
- [ECS.21] ECS 任务定义应在 Windows 容器定义中配置非管理员用户
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EFS.7] EFS 文件系统应启用自动备份
- [EFS.8] 应对 EFS 文件系统进行静态加密
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议
- [ELB.22] ELB 目标组应使用加密的传输协议
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷

- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.3] GuardDuty IPSets 应该被标记
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA

- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型

- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密

- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密

- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密
- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [RDS.50] RDS 数据库集群应设置足够的备份保留期
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.3] Amazon Redshift 集群应启用自动快照

- [Redshift.4] Amazon Redshift 集群应启用审核日志记录
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应标记 Redshift 集群
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网
- [Redshift.17] 应标记 Redshift 集群参数组
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置

- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（大阪）

亚太地区（大阪）区域不支持以下控件。

- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务

- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录

- [Detective.1] 应标记 Detective 行为图
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签

- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间

- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [RDS.31] 应标记 RDS 数据库安全组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（首尔）

亚太地区（首尔）区域不支持以下控件。

- [AppRunner.1] 应标记 App Runner 服务

- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [ECR.4] 应标记 ECR 公有存储库
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密

- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.18] Redshift 集群应启用多可用区部署
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

亚太地区（新加坡）

亚太地区（新加坡）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密

- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置

- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

亚太地区（悉尼）

亚太地区（悉尼）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IVS.1] 应标记 IVS 播放密钥对

- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

亚太地区（台北）

亚太地区（台北）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ACM.3] 应标记 ACM 证书
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 跟踪
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.5] API Gateway REST API 缓存数据应进行静态加密
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支

- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync Gr APIs aphQL
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [Athena.4] Athena 工作组应启用日志记录
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Autoscaling.5] 使用 Auto Scaling 组启动配置启动的 EC2 亚马逊实例不应具有公有 IP 地址
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.2] AWS Backup 应标记恢复点
- [Backup.3] AWS Backup 应给保管库加标签
- [Backup.4] AWS Backup 报告计划应加标签
- [Backup.5] AWS Backup 应标记备份计划
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境

- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudTrail.9] CloudTrail 路径应加标签
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.17] 应激 CloudWatch 活警报动作

- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.1] DataSync 任务应启用日志记录
- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权

- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamoDB.5] 应标记 DynamoDB 表
- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.10] 应将 Amazon EC2 配置为使用为亚马逊 EC2 服务创建的 VPC 终端节点
- [EC2.19] 安全组不应允许不受限制地访问高风险端口
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关
- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关

- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL
- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应标记 Amazon VPC
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.52] 应标记 EC2 传输网关
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.172] EC2 VPC 阻止公共访问设置应阻止互联网网关流量
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标

- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.2] ECS 服务不应自动分配公有 IP 地址
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [ECS.16] ECS 任务集不应自动分配公有 IP 地址
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [ECS.18] ECS 任务定义应对 EFS 卷使用传输中加密
- [ECS.19] ECS 容量提供商应启用托管终止保护
- [ECS.20] ECS 任务定义应在 Linux 容器定义中配置非 root 用户
- [ECS.21] ECS 任务定义应在 Windows 容器定义中配置非管理员用户
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份

- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EFS.7] EFS 文件系统应启用自动备份
- [EFS.8] 应对 EFS 文件系统进行静态加密
- [EKS.1] EKS 集群终端节点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.7] 经典负载均衡器应启用连接耗尽功能
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议
- [ELB.22] ELB 目标组应使用加密的传输协议
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证

- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不应公开访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [ES.5] Elasticsearch 域应启用审核日志
- [ES.6] Elasticsearch 域名应至少有三个数据节点
- [ES.7] 应将 Elasticsearch 域配置为至少三个专用主节点
- [ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器

- [Glue.1] 应该给 AWS Glue 工作加标签
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.3] GuardDuty IPSets 应该被标记
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字

- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.23] 应标记 IAM Access Analyzer 分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户

- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.2] 应标记 Kinesis 流
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- AWS KMS keys 不应无意中删除 [KMS.3]
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.6] 应标记 Lambda 函数
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控

- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制

- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.16] 应将 Aurora 数据库集群配置为将标签复制到数据库快照
- [RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照
- [RDS.19] 应为关键群集事件配置现有 RDS 事件通知订阅
- [RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅
- [RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅
- [RDS.22] 应为关键的数据库安全组事件配置 RDS 事件通知订阅
- [RDS.23] RDS 实例不应使用数据库引擎的默认端口
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密

- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [RDS.50] RDS 数据库集群应设置足够的备份保留期
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.4] Amazon Redshift 集群应启用审核日志记录
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应标记 Redshift 集群
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网
- [Redshift.17] 应标记 Redshift 集群参数组
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问

- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密

- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SecretsManager.1] Secrets Manager 密钥应启用自动轮换
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 主题
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动

- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（泰国）

亚太地区（泰国）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接

- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [Athena.4] Athena 工作组应启用日志记录
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.2] AWS Backup 应标记恢复点
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键

- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密

- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.1] DataSync 任务应启用日志记录
- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.172] EC2 VPC 阻止公共访问设置应阻止互联网网关流量
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表

- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.16] ECS 任务集不应自动分配公有 IP 地址
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [ECS.18] ECS 任务定义应对 EFS 卷使用传输中加密
- [ECS.19] ECS 容量提供商应启用托管终止保护
- [ECS.20] ECS 任务定义应在 Linux 容器定义中配置非 root 用户
- [ECS.21] ECS 任务定义应在 Windows 容器定义中配置非管理员用户
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联

- [EFS.7] EFS 文件系统应启用自动备份
- [EFS.8] 应对 EFS 文件系统进行静态加密
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名

- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch

- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密
- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照

- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网
- [Redshift.17] 应标记 Redshift 集群参数组
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能

- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

亚太地区（东京）

亚太地区（东京)区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

加拿大（中部）

加拿大（中部）区域不支持以下控件。

- [AppRunner.1] 应标记 App Runner 服务

- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果

- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [RDS.31] 应标记 RDS 数据库安全组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

加拿大西部（卡尔加里）

加拿大西部（卡尔加里）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Athena.4] Athena 工作组应启用日志记录
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权

- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

- [CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.1] DataSync 任务应启用日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表

- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.175] 应标记 EC2 启动模板
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性

- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.16] ECS 任务集不应自动分配公有 IP 地址
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EFS.7] EFS 文件系统应启用自动备份
- [EFS.8] 应对 EFS 文件系统进行静态加密
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密

- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护

- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户

- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置

- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署

- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch

- [RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密
- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除

- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问

- [SSM.4] SSM 文档不应公开
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

中国（北京）

中国（北京）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支

- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表

- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.36] 应标记 EC2 客户网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议
- [ELB.22] ELB 目标组应使用加密的传输协议
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份

- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.3] GuardDuty IPSets 应该被标记
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.23] 应标记 IAM Access Analyzer 分析器
- [IAM.24] 应标记 IAM 角色

- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch

- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构

- [RDS.7] RDS 集群应启用删除保护
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 Aurora 数据库集群配置为将标签复制到数据库快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [RDS.50] RDS 数据库集群应设置足够的备份保留期
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.17] 应标记 Redshift 集群参数组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询

- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则

- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

中国（宁夏）

中国（宁夏）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略

- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置

- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.36] 应标记 EC2 客户网关
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表

- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议
- [ELB.22] ELB 目标组应使用加密的传输协议
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.3] AWS Glue 机器学习转换应在静态时加密

- [GuardDuty.3] GuardDuty IPSets 应该被标记
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.23] 应标记 IAM Access Analyzer 分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关

- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Lambda.1] Lambda 函数策略应禁止公众访问
- [Lambda.2] Lambda 函数应使用支持的运行时
- [Lambda.3] Lambda 函数应位于 VPC 中
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.6] 应标记 Lambda 函数
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.3] Neptune 数据库集群快照不应公开
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.50] RDS 数据库集群应设置足够的备份保留期
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.17] 应标记 Redshift 集群参数组

- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SSM.5] 应标记 SSM 文档
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件

- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

欧洲地区（法兰克福）

欧洲地区（法兰克福）区域不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器

- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [RDS.31] 应标记 RDS 数据库安全组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

欧洲地区（爱尔兰）

欧洲地区（爱尔兰）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制

- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [ECR.4] 应标记 ECR 公有存储库
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

欧洲地区（伦敦）

欧洲地区（伦敦）区域不支持以下控件。

- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [RDS.31] 应标记 RDS 数据库安全组

- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

欧洲地区（米兰）

欧洲地区（米兰）区域不支持以下控件。

- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS

- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.177] 应标记 EC2 流量镜像会话
- [ECR.4] 应标记 ECR 公有存储库
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量

- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密

- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [RDS.1] RDS 快照应该是私有的
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密

- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

欧洲地区（巴黎）

欧洲地区（巴黎）区域不支持以下控件。

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组

- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务

- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [RDS.31] 应标记 RDS 数据库安全组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

欧洲（西班牙）

欧洲（西班牙）区域不支持以下控件。

- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密

- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份

- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.1] 不应将 Amazon EBS 快照配置为可公开还原
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.34] 应标记 EC2 传输网关路由表

- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.175] 应标记 EC2 启动模板
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果

- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目

- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.1] Lambda 函数策略应禁止公众访问
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份

- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应该是私有的
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.18] Redshift 集群应启用多可用区部署
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离

- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

欧洲地区（斯德哥尔摩）

欧洲地区（斯德哥尔摩）区域不支持以下控件。

- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密

- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组

- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

欧洲（苏黎世）

欧洲（苏黎世）区域不支持以下控件。

- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式

- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型

- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)

- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.175] 应标记 EC2 启动模板
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体

- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [Opensearch.1] OpenSearch 域名应启用静态加密

- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应该是私有的
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.18] Redshift 集群应启用多可用区部署
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密

- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

以色列（特拉维夫）

以色列（特拉维夫）区域不支持以下控件。

- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略

- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例

- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.175] 应标记 EC2 启动模板
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.8] 应对 EFS 文件系统进行静态加密

- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [ELB.2] 带 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签

- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch

- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应该是私有的
- [RDS.4] RDS 集群快照和数据库快照应在静态时加密
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级

- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.4] SSM 文档不应公开
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能

- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

墨西哥（中部）

墨西哥（中部）区域不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录

- [AppSync.4] 应标记 AWS AppSync Gr APIs aphQL
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Athena.4] Athena 工作组应启用日志记录
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.2] AWS Backup 应标记恢复点
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库 URLs 不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DataSync.1] DataSync 任务应启用日志记录

- [DataSync.2] 应标记 DataSync 任务
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.6] DynamoDB 表应启用删除保护
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点
- [EC2.56] 应为 VPC 配置 Docker Registry 的接口端点
- [EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.171] EC2 VPN 连接应启用日志记录
- [EC2.172] EC2 VPC 阻止公共访问设置应阻止互联网网关流量
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.182] 应为 Amazon EBS 快照启用阻止公开访问设置
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys

- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [ECS.16] ECS 任务集不应自动分配公有 IP 地址
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [ECS.18] ECS 任务定义应对 EFS 卷使用传输中加密
- [ECS.19] ECS 容量提供商应启用托管终止保护
- [ECS.20] ECS 任务定义应在 Linux 容器定义中配置非 root 用户
- [ECS.21] ECS 任务定义应在 Windows 容器定义中配置非管理员用户
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联
- [EFS.7] EFS 文件系统应启用自动备份
- [EFS.8] 应对 EFS 文件系统进行静态加密
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志
- [EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略

- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器

- [Glue.1] 应该给 AWS Glue 工作加标签
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控
- [GuardDuty.6] 应启用 Lamb GuardDuty da 保护
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.10] 应启用 GuardDuty S3 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应具有很强的配置
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码

- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间

- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.3] Kinesis 流应有足够的数据留存期
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch
- [MQ.4] 应给亚马逊 MQ 经纪人加标签
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名

- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划的保护
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch
- [RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch
- [RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密
- [RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.4] Amazon Redshift 集群应启用审核日志记录
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应标记 Redshift 集群
- [Redshift.13] 应标记 Redshift 集群快照

- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网
- [Redshift.17] 应标记 Redshift 集群参数组
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.7] S3 通用存储桶应使用跨区域复制
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.19] S3 接入点已启用屏蔽公共访问权限设置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签

- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [Transfer.4] 应标记 Transfer Family 协议

- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

中东（巴林）

中东（巴林）区域不支持以下控件。

- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移

- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.10] CloudTrail 湖泊事件数据存储应使用客户托管进行加密 AWS KMS keys
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DocumentDB.6] Amazon DocumentDB 集群应在传输过程中加密
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.20] 两个 VPN 隧道都用于 AWS Site-to-Site VPN 连接应该已开启
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC

- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.4] 应标记 ECR 公有存储库
- [ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys
- [ECS.17] ECS 任务定义不应使用主机网络模式
- [EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署
- [FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署
- [FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目

- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [NetworkFirewall.10] Network Firewall 防火墙应启用子网变更保护
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.41] 适用于 SQL Server 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.42] 适用于 MariaDB 的 RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.44] 适用于 MariaDB 数据库实例的 RDS 在传输过程中应进行加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.46] 不应将 RDS 数据库实例部署在具有通往 Internet 网关的路由的公共子网中
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.4] Redshift Serverless 命名空间应使用客户托管进行加密 AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 命名空间不应使用默认的管理员用户名
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询

- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.8] SageMaker 笔记本实例应在支持的平台上运行
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [Transfer.3] Transfer Family 连接器应启用日志记录
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

中东（阿联酋）：

中东（阿联酋）区域不支持以下控件。

- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器

- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [Backup.1] AWS Backup 恢复点应在静态状态下进行加密
- [Backup.4] AWS Backup 报告计划应加标签
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFormation.3] CloudFormation 堆栈应启用终止保护
- [CloudFormation.4] CloudFormation 堆栈应具有相关的服务角色
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组

- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [Detective.1] 应标记 Detective 行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] Redis OSS 的 DMS 端点应启用 TLS
- [DMS.13] DMS 复制实例应配置为使用多个可用区
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.4] 应在指定时间段后移除已停止的 EC2 实例
- [EC2.14] 安全组不应允许从 0.0.0 开始的入口。 0/0 或者:: /0 到端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密

- [EC2.175] 应标记 EC2 启动模板
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.179] 应标记 EC2 流量镜像目标
- [EC2.180] EC2 网络接口应启用 source/destination 检查功能
- [EC2.181] EC2 启动模板应为连接的 EBS 卷启用加密
- [EC2.183] EC2 VPN 连接应使用 IKEv2 协议
- [ECR.4] 应标记 ECR 公有存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EKS.9] EKS 节点组应在支持的 Kubernetes 版本上运行
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略
- [ELB.18] 应用程序和网络负载均衡器侦听器应使用安全协议对传输中数据进行加密
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器

- [Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue
- [GuardDuty.2] 应给 GuardDuty 过滤器加标签
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.18] 确保已创建支持角色来管理事件 AWS 支持
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess
- [Inspector.1] 应启用 Amazon Inspector EC2 扫描
- [Inspector.2] 应启用 Amazon Inspector ECR 扫描
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目

- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.7] Lambda 函数应该有 AWS X-Ray 已启用主动跟踪
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.4] MSK 集群应禁用公开访问
- [MSK.5] MSK 连接器应启用日志记录
- [MSK.6] MSK 集群应禁用未经身份验证的访问
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新

- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.18] Redshift 集群应启用多可用区部署
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集

- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [SSM.7] SSM 文档应启用“阻止公开共享”设置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

南美洲（圣保罗）

南美洲（圣保罗）区域不支持以下控件。

- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF

- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [ECR.4] 应标记 ECR 公有存储库
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoT.1] 应 AWS IoT Device Defender 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型

- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组

AWS GovCloud (US-East)

该 AWS GovCloud (US-East) 地区不支持以下控件。

- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分

- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务
- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync Gr APIs aphQL
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权

- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.2] Cognito 身份池不应允许未经身份验证的身份
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA

- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [Connect.2] Connect 客户实例应启用 CloudWatch 日志记录
- [DataSync.2] 应标记 DataSync 任务
- [DMS.2] 应标记 DMS 证书
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密
- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.52] 应标记 EC2 传输网关
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表

- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.8] EKS 集群应启用审核日志
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议
- [ELB.22] ELB 目标组应使用加密的传输协议
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证

- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷
- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.3] AWS Glue 机器学习转换应在静态时加密
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书

- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务
- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控

- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群

- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [RDS.50] RDS 数据库集群应设置足够的备份保留期
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.17] 应标记 Redshift 集群参数组
- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.16] SageMaker 模型应在主容器中使用 VPC 中的私有注册表
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.19] SageMaker 模型应在多容器推理管道中使用 VPC 中的私有注册表
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SNS.4] SNS 主题访问策略不应允许公共访问
- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [SSM.6] SSM 自动化应启用日志记录 CloudWatch
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件

- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch
- [WorkSpaces.1] WorkSpaces 用户卷应在静态时加密
- [WorkSpaces.2] WorkSpaces 根卷应在静态时加密

AWS GovCloud (US-West)

该 AWS GovCloud (US-West) 地区不支持以下控件。

- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [APIGateway.10] API Gateway V2 集成应使用 HTTPS 进行私有连接
- [APIGateway.11] API Gateway 域名应使用推荐的安全策略
- [Amplify.1] 应标记 Amplify 应用
- [Amplify.2] 应标记 Amplify 分支
- [AppConfig.1] 应为 AWS AppConfig 应用程序加标签
- [AppConfig.2] 应标记 AWS AppConfig 配置文件
- [AppConfig.3] 应该对 AWS AppConfig 环境进行标记
- [AppConfig.4] 应 AWS AppConfig 标记扩展关联
- [AppFlow.1] 应为亚马逊 AppFlow 流程加标签
- [AppRunner.1] 应标记 App Runner 服务

- [AppRunner.2] 应标记 App Runner VPC 连接器
- [AppSync.1] 应 AWS AppSync 对 API 缓存进行静态加密
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync Gr APIs aphQL
- [AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证
- [AppSync.6] AWS AppSync API 缓存应在传输过程中进行加密
- [AutoScaling.2] Amazon A EC2 uto Scaling 组应覆盖多个可用区域
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 A EC2 uto Scaling 小组应使用亚马逊 EC2 启动模板
- [Backup.4] AWS Backup 报告计划应加标签
- [Batch.1] 应标记批处理作业队列
- [Batch.2] 应标记批处理计划策略
- [Batch.3] 应标记批处理计算环境
- [Batch.4] 应标记托管批处理计算环境中的计算资源属性
- [BedrockAgentCore.1] 基岩 AgentCore 运行时应配置为 VPC 网络模式
- [BedrockAgentCore.2] Bedrock Gate AgentCore ways 应要求对入站请求进行授权
- [BedrockAgentCore.3] 基岩 AgentCore 内存应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.4] Bedrock AgentCore Gateway 应使用客户托管进行加密 AWS KMS 键
- [BedrockAgentCore.5] Bedrock AgentCore 自定义浏览器不应使用公共网络模式
- [BedrockAgentCore.6] Bedrock AgentCore 自定义浏览器应启用会话录制
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义证书 SSL/TLS
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应 CloudFront 标记发行版
- [CloudFront.15] CloudFront 发行版应使用推荐的 TLS 安全策略
- [CloudFront.16] CloudFront 分配应对 Lambda 函数 URL 来源使用源访问控制
- [CloudFront.17] CloudFront 发行版应使用可信密钥组进行签名 URLs 和 Cookie
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [CodeGuruProfiler.1] 应 CodeGuru 标记 Profiler 分析组
- [CodeGuruReviewer.1] 应标 CodeGuru 记 Reviewer 存储库关联
- [Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证
- [Cognito.3] Cognito 用户池的密码策略应具有可靠的配置
- [Cognito.4] Cognito 用户池应激活威胁防护，并使用全功能强制模式进行自定义身份验证
- [Cognito.5] 应为 Cognito 用户池启用 MFA
- [Cognito.6] Cognito 用户池应启用删除保护
- [Connect.1] 应标记 Amazon Connect 客户档案对象类型
- [DataSync.2] 应标记 DataSync 任务
- [DMS.2] 应标记 DMS 证书
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator（DAX）集群应在静态状态下进行加密

- [DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密
- [EC2.21] 网络 ACL 不应允许从 0.0.0 开始的入口。 0/0 到端口 22 或端口 3389
- [EC2.22] 应移除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.38] 应标记 EC2 实例
- [EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点
- [EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC
- [EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)
- [EC2.173] 带有启动参数的 EC2 Spot 队列请求应为连接的 EBS 卷启用加密
- [EC2.174] 应标记 EC2 DHCP 选项集
- [EC2.175] 应标记 EC2 启动模板
- [EC2.176] 应标记 EC2 前缀列表
- [EC2.177] 应标记 EC2 流量镜像会话
- [EC2.178] 应标记 EC2 流量镜像过滤器
- [EC2.179] 应标记 EC2 流量镜像目标
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公有存储库
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 任务定义应将容器配置为仅限于对根文件系统的只读访问权限
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应使用容器见解
- [EFS.3] EFS 接入点应强制使用根目录

- [EFS.4] EFS 接入点应强制使用用户身份
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.8] EKS 集群应启用审核日志
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.21] 应用程序和 Network Load Balancer 目标组应使用加密的运行状况检查协议
- [ELB.22] ELB 目标组应使用加密的传输协议
- [ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份
- [ElastiCache.2] ElastiCache 集群应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 复制组应启用自动故障切换
- [ElastiCache.4] ElastiCache 复制组应进行静态加密
- [ElastiCache.5] ElastiCache 复制组在传输过程中应加密
- [ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [EMR.3] Amazon EMR 安全配置应静态加密
- [EMR.4] Amazon EMR 安全配置应在传输过程中加密
- [ES.4] 应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [FraudDetector.1] 应标记 Amazon Fraud Detector 实体类型
- [FraudDetector.2] 应标记 Amazon Fraud Detector 标签
- [FraudDetector.3] 应标记 Amazon Fraud Detector 的结果
- [FraudDetector.4] 应标记 Amazon Fraud Detector 变量
- [FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷

- [FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.7] 应启用 GuardDuty EKS 运行时监控
- [GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护
- [GuardDuty.9] 应启用 GuardDuty RDS 保护
- [GuardDuty.11] 应启用 “ GuardDuty 运行时监控”
- [GuardDuty.12] 应启用 GuardDuty ECS 运行时监控
- [GuardDuty.13] 应启用 GuardDuty EC2 运行时监控
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.28] 应启用 IAM Access Analyzer 外部访问分析器
- [Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描
- [IoTEvents.1] AWS 应标记 IoT Events 输入内容
- [IoTEvents.2] AWS 应标记 IoT Events 探测器模型
- [IoTEvents.3] AWS 应标记 IoT Events 警报模型
- [Io TSite Wise.1] 应 AWS 标记物联网 SiteWise 资产模型
- [Io TSite Wise.2] 应标记物 AWS 联网 SiteWise 仪表板
- [Io TSite Wise.3] 应标记 AWS 物联 SiteWise 网网关
- [Io TSite Wise.4] 应标记 AWS 物联网 SiteWise 门户
- [Io TSite Wise.5] 应 AWS 标记物联网 SiteWise 项目
- [Io TTwin Maker.1] 应标记 AWS 物联网 TwinMaker 同步作业
- [Io TTwin Maker.2] 应标记 AWS 物联网 TwinMaker 工作空间
- [Io TTwin Maker.3] 应标记 AWS 物联网 TwinMaker 场景
- [Io TTwin Maker.4] 应标记物 AWS 联网 TwinMaker 实体
- [Io TWireless .1] 应标 AWS 记 IoT Wireless 组播组
- [Io TWireless .2] 应标记 AWS IoT Wireless 服务配置文件
- [Io TWireless .3] 应 AWS 标记物联网 FUOTA 任务

- [IVS.1] 应标记 IVS 播放密钥对
- [IVS.2] 应标记 IVS 录制配置
- [IVS.3] 应标记 IVS 频道
- [Keyspaces.1] 应标记 Amazon Keyspaces 密钥空间
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.5] KMS 密钥不应可公开访问
- [Lambda.5] VPC Lambda 函数应在多个可用区中运行
- [Macie.1] 应启用 Amazon Macie
- [Macie.2] 应启用 Macie 敏感数据自动发现
- [MQ.5] ActiveMQ 代理应使用部署模式 active/standby
- [MQ.6] RabbitMQ 代理应使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [MSK.3] MSK Connect 连接器应在传输过程中进行加密
- [MSK.5] MSK 连接器应启用日志记录
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构
- [PCA.2] 应标记 AWS 私有 CA 证书颁发机构
- [RDS.14] 亚马逊 Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.27] RDS 数据库集群应进行静态加密
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [RDS.43] RDS 数据库代理应要求对连接进行 TLS 加密
- [RDS.45] Aurora MySQL 数据库集群应启用审计日志
- [RDS.47] 应将 RDS for PostgreSQL 数据库集群配置为将标签复制到数据库快照
- [RDS.48] 应将 RDS for MySQL 数据库集群配置为将标签复制到数据库快照
- [RDS.50] RDS 数据库集群应设置足够的备份保留期
- [RDS.51] RDS 全局集群应在支持的 Aurora MySQL 版本上运行
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应标记 Redshift 集群
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.17] 应标记 Redshift 集群参数组

- [RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由
- [RedshiftServerless.2] 使用 SSL 需要连接到 Redshift 无服务器工作组
- [RedshiftServerless.3] Redshift 无服务器工作组应禁止公众访问
- [RedshiftServerless.6] Redshift Serverless 命名空间应将日志导出到日志 CloudWatch
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.10] 启用了版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- ACLs 不应使用 [S3.12] 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置
- [S3.25] S3 目录存储桶应具有生命周期配置
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.5] SageMaker 模型应启用网络隔离
- [SageMaker.6] SageMaker 应用映像配置应加标签
- [SageMaker.7] 应给 SageMaker 图片加标签
- [SageMaker.9] SageMaker 数据质量任务定义应启用容器间流量加密
- [SageMaker.10] SageMaker 模型可解释性任务定义应启用容器间流量加密
- [SageMaker.11] SageMaker 数据质量作业定义应启用网络隔离
- [SageMaker.12] SageMaker 模型偏差任务定义应启用网络隔离
- [SageMaker.13] SageMaker 模型质量任务定义应启用容器间流量加密
- [SageMaker.14] SageMaker 监控计划应启用网络隔离
- [SageMaker.15] SageMaker 模型偏差任务定义应启用容器间流量加密
- [SageMaker.17] SageMaker 功能组离线商店应使用以下方式进行加密 AWS KMS 键
- [SageMaker.18] SageMaker 具有标准存储空间的功能组在线商店应使用以下方式进行加密 AWS KMS 键
- [SES.3] SES 配置集应启用 TLS 以发送电子邮件
- [SNS.4] SNS 主题访问策略不应允许公共访问

- [SQS.3] SQS 队列访问策略不应允许公开访问
- [SSM.4] SSM 文档不应公开
- [SSM.5] 应标记 SSM 文档
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.4] 应标记 Transfer Family 协议
- [Transfer.5] 应标记 Transfer Family 证书
- [Transfer.6] 应标记 Transfer Family 连接器
- [Transfer.7] 应标记 Transfer Family 配置文件
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域网站 ACLs 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全球网站 ACLs 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch

使用创建 Security Hub CSPM 资源 CloudFormation

AWS Security Hub CSPM 与 AWS CloudFormation集成，后者是一项服务，可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础架构所花费的时间。您可以创建一个描述所需的所有 AWS 资源（例如自动化规则）的模板，并为您 CloudFormation 预置和配置这些资源。

使用时 CloudFormation，您可以重复使用模板来一致且重复地设置 Security Hub CSPM 资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中一遍又一遍地配置相同的资源。

Security Hub CSPM 和模板 CloudFormation

要为 Security Hub CSPM 和相关服务预置和配置资源，您必须了解 CloudFormation 模板的工作原理。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 CloudFormation 堆栈中配置的资源。

如果你不熟悉 JSON 或 YAML，可以使用 D CloudFormation esigner 来帮助你开始使用 CloudFormation 模板。有关更多信息，请参阅什么是 CloudFormation 设计器？ 在《AWS CloudFormation 用户指南》中。

您可以为以下类型的 Security Hub CSPM 资源创建 CloudFormation 模板：

- 启用 Security Hub CSPM
- 为组织指定 Security Hub CSPM 委派管理员
- 指定组织在 Security Hub CSPM 中的配置方式
- 启用安全标准
- 启用跨区域聚合
- 创建中央配置策略并将其与账户、组织单位 (OUs) 或根相关联
- 创建自定义见解
- 创建自动化规则
- 自定义控制参数
- 订阅第三方产品集成

有关更多信息（包括资源的 JSON 和 YAML 模板示例），请参阅《AWS CloudFormation 用户指南》中的 AWS Security Hub CSPM 资源类型参考。

了解更多关于 CloudFormation

要了解更多信息 CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- CloudFormation API 引用
- AWS CloudFormation 命令行界面用户指南

通过 Amazon SNS 订阅 Security Hub CSPM 公告

本节提供有关通过亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 订阅 Sec AWS urity Hub CSPM 公告以接收有关 Security Hub CSPM 的通知的信息。

订阅后，您将收到有关以下事件的通知（请注意每个事件相应的 AnnouncementType）：

- NEW_STANDARDS_CONTROLS – 添加了新的 Security Hub CSPM 控件或标准。
- RETIRED_STANDARDS_CONTROLS – 现有的 Security Hub CSPM 控件或标准已停用。

通知以 Amazon SNS 支持的所有格式提供。您可以在 Security Hub CSPM 可用的所有AWS 区域中订阅 Security Hub CSPM 公告。

用户必须拥有 Subscribe 权限才能订阅 Amazon SNS 主题。您可以通过 Amazon SNS 策略、IAM policy 或两者来实现这一目标。有关更多信息，请参阅 Amazon Simple Notification Service 开发者指南中的 IAM 和 Amazon SNS 策略。

> **Note**
>
> Security Hub CSPM 会向任何 AWS 账户订阅者发送有关 Security Hub 服务更新的 Amazon SNS 公告。要接收有关 Security Hub CSPM调查发现的通知，请参阅 在 Security Hub CSPM 中查看调查发现详细信息和历史记录。

您可以为 Amazon SNS 主题订阅 Amazon Simple Queue Service（Amazon SQS）队列，但必须使用同一区域内的 Amazon SNS 主题 Amazon 资源名称（ARN）。有关更多信息，请参阅《Amazon Simple Queue Service 开发人员指南》中的为队列订阅 Amazon SNS 主题。

您还可以在收到通知时使用 AWS Lambda 函数来调用事件。有关更多信息，包括示例函数代码，请参阅AWS Lambda 开发者指南中的教程： AWS Lambda 与 Amazon 简单通知服务一起使用。

每个区域的 Amazon SNS 主题 ARN 如下所示。

AWS 区域	Amazon SNS 主题 ARN
美国东部（俄亥俄州）	arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements
美国东部（弗吉尼亚州北部）	arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements

AWS 区域	Amazon SNS 主题 ARN
美国西部（北加利福尼亚）	arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements
美国西部（俄勒冈州）	arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements
非洲（开普敦）	arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements
亚太地区（香港）	arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements
亚太地区（海得拉巴）	arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements
亚太地区（雅加达）	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
亚太地区（孟买）	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
亚太地区（大阪）	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
亚太地区（首尔）	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements

AWS 区域	Amazon SNS 主题 ARN
亚太地区（新加坡）	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
亚太地区（悉尼）	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements
亚太地区（东京）	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
加拿大（中部）	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
中国（北京）	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements
中国（宁夏）	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
欧洲地区（法兰克福）	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
欧洲地区（爱尔兰）	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
欧洲地区（伦敦）	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements

AWS 区域	Amazon SNS 主题 ARN
欧洲地区（米兰）	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
欧洲地区（巴黎）	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
欧洲（西班牙）	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
欧洲地区（斯德哥尔摩）	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
欧洲（苏黎世）	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements
以色列（特拉维夫）	arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements
Middle East (Bahrain)	arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements
中东（阿联酋）：	arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements
南美洲（圣保罗）	arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements

AWS 区域	Amazon SNS 主题 ARN
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`

分区内各区域的消息通常相同，因此您可以订阅每个分区中的一个区域，以接收影响该分区中所有区域的公告。与成员账户关联的公告不会复制到管理员账户中。因此，每个账户（包括管理员账户）将只有一份每份公告的副本。您可以决定要使用哪个账户来订阅 Security Hub CSPM 公告。

有关订阅 Security Hub CSPM 公告的费用信息，请参阅 Amazon SNS 定价。

订阅 Security Hub CSPM 公告（控制台）

1. 从 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在“区域”列表中，选择要在其中订阅 Security Hub CSPM 公告的区域。此示例使用`us-west-2`区域。
3. 在导航窗格中，选择订阅，然后选择创建订阅。
4. 在主题 ARN 框中，输入主题 ARN。例如 `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`。
5. 在协议中，选择您希望如何接收 Security Hub CSPM 公告。如果您选择电子邮件，请在端点中输入要用于接收公告的电子邮件地址。
6. 选择创建订阅。
7. 确认订阅。例如，如果您选择电子邮件协议，Amazon SNS 会向您提供的电子邮件发送一条订阅确认消息。

订阅 Security Hub CSPM 公告 (AWS CLI)

1. 运行以下命令：

```
 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. 确认订阅。例如，如果您选择电子邮件协议，Amazon SNS 会向您提供的电子邮件发送一条订阅确认消息。

Amazon SNS 消息格式

以下示例显示了 Amazon SNS 发布的关于引入新安全控件的 Security Hub CSPM 公告。消息内容因公告类型而异，但所有公告类型的格式都相同。可选择包含一个 `Link` 字段，提供有关公告的详细信息。

示例：Security Hub CSPM 新控件公告（电子邮件协议）

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational 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 the AWS
 Foundational 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. "
}
```

示例：Security Hub CSPM 新控件公告（电子邮件-JSON 协议）

```
{
  "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 the AWS Foundational Security
 Best Practices standard\",\"Description\":\"We have added 36 new controls to the
 AWS Foundational 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 the AWS
 Foundational 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"
}
```


禁用 Security Hub CSPM

你可以使用 Sec AWS urity Hub CSPM 控制台或 Security Hub API 禁用 Security Hub CSPM。如果您禁用 Security Hub CSPM，则可以稍后重新启用它。

如果您的组织使用集中配置，则委派的 Security Hub CSPM 管理员可以创建配置策略，为特定账户和组织单位（OUs）禁用 Security Hub CSPM，并使其他账户和组织单位启用 Security Hub CSPM。配置策略影响主区域和所有关联区域。有关更多信息，请参阅 了解 Security Hub CSPM 中的中心配置。

如果禁用某个账户的 Security Hub CSPM，则会发生以下情况：

- 该账户的所有 Security Hub CSPM 标准和控件均已禁用。
- Security Hub CSPM 停止为该账户生成、更新和提取调查发现。
- 30 天后，Security Hub CSPM 将永久删除该账户的所有现有存档调查发现。使用 Security Hub CSPM 无法恢复这些调查发现。
- 90 天后，Security Hub CSPM 将永久删除该账户的所有现有活跃调查发现。使用 Security Hub CSPM 无法恢复这些调查发现。
- 90 天后，Security Hub CSPM 将永久删除该账户的所有现有见解和 Security Hub CSPM 配置设置。数据和设置无法恢复。

要保留现有调查发现，可以在禁用 Security Hub CSPM 之前将调查发现导出到 S3 存储桶。您可以通过使用带有 Amazon EventBridge 规则的自定义操作来实现此目的。有关更多信息，请参阅 EventBridge 用于自动响应和补救。

如果您在为账户禁用 Security Hub CSPM 后的 90 天内重新启用该功能，则可以重新获得该账户的现有活跃调查发现以及见解和 Security Hub CSPM 配置设置的访问权限。如果您在 30 天内重新启用 Security Hub CSPM，则还可以重新获得该账户的现有存档调查发现的访问权限。但是，现有发现可能不准确，因为它们将反映您禁用 Security Hub CSPM 时的 AWS 环境状态。此外，当您重新启用单个标准和控制时，Security Hub CSPM 最初可能会为特定 AWS 资源生成重复的结果，具体取决于您启用的标准和控件。出于这些原因，我们建议您执行以下操作之一：

- 在禁用 Security Hub CSPM 之前，请将所有现有调查发现的工作流状态更改为 `RESOLVED`。有关更多信息，请参阅 设置调查发现的工作流状态。
- 在禁用 Security Hub CSPM 之前至少六天禁用所有标准。然后，Security Hub CSPM 会尽最大努力将所有现有调查发现归档，通常在三到五天内。有关更多信息，请参阅 禁用标准。

在以下情况下，您无法禁用 Security Hub CSPM：

- 您的账户是某组织的 Security Hub CSPM 委派管理员帐户。如果使用中心配置，则无法将禁用 Security Hub CSPM 的配置策略与委派管理员账户关联。其他账户的关联可能会成功，但 Security Hub CSPM 不会将该策略应用于委派管理员账户。
- 您的账户是受邀的 Security Hub CSPM 管理员账户，并且您拥有成员账户。在禁用 Security Hub CSPM 之前，您必须解除关联所有成员账户。要了解如何操作，请参阅the section called “取消关联成员账户”。

在成员账户的所有者可以禁用 Security Hub CSPM 之前，您必须先解除该账户与其管理员账户的关联。对于组织账户，只有管理员账户可以解除成员账户关联。有关更多信息，请参阅 the section called “解除组织成员账户”。对于手动邀请的账户，管理员账户或成员账户可以解除成员账户关联。有关更多信息，请参阅 the section called “取消关联成员账户”或 the section called “从管理员账户取消关联”。如果使用中心配置，则不需要解除关联，因为 Security Hub CSPM 管理员可以创建一个策略来为特定成员账户禁用 Security Hub CSPM。

当你为账户禁用 Security Hub CSPM 时，它只能在当前版本中被禁用。 AWS 区域但是，如果使用中心配置为特定账户禁用 Security Hub CSPM，则会导致在主区域和所有关联区域禁用 Security Hub CSPM。

要禁用 Security Hub CSPM，请选择您喜欢的方法并按照步骤进行操作。

Security Hub CSPM console

请按照以下步骤使用控制台禁用 Security Hub CSPM。

禁用 Security Hub CSPM

1. 打开 S AWS ecurity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 在导航窗格中的设置下，选择常规。
3. 在禁用 Security Hub CSPM 部分中，选择禁用 Security Hub CSPM。
4. 当系统提示确认时，请选择禁用 Security Hub CSPM。

Security Hub API

要以编程方式禁用 Security Hub CSPM，请使用 Sec AWS urity Hub API 的DisableSecurityHub操作。或者，如果您使用的是 AWS CLI，请运行该disable-security-hub命令。例如，以下命令在当前版本中禁用 Security Hub CSPM： AWS 区域

```
$ aws securityhub disable-security-hub
```

中的安全性 AWS Security Hub CSPM

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。 Third-party作为AWS 合规计划的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 AWS Security Hub CSPM的合规性计划，请参阅合规性计划范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Security Hub CSPM 时如何应用责任共担模型。以下主题向您展示了如何配置 Security Hub CSPM 以满足您的安全和合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Security Hub CSPM 资源。

主题

- 中的数据保护 AWS Security Hub CSPM
- AWS Security Hub 的 Identity and Access 管理 CSPM
- 的合规性验证 AWS Security Hub CSPM
- 韧性在 AWS Security Hub
- 中的基础设施安全 AWS Security Hub CSPM
- AWS Security Hub CSPM 和接口 VPC 终端节点 (AWS PrivateLink)

中的数据保护 AWS Security Hub CSPM

AWS 责任共担模式适用于保护 AWS Security Hub CSPM中的数据。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题解答AWS条款。 有关欧洲数据保护的信息，请参阅通用数据保护条例（GDPR）中心。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。

- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当你 AWS 服务 使用控制台、API 或 SDK 与 Security Hub CSPM 或其他人合作 AWS CLI时。 AWS 在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

Security Hub CSPM 是一项多租户服务产品。为了确保数据保护，Security Hub CSPM 对静态数据和组件服务之间传输的数据进行加密。

AWS Security Hub 的 Identity and Access 管理 CSPM

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Security Hub 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Security Hub 如何与 IAM 协同工作
- Identity-based 的策略示例 AWS Security Hub CSPM
- Service-linked 的角色 AWS Security Hub CSPM
- AWS Security Hub 的托管策略
- 问题排查 AWS Security Hub CSPM 身份和访问权限

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅问题排查 AWS Security Hub CSPM 身份和访问权限）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅Security Hub 如何与 IAM 协同工作）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Identity-based 的策略示例 AWS Security Hub CSPM）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问，AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 根用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

Resource-based 策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略（ SCP ）– 指定 AWS Organizations中组织或组织单元的最大权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略（ RCP ）– 设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略（ RCP ）。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Security Hub 如何与 IAM 协同工作

在使用 AWS Identity and Access Management (IAM) 管理访问权限之前 AWS Security Hub CSPM，请先了解哪些 IAM 功能可用于 Security Hub CSPM。

您可以搭配使用的 IAM 功能 AWS Security Hub CSPM

IAM 功能	Security Hub CSPM 支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	否
策略条件键	是
访问控制列表 (ACL)	否
Attribute-based 访问控制 (ABAC)-策略中的标签	是

IAM 功能	Security Hub CSPM 支持
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
Service-linked 角色	是

有关 Security Hub CSPM 和其他功能如何与大多数 IAM 功能 AWS 服务 配合使用的高级视图，请参阅 AWS 服务 IAM 用户指南中的如何与 IAM 配合使用。

Identity-based Security Hub CSPM 的策略

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Security Hub CSPM 支持基于身份的策略。有关更多信息，请参阅 Identity-based 的策略示例 AWS Security Hub CSPM。

Resource-based Security Hub CSPM 的策略

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Security Hub CSPM 不支持基于资源的策略。您不能将 IAM 策略直接附加到 Security Hub CSPM 资源。

Security Hub CSPM 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

Security Hub CSPM 中的策略操作在操作前使用以下前缀：

```
securityhub:
```

例如，要向用户授予启用 Security Hub CSPM（该操作与 Security Hub CSPM API 的`EnableSecurityHub`操作相对应的操作）的权限，请将该`securityhub:EnableSecurityHub`操作包含在他们的策略中。策略语句必须包含 `Action` 或 `NotAction` 元素。Security Hub CSPM 定义了自己的一组操作，这些操作描述了您可以使用此服务执行的任务。

```
"Action": "securityhub:EnableSecurityHub"
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。例如：

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

您也可以使用通配符（*）指定多项操作。例如，要指定以单词 `Get` 开头的所有操作，包括以下操作：

```
"Action": "securityhub:Get*"
```

但作为最佳实践，您应创建遵循最低权限 原则的策略。换句话说，您应创建仅包含执行特定任务所需的权限的策略。

用户必须具有对 `DescribeStandardsControl` 操作的访问权限才能访问 `BatchGetSecurityControls`、`BatchGetStandardsControlAssociations` 和 `ListStandardsControlAssociations`。

用户必须具有对 `UpdateStandardsControls` 操作的访问权限才能访问 `BatchUpdateStandardsControlAssociations` 和 `UpdateSecurityControl`。

有关 Security Hub CSPM 操作的列表，请参阅《服务授权参考》 AWS Security Hub CSPM中定义的操作。有关指定 Security Hub CSPM 操作的策略示例，请参阅。Identity-based 的策略示例 AWS Security Hub CSPM

Security Hub CSPM 的策略资源

支持策略资源：否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

Security Hub CSPM 定义了以下资源类型：

- 中心
- 产品
- 调查发现聚合器，也称为跨区域聚合器
- 自动化规则
- 配置策略

您可以通过使用 ARN 在政策中指定这些类型的资源。

有关 Security Hub CSPM 资源类型的列表以及每种资源类型的 ARN 语法，请参阅《服务授权参考》 AWS Security Hub CSPM中定义的资源类型。要了解您可以为每种资源指定哪些操作，请参阅《Service Authorization Reference》中的 Actions defined by AWS Security Hub CSPM。有关指定资源的策略示例，请参阅 Identity-based 的策略示例 AWS Security Hub CSPM。

Security Hub CSPM 的策略条件密钥

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

有关 Security Hub CSPM 条件键的列表，请参阅《服务授权参考》 AWS Security Hub CSPM中的条件密钥。要了解您可以对哪些操作和资源使用条件键，请参阅 AWS Security Hub CSPM定义的操作。有关使用条件密钥的策略示例，请参阅 Identity-based 的策略示例 AWS Security Hub CSPM。

Security Hub CSPM 中的访问控制列表 (ACL)

支持 ACL：否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

Security Hub CSPM 不支持 ACL，这意味着你无法将 ACL 附加到 Security Hub CSPM 资源。

Attribute-based 使用 Security Hub CSPM 进行访问控制 (ABAC)

支持 ABAC（策略中的标签）：是

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/`*`key-name`*`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

您可以将标签附加到 Security Hub CSPM 资源。您还可以通过在策略的 `Condition` 元素中提供标签信息，控制对资源的访问权限。

有关标记 Security Hub CSPM 资源的信息，请参阅。标记 Security Hub 资源有关基于标签控制资源访问权的基于身份的策略示例，请参阅 Identity-based 的策略示例 AWS Security Hub CSPM。

在 Security Hub CSPM 中使用临时证书

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 AWS STS API 操作来获取临时安全证书GetFederationToken。

Security Hub CSPM 支持使用临时证书。

Security Hub CSPM 的转发访问会话

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

例如， AWS 服务 当你将 Security Hub CSPM 与 AWS Organizations Organiations 中的组织集成以及为组织中的组织指定委派的 Security Hub CSPM 管理员帐户时，Security Hub CSPM 会向下游发出 FAS 请求。

对于其他任务，Security Hub CSPM 使用服务相关角色代表您执行操作。有关此角色的详细信息，请参阅Service-linked 的角色 AWS Security Hub CSPM。

Security Hub CSPM 的服务角色

Security Hub CSPM 不担任或使用服务角色。为了代表您执行操作，Security Hub CSPM 使用服务相关角色。有关此角色的详细信息，请参阅Service-linked 的角色 AWS Security Hub CSPM。

> **Warning**
>
> 更改服务角色的权限可能会给您使用 Security Hub CSPM 带来操作问题。仅当 Security Hub CSPM 提供相关指导时才编辑服务角色。

Service-linked Security Hub CSPM 的角色

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。该服务可以代替您执行操作。 Service-linked 角色出现在您的， AWS 账户 并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

Security Hub CSPM 使用服务相关角色代表你执行操作。有关此角色的详细信息，请参阅Service-linked 的角色 AWS Security Hub CSPM。

Identity-based 的策略示例 AWS Security Hub CSPM

默认情况下，用户和角色无权创建或修改 Security Hub CSPM 资源。他们也无法使用 AWS 管理控制台 AWS CLI、或 AWS API 执行任务。管理员必须创建 IAM policy，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的在 JSON 选项卡上创建策略。

主题

- 策略最佳实践
- 使用 Security Hub CSPM 控制台
- 示例：允许用户查看自己的权限
- 示例：允许用户创建和管理配置策略
- 示例：允许用户查看调查发现
- 示例：允许用户创建和管理自动化规则

策略最佳实践

Identity-based 策略决定是否有人可以在您的账户中创建、访问或删除 Security Hub 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Security Hub CSPM 控制台

要访问 AWS Security Hub CSPM 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Security Hub CSPM 资源的详细信息。 AWS 账户如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保这些用户和角色可以使用 Security Hub CSPM 控制台，还要将以下 AWS 托管策略附加到实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

JSON

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

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

示例：允许用户查看自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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": "*"
        }
    ]
}
```

示例：允许用户创建和管理配置策略

此示例展示了如何创建 IAM 策略以允许用户创建、查看、更新和删除配置策略。此示例策略还允许用户启动、停止和查看策略关联。要使此 IAM 策略发挥作用，用户必须是组织委派的 Security Hub CSPM 管理员。

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": "*"
        }
    ]
}
```

示例：允许用户查看调查发现

此示例说明如何创建允许用户查看 Security Hub CSPM 发现结果的 IAM 策略。

JSON

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

```
}
```

示例：允许用户创建和管理自动化规则

此示例说明如何创建允许用户创建、查看、更新和删除 Security Hub CSPM 自动化规则的 IAM 策略。要使此 IAM 策略发挥作用，用户必须是 Security Hub CSPM 管理员。要限制权限（例如，允许用户仅查看自动化规则），您可以移除创建、更新和删除权限。

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 的角色 AWS Security Hub CSPM

AWS Security Hub CSPM 使用名AWSServiceRoleForSecurityHub为的 AWS Identity and Access Management (IAM) 服务相关角色。此服务相关角色是一个 IAM 角色，直接链接到 Security Hub CSPM。它由 Security Hub CSPM 预定义，它包括 Security Hub CSPM 代表你调用其他资源 AWS 服务 和监控 AWS 资源所需的所有权限。Security Hub CSPM 在 Security AWS 区域 Hub CSPM 可用的所有地方都使用此服务相关角色。

服务相关角色使设置 Security Hub CSPM 变得更加容易，因为您不必手动添加必要的权限。Security Hub CSPM 定义了其服务相关角色的权限，除非另有定义，否则只有 Security Hub CSPM 可以担任该角色。定义的权限包括信任策略和权限策略，您不能将该权限策略附加到任何其他 IAM 实体。

要查看服务相关角色的详细信息，可以使用 Security Hub CSPM 控制台。在导航窗格中的设置下，选择常规。然后，在服务权限部分，选择查看服务权限。

只有在所有启用了 Security Hub CSPM 的区域中禁用 Security Hub CSPM 服务相关角色后，才能将其删除。这样可以保护您的 Security Hub CSPM 资源，因为您不会无意中删除访问这些资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅AWS IAM 用户指南中的与 IAM 配合使用的服务，并在Service-linked 角色列中找到标有 “是” 的服务。选择带有链接的是可以查看该服务的服务相关角色文档。

主题

- Service-linked Security Hub CSPM 的角色权限
- 为 Security Hub CSPM 创建服务相关角色
- 编辑 Security Hub CSPM 的服务相关角色
- 删除 Security Hub CSPM 的服务相关角色

Service-linked Security Hub CSPM 的角色权限

Security Hub CSPM 使用名为的服务相关角色。AWSServiceRoleForSecurityHub这是访问您的资源所需的 AWS Security Hub CSPM 服务相关角色。此服务相关角色允许 Security Hub CSPM 执行任务，例如从他人那里接收调查结果， AWS 服务 并配置必要的 AWS Config 基础架构以运行安全检查以进行控制措施。AWSServiceRoleForSecurityHub 服务关联角色信任 securityhub.amazonaws.com 服务来代入角色。

AWSServiceRoleForSecurityHub 服务相关角色使用托管策略 AWSSecurityHubServiceRolePolicy。

必须授予权限，允许 IAM 身份（如角色、组或用户）创建、编辑或删除服务相关角色。要成功创建AWSServiceRoleForSecurityHub服务相关角色，您用于访问 Security Hub CSPM 的 IAM 身份必须具有所需的权限。要授予所需的权限，请将以下策略附加到 IAM 身份。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

为 Security Hub CSPM 创建服务相关角色

当您首次启用 Security Hub CSPM 或在以前未启用 Security Hub CSPM 的区域启用该角色时，系统会自动创建AWSServiceRoleForSecurityHub服务相关角色。您还可以使用 IAM 控制台、IAM API 或 IAM API 创建 AWSServiceRoleForSecurityHub 服务相关角色。有关手动创建角色的更多信息，请参阅 IAM 用户指南中的创建服务相关角色。

> **Important**
>
> 为 Security Hub CSPM 管理员账户创建的服务相关角色不适用于关联的 Security Hub CSPM 成员账户。

编辑 Security Hub CSPM 的服务相关角色

Security Hub CSPM 不允许你编辑AWSServiceRoleForSecurityHub服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 Security Hub CSPM 的服务相关角色

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

当你禁用 Security Hub CSPM 时，Security Hub CSPM 不会自动为你删除AWSServiceRoleForSecurityHub服务相关角色。如果您再次启用 Security Hub CSPM，则该服务可以重新开始使用现有的服务相关角色。如果您不再需要使用 Security Hub CSPM，则可以手动删除服务相关角色。

> **Important**
>
> 在删除AWSServiceRoleForSecurityHub服务相关角色之前，必须先在启用该角色的所有区域禁用 Security Hub CSPM。有关更多信息，请参阅 禁用 Security Hub CSPM。如果您在尝试删除服务相关角色时未禁用 Security Hub CSPM，则删除将失败。

要删除 AWSServiceRoleForSecurityHub 服务相关角色，您可以使用 IAM 控制台、IAM CLI 或 IAM API。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

AWS Security Hub 的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：AWSSecurityHubFullAccess

您可以将 `AWSSecurityHubFullAccess` 策略附加到 IAM 身份。

此策略授予管理权限，允许主体完全访问所有 Security Hub CSPM 操作。在主体为其账户手动启用 Security Hub CSPM 之前，必须将此策略附加到主体。例如，拥有这些权限的主体可以查看和更新调查发现的状态。他们还可以配置自定义见解、启用集成以及启用和禁用标准和控件。管理员账户的主体也可以管理成员账户。

权限详细信息

该策略包含以下权限：

- `securityhub` – 允许主体完全访问所有 Security Hub CSPM 操作。
- `guardduty`— 允许委托人在 Amazon 中对探测器、组织管理员管理、成员账户管理和组织范围的配置进行完整的生命周期管理。 GuardDuty这包括 API 操作： GetDetector、 ListDetector、 CreateDetector、 UpdateDetector、 DeleteDetector、 EnableOrganizationAdminAccount、、 ListOrganizationAdminAccounts、 CreateMembers、 UpdateOrganizationConfiguration、 DescribeOrganizationConfiguration。
- `iam`— 允许委托人为 Security Hub CSPM 和 Security Hub 创建服务相关角色并获取角色、策略和策略版本。
- `inspector`— 允许委托人在 Amazon Inspector 中获取有关账户状态的信息、启用或禁用、委派管理员管理以及执行组织配置管理。这包括 API 操作： BatchGetAccountStatus、启用、禁用 EnableDelegatedAdminAccount、 DisableDelegatedAdminAccount、、 ListDelegatedAdminAccounts、 UpdateOrganizationConfiguration、 DescribeOrganizationConfiguration。
- `pricing`— 允许校长获取 AWS 服务 和产品的价目表。
- `account`— 允许委托人获取有关账户区域的信息，以支持 Security Hub 中的区域管理。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubFullAccess。

AWS 托管策略：AWSSecurityHubReadOnlyAccess

您可以将 `AWSSecurityHubReadOnlyAccess` 策略附加到 IAM 身份。

此策略授予只读权限，允许用户查看 Security Hub CSPM 中的信息。附加了此策略的主体无法在 Security Hub CSPM 中进行任何更新。例如，拥有这些权限的主体可以查看与其账户关联的调查发现

列表，但不能改变调查发现的状态。他们可以查看见解的结果，但不能创建或配置自定义见解。他们无法配置控件或产品集成。

权限详细信息

该策略包含以下权限：

- `securityhub`：允许用户执行返回项目列表或项目详细信息的操作。这包括以`Get`、`List` 或 `Describe` 开头的 API 操作。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubReadOnlyAccess。

AWS 托管策略：AWSSecurityHubOrganizationsAccess

您可以将 `AWSSecurityHubOrganizationsAccess` 策略附加到 IAM 身份。

该策略授予管理权限，允许其为中的组织启用和管理 Security Hub、Security Hub CSPM、Amazon GuardDuty 和 Amazon Inspector。 AWS Organizations该策略的权限允许组织管理账户为 Security Hub、Security Hub CSPM、Amazon GuardDuty 和 Amazon Inspector 指定委托管理员账户。它们还允许委派管理员账户将组织账户启用为成员账户。

此策略仅为提供权限 AWS Organizations。组织管理账户和委派管理员账户也需要关联操作的权限。这些权限可以使用 `AWSSecurityHubFullAccess` 管理策略来授予。

在管理账户中创建或更新委派管理员策略需要此策略中未提供的其他权限。要执行这些操作，建议为策略添加权限`organizations:PutResourcePolicy`或附加 AWSOrganizationsFullAccess 策略。

权限详细信息

该策略包含以下权限：

- `organizations:ListAccounts`：允许主体检索属于某个组织的账户列表。
- `organizations:DescribeOrganization`：允许主体检索有关组织的信息。
- `organizations:ListRoots`：允许主体列出组织的根。
- `organizations:ListDelegatedAdministrators`：允许主体列出组织的委派管理员。
- `organizations:ListAWSServiceAccessForOrganization`— 允许委托人列出组织使用 AWS 服务 的。
- `organizations:ListOrganizationalUnitsForParent`：允许主体列出父组织单元（OU）的子 OU。

- organizations:ListAccountsForParent：允许主体列出父 OU 的子账户。
- organizations:ListParents – 列出根或组织单元（OU），它们作为指定子 OU 或账户的直接父级。
- organizations:DescribeAccount – 让委托人可以检索有关企业中某个账户的信息。
- organizations:DescribeOrganizationalUnit：允许主体检索有关组织中某个 OU 的信息。
- organizations:ListPolicies – 检索指定类型的组织中所有策略的列表。
- organizations:ListPoliciesForTarget – 列出直接附加到指定的目标根、组织单元（OU）或账户的策略。
- organizations:ListTargetsForPolicy – 列出指定的策略附加到的所有根、组织单元（OU）和账户。
- organizations:EnableAWSServiceAccess – 允许主体启用与 Organions 的集成。
- organizations:RegisterDelegatedAdministrator – 允许主体指定委派管理员账户。
- organizations:DeregisterDelegatedAdministrator – 允许主体移除委派管理员账户。
- organizations:DescribePolicy – 检索有关策略的信息。
- organizations:DescribeEffectivePolicy – 返回指定的策略类型和账户的有效策略的内容。
- organizations:CreatePolicy— 创建指定类型的策略，您可以将其附加到根帐户、组织单位 (OU) 或个人 AWS 账户。
- organizations:UpdatePolicy – 使用新的名称、描述或内容更新现有策略。
- organizations:DeletePolicy – 从您的组织中删除指定的策略。
- organizations:AttachPolicy – 将策略附加到根、组织单元（OU）或单个账户。
- organizations:DetachPolicy – 将策略从目标根、组织单元（OU）或账户分离。
- organizations:EnablePolicyType – 在根中启用一种策略类型。
- organizations:DisablePolicyType – 在根中禁用一种组织策略类型。
- organizations:TagResource – 将一个或多个标签添加到指定的资源。
- organizations:UntagResource – 从指定的资源中移除具有指定密钥的任何标签。
- organizations:ListTagsForResource – 列出附加到指定资源的标签。
- organizations:DescribeResourcePolicy— 检索有关资源策略的信息。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubOrganizationsAccess。

AWS 托管策略：AWSSecurityHubServiceRolePolicy

您不能将 AWSSecurityHubServiceRolePolicy 附加到自己的 IAM 实体。此策略附加到服务相关角色，允许 Security Hub CSPM 代表您执行操作。有关更多信息，请参阅 the section called “Service-linked 角色”。

此策略授予管理权限，允许服务相关角色为 Security Hub CSPM 控件执行运行安全检查等任务。

权限详细信息

该策略包含以下权限：

- cloudtrail— 检索有关 CloudTrail 路径的信息。
- cloudwatch— 检索当前 CloudWatch 警报和连接器运行状况指标。
- logs— 检索 CloudWatch 日志的指标筛选器。
- sns：检索 SNS 主题的订阅列表。
- config— 检索有关配置记录器、资源和 AWS Config 规则的信息。管理 Security Hub CSPM 与服务相关的配置记录器和第三方服务关联的配置记录器。创建和删除 AWS Config 规则，并根据规则进行评估。列出配置记录器并获取连接器信息，以支持第三方云集成。
- iam— 检索和生成账户的凭证报告，并为创建服务相关角色。 AWS Config
- organizations：检索组织的账户和组织单元（OU）信息。
- securityhub – 检索有关如何配置 Security Hub CSPM 服务、标准和控件的信息。
- tag：检索有关资源标签的信息。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSSecurityHubServiceRolePolicy。

Security Hub 更新至 AWS 托管策略

下表提供了自该服务开始跟踪这些更改以来对 Sec AWS urity Hub 和 Security Hub CSPM AWS 托管策略的更新的详细信息。有关策略更新的自动提醒，请订阅 Security Hub 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSSecurityHubServiceRolePolicy - 更新的策略	Security Hub CSPM 更新了政策以支持第三方集成。此更	2026 年 6 月 30 日

更改	描述	日期
	新增加了以下权限：管理第三方配置记录器、列出配置记录器、获取连接器信息以及检索 Connector 运行状况指标。	
AWSSecurityHubServiceRolePolicy - 更新的策略	Security Hub CSPM 更新了策略，增加了管理 Security Hub CSPM 服务相关配置记录器和创建服务相关角色的权限。AWS Config	2026 年 4 月 29 日
AWSSecurityHubOrganizationsAccess - 更新的策略	Security Hub 更新了策略，添加了描述支持 Security Hub 功能的资源策略的权限。Security Hub 目前为预览版，可能会发生变化。	2025 年 11 月 12 日
AWSSecurityHubFullAccess - 更新的策略	Security Hub 更新了政策，增加了管理 GuardDuty 、Amazon Inspector 和账户管理方面的功能，以支持 Security Hub 的功能。Security Hub 目前为预览版，可能会发生变化。	2025 年 11 月 17 日
AWSSecurityHubOrganizationsAccess：对现有策略的更新	Security Hub 为策略添加了新的权限。这些权限允许组织管理层为组织启用和管理 Security Hub 和 Security Hub CSPM。	2025 年 6 月 17 日
AWSSecurityHubFullAccess：对现有策略的更新	Security Hub CSPM 新增了权限，允许主体为 Security Hub 创建服务相关角色。	2025 年 6 月 17 日

更改	描述	日期
AWSSecurityHubFullAccess— 更新现有政策	Security Hub CSPM 更新了政策，以获取 AWS 服务 和产品的定价详情。	2024 年 4 月 24 日
AWSSecurityHubReadOnlyAccess— 更新现有政策	Security Hub CSPM 通过添加 `Sid` 字段更新了此托管策略。	2024 年 2 月 22 日
AWSSecurityHubFullAccess— 更新现有政策	Security Hub CSPM 更新了政策，因此它可以确定账户中是否启用了亚马逊 GuardDuty 和亚马逊 Inspector。这可以帮助客户汇集来自多个 AWS 服务与安全相关的信息。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess— 更新现有政策	Security Hub CSPM 更新了授予额外权限的策略，允许以只读方式访问 AWS Organizations 委派管理员功能。这包括根、组织单元（OU）、账户、组织结构和服务访问权限等详细信息。	2023 年 11 月 16 日
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 添加了 `BatchGetSecurityControls` 、`DisassociateFromAdministratorAccount` 和 `UpdateSecurityControl` 权限，用于读取和更新可自定义的安全控件属性。	2023 年 11 月 26 日
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 添加了 `tag:GetResources` 权限，以读取与调查发现相关的资源标签。	2023 年 11 月 7 日

更改	描述	日期
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 添加了 `BatchGetStandardsControlAssociations` 权限，以获取有关标准中控件的启用状态的信息。	2023 年 9 月 27 日
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 增加了获取 AWS Organizations 数据以及读取和更新 Security Hub CSPM 配置的新权限，包括标准和控制。	2023 年 9 月 20 日
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 将现有 `config:DescribeConfigRuleEvaluationStatus` 权限移至策略中的另一条语句。该 `config:DescribeConfigRuleEvaluationStatus` 权限现已应用于所有资源。	2023 年 3 月 17 日
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 将现有 `config:PutEvaluations` 权限移至策略中的另一条语句。该 `config:PutEvaluations` 权限现已应用于所有资源。	2021 年 7 月 14 日
AWSSecurityHubServiceRolePolicy：对现有策略的更新	Security Hub CSPM 添加了一项新权限，允许服务相关角色将评估结果传递给 AWS Config。	2021 年 6 月 29 日

更改	描述	日期
AWSSecurityHubServiceRolePolicy— 已添加到托管策略列表中	添加了有关托管策略的信息 AWSSecurityHubServiceRolePolicy，该策略由 Security Hub CSPM 服务相关角色使用。	2021 年 6 月 11 日
AWSSecurityHubOrganizationsAccess— 新政策	Security Hub CSPM 添加了一项新策略，该策略授予 Security Hub CSPM 与 Organizations 集成所需的权限。	2021 年 3 月 15 日
Security Hub CSPM 开始跟踪更改	Security Hub CSPM 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 15 日

问题排查 AWS Security Hub CSPM 身份和访问权限

使用以下信息来帮助您诊断和修复在使用 AWS Security Hub CSPM 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Security Hub CSPM 中执行操作
- 我无权执行 iam：PassRole
- 我想以编程方式访问 Security Hub CSPM
- 我是一名管理员，想允许其他人访问 Security Hub CSPM
- 我想允许我以外的人进入 AWS 账户 访问我的 Security Hub CSPM 资源

我无权在 Security Hub CSPM 中执行操作

如果 AWS 管理控制台 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当用户`mateojackson`尝试使用控制台查看有关某的详细信息*`widget`*但没有`securityhub:`*`GetWidget`*权限时，就会出现以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `securityhub:GetWidget` 操作访问 *my-example-widget* 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Security Hub。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Security Hub 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想以编程方式访问 Security Hub CSPM

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS 管理控制台。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
IAM	（推荐）使用控制台凭证作为临时凭证，签署向 AWS CLI、AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line

哪个用户需要编程式访问权限？	目的	方式
		Interface 用户指南》中的“登录 AWS 本地开发”。 • 对于 AWS SDK，请参阅 S AWS DK 和工具参考指南中的登录进行 AWS 本地开发。
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅《软件开发工具包和AWS 工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。

哪个用户需要编程式访问权限？	目的	方式
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

我是一名管理员，想允许其他人访问 Security Hub CSPM

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。

- 通过身份提供者在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对第三方身份提供者创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

我想允许我以外的人进入 AWS 账户 访问我的 Security Hub CSPM 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Security Hub 是否支持这些功能，请参阅 Security Hub 如何与 IAM 协同工作。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的合规性验证 AWS Security Hub CSPM

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

韧性在 AWS Security Hub

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。各区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

中的基础设施安全 AWS Security Hub CSPM

作为一项托管服务 AWS Security Hub CSPM ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Security Hub CSPM。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（短暂的）或 ECDHE（椭圆曲线短暂的 Diffie-Hellman）。 Diffie-Hellman大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

AWS Security Hub CSPM 和接口 VPC 终端节点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点在您 AWS Security Hub CSPM 的 VPC 和之间建立私有连接。接口端点由一项技术提供支持 AWS PrivateLink，该技术使您无需互联网网关、NAT 设备、VPN 连接或 Direct C AWS onnect 连接即可私密访问 Security Hub CSPM API。您的 VPC 中的实例不需要公有 IP 地址即可与 Security Hub CSPM API 通信。您的 VPC 和 Security Hub CSPM 之间的流量不会离开亚马逊网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。有关更多信息，请参阅《Amazon Virtual Private Cloud 指南》中的AWS 服务 使用接口 VPC 终端节点访问和。

Security Hub CSPM VPC 终端节点的注意事项

在为 Security Hub CSPM 设置接口 VPC 终端节点之前，请务必查看亚马逊虚拟私有云指南中的先决条件和其他信息。

Security Hub CSPM 支持从你的 VPC 调用其所有 API 操作。

为 Security Hub CSPM 创建接口 VPC 终端节点

您可以使用亚马逊 VPC 控制台或 AWS Command Line Interface ()AWS CLI为 Security Hub CSPM 服务创建 VPC 终端节点。有关更多信息，请参阅《Amazon Virtual Private Cloud 指南》中的创建 VPC 端点。

使用以下服务名称为 Security Hub CSPM 创建 VPC 终端节点：

`com.amazonaws.region.securityhub`

适*region*用的地区代码在哪里 AWS 区域。

如果您为终端节点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 Security Hub CSPM 发出 API 请求，`securityhub.us-east-1.amazonaws.com`例如美国东部（弗吉尼亚北部）区域。

为 Security Hub CSPM 创建 VPC 终端节点策略

您可以将终端节点策略附加到您的 VPC 终端节点，以控制对 Security Hub CSPM 的访问权限。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon Virtual Private Cloud 指南》中的使用端点策略控制对 VPC 端点的访问。

示例：Security Hub CSPM 操作的 VPC 终端节点策略

以下是 Security Hub CSPM 的端点策略示例。当连接到终端节点时，此策略允许所有委托人访问所有资源上列出的 Security Hub CSPM 操作。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

共享子网

您无法在与您共享的子网中创建、描述、修改或删除 VPC 端点。但是，您可以在与您共享的子网中使用 VPC 端点。有关 VPC 共享的信息，请参阅《Amazon Virtual Private Cloud 指南》中的与其他账户共享 VPC 子网。

使用记录 Security Hub API 调用 CloudTrail

AWS Security Hub CSPM 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Security Hub CSPM 中采取的操作的记录。 CloudTrail 将 Security Hub CSPM 的 API 调用捕获为事件。捕获的调用包含来自 Security Hub CSPM 控制台和代码的 Security Hub CSPM API 操作调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Security Hub CSPM 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 主机上的事件历史记录中查看最新的事件。使用 CloudTrail 收集到的信息，您可以确定向 Security Hub CSPM 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，包括如何配置和启用它，请参阅AWS CloudTrail 用户指南。

Security Hub CSPM 信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Security Hub CSPM 中出现支持的事件活动时，该活动将与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

要持续记录账户中的事件（包括 Security Hub CSPM 的事件），请创建跟踪记录。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。在控制台创建跟踪时，跟踪默认应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

Security Hub CSPM 支持将所有 Security Hub CSPM API 操作作为事件记录在日志中。 CloudTrail 要查看 Security Hub CSPM 操作的列表，请参阅 Security Hub CSPM API 参考。

将以下操作的活动记录到时 CloudTrail，的值将设置`responseElements`为`null`。这样可以确保 CloudTrail 日志中不包含敏感信息。

- `BatchImportFindings`
- `GetFindings`

- `GetInsights`
- `GetMembers`
- `UpdateFindings`

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出
- 请求是使用角色还是联合用户的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

示例：Security Hub CSPM 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该`CreateInsight`操作的 CloudTrail 日志条目。在该示例中，创建了一个名为 `Test Insight` 的见解。将 `ResourceId` 属性指定为 Group by（分组依据）聚合器，并且没有为该见解指定任何可选的筛选条件。有关见解的更多信息，请参阅 在 Security Hub CSPM 中查看见解。

```
{
    "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"
}
```

标记 Security Hub 资源

标签是一个可选标签，您可以定义并分配给 AWS 资源，包括某些类型的 Sec AWS urity Hub CSPM 资源。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。例如，您可以使用标签来区分资源、识别支持某些合规性要求或工作流程的资源或分配成本。

您可以向以下 Security Hub CSPM 资源类型添加标签：

- 自动化规则
- 配置策略
- Hub 资源

标签基础知识

一个资源可具有多达 50 个标签。每个标签都包含您定义的一个标签键和一个可选的标签值。标签键是一种常见的标签，充当更具体的标签值的类别。标签值 充当标签键的描述符。

例如，如果您为不同的环境创建不同的自动化规则（一组自动化规则用于测试账户，另一组用于生产账户），则可以为这些规则分配 `Environment` 标签密钥。关联的标签值可能是`Test`与测试账号关联`Prod`的规则以及与生产账户关联的规则和 OUs。

在为 Sec AWS urity Hub CSPM 资源定义和分配标签时，请记住以下几点：

- 每个资源最多可以有 50 个标签。
- 对于每个资源，每个标签键都必须是唯一的，并且每个标签键只能有一个标签值。
- 标签键和值区分大小写。作为最佳实践，我们建议您定义一个利用标签的策略，并在所有资源中一致地实施该策略。
- 一个标签键最多可包含 128 个 UTF-8 字符。一个标签值最多可包含 256 个 UTF-8 字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @
- 前`aws:`缀保留给使用 AWS。您不能在自己定义的任何标签键或值中使用此前缀。此外，您无法更改或删除使用此前缀的标签键或值。使用此前缀的标签不计入每个资源的 50 个标签限额中。
- 您分配的任何标签仅供您使用， AWS 账户 并且仅适用于您分配标签 AWS 区域 的标记。
- 如果您使用 Security Hub CSPM 为资源分配标签，则这些标签仅应用于适用 AWS 区域内直接存储在 Security Hub CSPM 中的资源。它们不适用于 Security Hub CSPM 在其他 AWS 服务为

您创建、使用或维护的任何关联的支持资源。例如，如果您为更新与 Amazon Simple Storage Service（Amazon S3）相关的调查发现的自动化规则分配标签，则这些标签仅应用于 Security Hub CSPM 中指定区域的自动化规则。它们不适用于您的 S3 存储桶。要同时为关联资源分配标签，您可以使用 AWS Resource Groups 或来存储资源，例如 AWS 服务 ，用于 S3 存储桶的 Amazon S3。为关联资源分配标签可以帮助您识别 Security Hub CSPM 资源的支持资源。

- 如果删除资源，则分配给该资源的所有标签也将被删除。

> **Important**
>
> 不要在标签中存储机密或其他类型的敏感数据。许多人都可以访问标签 AWS 服务，包括 AWS 账单与成本管理。它们不适合用于敏感数据。

要添加和管理 Security Hub CSPM 资源的标签，你可以使用 Security Hub CSPM 控制台、Security Hub CSPM API 或标记 API。 AWS Resource Groups 通过 Security Hub CSPM，在创建资源时，您可以将标签添加到资源中。您还可以为单个现有资源添加和管理标签。借助 Resource Groups，您可以为跨越多个资源的多个现有资源批量添加和管理标签 AWS 服务，包括 Security Hub CSPM。

有关其他标签提示和最佳实践，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

在 IAM policy 中使用标签

开始为资源添加标签后，您可以在 AWS Identity and Access Management （IAM）策略中定义基于标签的资源级权限。通过以这种方式使用标签，您可以精细控制您中的哪些用户和角色 AWS 账户 有权创建和标记资源，以及哪些用户和角色有权更笼统地添加、编辑和删除标签。要基于标签控制访问，您可以在 IAM policy 的条件元素中使用与标签关联的条件密钥。

例如，您可以创建一个 IAM 策略，允许用户拥有对所有 AWS Security Hub CSPM 资源的完全访问权限（如果资源的 `Owner` 标签指定了用户名）：

JSON

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

```
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

如果您定义基于标签的资源级权限，该权限立即生效。这意味着，您的资源在创建后会更安全，而且您可以快速地开始将标签用于新资源。您还可以使用资源级权限来控制哪些标签键和值可以与新的和现有资源关联。有关更多信息，请参阅 IAM 用户指南中的使用标签控制对 AWS 资源的访问权限。

向 Security Hub CSPM 资源添加标签

标签是您可以定义和分配给 AWS 资源的标签，包括某些类型的 Sec AWS urity Hub CSPM 资源。标签可以帮助您以不同的方式识别、分类和管理资源，例如按照用途、所有者、环境或其他标准。例如，您可以使用标签来应用策略、分配成本、区分资源版本，或识别支持特定合规性要求或工作流的资源。

您可以向以下 Security Hub CSPM 资源类型添加标签：

- 自动化规则
- 配置策略
- Hub 资源

一个资源最多可以有 50 个标签。每个标签都包含一个必需的标签键和一个可选的标签值。标签键是一种常见的标记，充当更具体的标签值的类别。标签值 充当标签键的描述符。有关添加标签选项和要求的更多信息，请参阅 标签基础知识。

要向 Security Hub CSPM 资源添加标签，您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。但是控制台不支持向 Hub 资源添加标签。

添加标签后，您可以编辑标签并更改标签键或标签值。

要同时添加或编辑多个 Security Hub CSPM 资源的标签，请使用 AWS Resource Groups Tagging API 的标记操作。

> **Important**
>
> 向资源添加标签可能会影响对该资源的访问。在向资源添加标签之前，请查看任何可能使用标签控制资源访问权限的 AWS Identity and Access Management (IAM) 策略。

Console

向 Security Hub CSPM 资源添加标签（控制台）

创建自动化规则或配置策略时，Security Hub CSPM 控制台会提供向其添加标签的选项。您可以在标签部分中提供标签密钥和标签值。

Security Hub CSPM API

向 Security Hub CSPM 资源添加标签（API）

要创建资源并以编程方式向其添加一个或多个标签，请使用适合您要创建的资源类型的操作：

- 要创建配置策略并向其添加一个或多个标签，请调用 CreateConfigurationPolicyAPI，或者，如果您使用的是 AWS CLI，则运行create-configuration-policy命令。
- 要创建自动化规则并向其添加一个或多个标签，请调用 CreateAutomationRuleAPI，或者，如果您使用的是 AWS CLI，则运行create-automation-rule命令。
- 要启用 Security Hub CSPM 并向Hub资源添加一个或多个标签，请调用 EnableSecurityHubAPI，或者，如果你使用的是 AWS Command Line Interface (AWS CLI)，则运行命令。enable-security-hub

在您的请求中，使用 `tags` 参数指定要添加到资源的每个标签的标签键和可选标签值。该 `tags` 参数指定对象数组。每个对象都指定一个标签密钥及其关联的标签值。

要向现有资源添加一个或多个标签，请使用 Security Hub CSPM API 的TagResource操作，或者，如果您使用的是，则运行 tag-res AWS CLI ource 命令。在您的请求中，指定您要向其添加标签的资源的 Amazon 资源名称（ARN）。使用 `tags` 参数为要添加的每个标签指定标签密钥（`key`）和可选的标签值（`value`）。`tags` 参数指定一个对象数组，每个标签密钥对应一个对象及其关联的标签值。

例如，以下 AWS CLI 命令将带有`Environment`标签值的`Prod`标签密钥添加到指定的配置策略中。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

示例 CLI 命令：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

其中：

- `resource-arn` 指定要向其添加标签的配置策略的 ARN。
- *`Environment`* 是要添加到规则中的标签的标签密钥。
- *`Prod`* 是指定标签键（*`Environment`*）的标签值。

在以下示例中，该命令向配置策略添加了多个标签。

```
$ 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"}'
```

对于 `tags` 数组中的每个对象，都需要 `key` 和 `value` 参数。但是，`value` 实际参数的值可以是空字符串。如果您不想将标签值与标签键相关联，请不要为 `value` 实际参数指定值。例如，以下命令添加一个没有关联标签值的 `Owner` 标签键：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

如果标记操作成功，Security Hub CSPM 将返回一个空的 HTTP 200 响应。否则，Security Hub CSPM 会返回 HTTP 4xx 或 500 响应，说明操作失败的原因。

编辑 Security Hub CSPM 资源的标签

当您的环境或要求随着时间的推移而发生变化时，您可以评估 Sec AWS urity Hub CSPM 资源的现有标签，并根据需要更改标签。标签是一个可选标记，您可以进行定义并将其分配给 AWS 资源，包括某些类型的 Macie 资源。每个标签都包含一个必需的标签键和一个可选的标签值。标签键是一种常见的标记，充当更具体的标签值的类别。标签值 充当标签键的描述符。

标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。例如，您可以使用标签来应用策略、分配成本、区分资源版本，或识别支持特定合规性要求或工作流的资源。

您可以向以下 Security Hub CSPM 资源类型添加标签：

- 自动化规则
- 配置策略
- Hub 资源

要编辑 Security Hub CSPM 资源的标签键或标签值，可以使用 Security Hub CSPM API。Security Hub CSPM 控制台目前不支持标签编辑。

> **Important**
>
> 编辑资源的标签可能会影响对资源的访问权限。在编辑资源的标签之前，请查看任何可能使用标签控制资源访问权限的 AWS Identity and Access Management (IAM) 策略。

Security Hub CSPM API

编辑 Security Hub CSPM 资源的标签（API）

当您以编程方式编辑资源的标签时，将使用新值覆盖现有标签。因此，编辑标签的最佳方法取决于您是要编辑标签键、标签值还是两者兼而有之。要编辑标签密钥，请删除当前标签并添加新标签。

要仅编辑或删除与标签密钥关联的标签值，请使用 Security Hub CSPM TagResourceAPI 的操作覆盖现有值。如果您使用的是 AWS CLI，请运行 tag-resource 命令。在您的请求中，指定要编辑或删除标签值的资源的 Amazon 资源名称（ARN）。

要编辑标签值，请使用 `tags` 参数指定要更改其标签值的标签密钥。您还应该为密钥指定新的标签值。例如，以下 AWS CLI 命令将分配给指定自动化规则`Test`的`Environment`标签键的标签值从`Prod`更改为。此示例的格式适用于 Linux、macOS 或 Unix，它使用了反斜杠 (\) 行继续符来提高可读性。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

其中：

- `resource-arn` 指定配置策略的 ARN。
- *`Environment`* 是与要更改的标签值关联的标签键。
- *`Test`* 是指定标签键（*`Environment`*）的新标签值。

要从标签键中删除标签值，请不要在 `tags` 形式参数中为该标签键的 `value` 实际参数指定值。例如：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

如果操作成功，Security Hub CSPM 将返回空的 HTTP 200 响应。否则，Security Hub CSPM 会返回 HTTP 4xx 或 500 响应，说明操作失败的原因。

查看 Security Hub CSPM 资源的标签

为 Sec AWS urity Hub CSPM 资源添加或编辑标签后，您可以查看资源当前具有的标签键和标签值。标签是一个可选标记，您可以进行定义并将其分配给 AWS 资源，包括某些类型的 Macie 资源。每个标签都包含一个必需的标签键和一个可选的标签值。标签键是一种常见的标记，充当更具体的标签值的类别。标签值 充当标签键的描述符。

标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。例如，您可以使用标签来应用策略、分配成本、区分资源版本，或识别支持特定合规性要求或工作流的资源。

您可以向以下 Security Hub CSPM 资源类型添加标签：

- 自动化规则
- 配置策略
- Hub 资源

您可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API 查看 Security Hub CSPM 自动化规则或配置策略的标签。控制台不支持查看 Hub 资源的标签。您可以通过编程方式查看任何资源的标签。

要同时查看多个 Security Hub CSPM 资源的标签，请使用 AWS Resource Groups Tagging API 的标记操作。

Console

查看 Security Hub CSPM 资源的标签（控制台）

1. 使用 Security Hub CSPM 管理员的凭据，打开 Sec AWS urity Hub CSPM 控制台，网址为。https://console.aws.amazon.com/securityhub/
2. 根据要添加标签的资源类型，请执行以下操作之一：
   - 要查看自动化规则的标签，请在导航窗格中选择自动化。然后，选择自动化规则。
   - 要查看配置策略的标签，请在导航窗格中选择配置。然后，在策略选项卡上，选择配置策略旁边的选项。将打开一个侧面板，其中显示分配给策略的标签数量。您可以展开标签标头以查看标签键和标签值。

标签部分列出当前分配给该资源的所有标签。

Security Hub CSPM API

查看 Security Hub CSPM 资源的标签（API）

要检索和查看现有资源的标签，请调用 ListTagsForResourceAPI。在您的请求中，使用 `resourceArn` 参数指定资源的 Amazon 资源名称（ARN）。

如果您使用的是 AWS CLI，请运行list-tags-for-resource命令并使用`resource-arn`参数指定资源的 ARN。例如：

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

如果操作成功，Security Hub CSPM 将返回一个 `tags` 数组。数组中的每个对象都指定了当前分配给资源的标签（包括标签密钥和标签值）。例如：

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
```

```
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

其中 Environment、CostCenter 和 Owner 是分配给资源的标签键。Prod 是与 Environment 标签键关联的标签值。12345 是与 CostCenter 标签键关联的标签值。Owner 标签密钥没有关联的标签值。

要检索所有带有标签的 Security Hub CSPM 资源以及分配给每个资源的所有标签的列表，请使用 AWS Resource Groups 标记 AP GetResourcesI 的操作。在您的请求中，将 ResourceTypeFilters 参数的值设置为 securityhub。要使用执行此操作 AWS CLI，请运行 get-resou rces 命令并将resource-type-filters参数的值设置为。securityhub例如：

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

如果操作成功，Resource Groups 将返回一个 ResourceTagMappingList 数组。该数组包含每个带有标签的 Security Hub CSPM 资源的一个对象。每个对象都指定 Security Hub CSPM 资源的 ARN 以及分配给该资源的标签键和值。

从 Security Hub CSPM 资源中移除标签

如果您向 Sec AWS urity Hub CSPM 资源添加标签，则随后可以删除其中一个或多个标签。标签是一个可选标记，您可以进行定义并将其分配给 AWS 资源，包括某些类型的 Security Hub CSPM 资源。您可以从以下类型的 Security Hub CSPM 资源中添加、编辑和移除标签：自动化规则、配置策略和 Hub 资源。

要从单个 Sec AWS urity Hub CSPM 资源中删除标签，你可以使用 Security Hub CSPM API。Security Hub CSPM 控制台目前不支持移除标签。

要同时从多个 Security Hub CSPM 资源中移除标签，请使用 AWS Resource Groups Tagging API 的标记操作。

> **Important**
>
> 从资源中删除标签可能对影响资源访问。在移除标签之前，请查看可能使用该标签控制资源访问权限的任何 AWS Identity and Access Management (IAM) 策略。

Security Hub CSPM API

从 Security Hub CSPM 资源中移除标签（API）

要以编程方式从资源中删除一个或多个标签，请使用 Security Hub CSPM API 的UntagResource操作。在请求中，使用 `resourceArn` 参数指定要从中删除标签的资源的 Amazon 资源名称（ARN）。使用 `tagKeys` 形式参数指定要删除的标签的标签键。要删除多个标签，请为要删除的每个标签添加 `tagKeys` 形式参数和实际参数，并用和符号（&）分隔，例如 `tagKeys=`*`key1`*`&tagKeys=`*`key2`* 如果仅从资源中删除特定的标签值（而不是标签键），请编辑标签而不是删除标签。

如果您使用的是 AWS CLI，请运行 untag-resource 命令从资源中移除一个或多个标签。在 `resource-arn` 参数中，指定要从中移除标签的资源的 ARN。使用 `tag-keys` 参数指定要删除的标签的标签键。例如，以下命令从指定配置策略中移除 `Environment` 标签（包括标签键和标签值）：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

其中，`resource-arn` 指定要移除标签的配置策略的 ARN，*`Environment`* 是要移除的标签的标签键。

要从资源中移除多个标签，请添加每个额外的标签密钥作为 `tag-keys` 参数的参数。例如：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

如果操作成功，Security Hub CSPM 将返回空的 HTTP 200 响应。否则，Security Hub CSPM 会返回 HTTP 4xx 或 500 响应，说明操作失败的原因。

Security Hub CSPM 的配额

您的每个配额 AWS 账户 都有特定的默认配额，以前称为限制 AWS 服务。这些限额是您的账户使用的服务资源或操作的最大数量。本主题链接到适用于您的账户的 Sec AWS urity Hub 资源和操作的配额。除非另有说明，否则每个限额均适用于您在每个 AWS 区域中的账户。

一些限额可以提升，而另一些限额不能提升。要请求增加限额，请使用服务限额控制台。要了解如何请求增加限额，请参阅服务限额用户指南中的请求增加限额。如果 Service Quotas 控制台上没有配额，请使用上的 “AWS Support Center Console 提高服务限额” 表单申请增加配额。

最大配额

有关适用于 AWS Security Hub 资源的配额列表，请参阅 AWS 一般参考 中的 AWS Security Hub 端点和限额。

速率配额

有关适用于 AWS Security Hub API 操作的配额列表，请参阅《AWS Security Hub API 参考》。

如果您在 Security Hub CSPM 中设置跨区域聚合，则对 `BatchImportFindings` 和 `BatchUpdateFindings` 的一次调用会影响关联区域和聚合区域。该 `GetFindings` 操作从关联区域和聚合区域检索调查发现。但是，`BatchEnableStandards` 和 `UpdateStandardsControl` 操作是特定于区域的。

的文档历史记录 AWS Security Hub 用户指南

下表描述了自上次发布 Sec AWS urity Hub 和 Security Hub CSPM 以来对文档所做的重要更改。对于新的 Security Hub CSPM 控件的发布，日期指定了这些控件何时开始在支持中可用。 AWS 区域控件可能需要 1-2 周才能在所有受支持的区域中可用。有关现有控件的重大更改的详细信息，请参阅Security Hub CSPM 控件的更改日志。

要接收有关《AWS Security Hub 用户指南》更新的通知，您可以订阅 RSS 源。

变更	说明	日期
托管策略的更新 — AWSSecurityHubV2ServiceRolePolicy	Security Hub 更新了名为的AWS 托管策略AWSSecurityHubV2ServiceRolePolicy 。这些更新增加了支持第三方集成的权限，包括管理第三方配置记录器、创建和管理连接器以及获取用于联合的 Web 身份令牌。	2026 年 6 月 30 日
托管策略的更新 — AWSSecurityHubServiceRolePolicy	Security Hub CSPM 更新了名为的AWS 托管策略。AWSSecurityHubServiceRolePolicy 这些更新增加了支持第三方集成的权限。其中包括管理第三方配置记录器和检索 Connector 运行状况指标。	2026 年 6 月 30 日
更新安全标准和控件	我们取消了 ECS.1 和 RDS.18 控件，并将其从所有适用的标准中删除。由于亚马逊 EC2-Classic 网络已停用，因此无法再在 VPC 外部部署亚马逊关系数据库服务 (Amazon RDS) 实例。	2026年6月5日

CSPM 服务关联录制器的更新	添加了与新的服务关联配置记录器相关的信息，该记录器使 Security Hub CSPM 能够根据资源配置信息执行安全控制检查。	2026年5月27日
未使用的访问发现结果	Security Hub 增加了生成和显示 IAM Access Analyzer 中未使用的访问结果的功能了解 Security Hub 中未使用的访问发现结果	2026年5月19日
新的安全控件	Security Hub CSPM 发布了五个新控件。有些控件支持AWS 基础安全最佳实践 (FSBP) 标准。大多数控件都支持 NIST SP 800-53 Rev. 5 的要求。 • 对于 AWS FSBP 标准，适用控件的 ID 为：BedrockAgentCore.5和。BedrockAgentCore.6 • 对于 NIST SP 800-53 Rev. 5，适用控件的 ID 为：BedrockAgentCore.3、和。BedrockAgentCore.4 SageMaker.18	2026 年 5 月 15 日
托管策略的更新 — AWSSecurityHubServiceRolePolicy	Security Hub CSPM 更新了名为的AWS 托管策略。AWSSecurityHubServiceRolePolicy 这些更新增加了管理 Security Hub CSPM 服务相关配置记录器和创建服务相关角色的权限。AWS Config	2026 年 4 月 29 日

新的安全控件	Security Hub CSPM 发布了四项针对AWS 基础安全最佳实践 (FSB P) 标准的新控件。新的控件是：BedrockAgentCore.1BedrockAgentCore.2、RDS.51、和SageMaker.19。	2026 年 4 月 22 日
新的安全控件	Security Hub CSPM 发布了五项针对AWS 基础安全最佳实践 (FSB P) 标准的新控件。新的控件是：APIGateway.11EC2.183、EKS.9、SageMaker.16、和SageMaker.17。	2026 年 4 月 7 日
更新安全标准和控件	我们停用了 AppSync.1 和 AppSync.6 控件，并将其从AWS 基础安全最佳实践 (FSBP) 标准中删除。 AWS AppSync 现在为所有当前和未来的 API 缓存提供默认加密。	2026年3月9日
更新安全标准和控件	我们停用了该 ECS.1 控件，并从AWS 基础安全最佳实践 (FSBP) 标准和 NIST SP 800-53 Rev. 5 标准中删除了该控件。	2026 年 3 月 4 日
新的安全控件	Security Hub CSPM发布了针对AWS 基础安全最佳实践 (FSB P) 标准的十一种新控件。新的控件是：APIGateway.10、ELB.21、ELB.22、RDS.50、SageMaker.9SageMaker.10SageMaker.11SageMaker.12SageMaker.13SageMaker.14、和SageMaker.15。	2026 年 2 月 16 日

更新安全标准和控件	我们取消了 MQ.3 控件，并从所有适用标准中删除了该控件。由于 Amazon MQ 要求自动升级次要版本，我们停用了该控件。 以前，此控件适用于AWS 基础安全最佳实践 (FSBP) 标准、NIST SP 800-53 Rev. 5 标准和 PCI DSS v4.0.1 标准。	2026 年 1 月 12 日
成本估算器文档的更新	在 Security Hub 成本估算器文档中添加了有关如何授予跨账户访问权限以便在管理账户以外的账户中进行估算的详细信息。	2026 年 1 月 12 日
新的安全控件	Security Hub CSPM 发布了五项针对AWS 基础安全最佳实践 (FSB P) 标准的新控件。新的控件是：CloudFormation.4CloudFront.17、ECS.19、ECS.20、和ECS.21。	2026 年 1 月 6 日
更新安全标准和控件	由于 Amazon MQ 要求自动升级次要版本，我们计划于 2026 年 1 月 12 日停用所有适用标准 MQ.3 并从所有适用标准中删除该控件。目前，该控制适用于AWS 基础安全最佳实践 (FSBP) 标准、NIST SP 800-53 Rev. 5 标准和 PCI DSS v4.0.1 标准。	2025 年 12 月 12 日

Service-Managed 标准版的更新内容： AWS Control Tower	更新了Service-Managed 标准版的内容： AWS Control Tower为在标准版中创建、查看和禁用控件提供了改进的指导 AWS Control Tower。	2025 年 12 月 8 日
新的安全控件	Security Hub CSPM 发布了针对AWS 基础安全最佳实践 (FSB P) 标准的七项新控件。新的控件是：Cognito.4、Cognito.5、Cognito.6、EC2.182、CloudFormation.3、ECS.18、和SES.3。	2025 年 12 月 8 日
Security Hub 正式发布内容已更新	增加了支持 Sec AWS urity Hub 正式发布版本的内容	2025 年 12 月 2 日
Security Hub 的更新内容	为趋势和区域聚合添加了内容。这些更改支持 Security Hub 预览版。	2025 年 11 月 21 日
托管策略的更新 — AWSSecurityHubV2ServiceRolePolicy	Security Hub 更新了名为的AWS 托管策略AWSSecurityHubV2ServiceRolePolicy 。这些更新增加了亚马逊弹性容器注册表、亚马逊的计量功能 AWS Lambda CloudWatch，并 AWS Identity and Access Management 支持 Security Hub 功能。这些更新还增加了对全局 AWS Config 录音机的支持。这些更改支持 Security Hub 预览版。	2025 年 11 月 17 日

托管策略的更新 — AWSSecurityHubOrganizationsAccess	Security Hub 更新了名为的AWS 托管策略AWSSecurityHubOrganizations Access 。更新增加了描述支持 Security Hub 功能的资源策略的权限。这些更改支持 Security Hub 预览版。	2025 年 11 月 17 日
托管策略的更新 — AWSSecurityHubFullAccess	Security Hub 更新了名为的AWS 托管策略AWSSecurityHubFullAccess 。这些更新增加了管理 GuardDuty 、Amazon Inspector 和账户管理方面的功能，以支持 Security Hub 的功能。这些更改支持 Security Hub 预览版。	2025 年 11 月 17 日
更新安全控件	我们更改了 10 个 Security Hub CSPM 控件的严重性：CloudFront.7 CloudTrail.5、ELB.7、 GuardDuty.7、、MQ.3、 Opensearch.10、、RDS.7、 ServiceCatalog.1 SNS.4、和。 SQS.3有关更改的明细，请参阅 Security Hub CSPM 控件的变更日志。	2025 年 11 月 13 日
新的安全控件	Security Hub CSPM 针对 AWS 基础安全最佳实践（FSBP）标准发布了六个新控件。新的控件是：Cognito.3、DMS.13、EC2.181、RDS.43、RDS.47、和RDS.48。	2025 年 10 月 28 日

新的安全标准	Security Hub CSPM 现在提供了与 CIS AWS 基金会基准 v5.0.0 一致的安全标准。这项新标准包括 40 个现有安全控件。这些控件执行自动检查来评估某些资源是否符合框架定义的部分要求。	2025 年 10 月 16 日
新的第三方集成	Elastic 是一种新的第三方集成，可以接收来自 Security Hub CSPM 的调查发现。	2025 年 10 月 3 日
更新安全标准和控件	我们取消了 Redshift.9 和 RedshiftServerless.7 控件，并将其从所有适用的标准中删除。我们停用了这些控件，这是因为 Amazon Redshift 固有的限制导致无法有效修复控件的 `FAILED` 调查发现。 以前，这些控件适用于 AWS 基础安全最佳实践（FSBP）标准和 NIST SP 800-53 Rev. 5 标准。该 Redshift.9 控制也适用于AWS Control Tower 服务管理标准。	2025 年 9 月 24 日
区域可用性	Security Hub CSPM 现已在亚太地区（新西兰）区域推出。有关 Security Hub CSPM 当前可用 AWS 区域 位置的完整列表，请参阅中的 Sec AWS urity Hub 端点和配额。AWS 一般参考	2025 年 9 月 19 日

新的安全控件	Security Hub CSPM 发布了两个针对AWS 基础安全最佳实践 (FSBP) 标准的新控件：和。CloudFront.16RDS.46	2025 年 9 月 3 日
区域可用性	AWS 资源标注标准现已在亚太地区（泰国）和墨西哥（中部）区域可用。	2025 年 8 月 29 日
更新安全标准和控件	由于亚马逊 Redshift 的限制，我们计划在 2025 年 9 月 15 日停用 Redshift.9 和 RedshiftServerless.7 控件，并将其从所有适用标准中删除。当前，这些控件适用于 AWS 基础安全最佳实践（FSBP）标准和 NIST SP 800-53 Rev. 5 标准。该 Redshift.9 控制也适用于AWS Control Tower 服务管理标准。	2025 年 8 月 15 日
ASFF 中的新资源详细信息对象	AWS 安全调查发现格式（ASFF）现在包括 `CodeRepository` 资源对象。此对象提供有关外部代码存储库的详细信息，您已将该代码存储库连接到 AWS 资源并将 Amazon Inspector 配置为扫描漏洞。	2025 年 8 月 1 日
区域可用性	Security Hub CSPM 现已在亚太地区（台北）区域推出。有关 Security Hub CSPM 当前可用的 AWS 区域 的完整列表，请参阅 AWS 一般参考 中的 AWS Security Hub 端点和限额。	2025 年 7 月 23 日

新的第三方集成	Dynatrace 是一种新的第三方集成，可以接收来自 Security Hub CSPM 的调查发现。	2025 年 7 月 18 日
新的安全控件	Security Hub CSPM 发布了 13 个新控件。大多数控件都支持 AWS 基础安全最佳实践（FSBP）标准。有些控件支持 NIST SP 800-53 Rev. 5 要求。 • 对于 AWS FSBP 标准，适用控件的 ID 为：CloudFront.15、、Cognito.2、、EC2.180、ELB.18、MSK.4、MSK.5、MSK.6、RDS.45、、Redsh18S3.25SSM.6、和。SSM.7 • 对于 NIST SP 800-53 Rev. 5，适用控件的 ID 为：和。Lambda.7RDS.45	2025 年 7 月 15 日
更新控件调查发现的生成	为了帮助您跟踪合规性更改，当单个资源的合规性状态发生变化时，Security Hub CSPM 现在会更新现有控件调查发现，而不是生成新的调查发现。这意味着您可以使用各项调查发现提供的数据，根据特定控件跟踪特定资源的合规性变化。	2025 年 7 月 3 日

更新安全标准和控件	我们从 PCI DSS v 4.0.1 标准中删除了该IAM.13控件。我们还从 NIST SP 800-171 修订版 2 标准中删除了该IAM.17控件。这些标准没有明确要求控件提供的检查。我们还针对某些检查 IAM 密码策略的控件更新了这些标准的相关要求详细信息： IAM.7和 IAM.10 通过 IAM.17。	2025 年 6 月 30 日
更新调查发现保留	Security Hub CSPM 现在会将存档的调查发现存储 30 天而不是 90 天，这样可以减少调查发现噪音。要获得长期保留，您可以通过使用带有 Amazon EventBridge 规则的自定义操作将发现结果导出到 S3 存储桶。	2025 年 6 月 20 日
更新为现有托管式策略	Security Hub CSPM 为名为的 `AWSSecurityHubOrganizationsAccess` 的 AWS 托管策略添加了新权限。该权限允许组织管理层在组织内启用和管理 Security Hub 和 Security Hub CSPM。Security Hub CSPM 还为名为的 `AWSSecurityHubFullAccess` 的 AWS 托管策略添加了新权限。该权限允许主体为 Security Hub 创建服务相关角色。	2025 年 6 月 18 日

Security Hub 的公共预览版和新的托管策略	Sec AWS urity Hub 和 S AWS ecurity Hub 用户指南的公开预览版。此版本包括一项新的 AWS 托管策略 `AWSSecurityHubV2ServiceRolePolicy` 。该策略允许 Security Hub 代表客户管理客户组织中的 AWS Config 规则和 Security Hub 资源。Security Hub 目前为预览版，可能会发生变化。	2025 年 6 月 17 日
更新安全标准和控件	我们从 PCI DSS v 4.0.1 标准中删除了该IAM.10控件。此控件检查 IAM 用户的账户密码策略是否满足最低要求，包括密码长度至少为 7 个字符。PCI DSS v4.0.1 现在要求密码至少包含 8 个字符。该 IAM.10 控件继续适用于 PCI DSS v3.2.1 标准，该标准具有不同的密码要求。	2025 年 5 月 30 日
新的安全标准	Security Hub CSPM 现在提供符合 NIST SP 800-171 修订版 2 网络安全和合规性框架的安全标准。这项新标准包括 60 多个现有安全控件。这些控件执行自动检查，评估某些 AWS 服务 资源是否符合框架定义的部分要求。	2025 年 5 月 29 日

更新安全控件	Security Hub CSPM 全面撤销了以下控件的发布 AWS 区域：[RDS.46] 不应将 RDS 数据库实例部署在具有通往互联网网关的路由的公共子网中。以前，此控件支持 AWS 基础安全最佳实践 (FSBP) 标准。	2025 年 5 月 8 日
新的安全控件	Security Hub CSPM 发布了 9 个新控件。大多数控件都支持 AWS 基础安全最佳实践（FSBP）标准。有些控件支持 NIST SP 800-53 Rev. 5 要求。 • 对于 AWS FSBP 标准，适用控件的 ID 为：DocumentDB.6、、RDS.44、RedshiftServerless.2、RedshiftServerless.3RedshiftServerless.5RedshiftServerless.6、和 RedshiftServerless.7（后来停用）。 • 对于 NIST SP 800-53 Rev. 5，适用控件的 ID 为：CloudTrail.10RedshiftServerless.4、和 RedshiftServerless.7（后来停用）。	2025 年 5 月 7 日

新的安全控件	Security Hub CSPM 发布了 24 个新控件。大多数控件都支持 AWS 基础安全最佳实践（FSBP）或 AWS 资源标注标准。有些控件支持 NIST SP 800-53 Rev. 5 要求。 • 对于 AWS FSBP 标准，适用控件的 ID 为：EC2.173、RDS.41RDS.42、和。SageMaker.8 • 对于 AWS 资源标记标准，适用控件的 ID 为：Amplify.1、、、、、、Amplify.2、Batch.4、DataSync.2、EC2.174、EC2.175、EC2.176、、EC2.177、EC2.178、EC2.179、17、SageMaker.6、SageMaker.7、、SSM.5、Transfer.4、Transfer.5、Transfer.6和Transfer.7。 • 对于 NIST SP 800-53 Rev. 5，适用控件的 ID 为：和。ECS.17RDS.42	2025 年 4 月 16 日

新的安全控件	Security Hub CSPM 针对 AWS 基础安全最佳实践标准发布了四个新控件。这些控件是： • the section called “[FSx.3] FSx 对于 OpenZFS 文件系统，应配置为多可用区部署” • the section called “[FSx.4] FSx 对于 NetApp ONTAP 文件系统，应配置为多可用区部署” • the section called “[FSx.5] FSx 对于 Windows 文件服务器，应为多可用区部署配置文件系统” • the section called “[RedshiftServerless.1] 亚马逊 Redshift 无服务器工作组应使用增强型 VPC 路由”	2025 年 3 月 18 日
更新安全标准和控件	我们从《 AWS 基础 RDS.18 安全最佳实践》标准中删除了安全控制（后来停用），并自动检查了 NIST SP 800-53 Rev. 5 的要求。由于亚马逊 EC2-Classic 网络已停用，因此无法再在 VPC 外部部署亚马逊关系数据库服务 (Amazon RDS) 实例。	2025 年 3 月 7 日

更新控件调查发现	现在，如果未为控件所检查的资源类型开启资源记录，Security Hub CSPM 会 AWS Config 为已启用的控件生成WARNING调查结果。这可以帮助您识别和解决安全控件检查中的潜在配置漏洞。	2025 年 2 月 25 日

新的安全控件	Security Hub CSPM 发布了 11 个新控件。这些控件是： • the section called “[Connect .2] Connect 客户实例应启用 CloudWatch 日志记录” • the section called “[ECR.5] ECR 存储库应使用客户托管进行加密 AWS KMS keys” • the section called “[ELB.17] 带有侦听器的应用程序和网络负载均衡器应使用推荐的安全策略” • the section called “[Glue.4] AWS Glue Spark 作业应在支持的版本上运行 AWS Glue” • the section called “[GuardDuty.11] 应启用 “ GuardDuty 运行时监控”” • the section called “[GuardDuty.12] 应启用 GuardDuty ECS 运行时监控” • the section called “[GuardDuty.13] 应启用 GuardDuty EC2 运行时监控” • the section called “[Network Firewall.10] Network Firewall 防火墙应启用子网变更保护” • the section called “[RDS.40] 适用于 SQL Server 数据库实例的 RDS 应将日志发布到 CloudWatch 日志”	2025 年 2 月 24 日

	• the section called “[SQS.3] SQS 队列访问策略不应允许公开访问” • the section called “[Transfer.3] Transfer Family 连接器应启用日志记录”	
新的安全控件	Security Hub CSPM 为 AWS 资源标注标准发布了 37 个新控件。Security Hub CSPM 还发布了以下新控件： • the section called “[EMR.3] Amazon EMR 安全配置应静态加密” • the section called “[EMR.4] Amazon EMR 安全配置应在传输过程中加密” • the section called “[SageMaker.5] SageMaker 模型应启用网络隔离”	2025 年 1 月 22 日
新的安全控件	Security Hub CSPM 发布的 EC2.172 EC2 VPC 阻止公共访问设置应该会阻止互联网网关流量。	2025 年 1 月 15 日

新的安全控件	以下新的 Security Hub CSPM 控件可用。 • the section called “[Cognito.1] Cognito 用户池应激活威胁防护，并采用完全功能强制模式进行标准身份验证” • the section called “[RDS.38] 适用于 PostgreSQL 数据库实例的 RDS 在传输过程中应进行加密” • the section called “[RDS.39] 适用于 MySQL 的 RDS 数据库实例应在传输过程中进行加密” • the section called “[Redshift.16] Redshift 集群子网组应具有来自多个可用区的子网”	2024 年 12 月 17 日
Security Hub CSPM 支持 PCI DSS v4.0.1	Security Hub CSPM 现在支持支付卡行业数据安全标准（PCI DSS）v4.0.1。有关该标准及其适用的控件的更多信息，请参阅 Security Hub CSPM 中的 PCI DSS。	2024 年 12 月 11 日
Security Hub CSPM 收到 GuardDuty 攻击序列结果	Security Hub CSPM 现在会收到来自亚马逊 GuardDuty 扩展威胁检测的攻击序列结果。攻击序列查找详细信息可在 AWS 安全查找格式 (ASFF) 的检测对象中找到。	2024 年 12 月 1 日

新版本支持 Security Hub CSPM AWS 区域	Security Hub CSPM 现已在亚太地区（马来西亚）区域推出。某些安全控件有区域限制。有关此区域不可用的控件列表，请参阅对 Security Hub CSPM 控件的区域限制。	2024 年 11 月 22 日
更改为 Config.1	Security Hub CSPM 将 Config.1 控制的严重性从提高 `MEDIUM`到`CRITICAL`，并为发现失败 Config.1 添加了新的状态代码和状态原因。有关更改的更多信息，请参阅 Security Hub CSPM 控件的更改日志中 2024 年 11 月 20 日的条目。	2024 年 11 月 20 日

新的安全控件	以下新的 Security Hub CSPM 控件可用。这些控件是《 AWS 基础安全最佳实践》和 NIST SP 800-53 Rev. 5 的一部分，它们用于评估您管理的虚拟私有云 (VPC) 是否具有用于或资源的接口 VPC 终端节点。AWS 服务 AWS • the section called “[EC2.55] 应为 VPC 配置用于 ECR API 的接口终端节点” • the section called “[EC2.56] 应为 VPC 配置 Docker Registry 的接口端点” • the section called “[EC2.57] 应为 VPC 配置一个适用于 Systems Manager 的接口端点” • the section called “[EC2.58] VPC 应配置 Systems Manager 事件管理器联系人的接口端点” • the section called “[EC2.60] 应使用 Systems Manager 事件管理器的接口端点配置 VPC”	2024 年 11 月 15 日

新的安全控件	以下新的 Security Hub CSPM 控件可用。 • the section called “[AppSync .1] 应 AWS AppSync 对 API 缓存进行静态加密” • the section called “[AppSync .6] AWS AppSync API 缓存应在传输过程中进行加密” • the section called “[EC2.170] EC2 启动模板应使用实例元数据服务版本 2 (imdsv2)” • the section called “[EC2.171] EC2 VPN 连接应启用日志记录” • the section called “[EFS.8] 应对 EFS 文件系统进行静态加密” • the section called “[KMS.5] KMS 密钥不应可公开访问” • the section called “[SNS.4] SNS 主题访问策略不应允许公共访问”	2024 年 10 月 18 日

新的安全控件	以下新的 Security Hub CSPM 控件可用。 • the section called “[ECS.16] ECS 任务集不应自动分配公有 IP 地址” • the section called “[GuardDuty.7] 应启用 GuardDuty EKS 运行时监控” • the section called “[Kinesis.3] Kinesis 流应有足够的数据留存期” • the section called “[MSK.3] MSK Connect 连接器应在传输过程中进行加密” • the section called “[RDS.36] 适用于 PostgreSQL 数据库实例的 RDS 应将日志发布到日志 CloudWatch” • the section called “[RDS.37] Aurora PostgreSQL 数据库集群应将日志发布到日志 CloudWatch” • the section called “[S3.24] S3 多区域接入点应启用屏蔽公共访问权限设置”	2024 年 10 月 3 日

新的安全控件	以下新的 Security Hub CSPM 控件可用。 • the section called “[Athena.4] Athena 工作组应启用日志记录” • the section called “[CodeBuild.7] 应对 CodeBuild 报告组导出进行静态加密” • the section called “[DataSync.1] DataSync 任务应启用日志记录” • the section called “[EFS.7] EFS 文件系统应启用自动备份” • Glue.2 （已退休） • the section called “[Glue.3] AWS Glue 机器学习转换应在静态时加密” • the section called “[WorkSpaces.1] WorkSpaces 用户卷应在静态时加密” • the section called “[WorkSpaces.2] WorkSpaces 根卷应在静态时加密”	2024 年 8 月 30 日
新调查发现面板	Security Hub CSPM 控制台上的新调查发现面板可帮助您快速对调查发现执行操作、查看资源详细信息和调查发现历史记录，以及找到有关调查发现的其他相关信息。	2024 年 8 月 16 日

更新以 Config.1 控制	该Config.1控件会检查 AWS Config 是否已启用，使用服务相关角色，并记录已启用控件的资源。Security Hub CSPM 添加了一个名为 `includeConfigServiceLinkedRoleCheck` 的自定义控件参数。通过将此参数设置为 `false`，您可以选择不检查 AWS Config 是否使用服务相关角色。	2024 年 8 月 15 日
指定没有关联区域的主区域	现在，您可以创建查找聚合器并建立主区域，而无需将任何聚合器链接 AWS 区域 到主区域。这使您无需指定关联区域即可启用中心配置。	2024 年 7 月 25 日

选择更多区域中可用的控件	以下控件现已在其他版本中提供 AWS 区域，包括美国东部（弗吉尼亚北部）和美国东部（俄亥俄州）。 • the section called “[DataFirehose.1] Firehose 传输流应在静态状态下进行加密” • the section called “[DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权” • the section called “[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制” • the section called “[DMS.12] Redis OSS 的 DMS 端点应启用 TLS” • the section called “[DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密” • the section called “[EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联” • the section called “[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥” • the section called “[FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份” • the section called “[MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch”	2024 年 7 月 15 日

- [MQ.3] Amazon MQ 代理应启用自动次要版本升级
- the section called “[Opensearch.11] OpenSearch 域名应至少有三个专用的主节点”
- the section called “[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口”
- the section called “[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1”
- the section called “[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享”
- the section called “[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接”

新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[GuardDuty.5] 应启 GuardDuty 用 EKS 审核日志监控” • the section called “[GuardDuty.6] 应启用 Lamb GuardDuty da 保护” • the section called “[GuardDuty.8] 应启用 EC2 GuardDuty 恶意软件防护” • the section called “[GuardDuty.9] 应启用 GuardDuty RDS 保护” • the section called “[GuardDuty.10] 应启用 GuardDuty S3 保护” • the section called “[Inspector.1] 应启用 Amazon Inspector EC2 扫描” • the section called “[Inspector.2] 应启用 Amazon Inspector ECR 扫描” • the section called “[Inspector.3] 应启用 Amazon Inspector Lambda 代码扫描” • the section called “[Inspector.4] 应启用 Amazon Inspector Lambda 标准扫描”	2024 年 7 月 11 日

CIS AWS 基金会基准测试版本 3.0.0 发布	Security Hub CSPM 发布了互联网安全中心 (CIS) AWS 基金会基准 v3.0.0。此发行版本包括以下新控件，以及与多个现有控件的映射。 • the section called “[EC2.53] EC2 安全组不应允许从 0.0.0 开始的入口。 0/0 到远程服务器管理端口” • the section called “[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口” • the section called “[IAM.26] 应移除 IAM 中管理的过期 SSL/TLS 证书” • the section called “[IAM.27] IAM 身份不应附加策略 AWSCloud ShellFullAccess” • the section called “[IAM.28] 应启用 IAM Access Analyzer 外部访问分析器” • the section called “[S3.22] S3 通用存储桶应记录对象级写入事件” • the section called “[S3.23] S3 通用存储桶应记录对象级读取事件”	2024 年 5 月 13 日

新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[DataFirehose.1] Firehose 传输流应在静态状态下进行加密” • the section called “[DMS.10] Neptune 数据库的 DMS 端点应启用 IAM 授权” • the section called “[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制” • the section called “[DMS.12] Redis OSS 的 DMS 端点应启用 TLS” • the section called “[DynamoDB.7] DynamoDB Accelerator 集群应在传输过程中进行加密” • the section called “[EFS.6] EFS 挂载目标不应与启动时分配公有 IP 地址的子网相关联” • the section called “[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥” • the section called “[FSx.2] FSx 对于 Lustre 文件系统，应配置为将标签复制到备份” • the section called “[MQ.2] ActiveMQ 代理应将审核日志流式传输到 CloudWatch” • [MQ.3] Amazon MQ 代理应启用自动次要版本升级	2024 年 5 月 3 日

	• the section called “[Opensearch.11] OpenSearch 域名应至少有三个专用的主节点” • the section called “[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口” • the section called “[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1” • the section called “[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享” • the section called “[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接”	
AWS 资源标签标准	Security Hub CSPM 中的 AWS 资源标注标准现已正式发布，同时还有适用于该标准的新控件。	2024 年 4 月 30 日
对现有托管策略的更新	Security Hub CSPM 更新了名为的AWS 托管策略`AmazonSecurityHubFullAccess` ，以获取 AWS 服务 和产品的定价详情。	2024 年 4 月 24 日
In-context 控制参数的配置	如果您使用中心配置，则现在可以从 Security Hub CSPM 控制台上控件的详细信息页面配置上下文中的控件参数。	2024 年 3 月 29 日

对现有托管策略的更新	Security Hub CSPM 通过添加 `Sid` 字段更新了名为 `AWSSecurityHubReadOnlyAccess` 的 AWS 托管策略。	2024 年 2 月 22 日
新的安全控件	应启用 Macie 自动发现敏感数据的控件 [Macie.2] 现已可用。有关此控件的区域限制，请参阅按区域划分的控件可用性。	2024 年 2 月 19 日
Security Hub CSPM 在加拿大西部（卡尔加里）可用	Security Hub CSPM 现已在加拿大西部（卡尔加里）可用。除了某些安全控件外，所有 Security Hub CSPM 功能现已在此区域可用。有关更多信息，请参阅根据区域的控件可用性。	2023 年 12 月 20 日

新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[Backup.1] AWS Backup 恢复点应在静态状态下进行加密” • the section called “[DynamodB.6] DynamoDB 表应启用删除保护” • the section called “[EC2.51] EC2 Client VPN 终端节点应启用客户端连接日志记录” • the section called “[EKS.8] EKS 集群应启用审核日志” • the section called “[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置” • the section called “[FSx.1] FSx 对于 OpenZFS 文件系统，应配置为将标签复制到备份和卷” • the section called “[Macie.1] 应启用 Amazon Macie” • the section called “[MSK.2] MSK 集群应配置增强型监控” • the section called “[Neptune.9] Neptune 数据库集群应跨多个可用区部署” • the section called “[Network Firewall.1] Network Firewall 防火墙应部署在多个可用区域中”	2023 年 12 月 14 日

	• the section called “[Network Firewall.2] 应启用 Network Firewall 日志记录” • the section called “[Opensearch.10] OpenSearch 域名应安装最新的软件更新” • the section called “[PCA.1] 应禁用 AWS 私有 CA 根证书颁发机构” • the section called “[S3.19] S3 接入点已启用屏蔽公共访问权限设置” • the section called “[S3.20] S3 通用存储桶应启用 MFA 删除”	
调查发现富集	Security Hub CSPM 在 AWS 安全查找格式 (ASF F) 中添加了新的查找字段`AwsAccountName` 和。`ApplicationName` `ApplicationArn`	2023 年 11 月 27 日
摘要控制面板的增强功能	现在，您可以在 Security Hub CSPM 控制台的摘要页面上访问更多控制面板小组件，保存控制面板筛选器集以快速关注特定的安全问题，还可以自定义控制面板布局。	2023 年 11 月 27 日
中心配置	中心配置现已可用。通过中心配置，Security Hub CSPM 委派管理员可以跨多个组织账户、组织单元（OU）和区域配置 Security Hub CSPM、标准和控件。	2023 年 11 月 27 日

托管式策略的更新	Security Hub CSPM 为 `AWSSecurityHubServiceRolePolicy` 托管策略添加了新的权限，允许 Security Hub CSPM 读取和更新可自定义的安全控件属性。	2023 年 11 月 26 日
自定义控制参数	现在，您可以为所选 Security Hub CSPM 控件自定义参数值。这可以使特定控件的调查发现与您的业务需求和安全期望更加相关。	2023 年 11 月 26 日
托管式策略的更新	Security Hub CSPM 更新了 `AWSSecurityHubFullAccess` 和 `AWSSecurityHubOrganizationsAccess` 托管策略，允许您分别使用 Security Hub CSPM 功能以及与 AWS Organizations 的集成。	2023 年 11 月 16 日

Service-Managed 标准版中添加的现有安全控制措施： AWS Control Tower	以下现有的 Security Hub CSPM 控件已添加到 Service-Managed 标准版:. 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	2023 年 11 月 14 日

托管式策略更新	Security Hub CSPM 为 `AWSSecurityHubServiceRolePolicy` 托管策略添加了新的标记权限，允许 Security Hub CSPM 读取与调查发现相关的资源标签。	2023 年 11 月 7 日

新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[AppSync.5] 不应使用 API AWS AppSync 密 APIs 钥对 GraphQL 进行身份验证” • the section called “[DMS.6] DMS 复制实例应启用自动次要版本升级” • the section called “[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录” • the section called “[DMS.8] 源数据库的 DMS 复制任务应启用日志记录” • the section called “[DMS.9] DMS 端点应使用 SSL” • the section called “[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开” • the section called “[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch” • the section called “[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护” • the section called “[ECS.9] ECS 任务定义应具有日志配置” • the section called “[EventBridge.3] EventBridge 自定义	2023 年 10 月 10 日

事件总线应附加基于资源的策略”

- the section called “[EventBridge.4] EventBridge 全局端点应启用事件复制”
- the section called “[MSK.1] MSK 集群应在代理节点之间传输时进行加密”
- the section called “[MQ.5] ActiveMQ 代理应使用部署模式 active/standby”
- the section called “[MQ.6] RabbitMQ 代理应使用集群部署模式”
- the section called “[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护”
- the section called “[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志”
- the section called “[RDS.35] RDS 数据库集群应启用自动次要版本升级”
- the section called “[Route53.2] Route 53 公有托管区域应记录 DNS 查询”
- the section called “[WAF.12] AWS WAF 规则应启用指标 CloudWatch”

托管式策略更新	Security Hub CSPM 为 `AWSSecurityHubServiceRolePolicy` 托管策略添加了新的 Organizations 操作，允许 Security Hub CSPM 检索账户和组织单元（OU）信息。我们还添加了新的 Security Hub CSPM 操作，允许 Security Hub CSPM 读取和更新服务配置，包括标准和控件。	2023 年 9 月 27 日

Service-Managed 标准版中添加的现有安全控制措施： AWS Control Tower	以下现有的 Security Hub CSPM 控件已添加到 Service-Managed 标准版:. AWS Control Tower • the section called “[Athena.1] Athena 工作组应进行静态加密” • the section called “[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密” • the section called “[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期” • the section called “[Neptune.1] 应对 Neptune 数据库集群进行静态加密” • the section called “[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch” • the section called “[Neptune.3] Neptune 数据库集群快照不应公开” • the section called “[Neptune.4] Neptune 数据库集群应启用删除保护” • the section called “[Neptune.5] Neptune 数据库集群应启用自动备份” • the section called “[Neptune.6] 应在静态状态下对	2023 年 9 月 26 日

	Neptune 数据库集群快照进行加密” • the section called “[Neptune .7] Neptune 数据库集群应启用 IAM 数据库身份验证” • the section called “[Neptune .8] 应将 Neptune 数据库集群配置为将标签复制到快照” • the section called “[RDS.27] RDS 数据库集群应进行静态加密”	
合并的控制视图和合并的控制结果可在中找到 AWS GovCloud (US)	整合的控件视图和整合的控件调查发现现已在 AWS GovCloud (US) Region中提供。Security Hub CSPM 控制台的控件页面显示了您跨标准的所有控件。每个控件在不同标准中都具有相同的控件 ID。当您启用整合的控件调查发现时，即使一项控件适用于多个启用的标准，您也会收到每项安全检查的单个调查发现。	2023 年 9 月 6 日
中国地区提供整合的控件视图和整合的控件调查发现	整合的控件视图和整合的控件调查发现现已在中国区域提供。Security Hub CSPM 控制台的控件页面显示了您跨标准的所有控件。每个控件在不同标准中都具有相同的控件 ID。当您启用整合的控件调查发现时，即使一项控件适用于多个启用的标准，您也会收到每项安全检查的单个调查发现。	2023 年 8 月 28 日

Security Hub CSPM 已在以色列（特拉维夫）区域可用	Security Hub CSPM 现已在以色列（特拉维夫）可用。除了某些安全控件外，所有 Security Hub CSPM 功能现已在此区域可用。有关更多信息，请参阅根据区域的控件可用性。	2023 年 8 月 8 日

新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[Athena.1] Athena 工作组应进行静态加密” • the section called “[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密” • the section called “[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期” • the section called “[Neptune.1] 应对 Neptune 数据库集群进行静态加密” • the section called “[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch” • the section called “[Neptune.3] Neptune 数据库集群快照不应公开” • the section called “[Neptune.4] Neptune 数据库集群应启用删除保护” • the section called “[Neptune.5] Neptune 数据库集群应启用自动备份” • the section called “[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密”	2023 年 7 月 28 日

	• the section called “[Neptune .7] Neptune 数据库集群应启用 IAM 数据库身份验证” • the section called “[Neptune .8] 应将 Neptune 数据库集群配置为将标签复制到快照” • the section called “[RDS.27] RDS 数据库集群应进行静态加密”	
自动化规则标准的新运算符	现在，您可以将 CONTAINS 和 NOT_CONTAINS 比较运算符用于自动化规则映射和字符串条件。	2023 年 7 月 25 日
自动化规则	Security Hub CSPM 现已提供自动化规则，这些规则会根据您指定的条件自动更新调查发现。	2023 年 6 月 13 日
新的第三方集成	Snyk 是一项新的第三方集成，会将调查发现发送到 Security Hub CSPM。	2023 年 6 月 12 日

Service-Managed 标准版中添加的现有安全控制措施： AWS Control Tower	以下现有的 Security Hub CSPM 控件已添加到 Service-Managed 标准版:. AWS Control Tower • the section called “[Account.1] 应为以下人员提供安全联系信息 AWS 账户” • the section called “[APIGateway.8] API Gateway 路由应指定授权类型” • the section called “[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志” • the section called “[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密” • the section called “[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP” • the section called “[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS” • the section called “[Redshift.10] Redshift 集群应在静态状态下进行加密” • the section called “[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动” • the section called “[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限”	2023 年 6 月 12 日

	• the section called “[WAF.10] AWS WAF Web ACLs 应至少有一个规则或规则组”	
新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度” • the section called “[AppSync.2] AWS AppSync 应该启用字段级日志记录” • the section called “[CloudFront.13] CloudFront 发行版应使用源站访问控制” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch” • the section called “[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys” • the section called “[StepFunctions.1] Step Functions 状态机应该开启日志功能”	2023 年 6 月 6 日
Security Hub CSPM 已在亚太地区（墨尔本）可用	Security Hub CSPM 现已在亚太地区（墨尔本）可用。除了某些安全控件外，所有 Security Hub CSPM 功能现已在此区域可用。有关更多信息，请参阅根据区域的控件可用性。	2023 年 5 月 25 日

调查发现历史记录	Security Hub CSPM 现在可以追踪过去 90 天内调查发现的历史记录。	2023 年 5 月 4 日
新的安全控件	以下新的 Security Hub CSPM 控件可用： • the section called “[EKS.1] EKS 集群终端节点不应公开访问” • the section called “[ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF” • the section called “[Redshift.10] Redshift 集群应在静态状态下进行加密” • the section called “[S3.15] S3 通用存储桶应启用对象锁定”	2023 年 3 月 29 日
扩大对整合的控件调查发现的支持	AWS v2.0.0 上的自动安全响应现在支持整合的控制结果。	2023 年 3 月 24 日
Security Hub CSPM 已推出全新版本 AWS 区域	Security Hub CSPM 现已在亚太地区（海得拉巴）、欧洲（西班牙）和欧洲（苏黎世）可用。这些区域中可用的控件存在限制。	2023 年 3 月 21 日
托管式策略的更新	Security Hub CSPM 更新了 `AWSSecurityHubServiceRolePolicy` 托管策略中的现有权限。	2023 年 3 月 17 日

适用于 NIST 800-53 标准的新安全控件	Security Hub CSPM 添加了以下安全控件，这些控件适用于 NIST 800-53 标准： • the section called “[账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分” • the section called “[CloudWatch.15] CloudWatch 警报应配置指定操作” • the section called “[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留” • the section called “[CloudWatch.17] 应激 CloudWatch 活警报动作” • the section called “[DynamoDB.4] 备份计划中应有 DynamoDB 表” • the section called “[EC2.28] 备份计划应涵盖 EBS 卷” • EC2.29 — EC2 实例应在 VPC 中启动（已停用） • the section called “[RDS.26] RDS 数据库实例应受备份计划的保护” • the section called “[S3.14] S3 通用存储桶应启用版本控制” • the section called “[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录”	2023 年 3 月 3 日

美国国家标准与技术研究院（NIST）800-53 Rev. 5	Security Hub CSPM 现在支持 NIST 800-53 Rev. 5 标准，具有 200 多种适用的安全控件。	2023 年 2 月 28 日
整合的控件视图和整合的控件调查发现	随着整合的控件视图发布，Security Hub CSPM 控制台的控件页面显示了您跨标准的所有控件。每个控件在不同标准中都具有相同的控件 ID。当您启用整合的控件调查发现时，即使一项控件适用于多个启用的标准，您也会收到每项安全检查的单个调查发现。	2023 年 2 月 23 日

新的安全控件	以下新的 Security Hub CSPM 控件可用。某些控件有区域限制。 • the section called “[ElastiCache.1] ElastiCache (Redis OSS) 集群应启用自动备份” • the section called “[ElastiCache.2] ElastiCache 集群应启用自动次要版本升级” • the section called “[ElastiCache.3] ElastiCache 复制组应启用自动故障切换” • the section called “[ElastiCache.4] ElastiCache 复制组应进行静态加密” • the section called “[ElastiCache.5] ElastiCache 复制组在传输过程中应加密” • the section called “[ElastiCache.6] ElastiCache （Redis OSS）早期版本的复制组应启用 Redis OSS 身份验证” • the section called “[ElastiCache.7] ElastiCache 群集不应使用默认子网组”	2023 年 2 月 16 日
新的 ASFF 字段	Security Hub CSPM 在 AWS 安全调查结果格式 (ASFF) 中添加了 ProductFields.ArchivalReasons:0/Description 和 ProductFields.ArchivalReasons:0/ReasonCode 。	2023 年 2 月 8 日

新的 ASFF 字段	Security Hub CSPM 在 AWS 安全调查结果格式 (ASFF) 中添加了 Compliance.AssociatedStandards 和 Compliance.SecurityControlId 。	2023 年 1 月 31 日
漏洞详情现已公布	现在，您可以在 Security Hub CSPM 控制台中查看漏洞详细信息，查看 Amazon Inspector 发送给 Security Hub CSPM 的调查发现。	2023 年 1 月 14 日
Security Hub CSPM 在中东（阿联酋）可用	Security Hub CSPM 现已在中东（阿联酋）可用。有些控件有区域限制。	2023 年 1 月 12 日
添加了与 MetricStream 的第三方集成	Security Hub CSPM 现在支持与除中国以外的所有MetricStream地区的第三方集成。AWS GovCloud (US)	2023 年 1 月 11 日
提高了组织账户限制	Security Hub CSPM 现在支持每个区域每个 Security Hub CSPM 管理员账户最多 11,000 个成员账户。	2022 年 12 月 27 日
ElasticBeanstalk.3 向后滚动	Security Hub CSPM 撤销了控制权 [ElasticBeanstalk.3] Elastic Beanstalk 应该将所有区域的日志从 FSBP 标准流式传输 CloudWatch到。	2022 年 12 月 21 日
Security Hub CSPM 添加了新的安全控件	启用了 FSBP 标准的客户可以使用新的 Security Hub CSPM 控件。某些控件有区域限制。	2022 年 12 月 15 日

即将推出的功能指南	Security Hub CSPM 计划发布两项新功能：整合的控件视图和整合的控件调查发现。这些即将推出的功能可能会影响依赖控件调查发现字段和值的现有工作流程。	2022 年 12 月 9 日
Amazon Security Lake 集成现已推出	Security Lake 现在通过接收 Security Hub CSPM 调查发现来与 Security Hub CSPM 集成。	2022 年 11 月 29 日
Support 对 Service-Managed 标准版的支持： AWS Control Tower	Security Hub CSPM 支持一种名为 “标准” Service-Managed 的新安全标准：。AWS Control Tower AWS Control Tower 管理这个标准。	2022 年 11 月 28 日
CIS AWS 基金会基准测试 v1.4.0 现已在中国地区推出	Security Hub CSPM 现在在中国地区支持 CIS AWS 基金会基准测试版本 1.4.0。	2022 年 11 月 18 日
Jira 服务管理云集成现已推出	Jira 服务管理云现在可以接收除中国区域之外的所有支持区域的 Security Hub CSPM 调查发现。	2022 年 11 月 17 日
AWS IoT Device Defender 集成现已推出	AWS IoT Device Defender 现在将所有可用区域的调查结果发送到 Security Hub CSPM。	2022 年 11 月 17 日
Support 对 CIS AWS 基金会基准测试 v1.4.0	Security Hub CSPM 现在提供支持 CIS Foundations Benchmark v1. AWS 4.0 的安全控制。该标准在除中国区域之外的所有支持区域可用。	2022 年 11 月 9 日

支持 Security Hub CSPM 公告 AWS GovCloud (US)	现在，您可以通过 () 和 () AWS GovCloud 中的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 订阅 Security Hub CSPM 公告，以接收有关 Secur AWS GovCloud it US-West y Hu US-East b CSPM 的通知。	2022 年 10 月 3 日
AWS Security Hub CSPM 添加了新的安全控件	启用了 FSBP 标准的客户可以使用新AutoScaling.9的 Security Hub CSPM 控件。控件可能有区域限制。	2022 年 9 月 1 日
订阅 Security Hub CSPM 公告	现在，您可以通过 Amazon Simple Notification Service（Amazon SNS）订阅 Security Hub CSPM 公告，以接收有关 Security Hub CSPM 的通知。	2022 年 8 月 29 日
跨区域聚合的区域扩展	Cross-Region 现在可以聚合以获取调查结果、最新发现和见解 AWS GovCloud (US)。	2022 年 8 月 2 日
新的第三方产品集成	Fortinet - FortiCNP 是接收 Security Hub CSPM 调查发现的第三方集成，而 JFrog 是将调查发现发送到 Security Hub CSPM 的第三方集成。	2022 年 7 月 26 日
EC2.27 已退休	Security Hub CSPM 已停用 EC2.27 -运行 EC2 实例不应使用密钥对，密钥对以前是 AWS 基础安全最佳实践 (FSBP) 标准中的控件。	2022 年 7 月 20 日

Lambda.2 不再支持 python3.6	Security Hub CSPM 不再支持 python3.6 作为参数 Lambda.2 -Lambda 函数应使用支持的运行时，这是基础安全最佳实践 (FSB P) 标准中的控件。 AWS	2022 年 7 月 19 日
AWS Security Hub CSPM 添加了新的安全控件	启用了 FSBP 标准的客户可以使用新的 Security Hub CSPM 控件。某些控件有区域限制。	2022 年 6 月 22 日
AWS Security Hub CSPM 支持新区域	Security Hub CSPM 现已在亚太地区（雅加达）可用。某些控件在此区域不可用。	2022 年 6 月 7 日
改进了 Sec AWS urity Hub CSPM 和 AWS Config	Security Hub CSPM 用户可以在 Security Hub CSPM 中将 AWS Config 规则评估的结果视为调查结果。	2022 年 6 月 6 日
增加了选择退出自动启用标准的功能	对于已与集成的用户 AWS Organizations，此功能允许您登录 Security Hub CSPM 管理员帐户，并选择新的成员帐户退出自动启用的标准。	2022 年 4 月 25 日
扩展的跨区域聚合	添加了跨区域聚合以控制状态和安全分数。	2022 年 4 月 20 日
CompanyName 现在 ProductName 是顶级属性	添加了新的顶级属性，用于设置与自定义集成关联的公司和产品名称	2022 年 4 月 1 日
在《 AWS 基础安全最佳实践》标准中添加了新的控件	在 AWS 基础安全最佳实践标准中添加了 5 个新控件。	2022 年 3 月 31 日
在 ASFF 中添加了新的资源详细信息对象	在 ASFF 中添加了 `AwsRdsDbSecurityGroup` 资源类型。	2022 年 3 月 25 日

在 ASFF 中添加了其他资源详情	在 `AwsAutoScalingScalingGroup` 、`AwsElbLoadBalancer` 、`AwsRedshiftCluster` 和 `AwsCodeBuildProject` 中添加了更多详细信息。	2022 年 3 月 25 日
在《 AWS 基础安全最佳实践》标准中添加了新的控件	在 AWS 基础安全最佳实践标准中添加了 15 个新控件。	2022 年 3 月 16 日
为 AWS 基础安全最佳实践标准和支付卡行业数据安全标准 (PCI DSS) 添加了新的控件	为亚马逊 OpenSearch 服务、亚马逊 RDS、Amazon EC2、Elastic Load Balancing 和 CloudFront AWS 基础安全最佳实践标准添加了新的控件。还在 PCI DSS 中添加了两个新的 OpenSearch 服务控件。	2022 年 2 月 15 日
在 ASFF 中添加了新字段	添加了新字段：示例。	2022 年 1 月 26 日
增加了与的集成 AWS Health	AWS Health 使用服务到服务事件消息将发现结果发送到 Security Hub CSPM。	2022 年 1 月 19 日
增加了与的集成 AWS Trusted Advisor	Trusted Advisor 将其检查结果作为 Security Hub CSPM 的调查结果发送给 Security Hub CSPM。Security Hub CSPM 将其 AWS 基础安全最佳实践检查结果发送给。 Trusted Advisor	2022 年 1 月 18 日

更新了 ASFF 中的资源详细信息对象	已将 `MixedInstancesPolicy` 和 `AvailabilityZones` 添加到 `AwsAutoScalingAutoScalingGroup` 。已将 `MetadataOptions` 添加到 `AwsAutoScalingLaunchConfiguration` 。已将 `BucketVersioningConfiguration` 添加到 `AwsS3Bucket` 。	2021 年 12 月 20 日
更新了 ASFF 文档的输出	ASFF 属性的描述以前是在一个主题中进行的。现在，每个顶级对象和每个资源详细信息对象都在自己的主题中。ASFF 语法主题包含指向这些主题的链接。	2021 年 12 月 20 日
在 ASFF 中添加了新的资源详细信息对象 AWS Network Firewall	为 AWS Network Firewall，添加了以下资源详细信息对象：`AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy` 、和`AwsNetworkFirewallRuleGroup` 。	2021 年 12 月 20 日
增加了对新版 Amazon Inspector 的支持	Security Hub CSPM 已与新版本的 Amazon Inspector 以及 Amazon Inspector Classic 集成。Amazon Inspector 将调查发现发送到 Security Hub CSPM。	2021 年 11 月 29 日

已更改严重性 EC2.19	EC2.19（安全组不应允许不受限制地访问具有高风险的端口）的严重性从 “高” 更改为 “严重”。	2021 年 11 月 17 日
与 Sonrai Dig 的新集成	Security Hub CSPM 现在提供了与 Sonrai Dig 的集成。Sonrai Dig 监控云环境以识别安全风险。Sonrai Dig 将调查发现发送到 Security Hub CSPM。	2021 年 11 月 12 日
更新了 CIS 2.1 的检查和 CloudTrail.1 控件	除了检查是否存在至少一条多区域 CloudTrail 跟踪外，CIS 2.1 和 CloudTrail.1 现在还要检查至少一个多区域 CloudTrail 跟踪中的`ExcludeManagementEventSources` 参数是否为空。	2021 年 11 月 9 日
添加了对 VPC 端点的支持	Security Hub CSPM 现已与 VPC 终端节点集成 AWS PrivateLink 并支持。	2021 年 11 月 3 日
为 AWS 基础安全最佳实践标准添加了控件	为 Elastic Load Balancing（ELB.2 和 ELB.8）和 AWS Systems Manager（SSM.4）添加了新的控件。	2021 年 11 月 2 日

在 EC2.19 控件检查中添加了端口	EC2.19 现在还会检查安全组是否不允许对以下端口进行不受限制的入口访问：3000（Go、和 Ruby Web 开发框架）Node.js、5000（Python 网络开发框架）、8088（传统 HTTP 端口）和 8888（替代 HTTP 端口）和 8888（替代 HTTP 端口）	2021 年 10 月 27 日
添加了与 Logz.io 云 SIEM 的集成	Logz.io 是 Cloud SIEM 的提供商，它提供日志和事件数据的高级关联，以帮助安全团队实时检测、分析和应对安全威胁。 Logz.io 收到 Security Hub CSPM 的调查结果。	2021 年 10 月 25 日
增加了对调查发现的跨区域聚合的支持	Cross-Region 聚合允许您查看所有发现，而无需更改区域。管理员账户选择聚合区域和关联区域。管理员账户及其成员账户的调查发现从关联的区域汇总到聚合区域。	2021 年 10 月 20 日
更新了 ASFF 中的资源详细信息对象	向 `AwsCloudFrontDistribution` 中添加了查看器证书详细信息。向 `AwsCodeBuildProject` 中添加了更多详细信息。向 `AwsElbV2LoadBalancer` 添加了负载均衡器属性。已将 S3 存储桶所有者账户标识符添加到 `AwsS3Bucket` 。	2021 年 10 月 8 日

向 ASFF 添加了新的资源详细信息对象	向 ASFF 添加了以下新的资源详细信息对象：`AwsEc2VpcEndpointService` 、`AwsEcrRepository` 、`AwsEksCluster` 、`AwsOpenSearchServiceDomain` 、`AwsWafRateBasedRule` 、`AwsWafRegionalRateBasedRule` 、`AwsXrayEncryptionConfig`	2021 年 10 月 8 日
从控件中移除了已弃用的运行时 Lambda.2	在 AWS 基础安全最佳实践标准中，从 [Lambda.2] 中删除的**`dotnetcore2.1`** 运行时 Lambda 函数应使用支持的运行时。	2021 年 10 月 6 日
检查点集成的新名称	与 Check Point Dome9 Arc 的集成现在是 Check Point CloudGuard 姿势管理。集成 ARN 没有改变。	2021 年 10 月 1 日
移除了与 Alcide 的集成	与 Alcide kAudit 的集成已停止。	2021 年 9 月 30 日
已更改严重性 EC2.19	[EC2.19] 安全组不应允许不受限制地访问具有高风险的端口，其严重性已从 “中” 更改为 “高”。	2021 年 9 月 30 日
中国区域 AWS Organizations 现已支持与集成	Security Hub CSPM 与 Organizations 集成功能现已在中国（北京）和中国（宁夏）推出。	2021 年 9 月 20 日

S3.1 和 PCI.S3.6 控件的新 AWS Config 规则	两者兼 S3.1 而有之，并 PCI.S3.6 验证 Amazon S3 阻止公共访问设置是否已启用。这些控件的 AWS Config 规则已从更改`s3-account-level-public-access-blocks` 为`s3-account-level-public-access-blocks-periodic` 。	2021 年 9 月 14 日
从控件中移除了已弃用的运行时 Lambda.2	在 AWS 基础安全最佳实践标准中，从 [] 中删除**`nodejs10.x`** 和**`ruby2.5`**运行时 Lambda.2 Lambda 函数应使用支持的运行时。	2021 年 9 月 13 日
已更改 CIS 2.2 控件的严重性	在 CIS AWS 基金会基准标准中，严重性为 2.2。— 确保启用 CloudTrail 日志文件验证已从 “低” 更改为 “中”。	2021 年 9 月 13 日
已更新 ECS.1 Lambda.2、和 SSM.1 《 AWS 基础安全最佳实践》标准	在 AWS 基础安全最佳实践标准中， ECS.1 现在有一个`SkipInactiveTaskDefinitions` 参数设置为。`true`这样可以确保控件仅检查活动任务定义。对于 Lambda.2，将 Python 3.9 添加到运行时列表中。 SSM.1 现在可以同时检查已停止和正在运行的实例。	2021 年 9 月 7 日
PCI.Lambda.2 控件现在不包括 Lambda @Edge 资源	在支付卡行业数据安全标准 (PCI DSS) 标准中，该 PCI.Lambda.2 控件现在不包括 Lambda @Edge 资源。	2021 年 9 月 7 日

添加了与 HackerOne Vulnerability Intelligence 的集成	Security Hub CSPM 现在提供与 HackerOne Vulnerability Intelligence 的集成。该集成会将调查发现发送到 Security Hub CSPM。	2021 年 9 月 7 日
更新了 ASFF 中的资源详细信息对象	为 AwsKmsKey 添加了 KeyRotationStatus 。对于 AwsS3Bucket ，已添加 AccessControlList 、BucketLoggingConfiguration 、BucketNotificationConfiguration 和 BucketWebsiteConfiguration 。	2021 年 9 月 2 日
向 ASFF 添加了新的资源详细信息对象	在 ASFF 中添加了以下新的资源详细信息对象：AwsAutoScalingLaunchConfiguration 、AwsEc2VpnConnection 和 AwsEcrContainerImage 。	2021 年 9 月 2 日
在 ASFF 中为 Vulnerabilities 对象添加了细节	在 Cvss 中添加了 Adjustments 和 Source。在 VulnerablePackages 中添加了文件路径和包管理器。	2021 年 9 月 2 日
中国区域现已支持 Systems Manager Explorer 和 OpsCenter 集成	Security Hub CSPM 与 SSM Explorer 集成， OpsCenter 现已在中国（北京）和中国（宁夏）提供支持。	2021 年 8 月 31 日

停用控件 Lambda.4	Security Hub CSPM 正在停用控件 [] Lambda.4 Lambda 函数应该配置死信队列。控件停用后，它将不再显示在控制台上，Security Hub CSPM 也不会对其进行检查。	2021 年 8 月 31 日
停用控件 PCI.EC2.3	Security Hub CSPM 正在停用控制权 [PCI.EC2.3] 应删除未使用的 EC2 安全组。控件停用后，它将不再显示在控制台上，Security Hub CSPM 也不会对其进行检查。	2021 年 8 月 27 日
更改了 Security Hub CSPM 将调查发现发送到自定义操作的方式	现在，当您将调查发现发送到自定义操作时，Security Hub CSPM 会在单独的 Security Hub Findings - Custom Action 事件中发送每个调查发现。	2021 年 8 月 20 日
为自定义 Lambda 运行时系统添加了新的合规状态原因代码	添加了新的 `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` 合规状态原因代码。此原因代码表明 Security Hub CSPM 无法对自定义 Lambda 运行时执行检查。	2021 年 8 月 20 日
AWS Firewall Manager 中国区域现已支持集成	Security Hub CSPM 与 Firewall Manager 集成功能现已在中国（北京）和中国（宁夏）推出。	2021 年 8 月 19 日

与 Caveonix Cloud 和 Forcepoint Cloud Security Gateway 的新集成	Security Hub CSPM 现在提供与 Caveonix Cloud 和 Forcepoint Cloud Security Gateway 的集成。这两种集成都会将调查发现发送到 Security Hub CSPM。	2021 年 8 月 10 日
在 ASFF 中添加了新的 CompanyName 、ProductName 和 Region 属性	在 ASFF 的顶层添加了 CompanyName 、ProductName 和 Region 字段。这些字段是自动填充的，除自定义产品集成外，无法使用 BatchImportFindings 或 BatchUpdateFindings 进行更新。在控制台上，调查发现筛选条件使用这些新字段。在 API 中，CompanyName 和 ProductName 筛选条件使用 ProductFields 下方的属性。	2021 年 7 月 23 日
在 ASFF 中添加和更新了资源详细信息对象	添加了新的 AwsRdsEventSubscription 资源类型和资源详细信息。为 AwsEcsService 资源类型添加了资源详细信息。为 AwsElasticsearchDomain 资源详细信息对象添加了属性。	2021 年 7 月 23 日

为 AWS 基础安全最佳实践标准添加了控件	为亚马逊 API Gateway (APIGateway.5)、亚马逊 EC2 ()、亚马逊 ECS (EC2.19)、Elastic Load Balancing (ELB.7)、亚马逊 OpenSearch 服务（通过）、亚马逊 RDS（ES.5 通过 ES.8）、亚马逊 RDS（RDS.16 通过 RDS.23）、亚马逊 Redshift (Redshift.4) 和亚马逊 SQ SQS.1 S () 添加了新的控件。ECS.2	2021 年 7 月 20 日
在服务相关角色托管式策略中移动权限	在托管策略 `AWSSecurityHubServiceRolePolicy` 中移动了 `config:PutEvaluations` 权限，使其适用于所有资源。	2021 年 7 月 14 日
为 AWS 基础安全最佳实践标准添加了控件	为亚马逊 API Gateway (APIGateway.4)、亚马逊 CloudFront（CloudFront.5 和 CloudFront.6）、亚马逊 EC2（EC2.17 和 EC2.18）、亚马逊 ECS (ECS.1)、亚马逊 OpenSearch 服务 (ES.4)、AWS Identity and Access Management (IAM.21)、亚马逊 RDS (RDS.15) 和亚马逊 S3 (S3.8) 添加了新的控件。	2021 年 7 月 8 日

为控件调查发现添加了新的合规状态原因代码	`INTERNAL_SERVICE_ERROR` 表示出现未知错误。`SNS_TOPIC_CROSS_ACCOUNT` 表示 SNS 主题由其他账户拥有。`SNS_TOPIC_INVALID` 表示关联的 SNS 主题无效。	2021 年 7 月 6 日
添加了与聊天应用程序中的 Amazon Q 开发者版的集成	添加了与聊天应用程序中的 Amazon Q 开发者版的集成。Security Hub CSPM 将调查发现发送至聊天应用程序中的 Amazon Q 开发者版。	2021 年 6 月 30 日
为服务相关的角色托管策略添加了新权限	为托管策略 `AWSSecurityHubServiceRolePolicy` 添加了新权限，允许服务相关角色向 AWS Config提供评估结果。	2021 年 6 月 29 日
ASFF 中新增的和更新的资源详细信息对象	为 ECS 群集和 ECS 任务定义添加了新的资源详细信息对象。更新了 EC2 实例对象以列出相关的网络接口。为 API Gateway V2 阶段添加了客户端证书 ID。为 S3 存储桶添加了生命周期配置。	2021 年 6 月 24 日
更新了汇总控件状态和标准安全分数的计算	现在，Security Hub CSPM 每 24 小时计算一次总体控件状态和标准安全分数。对于管理员账户，分数现在反映了每个账户是启用还是禁用了每个控件。	2021 年 6 月 23 日

更新了有关 Security Hub CSPM 处理暂停账户的信息	添加了有关 Security Hub CSPM 如何处理 AWS中被暂停账户的信息。	2021 年 6 月 23 日
添加了选项卡以显示个人管理员账户的启用和禁用控件	对于管理员账户，标准详细信息页面上的主要选项卡包含跨账户的汇总信息。新的为此账户启用和为此账户禁用选项卡列出了为单个管理员账户启用或禁用的账户。	2021 年 6 月 23 日
添加 `java8.al2` 到 `Lambda.2` 的参数	在 AWS 基础安全最佳实践标准中，已`java8.al2` 添加到控件支持的运行时中。`Lambda.2`	2021 年 6 月 8 日
与 NETSCOUT 网络 MicroFocus ArcSight 调查员的新集成	增加了与 NETSCOUT 网络 MicroFocus ArcSight 调查员的集成。 MicroFocus ArcSight 收到 Security Hub CSPM 的调查结果。NETSCOUT 网络调查员将调查发现发送到 Security Hub CSPM。	2021 年 6 月 7 日
为 `AWSSecurityHubServiceRolePolicy` 添加了详细信息	更新了托管式策略部分以添加现有托管式策略 `AWSSecurityHubServiceRolePolicy` 的详细信息，该策略由 Security Hub CSPM 服务相关角色使用。	2021 年 6 月 4 日
与 Jira 服务管理的新集成	Jira 的 AWS 服务管理连接器将调查结果发送到 Jira，并使用它们来创建 Jira 事务。当 Jira 问题更新时，Security Hub CSPM 中的相应调查发现也会更新。	2021 年 5 月 26 日

更新了亚太地区（大阪）区域支持的控件列表	更新了 CIS AWS 基金会标准和支付卡行业数据安全标准 (PCI DSS)，以指明亚太地区（大阪）不支持的控制措施。	2021 年 5 月 21 日
与适用于云的 Sysdig Secure 的新集成	添加了与 Sysdig Secure 云的集成。该集成会将调查发现发送到 Security Hub CSPM。	2021 年 5 月 14 日
为 AWS 基础安全最佳实践标准添加了控件	为 Amazon API Gateway（APIGateway.2 和 APIGateway.3）、 AWS CloudTrail（CloudTrail.4 和）、Amazon EC2（和 CloudTrail.5）、（EC2.15 和 EC2.16）、AWS Elastic Beanstalk（ElasticBeanstalk .1 ）、Amazon RDS AWS Lambda (—Lambda. 4)、Amazon Rds (RDS.12—RDS.14)、Amazon Redshift (Redshift.7)、 AWS Secrets Manager（SecretsManager.3 和 SecretsManager.4）和（ ）添加了新的控件。 ElasticBeanstalk.2 AWS WAF WAF.1	2021 年 5 月 10 日
Amazon RDS 控件的更新 GuardDuty 和	已将 `GuardDuty.1` 和 `PCI.GuardDuty.1` 的严重程度从“中”更改为“高”。向 `RDS.8` 中添加了一个 `databaseEngines` 参数。	2021 年 5 月 4 日

向 ASFF 添加了新的资源详细信息	在中`Resources .Details` ，为 Amazon EC2 网络 ACL、Amazon EC2 子网和 AWS Elastic Beanstalk 环境添加了新的资源详细信息对象。	2021 年 5 月 3 日
添加了控制台字段以提供 Amazon EventBridge 规则的筛选值	Security Hub CSPM EventBridge 规则的新预定义筛选模式提供了可用于指定筛选值的控制台字段。	2021 年 4 月 30 日
添加了与 AWS Systems Manager Explorer 的集成和 OpsCenter	Security Hub CSPM 现在支持与 Systems Manager Explorer 的集成。 OpsCenter该集成接收来自 Security Hub CSPM 的调查发现，并在 Security Hub CSPM 中更新这些调查发现。	2021 年 4 月 26 日
产品集成的新类型	新的集成类型 `UPDATE_FINDINGS_IN_SECURITY_HUB` 表示产品集成更新了从 Security Hub CSPM 收到的调查发现。	2021 年 4 月 22 日
将“主账户”更改为“管理员账户”	术语“主账户”已更改为“管理员账户”。该术语也在 Security Hub CSPM 控制台和 API 中进行了更改。	2021 年 4 月 22 日
更新 APIGateway.1 为用 Websocket 替换 HTTP	更新了的标题、描述和补救措施 APIGateway.1。该控件现在会检查 Websocket API 执行日志记录，而不是 HTTP API 执行日志记录。	2021 年 4 月 9 日

北京和宁夏现已支持亚马逊 GuardDuty 集成	现在，中国（北京）和中国（宁 GuardDuty 夏）区域支持与 Security Hub CSPM 的集成。	2021 年 4 月 5 日
已nodejs14.x 添加到支持的运行时中进行控制 Lambda.2	基础安全最佳实践标准中的 Lambda.2 控件现在支持nodejs14.x 运行时。	2021 年 3 月 30 日
Security Hub CSPM 在亚太地区（大阪）推出	Security Hub CSPM 现已在亚太地区（大阪）区域推出。	2021 年 3 月 29 日
在调查发现详细信息中添加了调查发现提供商字段	在调查发现详细信息面板上，新的调查发现提供商字段部分包含置信度、重要性、相关调查发现、严重性和类型的调查发现提供商值。	2021 年 3 月 24 日
增加了接收来自 Amazon Macie 的敏感调查发现的选项	现在可以将与 Macie 的集成配置为将敏感调查发现发送到 Security Hub CSPM。	2021 年 3 月 23 日
正在过渡到 AWS Organizations 用于账户管理	对于已有管理员账户和成员账户的客户，添加了有关如何从受邀管理账户改为使用 Organizations 管理账户的新信息。	2021 年 3 月 22 日

ASFF 中的新对象用于了解有关 Amazon S3 公共访问屏蔽设置的信息	在 Resources 中，新的 AwsS3AccountPublicAccessBlock 资源类型和详细信息对象提供了有关账户的 Amazon S3 公共访问屏蔽设置的信息。在 AwsS3Bucket 资源详细信息对象中，该 PublicAccessBlockConfiguration 对象提供了 S3 存储桶的公共访问屏蔽设置。	2021 年 3 月 18 日
ASFF 中的新对象允许调查发现提供商更新特定字段	ASFF 中的新 FindingProviderFields 对象用于在 BatchImportFindings 中为 Confidence 、Criticality 、RelatedFindings 、Severity 和 Types 提供值。只能使用 BatchUpdateFindings 更新原始字段。	2021 年 3 月 18 日
ASFF 中资源的新 DataClassification 对象	ASFF 中的新 Resources.DataClassification 对象用于提供有关在资源上检测到的敏感数据的信息。	2021 年 3 月 18 日
为可用的合规性状态代码增添了 CONFIG_RETURNS_NOT_APPLICABLE 值	对于 NOT_AVAILABLE 合规性状态，删除了原因代码 RESOURCE_NO_LONGER_EXISTS 并添加了原因代码 CONFIG_RETURNS_NOT_APPLICABLE 。	2021 年 3 月 16 日

用于与集成的新托管策略 AWS Organizations	新的托管策略 `AWSSecurityHubOrganizationsAccess` 提供组织管理账户和 Security Hub CSPM 委派管理员账户所需的 Organizations 权限。	2021 年 3 月 15 日
托管策略和服务相关角色信息已移至“安全”一章	对有关托管政策的信息进行了修订和扩展。托管策略信息和服务相关角色信息均已移至“安全”一章。	2021 年 3 月 15 日
修订了 CIS 1.1 和 CIS 3.1 — CIS 3.14 控件的严重性	CIS 1.1 和 CIS 3.1 — CIS 3.14 控件的严重性更改为“低”。	2021 年 3 月 3 日
已移除 RDS.11 控件	已从 “基础安全最佳实践” 标准中删除该 RDS.11 控件。	2021 年 3 月 3 日
更新了 Turbot 的集成	Turbot 集成已更新，可以发送和接收调查发现。	2021 年 2 月 26 日
为基础安全最佳实践标准添加了控件	为亚马逊 API Gateway (APIGateway.1)、亚马逊 EC2（EC2.9 和 EC2.10）、亚马逊弹性文件系统 ()、亚马逊 OpenSearch 服务（ES.2 和 EFS.2 ES.3）、Elastic Load Balancing (ELB.6) 和 AWS Key Management Service () (AWS KMS KMS.3) 添加了新的控件。	2021 年 2 月 11 日
在 `DescribeProducts` API 中添加了可选 `ProductArn` 筛选条件	`DescribeProducts` API 操作现在包含一个可选 `ProductArn` 参数。`ProductArn` 参数用于标识要返回其详细信息的特定产品集成。	2021 年 2 月 3 日

云存储安全与适用于 Amazon S3 的防病毒软件的新集成	与 Amazon S3 防病毒软件的集成会将病毒扫描结果作为调查发现发送到 Security Hub CSPM。	2021 年 1 月 27 日
更新了管理员账户的安全评分计算流程	对于管理员账户，Security Hub CSPM 使用单独的流程来计算安全分数。新流程可确保评分包括对成员账户启用但对管理员账户禁用的控件。	2021 年 1 月 21 日
ASFF 中的新字段和对象	添加了一个新 `Action` 对象来跟踪对资源执行的操作。在 `AwsEc2NetworkInterface` 对象中添加了用于跟踪 DNS 名称和 IP 地址的字段。在资源详细信息中添加了一个新 `AwsSsmPatchCompliance` 对象。	2021 年 1 月 21 日
为基础安全最佳实践标准添加了控件	为亚马逊 CloudFront（CloudFront.1 通过 CloudFront.4）、亚马逊 DynamoDB（通过）、Elastic Load BalancingDynamoDB.1（ DynamoDB.3直通）、亚马逊 RDSELB.3（直通 ELB.5）、亚马逊 RedshiftRDS.9（ RDS.11通过和）和亚马逊 SNSRedshift.1（ Redshift.3 ）添加了新的控件。 Redshift.6 SNS.1	2021 年 1 月 15 日

根据记录状态或合规性状态重置工作流状态	如果存档的调查发现处于活动状态，或者调查发现的合规性状态从 PASSED 更改为 FAILED、WARNING 或 NOT_AVAILABLE ，Security Hub CSPM 会自动将工作流状态从 NOTIFIED 或 RESOLVED 重置为 NEW。这些变化表明需要进一步调查。	2021 年 1 月 7 日
为基于控件的调查发现添加了 ProductFields 信息	对于通过控件生成的调查结果，添加了有关 AWS 安全查找结果格式 (ASFF) 中ProductFields 对象内容的信息。	2020 年 12 月 29 日
托管见解的更新	更改了 见解 5 的标题。添加了新的见解 32，用于检查是否存在可疑活动的 IAM 用户。	2020 年 12 月 22 日
更新 IAM.7 和 Lambda.1 控件	在 AWS 基础安全最佳实践标准中，更新了的参数。IAM.7更新了的标题和描述 Lambda.1。	2020 年 12 月 22 日
扩展了与 ServiceNow ITSM 的集成	ServiceNow ITSM 集成允许用户在收到 Security Hub CSPM 调查结果时自动创建事件或问题。对这些事件或问题的更新会导致对 Security Hub CSPM 中调查发现进行更新。	2020 年 12 月 11 日

与 Audit Manag AWS er 的新集成	Security Hub CSPM 现在提供与 Audit Manager 的集成 AWS 。该集成允许 Audit Manager 接收来自 Security Hub CSPM 的基于控件的调查发现。	2020 年 12 月 8 日
与 Aqua 安全的新集成 Kube-bench	Security Hub CSPM 增加了与 Aqua Security 的集成。 Kube-bench该集成会将调查发现发送到 Security Hub CSPM。	2020 年 11 月 24 日
云托管现已在中国区域推出	与云托管的集成，现已在中国（北京）和中国（宁夏）区域推出。	2020 年 11 月 24 日
BatchImportFindings 现在可以用来更新其他字段	以前，您无法使用 BatchImportFindings 更新 Confidence 、Criticality 、RelatedFindings 、Severity 和 Types 字段。现在，如果这些字段尚未由 BatchUpdateFindings 更新，则可以通过 BatchImportFindings 进行更新。它们一旦被 BatchUpdateFindings 更新，就不能由 BatchImportFindings 更新。	2020 年 11 月 24 日

Security Hub CSPM 现已与 AWS Organizations	客户现在可以使用他们的 Organizations 账户配置来管理成员账户。组织管理账户指定 Security Hub CSPM 管理员账户，该账户确定要在 Security Hub CSPM 中启用哪些组织账户。对于不属于组织的账户，仍可使用手动邀请流程。	2020 年 11 月 23 日
删除了高容量控件的单独调查发现列表格式	当存在大量调查发现时，控件的调查发现列表不再使用调查发现页面格式。	2020 年 11 月 19 日
新的和更新的第三方集成	Security Hub CSPM 现在支持与 cloudtamer.io、3CoreSec、Prowler 和 Kubernetes Security 集成。 StackRox IBM QRadar 不再发送调查发现。它只接收调查发现。	2020 年 10 月 30 日
添加了从控件详细信息页面下载调查发现列表的选项。	在控件详细信息页面上，新的下载选项允许您将调查发现列表下载到 .csv 文件。下载的列表会考虑列表中的所有筛选条件。如果您选择了特定的调查发现，则下载的列表仅包含这些调查发现。	2020 年 10 月 26 日
添加了从标准详细信息页面下载控件列表的选项。	在标准详细信息页面上，新的下载选项允许您将控制列表下载到 .csv 文件。下载的列表会考虑列表中的所有筛选条件。如果您选择了特定控件，则下载的列表仅包含该控件。	2020 年 10 月 26 日

新增的和更新的合作伙伴集成	Security Hub CSPM 现已与集成。 ThreatModeler更新了以下合作伙伴集成，以反映他们的新产品名称。Twistlock 企业版现在是 Palo Alto Networks-Prisma Cloud Compute。Demisto 同样来自 Palo Alto Networks，现在是 Cortex XSOAR，Redlock 现在是 Prisma Cloud Enterprise。	2020 年 10 月 23 日
Security Hub CSPM 在中国（北京）和中国（宁夏）推出	Security Hub CSPM 现已在中国（北京）和中国（宁夏）区域推出。	2020 年 10 月 21 日
修改了 ASFF 属性和第三方集成的格式	ASFF 属性和合作伙伴集成现在使用基于列表的格式，而不是表格。ASFF 语法、属性和类型分类法现在位于不同的主题中。	2020 年 10 月 15 日
重新设计的标准详情页面	启用标准的标准详细信息页面现在会显示选项卡式控件列表。这些选项卡根据控件状态筛选控制列表。	2020 年 10 月 7 日
将 CloudWatch 事件替换为 EventBridge	将提及亚马逊 CloudWatch 活动的内容替换为亚马逊 EventBridge。	2020 年 10 月 1 日

与 Blue Hexagon AWS、Alcide kAudit 和 Palo Alto Networks 的新集成。 VM-Series	Security Hub CSPM 现已与 Blue Hexagon AWS、Alcide kAudit 和 Palo Alto Networks 集成。 VM-SeriesBlue Hexagon for AWS 和 kAudit 将调查结果发送给 Security Hub CSPM。 VM-Series 收到 Security Hub CSPM 的调查结果。	2020 年 9 月 30 日
ASFF 中新增和更新的资源详细信息对象	为 `AwsApiGatewayRestApi` 、`AwsApiGatewayStage` 、`AwsApiGatewayV2Api` 、`AwsApiGatewayV2Stage` 、`AwsCertificateManagerCertificate` 、`AwsElbLoadBalancer` 、`AwsIamGroup` 和 `AwsRedshiftCluster` 添加了新 `Resources.Details` 对象。为 `AwsCloudFrontDistribution` 、`AwsIamRole` 和 `AwsIamAccessKey` 对象添加了详细信息。	2020 年 9 月 30 日
ASFF 中资源的新 `ResourceRole` 属性，用于跟踪资源是角色还是目标。	资源的 `ResourceRole` 属性表示资源是调查发现活动的目标还是调查发现活动的实施者。有效值为 `ACTOR` 和 `TARGET`。	2020 年 9 月 30 日

在可用的 AWS 服务集成中添加了 AWS Systems Manager 补丁管理器	AWS Systems Manager 补丁管理器现已与 Security Hub CSPM 集成。当客户实例集中的实例不符合其补丁合规性标准时，补丁管理器会将调查发现发送到 Security Hub CSPM。	2020 年 9 月 22 日
在《 AWS 基础安全最佳实践》标准中添加了新的控件	为以下服务添加了新的控件：亚马逊 EC2（EC2.7 和 EC2.8）、亚马逊 EMR (EMR.1)、IAM (IAM.8)、Amazon RDS（RDS.4 通过 RDS.8）、Amazon S3 (S3.6) 和 AWS Secrets Manager（SecretsManager.1 和 SecretsManager.2）。	2020 年 9 月 15 日
用于控制 `BatchUpdateFindings` 字段访问权限的 IAM policy 的新上下文密钥	现在可以将 IAM policy 配置为在使用 `BatchUpdateFindings` 时限制对字段和字段值的访问。	2020 年 9 月 10 日
扩大了成员账户 `BatchUpdateFindings` 的访问权限	默认情况下，成员账户现在拥有与管理员账户相同的 `BatchUpdateFindings` 访问权限。	2020 年 9 月 10 日
《基础安全最佳实践标准》AWS KMS 中的新控件	在《基础安全最佳实践标准》中添加了两个新控件（KMS.1 和 KMS.2）。新的控制措施会检查 IAM 策略是否限制对 AWS KMS 解密操作的访问。	2020 年 9 月 9 日
删除了账户级别的控件调查发现	Security Hub CSPM 不再为控件生成账户级别的调查发现。仅生成资源级别的调查发现。	2020 年 9 月 1 日

ASFF 中的新 PatchSummary 对象	已将 `PatchSummary` 对象添加到 ASFF 中。`PatchSummary` 对象提供有关资源相对于所选合规性标准的补丁合规性的信息。	2020 年 9 月 1 日
重新设计的控件详情页面	重新设计了控件详细信息页面。控件调查发现列表提供选项卡，允许您根据合规性状态快速筛选列表。您还可以快速查看隐藏的调查发现。每个条目都允许访问有关查找资源、AWS Config 规则和查找结果注释的其他详细信息。	2020 年 8 月 28 日
新的调查发现筛选选项	对于调查发现筛选条件，可以使用 is not 筛选条件来查找字段值不等于筛选条件值的调查发现。您可以使用 does not start with 来查找字段值不是以指定筛选值开头的调查发现。	2020 年 8 月 28 日
ASFF 中的新资源详细信息对象	为以下资源类型添加了新 `Resources.Details` 对象：`AwsDynamoDbTable` 、`AwsEc2Eip` 、`AwsIamPolicy` 、`AwsIamUser` 、`AwsRdsDbCluster` 、`AwsRdsDbClusterSnapshot` 、`AwsRdsDbSnapshot` 、`AwsSecretsManagerSecret`	2020 年 8 月 18 日

与 RSA Archer 的新集成	Security Hub CSPM 现已与 RSA Archer 集成。RSA Archer 从 Security Hub CSPM 接收调查发现。	2020 年 8 月 18 日
的新描述字段 AwsKmsKey	为 `Resources.Details` 下面的 `AwsKmsKey` 对象添加了一个 `Description` 字段。	2020 年 8 月 18 日
向添加了字段 AwsRdsDbInstance	为 `Resources.Details` 下面的 `AwsRdsDbInstance` 对象添加了几个属性。	2020 年 8 月 18 日
更新了 Security Hub CSPM 确定控件总体状态的方式	对于没有调查发现的控件，状态为无数据，而不是未知。控制状态包括账户级别和资源级别的调查发现。控制状态不使用调查发现的工作流状态，但忽略隐藏的调查发现除外。	2020 年 8 月 13 日
更新了 Security Hub CSPM 计算标准安全分数的方式	在计算标准的安全分数时，Security Hub CSPM 现在会忽略状态为无数据的控件。安全分数是已通过的控件与已启用的控件的比例，不包括没有数据的控件。	2020 年 8 月 13 日
在已启用的标准中自动启用新控件的新选项	添加了设置选项，以自动启用已启用的标准中的新控件。您还可以使用 `UpdateSecurityHubConfiguration` API 操作配置此选项。	2020 年 7 月 31 日

支付卡行业数据安全标准（PCI DSS）标准的新控件	在 PCI DSS 标准中添加了新的控件。新控件的标识符是 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、和 PCI.SSM.3。	2020 年 7 月 29 日
基础安全最佳实践标准中新增的和更新的控件	在基础安全最佳实践标准中添加了新的控件。新控件的标识符是 AutoScaling.1 DMS.1、EC2.4、 EC2.6、 S3.5、和 SSM.3。更新了标题 ACM.1 并将`daysToExpiration` 参数的值更改为 30。	2020 年 7 月 29 日
ASFF 中的新 `Vulnerabilities` 对象	添加了 `Vulnerabilities` 对象，该对象提供与调查发现相关的漏洞的相关信息。	2020 年 7 月 1 日
ASFF 中适用于自动扩缩组、EC2 卷和 EC2 VPC 的新 `Resource.Details` 对象	在 `Resource.Details` 中新增了 `AwsAutoScalingAutoScalingGroup` 、`AWSEc2Volume` 和 `AwsEc2Vpc` 对象。	2020 年 7 月 1 日
ASFF 中的新 `NetworkPath` 对象	添加了 `NetworkPath` 对象，它提供与调查发现相关的网络路径的相关信息。	2020 年 7 月 1 日
当 `Compliance.Status` 为 `PASSED` 时自动解决发现的问题	对于来自控件的调查发现，如果 `Compliance.Status` 是 `PASSED`，则 Security Hub CSPM 会自动将 `Workflow.Status` 设置为 `RESOLVED`。	2020 年 6 月 24 日

AWS Command Line Interface 例子	为多个 Security Hub CSPM 任务添加了 AWS CLI 语法和示例。包括启用 Security Hub CSPM、管理见解、管理标准和控件、管理产品集成以及禁用 Security Hub CSPM。	2020 年 6 月 24 日
ASFF 中的新 Severity.Original 属性	添加了 Severity.Original 属性，该属性是来自调查发现提供商的原始严重性。这将替代已弃用的 Severity.Product 属性。	2020 年 5 月 20 日
ASFF 中的新 Compliance.StatusReasons 对象，与控件状态的详细信息有关	添加了 Compliance.StatusReasons 对象，该对象为控制的当前状态提供了附加上下文。	2020 年 5 月 20 日
新的 AWS 基础安全最佳实践标准	添加了新的 AWS 基础安全最佳实践标准，该标准是一组控件，用于检测您部署的账户和资源何时偏离安全最佳实践。	2020 年 4 月 22 日
用于更新调查发现工作流状态的新控制台选项	添加了有关使用 Security Hub 控制台或 API 设置调查发现的工作流状态的信息。	2020 年 4 月 16 日
用于客户更新调查发现的新 BatchUpdateFindings API	添加了有关使用 BatchUpdateFindings 更新与某个调查发现的调查过程相关的信息的信息。BatchUpdateFindings 替换了 UpdateFindings ，后者已被弃用。	2020 年 4 月 16 日

AWS 安全调查结果格式 (ASFF) 的更新	添加了几种新的资源类型。向 Severity 对象添加了一个新的 Label 属性。Label 将用于替换 Normalized 字段。添加了一个新的 Workflow 对象来跟踪调查过程以获得调查发现。Workflow 包含一个 Status 属性，该属性将替换现有的 Workflowstate 属性。	2020 年 3 月 12 日
对“集成”页面的更新	已更新以反映对集成页面的更改。对于每个集成，此页面现在显示集成类别，以及每个集成是向 Security Hub CSPM 发送调查发现还是从中接收调查发现。它还提供了启用每个集成所需的特定步骤。	2020 年 2 月 26 日
新的第三方产品集成	添加了以下新产品集成：Cloud Custodian、FireEye Helix、Forcepoint CASB、Forcepoint DLP、Forcepoint NGFW、Rackspace 云原生安全和 Cognito Detect。Vectra.ai	2020 年 2 月 21 日
支付卡行业数据安全标准（PCI DSS）的新安全标准	为支付卡行业数据安全标准（PCI DSS）添加了 Security Hub CSPM 安全标准。如果启用了该标准，Security Hub CSPM 将针对与 PCI DSS 要求相关的控件执行自动检查。	2020 年 2 月 13 日

AWS 安全调查结果格式 (ASFF) 的更新	为标准控制的相关要求添加了一个字段。添加了新的资源类型和新的资源详细信息。ASFF 现在还允许您提供最多 32 个资源。	2020 年 2 月 5 日
禁用各个安全标准控件的新选项	添加了有关如何控制是否启用每个单独的安全标准控制的信息。	2020 年 1 月 15 日
更新 Security Hub CSPM 概念	更新了一些描述并向 Security Hub CSPM 概念添加了新术语。	2019 年 9 月 21 日
AWS Security Hub CSPM 正式发布版本	更新内容以反映 Beta 测试期间对 Security Hub CSPM 所做的改进。	2019 年 6 月 25 日
为 CIS AWS 基金会检查添加了补救步骤	在 Security Hub CSPM 支持 AWS 的安全标准中添加了补救步骤。	2019 年 4 月 15 日
Sec AWS urity Hub CSPM 的测试版	发布了 AWS Security Hub CSPM 用户指南的测试版。	2018 年 11 月 18 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。