
Amazon Security Hub

用户指南

亚马逊云科技

The Amazon logo, a curved orange arrow pointing from left to right, is positioned below the Chinese text.

Amazon Security Hub: 用户指南

Copyright © 2022 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 拥有的其它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。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 [中国的 Amazon Web Services 服务入门 \(PDF\)](#)。

Table of Contents

是什么AmazonSecurity Hub ?	1
Security Hub 的好处	1
减少了收集结果并确定其优先次序的工作	1
根据最佳实践和标准进行自动安全检查	1
跨账户和提供商的结果的综合视图	1
自动修复结果的能力	1
Security Hub 的工作原理	1
Security Hub 免费试用、使用和定价	2
查看使用详细信息和预计成本	2
查看定价详细信息	2
术语和概念	3
先决条件和建议	7
使用Organizations	7
启用 Amazon Config	7
如何启用Amazon Config	8
在中配置资源记录Amazon Config	8
设置 Security Hub	10
手动启用 Security Hub	10
将所需的 IAM 策略附加到 IAM 身份	10
启用 Security Hub (控制台)	11
启用 Security Hub (Security Hub API) Amazon CLI)	11
启用 Security Hub (多账户脚本)	12
分配给 Security Hub 的服务相关角色	12
安全性	13
数据保护	13
Amazon Identity and Access Management	14
Audience	14
使用身份进行身份验证	14
Amazon Web Services 账户根用户	15
IAM 用户和组	15
IAM 角色	15
使用策略管理访问	16
Amazon Security Hub 如何与 IAM 协同工作	17
使用服务相关角色	22
Security Hub 的服务相关角色权限	22
为 Security Hub 创建服务相关角色	23
编辑 Security Hub 的服务相关角色	23
删除 Security Hub 的服务相关角色	23
Amazon托管策略	24
AWSSecurityHubFullAccess	24
AWSSecurityHubReadOnlyAccess	25
AWSSecurityHubOrganizationsAccess	25
AWSSecurityHubServiceRolePolicy	26
策略更新	27
合规性验证	28
基础设施安全性	28
VPC 终端节点 (Amazon PrivateLink)	29
Security Hub VPC 终端节点的注意事项	29
为 Security Hub 创建接口 VPC 终端节点	29
为 Security Hub 创建 VPC 终端节点策略	29
管理账户	31
管理员-成员关系的影响	31
限制和建议	31
成员账户的最大数量	31

账户和区域	32
管理员与成员关系的限制	32
跨服务协调管理员账户	32
向 Organizations 过渡	32
为您的组织指定 Security Hub 管理员账户	33
启用组织账户作为成员账户	33
允许的账户操作	34
指定 Security Hub 管理员帐户	34
Security Hub 管理员帐户的方式	35
配置 Security Hub 管理员帐户所需的权限	36
指定 Security Hub 管理员帐户 (控制台)	36
指定 Security Hub 管理员帐户 (Security Hub API) Amazon CLI)	37
删除 Security Hub 管理员帐户 (控制台)	37
删除 Security Hub 管理员帐户 (Security Hub API) Amazon CLI)	37
删除委派管理员帐户 (Organizations API , Amazon CLI)	38
管理组织成员账户	38
自动启用新账户	39
启用成员账户	40
取消成员账户的关联	41
通过邀请管理会员账户	41
添加和邀请会员账户	42
响应邀请	44
取消成员账户的关联	45
删除成员账户	46
取消与管理员帐户的关联	47
帐户操作对 Security Hub 数据的影响	47
禁用 Security Hub	47
成员账户与管理员账户取消关联	48
会员账户已从组织中删除	48
暂停账户	48
账户已关闭	48
跨区域聚合	50
跨区域聚合合合合合合合合	50
聚合新数据并复制数据更新	51
确定要从中汇总数据的账户	51
查看当前配置	52
查看跨区域聚合配置 (控制台)	52
查看当前的跨区域聚合配置 (Security Hub API、Amazon CLI)	52
启用跨区域聚合	52
启用跨区域聚合 (控制台)	52
启用跨区域聚合 (Security Hub API、Amazon CLI)	53
更新配置	53
更新跨区域聚合配置 (控制台)	54
更新跨区域聚合配置 (Security Hub API、Amazon CLI)	54
停止跨区域聚合	55
停止跨区域聚合 (控制台)	55
停止跨区域聚合 (Security Hub API、Amazon CLI)	55
结果	56
创建和更新结果	56
使用 BatchImportFindings	57
使用 BatchUpdateFindings	59
查看跨区域调查结果摘要	62
查看查找结果列表和详细信息	63
对发现结果进行筛选和分组 (控制台)	63
查看结果详细信息 (控制台)	65
检索查找详情 (Security Hub API , Amazon CLI)	66
对结果采取措施	66

设置结果的工作流状态	66
将结果发送到自定义操作	68
结果格式	68
ASFF 语法	69
ASFF 示例	113
见解	195
查看和筛选洞察列表	195
查看见解结果和调查结果	195
查看见解结果并采取相应措施（控制台）	196
查看见解结果（Security Hub API，Amazon CLI）	196
查看见解结果的结果（控制台）	197
托管见解	197
自定义见解	204
创建自定义见解（控制台）	204
创建自定义见解（Security Hub）Amazon CLI）	205
修改自定义见解（控制台）	205
修改自定义见解（Security HubAmazon CLI）	206
从托管见解创建新的自定义见解（控制台）	206
删除自定义见解（控制台）	207
删除自定义见解（Security HubAmazon CLI）	207
产品集成	208
管理产品集成	208
查看和筛选集成列表（控制台）	208
查看有关产品集成的信息（Security Hub API，Amazon CLI）	209
启用集成	209
禁用和启用来自集成的结果流（控制台）	210
禁用来自集成的结果流（Security Hub API，Amazon CLI）	210
启用来自集成的结果流（Security Hub API，Amazon CLI）	210
查看来自集成的结果	210
Amazon 服务集成	211
与 Security Hub 的Amazon服务集成概述	211
Amazon将结果发送到 Security Hub 的服务	212
Amazon接收来自 Security Hub 的结果的服务	220
第三方产品集成	221
第三方与 Security Hub 集成的概述	222
将结果发送到 Security Hub 的第三方集成	226
接收来自 Security Hub 结果的第三方集成	236
向 Security Hub 发送调查结果和从安全中心接收发现结果的第三方集成	239
使用自定义产品集成	241
从自定义安全产品发送结果的要求和建议	241
更新来自自定义产品的结果	242
示例自定义集成	242
标准和控件	243
运行 vacuum 检查	243
Security Hub 如何使用Amazon Config运行安全规则的规则	244
有关运行安全计划的计划	244
生成和更新控制结果	245
确定控制状态	250
确定标准安全分数	251
查看和管理标准	251
禁用或启用安全标准	252
查看有关标准的详细信息	254
查看和管理控件	257
查看控制的详细信息	257
自动启用新控件	258
禁用和启用各项控制	258
查看控制结果并采取相应措施	261

可用标准	263
CIS Amazon 基金会基准	263
PCI DSS	310
Amazon 基础安全最佳实践标准	361
带 CloudTrail 的 Security Hub	498
CloudTrail 中的 Security Hub 信息	498
例如：Security Hub 日志文件条目	499
自动响应和补救	500
的类型 EventBridge 一体化	500
所有结果 (Security Hub Findings - Imported)	500
自定义操作的结果 (Security Hub Findings - Custom Action)	501
自定义操作的见解结果 (Security Hub Insight Results)	501
EventBridge 事件格式	501
Security Hub Findings - Imported	502
Security Hub Findings - Custom Action	502
Security Hub Insight Results	503
为自动发送的结果配置规则	503
事件模式的格式	503
创建事件规则	504
.....	506
配置和使用自定义操作	506
创建自定义操作 (控制台)	506
创建自定义操作 (Security Hub API , Amazon CLI)	507
在中定义规则 EventBridge	507
为调查结果和洞察结果选择自定义操作	508
订阅Security Hub 公告	510
Amazon SNS 消息格式	512
配额	514
最大配额	514
速率配额	514
区域限制	516
跨区域聚合限制	516
并非所有区域都支持集成	517
中国 (北京) 和中国 (宁夏) 支持的集成	517
Amazon GovCloud (美国东部) 和Amazon GovCloud (美国西部) 中支持的集成	517
所有区域中均不支持控件	518
美国东部 (俄亥俄州)	518
美国西部 (北加利福尼亚)	519
美国西部 (俄勒冈州)	519
非洲 (开普敦)	520
亚太地区 (香港)	523
亚太地区 (雅加达)	523
亚太地区 (孟买)	529
亚太地区 (大阪)	530
亚太地区 (首尔)	533
亚太地区 (新加坡)	534
亚太地区 (悉尼)	534
亚太地区 (东京)	535
加拿大 (中部)	535
中国 (北京)	536
中国 (宁夏)	540
欧洲 (法兰克福)	543
欧洲 (爱尔兰)	544
欧洲 (伦敦)	544
欧洲 (米兰)	545
欧洲 (巴黎)	548
欧洲 (斯德哥尔摩)	548

中东 (巴林)	549
南美洲 (圣保罗)	550
Amazon GovCloud (美国东部)	551
Amazon GovCloud (美国西部)	555
禁用 SSecurity Hub	559
禁用Security Hub (控制台)	559
禁用Security Hub (Security Hub API) Amazon CLI)	559
文档历史记录	561
.....	dlxxxi

是什么AmazonSecurity Hub ?

AmazonSecurity Hub 在中向您提供安全状态的全面视图Amazon并帮助您根据安全行业标准和最佳实践检查您的环境。

Security Hub 跨各 Amazon 账户、服务和受支持的第三方合作伙伴产品收集安全数据，帮助您分析安全趋势并确定最高优先级的安全问题。

主题

- [的优势AmazonSecurity Hub \(p. 1\)](#)
- [Security Hub 的工作原理 \(p. 1\)](#)
- [AmazonSecurity Hub 免费试用、使用和定价 \(p. 2\)](#)

的优势AmazonSecurity Hub

减少了收集结果并确定其优先次序的工作

Security Hub 减少了跨账户从集成的账户中收集安全结果并确定其优先级Amazon服务和Amazon合作伙伴产品。Security Hub 使用标准结果格式处理数据的结果数据，从而无需管理多种格式的结果数据。然后，Security Hub 将各提供商的结果相关联，帮助确定最重要结果的优先级。

根据最佳实践和标准进行自动安全检查

Security Hub 会自动运行连续的账户级配置和安全性检查Amazon最佳做法和行业标准。Security Hub 将这些检查的结果作为就绪分数提供结果，并确定需要注意的特定账户和资源。

跨账户和提供商的结果的综合视图

Security Hub 将合并账户和提供商产品的安全结果，然后在 Security Hub 控制台上显示结果。这让您能够查看整体当前安全性状态，以发现趋势、识别潜在问题并采取必要的补救措施。

自动修复结果的能力

Security Hub 支持与亚马逊集成EventBridge。要自动修复特定结果，您可以定义在收到结果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。

Security Hub 的工作原理

您可以通过以下方式使用 Security Hub：

Security Hub 控制台

登录到Amazon Web Services Management Console然后打开AmazonSecurity Hub 控制台<https://console.aws.amazon.com/securityhub/>.

Security Hub API

要以编程方式访问 Security Hub，请使用 Security Hub API，该 API 允许您直接向服务发出 HTTPS 请求。有关更多信息，请参阅。[AmazonSecurity Hub API 参考](#).

启用 Security Hub 后，它将开始使用、聚合、组织以及确定其优先级的结果。Amazon 您已启用的服务，例如 [亚马逊 GuardDuty](#)、[Amazon Inspector](#)，和 [Amazon Macie](#)。您还可以启用与 Amazon 合作伙伴安全产品的集成。然后，这些合作伙伴产品也可以向 Security Hub 发送结果。请参阅 [产品集成](#) (p. 208)。

Security Hub 还可以通过运行连续的自动化安全检查，从而生成自己的结果，Amazon 最佳做法和支持的行业标准。请参阅 [标准和控件](#) (p. 243)。

然后，Security Hub 关联并整合各提供商的结果，帮助确定最重要结果的优先级。请参阅 [the section called “查看查找结果列表和详细信息”](#) (p. 63) 和 [the section called “对结果采取措施”](#) (p. 66)。

您也可以创建见解在 Security Hub 中。见解是当您应用 Group by (分组依据) 筛选条件时组合到一起的结果集合。见解可帮助您识别可能需要采取补救措施的常见安全问题。Security Hub 包括多个托管见解，您也可以创建自己的自定义见解。请参阅 [见解](#) (p. 195)。

Important

Security Hub 仅检测和合并启用 Security Hub 后生成的结果。它不会以追溯方式检测和合并启用 Security Hub 之前生成的安全结果。

Security Hub 仅接收和处理您在账户中启用 Security Hub 的区域中的结果。

为了完全遵守 CIS Amazon 基金会基准安全检查，您必须启用 Security Hub Amazon 地区。

Amazon Security Hub 免费试用、使用和定价

首次启用 Security Hub 时，Amazon 账户会自动注册 30 天的 Security Hub 免费试用。

当您在免费试用期间使用 Security Hub 时，您需要为使用 Security Hub 交互的其他服务付费，例如 Amazon Config 项目。您无需为此付费。Amazon Config Security Hub 的安全标准启用的规则。

在免费试用期结束前，您无需为使用 Security Hub 付费。

Note

中国（北京）区域不支持 Security Hub 免费试用。

查看使用详细信息和预计成本

Security Hub 提供使用信息，包括使用 Security Hub 的预计 30 天成本。使用详细信息包括免费试用的剩余时间。在免费试用期间，使用信息可以帮助您了解免费试用期结束后 Security Hub 的费用。

显示使用信息

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 在导航窗格中，选择 Settings (设置)。
3. 在 Settings (设置) 页面上，选择 Usage (使用情况)。

预计月度成本是将您账户对于结果和 Security Hub 查的使用情况投射到 30 天的时段估算出来的。

使用信息和预计成本仅适用于当前区域，不适用于启用 Security Hub 的所有区域。在聚合区域中，使用信息和估计成本不包括链接的区域。有关链接区域的更多信息，请参阅 [the section called “跨区域聚合”](#) (p. 50)。

查看定价详细信息

有关 Security Hub 如何为提取结果和安全检查付费的更多信息，请参阅 [Security Hub 定价](#)。

术语和概念

本主题介绍中的关键概念 Amazon 可帮助您入门的 Security Hub。

账户

包含您的 Amazon 资源的标准 Amazon Web Services (Amazon) 账户。您可以登录到 Amazon 使用您的账户并启用 Security Hub。

账户可以邀请其他账户启用 Security Hub 并在 Security Hub 中与该账户关联。接受成员资格邀请是可选的。如果邀请被接受，则该账户将成为管理员账户，并且添加的账户将成为成员账户。管理员账户可以在其成员账户中查看发现。

如果您注册了 Amazon Organizations，则您的组织将指定组织的 Security Hub 管理员账户。Security Hub 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 [管理管理员和成员账户 \(p. 31\)](#)。

管理员账户

Security Hub 中的帐户，被授予查看关联成员账户的调查结果的访问权限。

账户可通过以下任一方式成为管理员账户：

- 该帐户邀请其他账户在 Security Hub 中与其关联。当这些帐户接受邀请时，它们将成为成员账户，邀请帐户将成为其管理员帐户。
- 组织管理帐户将该帐户指定为 Security Hub 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。

一个账户只能有一个管理员帐户。账户不能既是管理员账户又是成员账户。

聚合区域

通过设置聚合区域，您可以在单个窗格中查看来自多个区域的安全结果。

聚合区域是您从中查看和管理结果的区域。调查结果将汇总到链接区域的聚合区域中。调查结果的更新将在不同地区复制。

在聚合区域中，安全标准、见解，和结果页面包含来自所有链接区域的数据。

请参阅 [跨区域聚合 \(p. 50\)](#)。

存档的结果

将 RecordState 设置为 ARCHIVED 的结果。归档调查结果表明查找提供商认为该调查结果不再相关。记录状态与工作流程状态分开，后者跟踪结果的调查状态。

查找提供商可以使用 [BatchImportFindings](#) 操作 Security Hub API 来存档他们创建的调查结果。如果禁用或删除了关联的资源，Security Hub 会根据以下条件之一自动存档控件的查找结果。

- 该调查结果在三到五天内没有更新（请注意，这是最大努力，不能保证）。
- 关联的 Amazon Config 评估回报 NOT_APPLICABLE。

默认情况下，存档的查找结果将从 Security Hub 控制台的结果列表中排除。您可以更新筛选器以包括已存档的查找结果。

这些区域有：[GetFindings](#) Security Hub API 的操作会返回活动和存档的查找结果。您可以包含记录状态的筛选器。

```
"RecordState": [
  {
    "Comparison": "EQUALS",
    "Value": "ARCHIVED"
  }
],
```

Amazon Security Finding 格式 (ASFF)

Security Hub 聚合或生成的结果内容的标准化格式。这些区域有：Amazon通过 Security Hub，您可以使用 Security Hub 查看和分析由Amazon通过运行安全检查的安全服务、第三方解决方案或 Security Hub 本身。有关更多信息，请参阅 [Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。

控制

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。安全标准由一些控制组成。

自定义操作

将选定结果发送到的 Security Hub 机制 EventBridge。将在 Security Hub 中创建一个自定义操作。然后它链接到 EventBridge 规则。该规则定义在收到与自定义操作 ID 关联的结果时执行的特定操作。例如，可以使用自定义操作将特定结果或一小部分结果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 \(控制台\)” \(p. 506\)](#)。

委托管理员账户 (Organizations)

在 Organizations 中，服务的委派管理员帐户能够管理组织服务的使用情况。

在 Security Hub 中，Security Hub 管理员帐户也是 Security Hub 的委派管理员帐户。当 Organizations 管理帐户首次指定 Security Hub 管理员帐户时，Security Hub 会调用组织以使该帐户成为委派管理员帐户。

然后，组织管理帐户必须选择委派管理员帐户作为所有区域中的 Security Hub 管理员帐户。

结果

安全检查或与安全相关的检测的可观察记录。

有关 Security Hub 中的结果的更多信息，请参阅[结果 \(p. 56\)](#)。

Note

结果将在最近更新后 90 天或创建后 90 天（如果未发生更新）后删除。要将结果存储 90 天以上，您可以在中配置规则 EventBridge 将结果路由到您的 Amazon S3 存储桶。

跨区域聚合

从关联区域到聚合区域的调查结果、见解、控制合规状态和安全评分的汇总。然后，您可以查看聚合区域中的所有数据，并更新聚合区域的调查结果和见解。

请参阅 [跨区域聚合 \(p. 50\)](#)。

寻找摄取

将结果从其他方面导入 Security HubAmazon服务和第三方合作伙伴提供商。

查找摄取事件包括新发现和对现有结果的更新。

见解

由聚合语句和可选的筛选器定义的相关结果的集合。见解确定了需要注意和干预的安全区域。Security Hub 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 见解，以跟踪特定于您的安全问题。Amazon环境和使用情况。有关更多信息，请参阅 [见解 \(p. 195\)](#)。

链接区域

启用跨区域聚合时，链接区域是将调查结果、见解、控制合规状态和安全评分汇总到聚合区域的区域。

在链接的区域中，结果和见解页面仅包含来自该区域的调查结果。

请参阅 [跨区域聚合 \(p. 50\)](#)。

成员账户

已向管理员帐户授予查看结果并对其采取措施的权限的帐户。

账户可通过以下任一方式成为成员账户：

- 该账户接受来自另一个账户的邀请。
- 对于组织帐户，Security Hub 管理员帐户将该帐户作为成员帐户启用。

相关要求

与某个控件对应的一组行业或监管要求。

Rule

一组自动化标准，用于评估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

特定的 point-in-time 针对单个资源的规则评估，将导致通过、失败、警告或不可用状态。运行安全检查将生成一个结果。

Security Hub 管理员账户

管理组织的 Security Hub 成员资格的组织帐户。

组织管理帐户指定每个区域中的 Security Hub 管理员帐户。组织管理帐户必须在所有区域中选择相同的 Security Hub 管理员帐户。

Security Hub 管理员帐户也是 Organizations 中 Security Hub 的委派管理员帐户。

Security Hub 管理员账户可以启用任何组织账户作为成员账户。Security Hub 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。要了解 Security Hub 中的安全标准的更多信息，请参阅[标准和控件 \(p. 243\)](#)。

严重性

分配给 Security Hub 控件的严重性标识了控制的重要性。控制的严重性可以是重大、High、中等、低，或者信息性。分配给控制结果的严重程度等于控件本身的严重程度。要了解 Security Hub 如何为控件分配严重性，请参阅[为控制结果分配严重性 \(p. 248\)](#)。

工作流程状态

对发现的调查状态。使用 Workflow.Status 属性进行跟踪。

工作流程状态初始为 NEW。如果已通知资源所有者对发现执行操作，可以将工作流程状态设置为 NOTIFIED。如果发现没有问题，不需要执行任何操作，可以将工作流程状态设置为 SUPPRESSED。查看并修复发现后，可以将工作流程状态设置为 RESOLVED。

默认情况下，大多数发现列表仅包含工作流程状态为 NEW 或 NOTIFIED 的发现。控件的发现列表还包括 RESOLVED 发现。

要进行 [GetFindings](#) 操作，您可以包含工作流程状态筛选器。

```
"WorkflowStatus": [  
  {  
    "Comparison": "EQUALS",  
    "Value": "RESOLVED"  
  }  
],
```

Security Hub 控制台提供了一个选项来设置发现的工作流程状态。客户（或 SIEM、票证、事件管理或代表客户更新发现提供商的发现的 SOAR 工具）也可以使用 [BatchUpdateFindings](#) 更新工作流程状态。

先决条件和建议

您必须拥有 Amazon 账户才能启用 Amazon Security Hub。如果您还没有账户，请使用以下步骤创建。

注册 Amazon

1. 打开 <https://portal.aws.amazon.com/billing/signup>。
2. 按照屏幕上的说明进行操作。

在注册时，您将接到一通电话，要求您使用电话键盘输入一个验证码。

当您注册 Amazon Web Services 账户时，系统将会创建一个 Amazon Web Services 账户根用户。根用户有权访问该账户中的所有 Amazon Web Services 和资源。作为安全最佳实践，请 [为管理用户分配管理访问权限](#)，并且只使用根用户执行 [需要根用户访问权限的任务](#)。

Security Hub 强烈建议您启用 Amazon Organizations。使用 Organizations 来管理您的账户可以简化管理成员账户的流程。

Security Hub 要求 Amazon Config 在所有启用了安全中心的账户中启用 Security Hub。Security Hub 控件使用 Amazon Config 规则来完成安全检查。

主题

- [Amazon Organizations 用于管理账户 \(p. 7\)](#)
- [启用和配置 Amazon Config \(p. 7\)](#)

Amazon Organizations 用于管理账户

为了帮助自动化和简化账户管理，Security Hub 强烈建议您启用 Amazon Organizations。

如果您启用了“Organizations”，则 Security Hub 会在将新帐户添加到您的组织时自动检测这些帐户。

有关设置组织的信息，请参阅《Amazon Organizations 用户指南》中的 [创建和管理 Organizations](#)。

在您设置组织后，您的组织管理帐户将指定 Security Hub 管理员帐户。请参阅 [the section called “指定 Security Hub 管理员帐户” \(p. 34\)](#)。Security Hub 管理员帐户也是 Organizations 中的委托管理员帐户。

然后，Security Hub 管理员帐户将其他组织帐户作为 Security Hub 成员帐户启用并管理。请参阅 [the section called “管理组织成员帐户” \(p. 38\)](#)。

启用和配置 Amazon Config

Amazon Security Hub 使用与服务相关的 Amazon Config 规则来执行大部分安全控制检查。

要支持这些控制，Amazon Config 必须在启用 Security Hub 的每个区域中的所有帐户（包括管理员帐户和成员帐户）上启用。Amazon Config 必须配置为至少记录您启用的标准所需的资源。

- [the section called “所需的 Amazon Config 资源” \(p. 264\)](#)
- [the section called “所需的 Amazon Config 资源” \(p. 311\)](#)
- [the section called “所需的 Amazon Config 资源” \(p. 361\)](#)

Security Hub 建议您在启用 Security Hub 标准Amazon Config之前启用资源记录。如果 Security Hub 在未启用资源记录时尝试运行安全检查，则检查会返回错误。

Security Hub 无法Amazon Config为您管理。如果您已经Amazon Config启用，则可以继续通过Amazon Config控制台或 API 配置其设置。

如果您Amazon Config在启用标准后启用，Security Hub 仍会创建Amazon Config规则，但前提是您在启用标准后的 31 天Amazon Config内启用。如果您Amazon Config在 31 天内未启用，则必须在启用后禁用并重新启用该标准Amazon Config。

启用标准后，Security Hub 会在 31 天内最多尝试创建六次Amazon Config规则。

- 在你启用标准的那一天
- 启用标准后的第二天
- 启用标准三天后
- 启用标准七天后
- 启用标准 15 天后
- 启用标准后 31 天

如何启用Amazon Config

如果您Amazon Config尚未设置，则可以通过以下方式之一进行设置：

1. 控制台或 CLI-您可以Amazon Config使用Amazon Config控制台或 CLI 手动启用。请参阅Amazon Config 开发者指南Amazon Config中的[入门](#)指南。
2. Amazon CloudFormation模板-如果您已集成Amazon Organizations或想要Amazon Config在大量帐户上启用，则可以使用 CloudFormation 模板启用Amazon Config轻松启用Amazon Config。要访问此模板，请参阅Amazon CloudFormation用户指南中的[Amazon CloudFormation StackSets 示例模板](#)。有关使用此模板的更多详细信息，请参阅[使用Amazon Config和管理Amazon Organizations账户Amazon CloudFormation StackSets](#)。
3. Github 脚本 — Security Hub [在中提供了一个脚本 GitHub](#)，允许您跨区域启用多个帐户。如果您尚未与 Organizations 集成，或者您的帐户不属于您的组织，则此脚本非常有用。当您使用此脚本启用 Security Hub 时，它还会自动Amazon Config为这些帐户启用。

在中配置资源记录Amazon Config

当您在Amazon Config安装期间启用资源Amazon Config记录时，会记录在运行区域中Amazon Config发现的所有受支持的区域资源类型。您还可以配置Amazon Config为记录支持的全局资源类型。您只需要在单个区域中记录全球资源。

如果你使用的是启用 CloudFormation StackSets Amazon Config，我们建议你运行两个不同的版本 StackSets。运行一个 StackSet，记录单个区域中的所有资源，包括全球资源。运行一秒钟 StackSet 以记录除其他区域的全局资源之外的所有资源。

您还可以使用 Quick Setup（一项功能）在您的账户和区域Amazon Config中快速配置资源记录。Amazon Systems Manager在快速设置期间，您可以选择要在哪个区域记录全球资源。有关更多信息，请参阅《Amazon Systems Manager用户指南》中的[Amazon Config录制](#)。

如果您未在所有区域记录全球资源，则在未记录全球资源的区域中，必须禁用该控件[the section called “2.5 — 确保Amazon Config已启用” \(p. 277\)](#)。CIS 2.5 在未记录全球资源的区域生成失败的调查结果。有关您可能要在未记录全球资源的区域中禁用的其他控件的详细信息，请参阅以下主题。

- [the section called “您可能希望禁用的控件” \(p. 310\)](#)
- [the section called “您可能希望禁用的控件” \(p. 360\)](#)

- [the section called “您可能希望禁用的控件” \(p. 496\)](#)

请注意，如果您使用[多账户脚本](#)启用 Security Hub，它将自动为所有区域的所有资源（包括全球资源）启用资源记录。它不会将全球资源的记录限制在单个区域。然后，您可以更新配置以仅记录单个区域中的全球资源。请参阅Amazon Config开发者指南中的[选择哪些资源Amazon Config记录](#)。

以下主题列出了每个标准所需的资源。您只能为所需资源启用录制。但是，Security Hub 继续添加新控件并支持新资源。

Note

要在安全检查后生成新的发现并避免过时的发现，您必须对附加到配置记录器的 IAM 角色具有足够的权限才能评估底层资源。

- [the section called “所需的 Amazon Config 资源” \(p. 264\)](#)
- [the section called “所需的 Amazon Config 资源” \(p. 311\)](#)
- [the section called “所需的 Amazon Config 资源” \(p. 361\)](#)

有关与资源记录相关的费用的详细信息，请参阅[Amazon Config价页面](#)。

设置 Amazon Security Hub

是否需要启用账户 Amazon Security Hub 手动取决于账户的管理方式。

您可以使用集成 Amazon Organizations，或者您可以手动管理帐户。

在这两种情况下，您都可以在每个地区分别设置 Security Hub 并管理帐户。所有账户还必须启用 Amazon Config，这是针对安全控制措施进行安全检查所需的。请参阅 [the section called “启用 Amazon Config” \(p. 7\)](#)。

Organizations 集成

如果你使用集成 Amazon Organizations，那么大多数组织帐户都自动启用了 Security Hub。

组织管理帐户选择 Security Hub 管理员帐户。为所选帐户自动启用 Security Hub。请参阅 [the section called “指定 Security Hub 管理员帐户” \(p. 34\)](#)。

Security Hub 管理员帐户将组织帐户作为成员帐户启用。这些组织帐户还自动启用了 Security Hub。请参阅 [the section called “管理组织成员帐户” \(p. 38\)](#)。

唯一未自动启用 Security Hub 的组织帐户是组织管理帐户。组织管理帐户在指定 Security Hub 管理员帐户之前无需启用 Security Hub。组织管理帐户必须先启用 Security Hub，然后才能将其作为成员帐户启用。

手动管理账户

未使用 Organizations 集成管理的帐户必须手动启用 Security Hub。

当成员帐户接受来自管理员帐户的邀请时，将建立 Security Hub 管理员与成员关系。请参阅 [the section called “通过邀请管理会员帐户” \(p. 41\)](#)。

目录

- [手动启用 Security Hub \(p. 10\)](#)
 - [将所需的 IAM 策略附加到 IAM 身份 \(p. 10\)](#)
 - [启用 Security Hub \(控制台\) \(p. 11\)](#)
 - [启用 Security Hub \(Security Hub API\) Amazon CLI \(p. 11\)](#)
 - [启用 Security Hub \(多账户脚本\) \(p. 12\)](#)
- [分配给 Security Hub 的服务相关角色 \(p. 12\)](#)

手动启用 Security Hub

在将所需策略附加到 IAM 身份后，您可以使用该身份启用 Security Hub。您可 Security Hub 从 Amazon Web Services Management Console 或者 API。

Security Hub 还提供了一个脚本 GitHub 这允许您在不同地区启用多个账户。

将所需的 IAM 策略附加到 IAM 身份

用于启用 Security Hub 的 IAM 身份 (用户、角色或组) 必须具有所需的权限。

启用集成的方式Amazon Organizations，那么组织中的帐户将自动启用 Security Hub。所需的权限也会自动处理。

未使用 Organizations 管理的帐户必须手动启用 Security Hub。用于启用 Security Hub 的 IAM 身份（用户、角色或组）必须具有所需的权限。

要授予启用 Security Hub 所需的权限，请附加 Security Hub 托管策略 [AWSSecurityHubFullAccess \(p. 24\)](#) 将其转到 IAM 用户、组或角色。

启用 Security Hub (控制台)

从控制台中启用 Security Hub 时，您还可以选择启用支持的安全标准。

启用 Security Hub

1. 使用 IAM 身份的凭证登录 Security Hub 控制台。
2. 首次打开 Security Hub 控制台时，选择启用AmazonSecurity Hub.
3. 在欢迎页面上，安全标准列出 Security Hub 支持的安全标准。

要启用标准，请选中其复选框。

要禁用标准，请清除其复选框。

您可以随时启用或禁用标准或其各个控制。有关安全标准以及如何管理它们的信息，请参阅[标准和控件 \(p. 243\)](#)。

4. 选择 Enable Security Hub (启用 Security Hub)。

启用 Security Hub (Security Hub API) Amazon CLI)

要启用 Security Hub，您可以使用 API 调用或Amazon Command Line Interface。

要启用 Security Hub (安全 HubAPI)，Amazon CLI)

- Security Hub API— 使用[EnableSecurityHub](#)operation. 从 API 中启用 Security Hub 时，它会自动启用这些安全标准。
 - CIS Amazon 基金会基准
 - Amazon基础安全最佳实践标准

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参数以将标签值分配给 Hub 资源。

- Amazon CLI— 在命令行处，运行[enable-security-hub](#)命令。要启用默认标准，请包括--enable-default-standards. 要不启用默认标准，请包括--no-enable-default-standards.

```
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"}'
```

启用 Security Hub 后，您可以启用或禁用标准。请参阅 [the section called “禁用或启用安全标准” \(p. 252\)](#)。

启用 Security Hub (多账户脚本)

这些区域有：[GitHub 中的 Security Hub 多账户启用脚本](#)允许您在账户和区域之间启用 Security Hub。该脚本还自动执行向成员账户发送邀请并启用邀请的过程Amazon Config。

该脚本会自动为所有区域中的所有资源启用资源记录功能，包括全局资源。它不会将全球资源的记录限制在单个地区。

有一个相应的脚本可以在账户和区域之间禁用 Security Hub。

自述文件提供了有关如何使用脚本的详细信息。其中包含以下信息：

- 如何将所需的 IAM 策略添加到账户
- 如何配置执行环境
- 如何运行脚本

分配给 Security Hub 的服务相关角色

启用 Security Hub 时，系统会为其分配一个名为的服务相关角色AWSServiceRoleForSecurityHub。此服务相关角色包括 Security Hub 执行以下操作所需的权限和信任策略：

- 检测并聚合来自 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie 的结果
- 配置必需的 Amazon Config 基础设施来运行支持的标准（在该版本中为 CIS Amazon Foundations）的安全检查

查看的详细信息AWSServiceRoleForSecurityHub，在设置页面，选择普通的然后查看服务权限。有关更多信息，请参阅[将服务相关角色用于 Amazon Security Hub \(p. 22\)](#)。

有关服务相关角色的更多信息，请参见 IAM 用户指南中的[使用服务相关角色](#)。

Amazon Security Hub 中的安全性

Amazon 的云安全性的优先级最高。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。[责任共担模型](#)将其描述为云的安全性和云中的安全性：

- 云的安全性 – Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为 [Amazon 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 Amazon Security Hub 的合规性计划，请参阅[合规性计划范围内的 Amazon 服务](#)。
- 云中的安全性 – 您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您的要求以及适用的法律法规。

该文档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。您还将了解如何使用其他 Amazon 帮助您监控和保护您的 Security Hub 资源的服务。

主题

- [中的数据保护 Amazon Security Hub \(p. 13\)](#)
- [Amazon 适用于的 Identity and Access Management Amazon Security Hub \(p. 14\)](#)
- [将服务相关角色用于 Amazon Security Hub \(p. 22\)](#)
- [Amazon 适用于的托管策略 Amazon Security Hub \(p. 24\)](#)
- [Amazon Security Hub 的合规性验证 \(p. 28\)](#)
- [Amazon Security Hub 中的基础设施安全性 \(p. 28\)](#)
- [Amazon Security Hub 和接口 VPC 终端节点 \(Amazon PrivateLink\) \(p. 29\)](#)

中的数据保护 Amazon Security Hub

Amazon [责任共担模式](#) 适用于 Amazon Security Hub 中的数据保护。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 Amazon Web Services 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](#)。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户凭证并使用 Amazon Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。
- 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 Simple Storage Service (Amazon S3) 中的个人数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 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 140-2 版》](#)。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用 Security Hub 或其他工具包 Amazon 使用控制台、API、Amazon CLI，或者

Amazon。您在用于名称的标签或自由格式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，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

Security Hub 是一种多租户服务产品。为确保数据安全，会对静态数据和在组件服务之间传输的数据进行加密。

Amazon 适用于的 Identity and Access ManagementAmazon Security Hub

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以成为身份验证（已登录）和授权（有权限）使用 Security Hub 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题

- [Audience \(p. 14\)](#)
- [使用身份进行身份验证 \(p. 14\)](#)
- [Amazon Web Services 账户根用户 \(p. 15\)](#)
- [IAM 用户和组 \(p. 15\)](#)
- [IAM 角色 \(p. 15\)](#)
- [使用策略管理访问 \(p. 16\)](#)
- [Amazon Security Hub 如何与 IAM 协同工作 \(p. 17\)](#)

Audience

如何使用 Amazon Identity and Access Management (IAM) 因您可以在 Security Hub 中执行的操作而异。

服务用户— 如果您使用 Security Hub 服务来完成作业，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Security Hub 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Security Hub 中的一项功能，请参阅[对 Amazon Security Hub 身份和访问进行故障排除 \(p. 21\)](#)。

服务管理员— 如果您在公司负责管理 Security Hub 资源，则您可能对 Security Hub 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Security Hub 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Security Hub 搭配使用的更多信息，请参阅[Amazon Security Hub 如何与 IAM 协同工作 \(p. 17\)](#)。

IAM 管理员— 如果您是 IAM 管理员，您可能希望了解有关您可以如何编写策略以管理 Security Hub 的访问权限的详细信息。要查看您可在 IAM 中使用的 Security Hub 基于身份的策略示例，请参阅[Amazon Security Hub 基于身份的策略示例 \(p. 19\)](#)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。有关使用 Amazon Web Services Management Console 登录的更多信息，请参阅 IAM 用户指南中的以[IAM 用户或根用户身份登录 Amazon Web Services Management Console](#)。

您必须作为 Amazon Web Services 账户根用户、IAM 用户或代入 IAM 角色以进行身份验证（登录到 Amazon）。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管理员以前使用 IAM 角色设置了联合身份验证。在您使用来自其它公司的凭证访问 Amazon 时，您间接地代入了角色。

要直接登录到[Amazon Web Services Management Console](#)，请将密码与根用户电子邮件地址或 IAM 用户名一起使用。您可以使用根用户或 IAM 用户访问密钥以编程方式访问 Amazon。Amazon 提供了 SDK 和命令行工具，可使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。使用 Signature Version 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅《Amazon 一般参考》中的[Signature Version 4 签名流程](#)。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的[在 Amazon 中使用多重身份验证 \(MFA\)](#)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《Amazon 一般参考》中的[需要根用户凭证的任务](#)。

IAM 用户和组

[IAM 用户](#)是 Amazon Web Services 账户内对某个人或应用程序具有特定权限的一个身份。在可能的情况下，我们建议依赖于临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#)是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的[何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

[IAM 角色](#)是 Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过[切换角色](#)，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南中的[使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色信息，请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的[IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问 – 某些 Amazon Web Services 使用其它 Amazon Web Services 中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
- 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下

下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作，请参阅服务授权参考中的 [Amazon Security Hub 的操作、资源和条件键](#)。

- 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的 [创建向 Amazon Web Service 委派权限的角色](#)。
- 服务相关角色 – 服务相关角色是与 Amazon Web Service 关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的 [使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的 [何时创建 IAM 角色（而不是用户）](#)。

使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源，以控制 Amazon 中的访问。策略是 Amazon 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 [JSON 策略概览](#)。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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。

每个 IAM 实体（用户或角色）最初没有任何权限。原定设置情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

基于身份的策略

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 [创建 IAM policy](#)。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到 Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的 [在托管式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。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (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](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

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来自 IAM 的 Amazon 托管式策略。

其它策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体的基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，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) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体的权限，包括每个 Amazon Web Services 账户根用户。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的 [SCP 的工作原理](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。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 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的 [策略评估逻辑](#)。

Amazon Security Hub 如何与 IAM 协同工作

在使用 IAM 管理对 Security Hub 的访问之前，您应了解哪些 IAM 功能可与 Security Hub 协同工作。大致了解 Security Hub 和其他方面 Amazon 服务与 IAM 一起使用，请参阅 [Amazon 使用 IAM 的服务](#) 在 IAM 用户指南。

主题

- [Security Hub 基于身份的策略 \(p. 17\)](#)
- [Security Hub 基于资源的策略 \(不支持\) \(p. 19\)](#)
- [根据 Security Hub 标签进行授权 \(p. 19\)](#)
- [Security Hub IAM 角色 \(p. 19\)](#)
- [服务相关角色 \(p. 19\)](#)
- [服务角色 \(p. 19\)](#)
- [Amazon Security Hub 基于身份的策略示例 \(p. 19\)](#)

Security Hub 基于身份的策略

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。Security Hub 支持特定的操作、资源和条件键。要了解在 JSON 策略中使用的所有元素，请参阅 IAM 用户指南中的 [IAM JSON 策略元素参考](#)。

操作

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

Security Hub 中的策略操作在操作前使用以下前缀：securityhub:。例如，要向用户授予启用 Security Hub 的权限，请使用 EnableSecurityHubAPI 操作，您包括 securityhub:EnableSecurityHub 分配给该用户的策略中的操作。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。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
    "securityhub:action1",
    "securityhub:action2"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 Get 开头的所有操作，请在策略中包含以下行：

```
"Action": "securityhub:Get*"
```

要查看 Security Hub 操作的列表，请参阅[操作定义于 Amazon Security Hub](#)在服务授权参考。

资源

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon Resource Name \(ARN\)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*" 
```

有关 ARN 格式的更多信息，请参阅 [Amazon Resource Name \(ARN \)](#) 和 [Amazon 服务命名空间](#)。

要查看 Security Hub 资源类型及其 ARN 的列表，请参阅[定义的资源类型 Amazon Security Hub](#)在服务授权参考。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Amazon Security Hub 定义的操作](#)。

条件键

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。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。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南 中的 [IAM policy 元素：变量和标签](#)。

Amazon 支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 Amazon 全局条件上下文键。

Security Hub 定义了自己的一组条件键，还支持使用一些全局条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 [Amazon 全局条件上下文键](#)。

Security Hub 操作支持 securityhub:TargetAccount 条件键。

控制对[BatchUpdateFindings](#)，Security Hub 支持securityhub.ASFFSyntaxPath条件键。有关配置访问权限的详细信息[BatchUpdateFindings](#)，请参阅[the section called “配置对的访问权限 BatchUpdateFindings” \(p. 60\)](#)。

要查看 Security Hub 条件键的列表，请参阅[条件键Amazon Security Hub](#)在服务授权参考。要了解您可以对哪些操作和资源使用条件键，请参阅[Amazon Security Hub 定义的操作](#)。

Security Hub 基于资源的策略（不支持）

Security Hub 不支持基于资源的策略。

根据Security Hub 标签进行授权

您可以将标签添加到 Security Hub 资源或将请求中的标签传递到 Security Hub。要基于标签控制访问，您需要使用 securityhub: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。

Security Hub IAM 角色

[IAM 角色](#)是 Amazon 账户中具有特定权限的实体。

在Security Hub 使用临时凭证

您可以使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以通过调用获取临时安全证书Amazon STS API 操作，例如[AssumeRole](#)要么[GetFederationToken](#)。

Security Hub 支持使用临时凭证。

服务相关角色

[服务相关角色](#)允许 Amazon 服务访问其它服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Security Hub 支持服务相关角色。

服务角色

此功能允许服务代表您担任[服务角色](#)。此角色允许服务访问其它服务中的资源以代表您完成操作。服务角色显示在您的 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Security Hub 支持服务角色。

Amazon Security Hub 基于身份的策略示例

预设情况下，IAM 用户和角色没有创建或修改 Security Hub 资源的权限。它们还无法使用 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 执行任务。IAM 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 IAM 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 \(p. 20\)](#)
- [使用 Security Hub 控制台 \(p. 20\)](#)
- [对 Amazon Security Hub 身份和访问进行故障排除 \(p. 21\)](#)

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 Amazon Web Services 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- Amazon 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 Amazon 托管策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 Amazon 客户管理型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 [Amazon 托管策略](#) 或 [工作职能的 Amazon 托管策略](#)。
- 应用最低权限 – 在使用 IAM policy 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 policy 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。如果通过特定 Amazon Web Service（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅 [IAM JSON 策略元素：Condition](#) 在 IAM 用户指南。
- 使用 IAM Access Analyzer 验证您的 IAM policy，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 policy 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 [IAM Access Analyzer 策略验证](#)。
- 需要多重身份验证 (MFA) – 如果您的账户需要 IAM 用户或根用户，请启用 MFA 来提高安全性。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 [配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

使用 Security Hub 控制台

要访问 Amazon Security Hub 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您中 Security Hub 资源的详细信息 Amazon 账户。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

要确保这些实体仍可使用 Security Hub 控制台，也可附加以下 Amazon 对实体实施托管策略。有关更多信息，请参阅 IAM 用户指南中的 [为用户添加权限](#)：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

对 Amazon Security Hub 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Security 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 \(p. 21\)](#)
- [我无权执行 iam:PassRole \(p. 21\)](#)
- [我想要查看我的访问密钥 \(p. 21\)](#)
- [我是管理员并希望允许其他人访问 Security Hub \(p. 22\)](#)
- [我想要允许有人在外面的 Amazon 用于访问我的 Security Hub 资源的帐户 \(p. 22\)](#)

我无权在 Security Hub 中执行操作

如果 Amazon Web Services Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。

当 mateojackson IAM 用户尝试使用控制台查看有关 *widget* 的详细信息，但不具有 securityhub:GetWidget 权限时，会发生以下示例错误。

```
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

如果您收到错误消息，提示您无权执行 iam:PassRole 操作，必须更新您的策略，以便允许您将角色传递给 Security Hub。

有些 Amazon Web Services 允许您将现有角色传递到该服务，而不是创建新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。

当名为的 IAM 用户时，会发生以下示例错误 marymajor 尝试使用控制台在 Security Hub 中执行操作。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 Amazon 管理员。管理员是向您提供登录凭证的人。

我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 AKIAIOSFODNN7EXAMPLE）和秘密访问密钥（例如 wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

Important

请不要向第三方提供访问密钥，即便是为了帮助[找到您的规范用户 ID](#)也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的[管理访问密钥](#)。

我是管理员并希望允许其他人访问 Security Hub

要允许其他人访问 Security Hub，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 Amazon。然后，您必须将策略附加到实体，以便在 Security Hub 中向其授予正确的权限。

要立即开始使用，请参阅 IAM 用户指南中的[创建您的第一个 IAM 委派用户和组](#)。

我想要允许有人在我外面我的 Amazon 用于访问我的 Security Hub 资源的帐户

您可以创建一个角色，以便其它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[Amazon Security Hub 如何与 IAM 协同工作 \(p. 17\)](#)。
- 要了解如何为您拥有的 Amazon Web Services 账户中的资源提供访问权限，请参阅 IAM 用户指南中的[为您拥有的另一个 Amazon Web Services 账户中的 IAM 用户提供访问权限](#)。
- 要了解如何为第三方 Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的[为第三方拥有的 Amazon Web Services 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的[为经过外部身份验证的用户（联合身份验证）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 角色与基于资源的策略有何不同](#)。

将服务相关角色用于 Amazon Security Hub

Amazon Security Hub 使用 Amazon Identity and Access Management (IAM) [服务相关角色](#)。服务相关角色是一种独特类型的 IAM 角色，它与 Security Hub 直接相关。服务相关角色由 Security Hub 预定义，并包含 Security Hub 调用其他时所需的一切权限。Amazon 服务代表您。

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，除非另外定义权限，否则，仅 Security Hub 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。

Security Hub 支持在 Security Hub 可用的所有区域中使用服务相关角色。有关更多信息，请参阅[区域限制 \(p. 516\)](#)。

您必须首先在启用了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[Amazon 使用 IAM 的服务](#)中的 IAM 用户指南然后找到具有的服务是中的服务相关角色 column。选择是和链接，查看该服务的[服务相关角色文档](#)。

Security Hub 的服务相关角色权限

Security Hub 使用名为的服务相关角色。AWSServiceRoleForSecurityHub。这是以下所需的服务相关角色。Amazon Security Hub 访问您的资源。

AWSServiceRoleForSecurityHub 服务相关角色信任以下服务代入该角色：

- securityhub.amazonaws.com

这些区域有：AWSServiceRoleForSecurityHub服务相关角色使用托管策略[AWSSecurityHubServiceRolePolicy \(p. 26\)](#)。

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。对于AWSServiceRoleForSecurityHub为了能够成功创建服务相关角色，用于 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此 IAM 用户、组或角色。

```
{
  "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

这些区域有：AWSServiceRoleForSecurityHub在您首次启用 Secure Hub 或者在之前未启用的支持区域中启用 Security Hub 时，将自动创建服务相关角色。您也可以创建AWSServiceRoleForSecurityHub使用 IAM 控制台、IAM CLI 或 IAM API 手动使用服务相关角色。

Important

为 Security Hub 管理员帐户创建的服务相关角色不应用到 Security Hub 成员帐户。

有关手动创建角色的更多信息，请参阅[创建服务相关角色](#)中的IAM 用户指南。

编辑 Security Hub 的服务相关角色

Security Hub 不允许您编辑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 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。

Important

删除AWSServiceRoleForSecurityHub您必须先启用了的所有区域中禁用它。

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。有关更多信息，请参阅 [禁用 SSecurity Hub \(p. 559\)](#)。

禁用 Security Hub 时，AWSServiceRoleForSecurityHub服务相关角色是不自动删除。如果您再次启用 Security Hub，它会开始使用现有的AWSServiceRoleForSecurityHub服务相关角色。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForSecurityHub 服务相关角色。有关更多信息，请参阅 IAM 用户指南中的 [删除服务相关角色](#)。

Amazon适用于 的托管策略AmazonSecurity Hub

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 [IAM 客户托管策略](#)需要时间和专业知识。要快速入门，您可以使用我们的 Amazon 托管策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户 中使用。有关 Amazon 托管策略的更多信息，请参阅 IAM 用户指南中的[Amazon 托管策略](#)。

Amazon Web Services 负责维护和更新 Amazon 托管策略。您无法更改 Amazon 托管策略中的权限。服务偶尔会向 Amazon 托管策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能更新 Amazon 托管策略。服务不会从 Amazon 托管策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon 还支持跨多种服务的工作职能的托管策略。例如，ViewOnlyAccess Amazon托管策略提供对许多的只读访问Amazon Web Services和资源。当服务启动新功能时，Amazon会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的[适用于工作职能的 Amazon 托管策略](#)。

Amazon 托管策略：AWSSecurityHubFullAccess

您可以将 AWSSecurityHubFullAccess 策略附加得到 IAM 身份。

此策略授予管理权限，允许委托人完全访问所有 Security Hub 操作。必须先将此策略附加到委托人，然后才能为其帐户手动启用 Security Hub。例如，拥有这些权限的承担者可以查看和更新查找结果的状态。他们可以配置自定义见解并启用集成。它们可以启用和禁用标准和控制。管理员帐户的委托人也可以管理成员帐户。

权限详细信息

此策略包含以下权限。

- securityhub— 允许委托人完全访问所有 Security Hub 操作。
- iam— 允许委托人创建服务相关角色。

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

```
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": "securityhub.amazonaws.com"
            }
        }
    }
}
]
```

Security Hub 托管策略： AWSSecurityHubReadOnlyAccess

您可以将 AWSSecurityHubReadOnlyAccess 策略附加得到 IAM 身份。

此策略授予只读权限，允许用户查看 Security Hub 中的信息。附加此策略的委托人无法在 Security Hub 中进行任何更新。例如，拥有这些权限的委托人可以查看与其帐户关联的调查结果列表，但不能更改查找结果的状态。他们可以查看见解的结果，但无法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

此策略包含以下权限。

- securityhub— 允许用户执行返回项目列表或项目详细信息的操作。这包括从开始的 API 操作 Get、List，或者 Describe。

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

Amazon 托管策略： AWSSecurityHubOrganizationsAccess

您可以将 AWSSecurityHubOrganizationsAccess 策略附加得到 IAM 身份。

此策略授予管理权限 Amazon Organizations 这是支持 Security Hub 与 Organizations 集成所需的。

这些权限允许组织管理帐户为 Security Hub 指定委派管理员帐户。它们还允许委派 Security Hub 管理员帐户启用组织帐户作为成员帐户。

此策略仅为 Organizations 提供权限。组织管理帐户和委派的 Security Hub 管理员帐户还需要在 Security Hub 中执行相关操作的权限。这些权限可通过 AWSSecurityHubFullAccess 托管策略。

权限详细信息

此策略包含以下权限。

- `organizations:ListAccounts`— 允许委托人检索属于组织的账户列表。
- `organizations:DescribeOrganization`— 允许承担者检索有关组织配置的信息。
- `organizations:EnableAWSServiceAccess`— 允许委托人启用 Security Hub 与 Organizations 的集成。
- `organizations:RegisterDelegatedAdministrator`— 允许委托人为 Security Hub 指定委托管理员帐户。
- `organizations:DeregisterDelegatedAdministrator`— 允许委托人删除 Security Hub 的委托管理员帐户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "arn:aws:organizations::*:account/o-*/*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

Amazon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，该角色允许 Security Hub 代表您执行操作。有关更多信息，请参阅 [the section called “使用服务相关角色” \(p. 22\)](#)。

此策略授予管理权限，允许服务相关角色执行 Security Hub 控件的安全检查。

权限详细信息

此策略包括执行以下操作的权限：

- cloudtrail— 检索有关的信息CloudTrail跟踪。
- cloudwatch— 检索当前的CloudWatch警报。
- logs— 检索指标筛选器CloudWatch日志。
- sns— 检索 SNS 主题的订阅列表。
- config— 检索有关配置记录器、资源和的信息Amazon Config规则。此外，允许服务相关角色创建和删除Amazon Config规则，并根据规则进行评估。
- iam— 获取并生成账户的凭证报告。
- organizations— 检索组织的帐户信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:BatchGetResourceConfig",
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "iam:GetCredentialReport",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "config:PutConfigRule",
        "config>DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:DescribeConfigRuleEvaluationStatus"
      ],
      "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    }
  ]
}
```

Security Hub 更新为Amazon托管策略

查看有关更新的详细信息AmazonSecurity Hub 的托管策略（从该服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 Security Hub 上的 RSS 源。[文档历史记录 \(p. 561\)](#)页。

更改	描述	日期
AWSecurityHubServiceRolePolicy – 对现有策略的更新	Security Hub 移动了现有 config:PutEvaluations 允许在策略中使用其他语句。 这些区域有：config:PutEvaluations 权限现在适用于所有资源。	2021 年 7 月 14 日
AWSecurityHubServiceRolePolicy – 对现有策略的更新	Security Hub 添加了新的权限，允许服务相关角色向 Amazon Config。	2021 年 6 月 29 日
AWSecurityHubServiceRolePolicy 添加到托管策略列表	添加了有关托管策略的信息 AWSecurityHubServiceRolePolicy，该角色由 Security Hub 服务相关角色使用。	2021 年 6 月 11 日
AWSecurityHubOrganizationPolicy – 新策略	Security Hub 添加了一项新策略，该策略授予 Security Hub 与 Organizations 集成所需的权限。	2021 年 3 月 15 日
Security Hub 开启跟踪更改	Security Hub 开启跟踪其的更改 Amazon 托管策略。	2021 年 3 月 15 日

Amazon Security Hub 的合规性验证

作为多个 Amazon Security Hub 合规性计划的一部分，第三方审核员将评估 Amazon 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 Amazon 服务的列表，请参阅[合规性计划范围内的 Amazon 服务](#)。有关一般信息，请参阅[Amazon 合规性计划](#)。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅[在 Amazon Artifact 中下载报告](#)。

您在使用 Security Hub 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。Amazon 为您提供以下资源来帮助实现合规性：

- [安全性与合规性快速入门指南](#) – 这些部署指南讨论了架构注意事项，并提供了在 Amazon 上部署基于安全性和合规性的基准环境的步骤。
- [Amazon 合规性资源](#) – 此业务手册和指南集合可能适用于您的行业和位置。
- [Amazon Config](#) – 此 Amazon 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- [Amazon Security Hub](#) – 此 Amazon 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon Security Hub 中的基础设施安全性

作为托管服务，Amazon Security Hub 受保护 Amazon 中描述的全局网络安全程序[Amazon Web Services：安全过程概述](#)白皮书。

你用 Amazon 使用发布的 API 调用通过网络访问 Security Hub。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如

Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [Amazon Security Token Service](#) (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon Security Hub 和接口 VPC 终端节点 (Amazon PrivateLink)

您可以通过创建接口 VPC 终端节点在 VPC 和 Amazon Security Hub 之间建立私有连接。接口终端节点由以下公司提供支持 [Amazon PrivateLink](#)，该技术支持您通过私有连接访问 Security Hub API，而无需采用互联网网关、NAT 设备、VPN 连接或 Amazon Direct Connect 连接。VPC 中的实例即使没有公有 IP 地址也可与 Security Hub API 进行通信。VPC 和 Security Hub 之间的流量不会脱离 Amazon 网络。

每个接口终端节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 [接口 VPC 终端节点 \(Amazon PrivateLink\)](#) 中的 Amazon PrivateLink 指南。

Security Hub VPC 终端节点的注意事项

在为 Security Hub 设置接口 VPC 终端节点之前，请务必查看 [接口终端节点属性和限制](#) 中的 Amazon PrivateLink 指南。

Security Hub 支持从 VPC 调用它的所有 API 操作。

Note

Security Hub 不支持亚太地区（大阪）区域的 VPC 终端节点。

为 Security Hub 创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或 Amazon Command Line Interface (Amazon CLI)。有关更多信息，请参阅 [创建接口终端节点](#) 中的 Amazon PrivateLink 指南。

使用以下服务名称为 Security Hub 创建 VPC 终端节点：

- `com.amazonaws.region.securityhub`

如果为终端节点启用私有 DNS，则可以使用针对区域的默认 DNS 名称向 Security Hub 发出 API 请求，例如 `securityhub.us-east-1.amazonaws.com`。

有关更多信息，请参阅 [通过接口终端节点访问服务](#) 中的 Amazon PrivateLink 指南。

为 Security Hub 创建 VPC 终端节点策略

您可以为 VPC 终端节点附加控制对 Security Hub 的访问的终端节点策略。该策略指定以下信息：

- 可执行操作的委托人。
- 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 [使用 VPC 终端节点控制对服务的访问权限](#) 中的 Amazon PrivateLink 指南。

例如：Security Hub 操作的 VPC 终端节点策略

下面是用于 Security Hub 的终端节点策略示例。当附加到终端节点时，此策略会向所有委托人授予对列出的针对所有资源的 Security Hub 操作的访问权限。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
      ],
      "Resource": "*"
    }
  ]
}
```

管理管理员和成员账户

管理员帐户可以查看来自其成员账户的数据并管理其配置。管理员与成员关系的建立方式有所不同，具体取决于您是否使用集成 Amazon Organizations。

如果您已与 Organizations 集成，则组织管理帐户将指定 Security Hub 管理员帐户。请参阅 [the section called “指定 Security Hub 管理员帐户” \(p. 34\)](#)。Security Hub 管理员帐户自动访问组织中的所有帐户。Security Hub 管理员帐户决定要启用的组织帐户状态。请参阅 [the section called “管理组织成员帐户” \(p. 38\)](#)。这些成员帐户无法解除自己与管理员帐户的关联。

否则，成员帐户接受来自管理员帐户的邀请。Security Hub 管理员帐户还可以邀请不属于组织的成员帐户。请参阅 [the section called “通过邀请管理成员帐户” \(p. 41\)](#)。通过邀请添加的帐户可以取消自己与管理员帐户的关联。

主题

- [管理员-成员关系的影响 \(p. 31\)](#)
- [限制和建议 \(p. 31\)](#)
- [转换到 Amazon Organizations 用于帐户管理 \(p. 32\)](#)
- [允许的帐户操作 \(p. 34\)](#)
- [指定 Security Hub 管理员帐户 \(p. 34\)](#)
- [管理组织成员帐户 \(p. 38\)](#)
- [通过邀请管理成员帐户 \(p. 41\)](#)
- [帐户操作对 Security Hub 数据的影响 \(p. 47\)](#)

管理员-成员关系的影响

管理员帐户被授予查看与其成员帐户关联的调查结果的权限。这还允许管理员帐户查看见解结果并控制其成员帐户的状态。管理员帐户还可以对其成员帐户的调查结果采取措施。

Security Hub 不会将成员帐户查找结果复制到管理员帐户中。管理员帐户也无法更改成员帐户的 Security Hub 配置。请参阅 [the section called “允许的帐户操作” \(p. 34\)](#)。

在 Security Hub 中，所有调查结果都被提取到特定帐户的特定区域。

在每个区域中，管理员帐户可以查看和管理其在该区域中的成员帐户的调查结果。

在聚合区域中，管理员帐户可以查看和管理复制到聚合区域的关联区域中的成员帐户查找结果。有关跨区域聚合的更多信息，请参阅 [跨区域聚合 \(p. 50\)](#)。

限制和建议

成员账户的最大数量

Security Hub 在每个区域中，每个管理员帐户最多支持 5,000 个成员帐户。

账户和区域

按组织成员资格

如果你已注册 Amazon Organizations，组织管理账户可以在每个区域中指定一个 Security Hub 管理员账户。

区域的 Security Hub 管理员帐户也成为该区域针对 Organizations 中 Security Hub 的委派管理员帐户。例外情况是，如果组织管理帐户将自己指定为 Security Hub 管理员帐户。Organizations 管理帐户不能是组织中的委派管理员。

在 Organizations 中设置了区域的委派管理员帐户后，组织管理帐户可以选择委派管理员帐户，也可以选择自己作为该区域中的 Security Hub 管理员帐户。我们建议您在所有区域中选择相同的委托管理员账户。

Security Hub 管理员帐户分别管理每个区域中的成员帐户。

按邀请成员资格

对于通过邀请创建的成员账户，仅在发送邀请的区域中创建管理员-成员账户关联。管理员账户必须在要使用的每个区域中启用 Security Hub。然后，管理员帐户邀请每个账户作为该区域的成员账户关联。

管理员与成员关系的限制

账户不能既是管理员账户又是成员账户。

成员账户只能与一个管理员帐户关联。如果 Security Hub 管理员账户启用了组织账户，则该账户不能接受来自其他账户的邀请。如果帐户已接受邀请，则 Security Hub 管理员帐户无法为组织启用该帐户。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。

跨服务协调管理员账户

Security Hub 汇总了来自各种 Amazon 服务，例如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie。Security Hub 还允许用户从 GuardDuty 寻找在亚马逊 Detective 中开始调查。

但是，您在其他这些服务中设置的管理员-成员关系不会自动应用于 Security Hub。对于所有这些服务，Security Hub 建议您为管理员账户使用相同的账户。此管理员账户应该是负责安全工具的账户。同一账户也应该是用于的聚合器账户 Amazon Config。

例如，来自 GuardDuty 管理员帐户 A 可以查看 GuardDuty 上的成员帐户 B 和 C GuardDuty 控制台。如果帐户 A 然后启用了 Security Hub，则帐户 A 中的用户可以。不自动查看 GuardDuty Security Hub 帐户 B 和 C 的调查结果。这些帐户还需要 Security Hub 管理员与成员之间的关系。

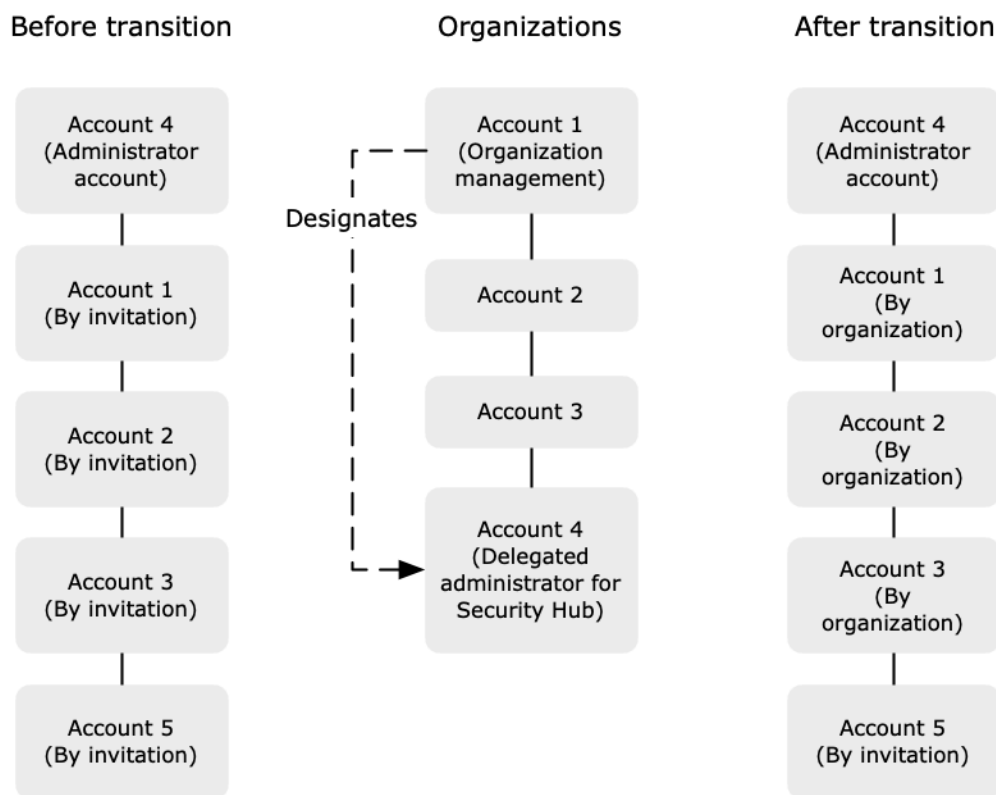
为此，请将帐户 A 设为 Security Hub 管理员账户，并启用帐户 B 和 C 成为 Security Hub 成员账户。

转换到 Amazon Organizations 用于账户管理

您可能有一个现有的管理员帐户，其成员帐户已接受手动邀请。如果你注册了 Amazon Organizations，请使用以下步骤使用 Organizations 启用和管理成员账户，而不是使用手动邀请流程：

1. [为您的组织指定 Security Hub 管理员账户。](#) (p. 33)
2. [启用 Security Hub 管理员账户。现有会员账户自动启用。](#) (p. 33)

下图显示了过渡之前的管理员和成员帐户结构、Organizations 中的配置以及过渡后的帐户结构的概述。



为您的组织指定 Security Hub 管理员账户

您的组织管理账户指定组织的 Security Hub 管理员账户。请参阅 [the section called “指定 Security Hub 管理员帐户” \(p. 34\)](#)。Security Hub 管理员帐户也成为 Organizations 中 Security Hub 的委派管理员帐户。

为了简化过渡，Security Hub 建议您选择当前管理员帐户作为组织的 Security Hub 管理员帐户。这是因为成员帐户不能属于多个管理员帐户。组织的管理员帐户无法启用属于另一管理员帐户下的成员帐户的任何组织帐户。

启用组织账户作为成员账户

Security Hub 管理员帐户决定要启用哪些组织账户作为成员账户状态。请参阅 [the section called “管理组织成员帐户” \(p. 38\)](#)。

在存储库的账户页面中，Security Hub 管理员账户将看到组织中的所有账户。组织账户有一种按组织，即使他们以前是邀请的会员账户。

如果 Security Hub 管理员帐户已经是管理员帐户，则其所有现有成员帐户都将自动作为成员帐户启用。非组织账户的现有成员帐户具有一种类型通过邀请。

这些区域有：账户页面还提供了在将新账户添加到组织时，自动启用这些账户。请参阅 [the section called “自动启用新账户” \(p. 39\)](#)。该选项最初处于关闭状态（已关闭“自动启用”）。

在启用该选项之前，账户页面显示一条消息，其中包含启用按钮。当你选择启用，Security Hub 将执行以下操作：

- 将所有组织帐户作为成员帐户启用，但属于另一管理员帐户下的成员帐户除外。

在 Security Hub 管理员帐户可以启用这些帐户之前，必须将它们与其他管理员帐户取消关联。请参阅 [the section called “取消成员账户的关联” \(p. 45\)](#)。

如果组织账户未启用 Security Hub，则会自动启用该账户的 Security Hub 和默认标准。

对于已启用 Security Hub 的组织帐户，Security Hub 不会对该帐户进行任何其他更改。它只能启用会员资格。

- 切换设置以自动启用新帐户 (已启用“自动启用”)。

允许的账户操作

管理员和成员帐户可以访问以下 Security Hub 操作。在表中，值具有以下含义：

- 任何 —该账户可以对同一管理员或账户下的所有账户执行操作。
- Self —该账户只能在自己的账户上执行操作。

短划线 (—) 表示该账户无法执行操作。

此表反映了管理员帐户和成员帐户的默认权限。您可以使用自定义 IAM 策略进一步限制对 Security Hub 功能和功能的访问。有关指导和示例，请参阅博客帖子。 [将 IAM 策略与用户角色保持一致Amazon Security Hub](#)。

操作	Security Hub 管理员帐户 (组织)	管理员帐户 (邀请)	成员 (组织)	会员 (邀请函)
查看账户	任何	任何	-	-
取消关联成员账户	任何	任何	-	自身
删除成员账户	任何非组织账户	任何	-	-
禁用 Security Hub	-	自我-如果没有启用的成员账户	Self Self (如果与 Security Hub 管理员帐户取消关联)	Self-如果与管理员帐户取消关联
查看 发现结果	任何	任何	自身	自身
更新发现	任何	任何	自身	自身
查看洞察结果	任何	任何	自身	自身
查看控制细节	任何	任何	自身	自身
启用和禁用控件	自身	自身	自身	自身
启用和禁用标准	自身	自身	自身	自身
启用和禁用集成	自身	自身	自身	自身
配置自定义操作	自身	自身	自身	自身

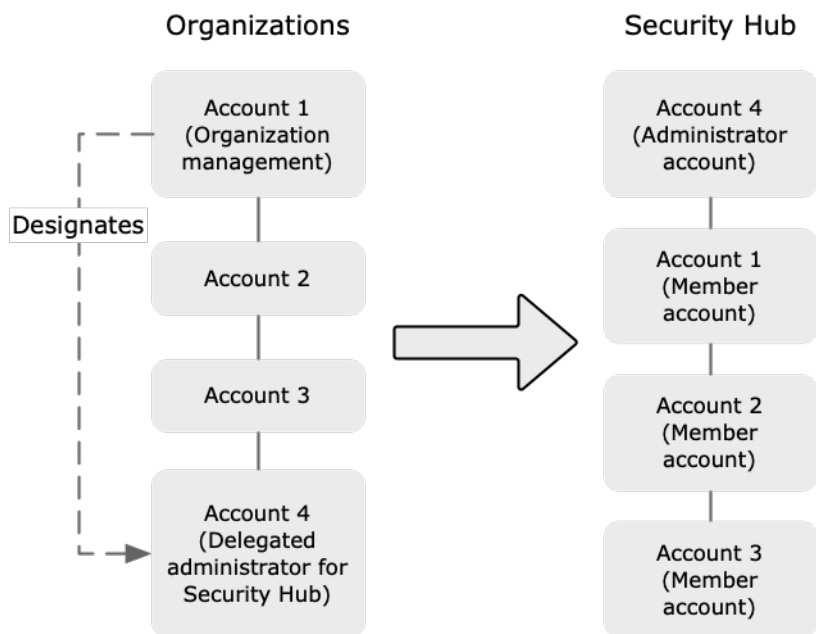
指定 Security Hub 管理员帐户

Security Hub 管理员帐户管理组织的 Security Hub 成员资格。

Security Hub 管理员帐户的方式

组织管理帐户指定每个区域中的 Security Hub 管理员帐户。

然后 Security Hub 管理员帐户启用组织账户作为成员账户。他们还可以邀请其他账户成为成员账户。请参阅 [the section called “管理组织成员账户” \(p. 38\)](#) 和 [the section called “通过邀请管理会员账户” \(p. 41\)](#)。



会员账户只能与单个管理员帐户关联。Security Hub 管理员帐户无法启用属于其他管理员帐户的成员帐户。

所有 Security Hub 帐户都必须具有 Amazon Config 已启用并配置为记录所有资源。有关要求的详细信息 Amazon Config，请参阅 [the section called “启用 Amazon Config” \(p. 7\)](#)。

将 Security Hub 管理员帐户设置为委托管理员帐户

当您第一次选择 Security Hub 管理员帐户时，Security Hub 会调用 Organizations 以使该帐户成为 Security Hub 的委派管理员帐户。

在 Organizations 中拥有委派管理员帐户后，您可以在所有区域中选择该帐户或组织管理帐户作为 Security Hub 管理员帐户。我们建议在所有区域中选择相同的委托管理员帐户。

要选择其他帐户，必须删除所有区域中的当前 Security Hub 管理员帐户。

选择 Security Hub 管理员帐户的建议

如果在手动邀请过程中有管理员帐户，那么 Security Hub 建议您将该帐户指定为 Security Hub 管理员帐户。

我们还建议您不要将组织管理帐户本身指定为 Security Hub 管理员帐户。这是因为有权访问组织管理帐户来管理账单的用户可能与需要访问 Security Hub 进行安全管理的用户不同。

Organizations 管理帐户也不能作为组织中某项服务的委托管理员帐户。

删除 Security Hub 管理员帐户

组织管理帐户可以删除 Security Hub 管理员帐户。

当组织管理帐户使用控制台删除一个区域中的 Security Hub 管理员帐户时，系统会在所有区域中自动删除该帐户。Security Hub 还致电 Organizations 以删除委派的管理员帐户。

Security Hub API 只会从发出 API 调用或命令的区域中删除 Security Hub 管理员帐户。它不会更新其他区域，也不会删除 Organizations 中的委派管理员帐户。

当您使用 Organizations API 删除 Security Hub 的委派管理员帐户时，Security Hub 还会删除所有区域中的 Security Hub 管理员帐户。

配置 Security Hub 管理员帐户所需的权限

要指定和删除 Security Hub 管理员帐户，组织管理帐户必须具有 `EnableOrganizationAdminAccount` 和 `DisableOrganizationAdminAccount` Security Hub 中的操作。Organizations 管理帐户还必须具有组织的管理权限。

要授予所有必需的权限，请将以下 Security Hub 托管策略附加到组织管理账户的 IAM 委托人：

- [AWSSecurityHubFullAccess \(p. 24\)](#)
- [AWSSecurityHubOrganizationsAccess \(p. 25\)](#)

指定 Security Hub 管理员帐户（控制台）

组织管理帐户可以使用 Security Hub 控制台指定 Security Hub 管理员帐户。

组织管理帐户不必启用 Security Hub 即可管理 Security Hub 管理员帐户。

Security Hub 建议组织管理帐户不是 Security Hub 管理员帐户。但是，如果组织管理帐户确实选择自己作为 Security Hub 管理员帐户，则必须启用 Security Hub。如果没有启用 Security Hub，则必须手动启用 Security Hub。无法为组织管理帐户自动启用 Security Hub。

Security Hub 从欢迎来到 Security Hub 页

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 选择转到 Security Hub。
3. 如果当前分配了 Security Hub 管理员帐户，则必须先删除当前帐户，然后才能指定新帐户。

要删除当前账户，请在委托管理员，选择 Remove。

4. 在委托管理员，输入要指定为的账户的帐户 ID Security Hub 管理员账户。

您必须在所有区域指定同一个 Security Hub 管理员帐户。如果您指定的帐户与其他区域中指定的帐户不同，Security Hub 将返回错误消息。

5. 选择 Delegate (委派)。

如果启用了 Security Hub，则还可以从设置页。

Security Hub 从设置页

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 在 Security Hub 导航窗格中，选择设置。然后选择。普通的。
3. 如果当前分配了 Security Hub 管理员帐户，则必须先删除当前帐户，然后才能指定新帐户。

在委托管理员，要删除当前账户，请选择 Remove。

4. 输入要指定为的账户的帐户 ID Security Hub 管理员账户。

您必须在所有区域指定同一个 Security Hub 管理员帐户。如果您指定的帐户与其他区域中指定的帐户不同，Security Hub 将返回错误消息。

5. 选择 Delegate (委派)。

指定 Security Hub 管理员帐户 (Security Hub API) Amazon CLI)

要指定 Security Hub 管理员帐户，您可以使用 API 调用或 Amazon Command Line Interface。您必须使用组织管理帐户凭据。

要指定 Security Hub 管理员帐户 (Security Hub API , Amazon CLI)

- Security Hub API — 使用 [EnableOrganizationAdminAccount](#) operation。您必须提供 Amazon Security Hub 管理员帐户的帐户 ID。
- Amazon CLI — 在命令行处，运行 [enable-organization-admin-account](#) 命令。

```
aws securityhub enable-organization-admin-account --admin-account-id <admin account ID>
```

示例

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

删除 Security Hub 管理员帐户 (控制台)

组织管理帐户可以删除当前的 Security Hub 管理员帐户。当您使用控制台删除 Security Hub 管理员帐户时，所有区域中的 Security Hub 管理员帐户都将被删除。Security Hub 还呼叫 Organizations 以删除 Security Hub 的委托管理员帐户。

删除 Security Hub 管理员帐户后，会员帐户与已删除的 Security Hub 管理员帐户取消关联。

启用的成员帐户仍然启用了 Security Hub。在新的 Security Hub 管理员将其作为成员帐户启用之前，他们将成为独立帐户

如果组织管理帐户不是 Security Hub 中启用的帐户，则使用欢迎来到 Security Hub 页。

Security Hub 从欢迎来到 Security Hub 页

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 选择转到 Security Hub。
3. 在委托管理员，选择 Remove。

如果组织管理帐户是中的已启用帐户 Security Hub，然后使用普通的选项卡设置页。

Security Hub 从设置页

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 在 Security Hub 导航窗格中，选择设置。然后选择。普通的。
3. 在委托管理员，选择 Remove。

删除 Security Hub 管理员帐户 (Security Hub API) Amazon CLI)

要删除 Security Hub 管理员帐户，可以使用 API 调用或 Amazon Command Line Interface。您必须使用组织管理帐户凭据。

当您使用 API 或 Amazon CLI 要删除 Security Hub 管理员帐户，只能在发出 API 调用或命令的区域中删除该帐户。Security Hub 不更新其他区域，也不会删除 Organizations 中的委派管理员帐户。

要删除 Security Hub 管理员帐户 (Security Hub API) , Amazon CLI)

- Security Hub API —使用 [DisableOrganizationAdminAccount](#) operation. 您必须提供 Security Hub 管理员帐户的帐户 ID。
- Amazon CLI—在命令行处，运行 [disable-organization-admin-account](#) 命令。

```
aws securityhub disable-organization-admin-account --admin-account-id <admin account ID>
```

示例

```
aws securityhub disable-organization-admin-account --admin-account-id 777788889999
```

删除委派管理员帐户 (Organizations API , Amazon CLI)

当您使用 Security Hub API 删除 Security Hub 管理员帐户时，只会在发出 API 调用或命令的区域中删除该帐户。Security Hub 不更新其他区域，也不会删除 Organizations 中的委派管理员帐户。

借助 Organizations API，您可以删除委派的管理员帐户。当您删除 Security Hub 的委派管理员帐户时，Security Hub 还会从所有区域中删除 Security Hub 管理员帐户。

要删除委派管理员帐户 (Organizations API) , Amazon CLI)

- Organizations API —使用 [DeregisterDelegatedAdministrator](#) operation. 您必须提供委派管理员帐户的帐户 ID 和 Security Hub 的服务委托人，即 securityhub.amazonaws.com。
- Amazon CLI—在命令行处，运行 [deregister-delegated-administrator](#) 命令。

```
aws organizations deregister-delegated-administrator --account-id <admin account ID> --service-principal <Security Hub service principal>
```

示例

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --service-principal securityhub.amazonaws.com
```

管理组织成员账户

对于组织帐户，Security Hub 管理员帐户可以执行以下操作。

- 自动 TREAT 新的将组织账户添加到组织 Security Hub 成员账户。
- REAT 现有的组织账户作为 Security Hub 成员账户。
- 取消关联并删除属于该组织的成员帐户。

要确保 Security Hub 管理员账户具有管理组织账户所需的权限，请将以下托管策略附加到关联的 IAM 委托人。

- [AWSSecurityHubFullAccess \(p. 24\)](#)

- [AWSSecurityHubOrganizationsAccess \(p. 25\)](#)

如果 Security Hub 管理员帐户尚未启用自动启用新组织帐户的选项，则账户页面顶部将显示一条消息。该消息包含一个启用选项。

Note

选择启用来自此消息会影响新添加的和现有的组织帐户。启用自动启用账户仅影响新添加的组织帐户。有关更多信息，请参阅 [自动启用新的组织账户 \(p. 39\)](#)。

在选择的时候启用，Security Hub 将所有现有组织账户视为成员账户，并在将新组织账户添加到组织时，自动将其视为成员账户。

对于未启用 Security Hub 的组织帐户，请启用 Security Hub 并启用 CISAmazon基金会基准标准和Amazon基础最佳实践标准。对于已启用 Security Hub 的组织帐户，Security Hub 不会对这些帐户进行任何其他更改。它不会更改其启用的标准或控件。

主题

- [自动启用新的组织账户 \(p. 39\)](#)
- [从您的组织启用成员账户 \(p. 40\)](#)
- [解除成员账户与组织的关联 \(p. 41\)](#)

自动启用新的组织账户

Security Hub 配置为自动启用新组织账户作为成员账户。

将新账户添加到您的组织后，它们会被添加到账户页。对于组织账户，类型是按组织。默认情况下，新账户未启用为成员账户。他们的状态是否为不是成员。

开启自动启用后，Security Hub 会处理新的在将账户添加到组织时，作为成员账户。开启自动启用不会处理现有的组织账户作为成员账户，除非已启用这些账户作为成员账户。如果帐户已经属于其他管理员帐户，Security Hub 也无法自动将其视为成员。

如果组织账户未启用 Security Hub，则Security Hub 和[默认标准 \(p. 252\)](#)会自动为该账户启用。

对于已启用 Security Hub 的组织帐户，Security Hub 不会对该帐户进行任何其他更改。它只创建成员资格。

请记住，所有Security Hub 账户都必须具有Amazon Config已启用并配置为记录所有资源。有关要求的详细信息Amazon Config，请参阅[the section called “启用 Amazon Config” \(p. 7\)](#)。

自动为新账户启用 Security Hub (控制台)

这些区域有：账户页面包含自动添加新帐户的配置选项。

自动启用新组织账户作为成员账户

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在 Security Hub 导航窗格中，选择设置。
3. 在存储库的设置页面上，选择账户。
4. 在存储库的账户选项卡上，将自动启用设置切换为“自动启用”功能。

自动为新组织帐户启用Security Hub (Security Hub API、Amazon CLI)

要确定是否自动启用新的组织帐户，Security Hub 管理员帐户可以使用 Security Hub API 或Amazon Command Line Interface。

自动启用新组织账户

- Security Hub (使用[UpdateOrganizationConfiguration](#) operation. 要自动启用新组织账户，将autoEnable到true.
- Amazon CLI–在命令行处，运行[update-organization-configuration](#)命令。

```
aws securityhub update-organization-configuration --auto-enable
```

从您的组织启用成员账户

如果您未自动启用新组织账户作为成员账户，则可手动启用这些账户作为成员账户。您还必须手动启用已取消关联的帐户。

如果某个账户已经是其他管理员账户的成员账户，则无法启用该账户。

您也无法启用当前已暂停的账户。如果您尝试启用已暂停的账户，账户状态将变为账户暂停账户。

在启用组织账户作为成员账户时，会出现以下情况：

- 如果账户未启用 Security Hub，则会为该账户启用 Security Hub。这些区域有：Amazon基础安全最佳实践和 CISAmazon该账户也启用了基金会基准标准。账户未收到邀请。

组织管理账户是例外。无法为组织管理帐户自动启用 Security Hub。在将组织管理帐户启用为成员帐户之前，组织管理帐户必须启用 Security Hub。

- 如果账户已启用 Security Hub，则 Security Hub 不会对该帐户进行任何其他更改。它仅启用成员资格。

请记住，所有Security Hub 账户都必须具有Amazon Config已启用并配置为记录所有资源。有关要求的详细信息Amazon Config，请参阅[the section called “启用 Amazon Config” \(p. 7\)](#)。

启用组织账户作为成员账户 (控制台)

在账户列表中，从未启用或已取消与 Security Hub 管理员帐户关联的组织帐户的状态为不是成员。

启用组织账户作为成员账户

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在 Security Hub 导航窗格中，选择设置. 然后选择 。账户.
3. 在账户列表中，选中要启用的每个组织账户的复选框。
4. 选择操作，然后选择添加成员。

启用组织账户作为成员账户 (Security Hub)Amazon CLI)

Security Hub 管理员账户可以使用 Security Hub API 或Amazon Command Line Interface以启用组织帐户。与手动邀请流程不同，当你使用[CreateMembers](#)要启用组织账户，您无需发送邀请。

启用组织账户作为成员账户

- Security Hub (使用[CreateMembers](#) operation. 对于要启用的每个账户，您需要提供账户 ID。
- Amazon CLI–在命令行处，运行[create-members](#)命令。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

示例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

解除成员账户与组织的关联

要停止接收和查看来自自己启用的成员帐户的调查结果，您可以取消关联该成员账户。

取消成员账户的关联，状态将更改为不是成员。

取消关联成员账户（控制台）

取消成员账户的关联

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在导航窗格中，选择 Settings (设置)。然后选择 帐户。
3. 在帐户列表中，选择要取消关联的帐户。你只能取消关联Enabled (已启用)帐户。
4. 选择操作，然后选择取消账户的关联。

取消关联账户（Security Hub API、Amazon CLI）

要取消关联成员账户，您可以使用 Security Hub API 或Amazon Command Line Interface。

要取消关联成员账户（Security Hub API，Amazon CLI）

- Security Hub (使用[DisassociateMembers](#)operation. 您必须提供Amazon要取消关联的成员账户的帐户ID。要查看成员帐户列表，请使用[ListMembers](#)operation.
- Amazon CLI–在命令行处，运行[disassociate-members](#)命令。

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

示例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

通过邀请管理会员账户

Amazon Security Hub还支持手动邀请过程。如果你不使用，你可以使用手动过程Amazon Organizations。

您还可以将此过程用于不属于您的组织的账户。例如，您可能不在组织中包含测试帐户。或者，您可能希望将来自多个组织的帐户合并到一个 Security Hub 管理员帐户下。Security Hub 管理员帐户必须向属于其他组织的帐户发送邀请。

在存储库的帐户选项卡的设置页面，通过邀请添加的帐户有类型设置为通过邀请。

如果您根本不使用 Organizations，那么当成员帐户接受邀请时，帐户将成为管理员帐户。

主题

- [添加和邀请会员账户 \(p. 42\)](#)
- [响应成为会员账户的邀请 \(p. 44\)](#)
- [取消成员账户的关联 \(p. 45\)](#)

- [删除成员账户 \(p. 46\)](#)
- [取消与管理员帐户的关联 \(p. 47\)](#)

添加和邀请会员账户

您的账户将成为接受邀请的账户的管理员账户。

当您接受其他账户的邀请时，您的账户将成为成员账户，该账户将成为您的管理员账户。

如果您的账户是管理员账户，则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. 管理员帐户将成员帐户添加到其成员账户列表中。
2. 管理员账户向成员账户发送邀请。
3. 会员账户接受邀请。

添加成员账户（控制台）

在 Security Hub 控制台中，您可以将帐户添加到成员帐户列表中。您可以单独选择账户，也可以上传 .csv 包含账户信息的文件。

对于每个账户，您必须提供账户 ID 和电子邮件地址。电子邮件地址应该是就帐户中的安全问题联系的电子邮件地址。它不用于验证账户。

将账户添加到成员账户列表

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 在左侧窗格中，选择 Settings (设置)。
3. 在存储库的设置选择页面，选择账户选择然后选择添加账户。然后，您可以单独添加帐户或上传 .csv 包含帐户列表的文件。
4. 要选择账户，请执行以下操作之一：
 - 要单独添加账户，请在下面输入账户，请输入要添加的账户的账户 ID 和电子邮件地址，然后选择 Add。

对每个账户重复此过程。

- 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。

在你的 .csv 列表中，账户必须每行一个。的第一行 .csv 文件必须包含标头。在标题中，第一列是 **Account ID** 第二栏是 **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。

下面是一个示例。 .csv 在文本编辑器中查看文件时。

```
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。底层格式仍以逗号分隔。您必须将账户 ID 格式化为非十进制数字。例如，账户 ID 444455556666 不能格式化为 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，请在控制台中，选择。上传列表 (.csv)。然后选择 。浏览。

选择文件后，选择。添加账户。

5. 添加完账户后，在下面。要添加的账户，选择下一步。

邀请会员账户 (控制台)

在添加成员账户后，您将向成员账户发送邀请。您还可以向已取消关联的账户重新发送邀请。

向新账户发送邀请

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>。
2. 在导航窗格中，选择和。设置选择，然后选择账户。
3. 要邀请的帐户，请选择邀请中的状态column。
4. 当系统提示确认时，选择。邀请。

向已取消关联的账户重新发送邀请

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>。
2. 在导航窗格中，选择和。设置选择，然后选择账户。
3. 选择要重新发送邀请的每个已取消关联的账户。
4. 从操作，选择重新发送邀请。

添加成员账户 (Security Hub API , Amazon CLI)

要添加成员账户，您可以使用 API 调用或Amazon Command Line Interface。您必须使用管理员帐户凭据。只有管理员帐户可以执行此操作。

要添加成员账户 (Security Hub API) , Amazon CLI)

- Security Hub API— 使用[CreateMembers](#)operation。对于要添加的每个会员账户，您必须提供Amazon账户 ID。
- Amazon CLI— 在命令行处，运行[create-members](#)命令。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

示例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

邀请会员账户 (Security Hub API , Amazon CLI)

要邀请添加的账户，可以使用 API 调用或Amazon Command Line Interface。你使用相同的 API 操作或者Amazon CLI命令可将邀请重新发送到已取消关联的成员帐户。您必须使用管理员帐户凭据。只有管理员帐户可以执行此操作。

要邀请成员账户 (Security Hub API) , Amazon CLI)

- Security Hub API— 使用[InviteMembers](#)operation。对于每个要邀请的账户，您必须提供Amazon账户 ID。

- Amazon CLI— 在命令行处，运行[invite-members](#)命令。

```
aws securityhub invite-members --account-ids <accountIDs>
```

示例

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

响应成为会员账户的邀请

您可以接受或拒绝成为成员账户的邀请。

在您接受邀请后，您的账户将变成Amazon Security Hub成员账户。发送邀请的账户将成为 Security Hub 管理员账户。管理员账户用户可以在 Security Hub 中查看成员账户的调查结果。

如果您拒绝邀请，则您的账户将被标记为已辞职在管理员帐户的成员帐户列表中。

你只能接受一个邀请成为会员账户。

在接受或拒绝邀请之前，您必须启用 Security Hub。有关如何启用 Security Hub 的信息，请参阅[the section called “手动启用 Security Hub” \(p. 10\)](#)。

请记住，所有 Security Hub 帐户都必须有Amazon Config启用并配置为记录所有资源。有关要求的详细信息Amazon Config请参阅[the section called “启用 Amazon Config” \(p. 7\)](#)。

接受邀请 (控制台)

在存储库的账户页面，管理员账户包含帐户的邀请和会员资格信息。

接受成为会员账户的邀请

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>。
2. 在导航窗格中，选择[和](#)。设置选择，然后选择账户。
3. 在管理员账户切换，切换Accept到开仓位，然后选择接受邀请。

接受邀请 (Security Hub API , Amazon CLI)

要接受成为会员账户的邀请，您可以使用 API 调用或Amazon Command Line Interface. 您必须使用收到邀请的成员账户的凭证。

要接受邀请 (Security Hub API) , Amazon CLI)

- Security HubAPI — 使用[AcceptAdministratorInvitation](#)operation. 您必须提供邀请标识符和Amazon管理员账户的账户 ID。要检索有关邀请的详细信息，请使用[ListInvitations](#)operation.
- Amazon CLI— 在命令行处，运行[accept-administrator-invitation](#)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 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 策略都必须继续使用AcceptInvitation. 您还应该添加AcceptAdministratorInvitation以确保在控制台开始使用之后存在正确的权限AcceptAdministratorInvitation.

拒绝邀请 (控制台)

您可以拒绝成为会员账户的邀请。当您拒绝邀请时，您的帐户会被标记为已辞职在管理员帐户的成员帐户列表中。

拒绝成为会员账户的邀请

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在导航窗格中，选择和。设置选择，然后选择账户。
3. 在管理员账户，选择拒绝邀请。

拒绝邀请 (Security Hub API , Amazon CLI)

要拒绝邀请，您可以使用 API 调用或Amazon Command Line Interface.

要拒绝邀请 (Security Hub API) , Amazon CLI)

- Security Hub API— 使用[DeclineInvitations](#)operation. 您必须提供Amazon发出邀请的管理员帐户的帐户 ID。要查看有关邀请的信息，请使用[ListInvitations](#)operation.
- Amazon CLI— 在命令行处，运行[decline-invitations](#)命令。

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

示例

```
aws securityhub decline-invitations --account-ids "123456789012"
```

取消成员账户的关联

登录管理员帐户后，可以取消成员帐户的关联，以停止接收和查看该账户的调查结果。要删除成员账户，必须先将其解除关联。

当您取消关联成员账户时，该账户将保留在您的会员账户列表中，状态为已删除（已取消关联）。您的账户将从成员账户的管理员帐户信息中删除。

要恢复接收账户的调查结果，您可以重新发送邀请。要完全删除成员账户，您可以删除成员账户。

取消关联成员账户 (控制台)

从账户页面中，您可以取消一个或多个成员账户的关联。

取消成员账户的关联

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在导航窗格中，选择和。设置选择，然后选择账户。

3. 在成员账户中，选择要取消关联的帐户。
4. 选择操作选择，然后选择取消账户的关联。

取消关联成员账户 (Security Hub API , Amazon CLI)

要取消关联会员账户，您可以使用 API 调用或Amazon Command Line Interface。

要取消关联成员账户 (Security Hub API) ， Amazon CLI)

- Security Hub API— 使用[DisassociateMembers](#)operation. 您必须提供Amazon要取消关联的成员账户的账户 ID。要查看成员账户列表，请使用[ListMembers](#)operation.
- Amazon CLI— 在命令行处，运行[disassociate-members](#)命令。

```
aws securityhub disassociate-members --account-ids <accountIds>
```

示例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

删除成员账户

作为管理员帐户，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，必须先将其解除关联。

删除成员账户时，它将从列表中完全删除。要恢复账户的会员资格，您必须添加它并邀请它，就好像它是一个全新的会员帐户一样。

删除成员账户 (控制台)

在 Security Hub 控制台中，您可以删除一个或多个账户。

删除成员账户

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在导航窗格中，选择和。设置选择，然后选择账户。
3. 在成员账户中，选择要删除的帐户。
4. 选择操作选择，然后选择删除账户。

删除成员账户 (Security Hub API , Amazon CLI)

要删除成员账户，您可以使用 API 调用或Amazon Command Line Interface。

要删除成员账户 (Security Hub API) ， Amazon CLI)

- Security Hub API— 使用[DeleteMembers](#)operation. 您必须提供Amazon要删除的成员账户的账户 ID。要检索成员账户列表，请使用[ListMembers](#)operation.
- Amazon CLI— 在命令行处，运行[delete-members](#)命令。

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

示例


```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

取消与管理员帐户的关联

如果您的账户是通过邀请添加为成员帐户的，则可以取消该成员账户与管理员帐户的关联。取消关联成员帐户后，Security Hub 不会将帐户中的调查结果发送到管理员帐户。使用 Organizations 管理的成员账户无法取消其账户与管理员帐户的关联。

当您取消与管理员帐户的关联时，您的帐户将保留在管理员帐户的成员列表中，状态为已辞职。但是，管理员帐户没有收到您账户的任何调查结果。

解除自己与管理员帐户的关联后，您可以再次接受邀请。

取消与管理员账户的关联（控制台）

您可以拒绝成为会员账户的邀请。要做到这一点，你需要更新Accept管理员账户的选项。

取消与管理员帐户的关联

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 在导航窗格中，选择。设置选择，然后选择账户。
3. 在管理员账户切换，切换Accept到关闭仓位，然后选择更新。

取消与管理员帐户的关联（Security Hub API，Amazon CLI）

要取消账户与管理员帐户的关联，您可以使用 API 调用或Amazon Command Line Interface.

要取消与管理员帐户的关联（Security Hub API），Amazon CLI）

- Security Hub API— 使用[DisassociateFromAdministratorAccount](#)operation.
- Amazon CLI— 在命令行处，运行[disassociate-from-administrator-account](#)命令。

```
aws securityhub disassociate-from-administrator-account
```

Note

Security Hub 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 策略都必须继续使用DisassociateFromMasterAccount. 您还应该添加DisassociateFromAdministratorAccount以确保在控制台开始使用之后存在正确的权限DisassociateFromAdministratorAccount.

帐户操作对 Security Hub 数据的影响

这些账户操作将对以下影响：Amazon Security Hub“数据”。

禁用 Security Hub

禁用 Security Hub 为账户禁用 Security Hub 时，将仅在Amazon禁用它时选择的区域。

您必须在启用 Security Hub 的每个区域分别禁用 Security Hub。

禁用 Security Hub 时，不会为管理员账户生成新的结果。现有结果将在 90 天后删除。

已删除与 Amazon Macie、Amazon GuardDuty 和 Amazon Inspector 的集成。

不会删除 Security Hub 的其他数据和设置，包括自定义操作、见解和第三方产品订阅。

已启用的安全标准将被禁用。

成员账户与管理员账户取消关联

成员账户与管理员账户取消关联后，管理员账户将失去查看该成员账户中的结果的权限。

Security Hub 继续在主账户及成员账户中运行。

为管理员账户定义的自定义设置或集成不会应用到前成员账户中的结果。例如，取消账户关联后，您可能在管理员账户中执行自定义操作，将其用作 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。

会员账户已从组织中删除

成员账户从组织中删除后，Security Hub 管理员账户将失去查看该成员账户中的结果的权限。

Security Hub 继续在主账户及成员账户中运行。

在账户 Security Hub 管理员账户的列表，该账户的状态为取消关联。

暂停账户

暂停账户的时间 Amazon，该账户失去了在 Security Hub 中查看其调查结果的权限。不会为该账户生成新的结果。暂停账户的管理员账户可以查看现有的账户调查结果。

对于组织账户，成员账户状态也可以更改为已暂停账户。如果账户在管理员账户尝试启用该账户的同时被暂停，则会发生这种情况。的管理员账户已暂停账户无法查看该账户的调查结果。

否则，暂停状态不会影响成员账户状态。

90 天后，账户要么被终止或重新激活。重新激活账户后，其 Security Hub 权限将恢复。如果会员账户状态为已暂停账户，管理员账户必须手动启用该账户。

账户已关闭

当 Amazon 账户已关闭，Security Hub 对关闭做出如下响应。

Security Hub 将在账户关闭生效之日起 90 天内保留该账户的结果。在 90 天期限结束时，Security Hub 将永久删除该账户的所有结果。

- 要将结果保留 90 天以上，您可以使用采用 EventBridge 规则的自定义操作将结果存储到 Amazon S3 存储桶中。只要 Security Hub 保留调查结果，当您重新打开已关闭的账户时，Security Hub 就会恢复该账户的调查结果。
- 如果该账户是 Security Hub 管理员账户，则以管理员身份删除该账户，并删除所有成员账户。如果该账户是成员账户，则会将其取消关联并将其作为成员从 Security Hub 管理员账户中删除。
- 有关更多信息，请参阅 [关闭账户](#)。

Important

对于 Amazon GovCloud (US) 区域的客户：

- 在关闭账户前，备份并删除您的策略数据和其他账户资源。关闭账户后，您将不再拥有其访问权限。

跨区域聚合

借助跨区域聚合，您可以将调查结果、查找更新、洞察、控制合规性状态和安全分数从多个区域汇总到单个聚合区域。然后，您可以从聚合区域管理所有这些数据。

Note

跨区域聚合可用，但存在以下限制Amazon GovCloud (US)和中国区域。在Amazon GovCloud (US)，跨区域聚合仅支持调查结果、查找更新和洞察Amazon GovCloud (US)。具体而言，您只能汇总调查结果、查找更新和洞察Amazon GovCloud (US-East) Amazon GovCloud (美国西部)。在中国区域中，跨区域聚合仅支持跨中国区域的调查结果、查找更新和洞察。具体而言，您只能汇总中国（北京）和中国（宁夏）之间的发现、更新和见解。

假定您将美国东部（弗吉尼亚北部）设置为聚合区域，将美国西部（俄勒冈）和美国西部（加利福尼亚北部）设置为链接区域。当您查看结果页面上的美国东部（弗吉尼亚北部），您可以看到所有三个区域的调查结果。这些调查结果的最新情况也反映在所有三个区域。

在聚合区域中，摘要页面提供了跨链接区域的活跃调查结果的视图。请参阅 [the section called “查看跨区域调查结果摘要” \(p. 62\)](#)。其他摘要分析结果的页面面板还会显示来自链接区域的信息。

您在聚合区域中的安全分数是通过比较所有关联区域中已通过控制的数量与已启用控件的数量来计算的。此外，如果某个控件在至少一个链接的区域中启用，则该控件在安全标准聚合区域的详细信息页面。标准详情页面上控制措施的合规性状态反映了各个关联区域的调查结果。如果在一个或多个关联区域中与控件关联的安全检查失败，则该控件的合规性状态将显示为已失败在聚合区域的标准详情页面上。安全检查的数量包括来自所有关联区域的调查结果。

必须在每个区域修改控件的启用状态。如果在链接区域中启用了控件，但在聚合区域中禁用了控件，则可以从聚合区域中查看该控件的合规性状态，但不能从聚合区域启用或禁用该控件。

要查看跨区域安全分数和合规性状态，请在您的 IAM 策略中添加以下权限：

- ListSecurityControlDefinitions
- BatchGetStandardsControlAssociations
- BatchUpdateStandardsControlAssociations

请注意，这些 IAM 权限名称与当前Security Hub API 不直接对应。

主题

- [跨区域聚合 \(p. 50\)](#)
- [查看当前的跨区域聚合配置 \(p. 52\)](#)
- [启用跨区域聚合 \(p. 52\)](#)
- [更新跨区域聚合配置 \(p. 53\)](#)
- [停止跨区域聚合 \(p. 55\)](#)

跨区域聚合

跨区域聚合由独立账户和管理员账户配置。成员账户从其管理员账户继承跨区域聚合配置。

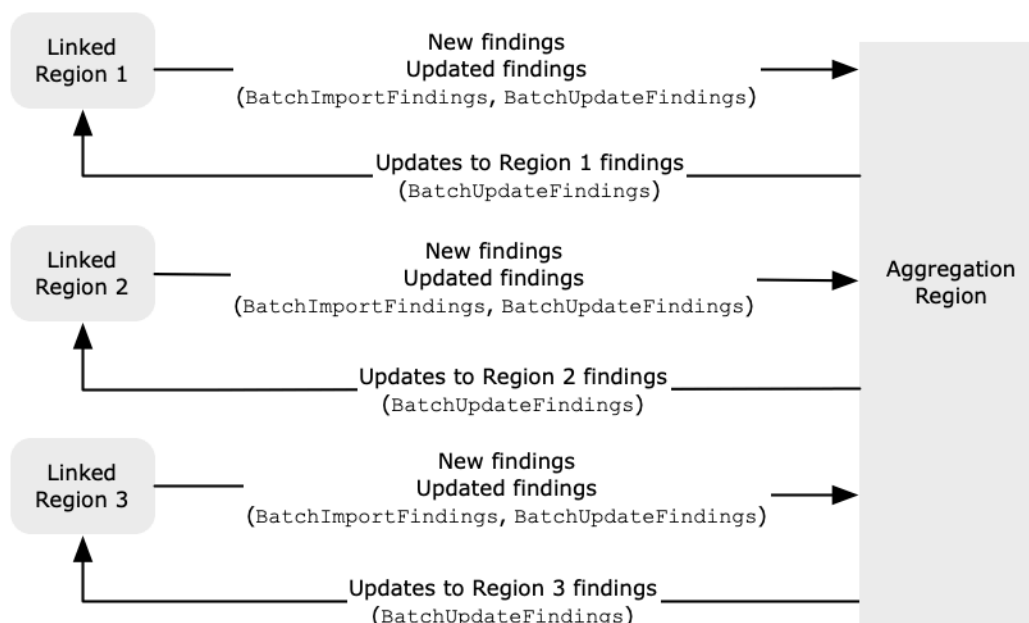
成员账户与管理员账户取消关联后，该成员账户的跨区域聚合将停止。即使账户在成为成员账户之前已启用跨区域聚合，也是如此。

跨区域聚合基于聚合区域和关联区域。

聚合新数据并复制数据更新

启用跨区域聚合后，Security Hub 会将链接区域的新发现、见解、控制合规性状态和安全分数汇总到聚合区域。

Security Hub 还会在链接的区域和聚合区域之间复制此数据的更新。链接区域中发生的更新将复制到聚合区域。聚合区域中发生的更新将复制回原始链接区域。



如果聚合区域和链接区域中存在冲突的更新，则使用最新的更新。

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

确定要从中汇总数据的账户

Security Hub 仅汇总账户启用了 Security Hub 区域的数据。根据跨区域聚合配置，不会为账户自动启用 Security Hub。

当管理员账户配置跨区域聚合时，Security Hub 会在链接的区域中标识该管理员账户的成员账户。

在每个关联的区域中，该管理员账户的每个成员账户都将继承跨区域聚合配置。Security Hub 将他们的发现、见解、控制状态和安全分数汇总到聚合区域。

如果来自聚合区域的成员账户不是关联区域中的成员账户，则 Security Hub 不会汇总该区域中该账户的数据。

如果您计划使用跨区域聚合，并且有多个管理员账户，那么 Security Hub 推荐以下最佳实践：

- 每个管理员账户在不同区域都有相同的成员账户。
- 每个管理员账户都有不同的成员账户。
- 每个管理员账户使用不同的聚合区域。

查看当前的跨区域聚合配置

您可以从任何区域查看当前的跨区域聚合配置。该配置包括聚合区域、链接的区域以及是否自动链接新区域。

查看跨区域聚合配置（控制台）

这些区域有：区域的选项卡设置页面显示当前的跨区域聚合配置。您可以从任何区域查看配置。成员账户还可以查看管理员账户配置的跨区域配置。

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。请参阅 [the section called “启用跨区域聚合” \(p. 52\)](#)。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：

- 聚合区域
- 是否自动汇总来自 Security Hub 支持且您选择加入的新区域的调查结果、见解、控制状态和安全分数
- 链接的区域列表

查看当前的跨区域聚合配置（Security Hub API、Amazon CLI）

您可以使用 Security Hub API 或 Amazon CLI 以查看当前的跨区域聚合配置。您可以从任何区域查看跨区域聚合配置。

要查看当前的跨区域聚合配置（Security Hub API），Amazon CLI）

- Security Hub 使用 [GetFindingAggregator](#) API。当您发出请求时，必须提供查找聚合器 ARN。要获取查找聚合器 ARN，请使用 [ListFindingAggregators](#)。
- Amazon CLI：在命令行处，运行 [get-finding-aggregator](#) 命令。要获取查找聚合器 ARN，请使用 [list-finding-aggregators](#)。

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator ARN>
```

启用跨区域聚合

您必须从将成为聚合区域的区域启用跨区域聚合。

您不能将默认禁用的区域用作聚合区域。有关默认情况下禁用的区域的列表，请参阅 [启用区域](#) 中的 Amazon 一般参考。

启用跨区域聚合（控制台）

启用跨区域聚合时，您可以选择关联的地区。您还可以选择在 Security Hub 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。

启用跨区域聚合

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 将更改为您要用作聚合区域的区域。

3. 在Security Hub设置，然后选择区域。
4. UN调查结果，选择配置查找聚合。

默认情况下，聚合区域设置为没有聚合区域。

5. UN聚合区域，请选择单选按钮将当前区域指定为聚合区域。
6. UN已关联区域中，选择要从中聚合数据的区域。
7. 要自动聚合分区中新区域的数据，因为 Security Hub 支持这些区域并且您选择加入这些区域，请选择链接future 区域。
8. 选择Save (保存)。

启用跨区域聚合 (Security Hub API、Amazon CLI)

您可以使用Security Hub API 来启用跨区域聚合。

要从 Security Hub API 启用跨区域聚合，请创建查找聚合器。您必须从要用作聚合区域的区域创建查找聚合器。

要创建查找聚合器 (Security Hub API) , Amazon CLI)

- Security Hub 在要用作聚合区域的区域中，使用 [CreateFindingAggregator](#) operation。适用于 `RegionLinkingMode`，您可以从以下选项中进行选择：
 - `ALL_REGIONS`— Security Hub 汇总来自所有区域的数据。Security Hub 还会汇总来自新区域的数据，因为它们受支持且您选择加入这些区域。
 - `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub 汇总除要排除的区域之外的所有区域的数据。Security Hub 还会汇总来自新区域的数据，因为它们受支持且您选择加入这些区域。使用 `Regions` 以提供要从聚合中排除的区域列表。
 - `SPECIFIED_REGIONS`— Security Hub 汇总选定区域列表中的数据。Security Hub 不会自动聚合来自新区域的数据。使用 `Regions` 以提供要从中进行聚合的区域列表。
- Amazon CLI：在命令行处，运行 `create-finding-aggregator` 命令。

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-linking-  
mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region  
list>
```

在以下示例中，为选定的区域配置了跨区域聚合。聚合合合合合合合合合合合合合合合合合合合合合合合相关的区域是美国西部（加利福尼亚北部）和美国西部（俄勒冈）。

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
SPECIFIED_REGIONS --regions us-west-1,us-west-2
```

更新跨区域聚合配置

您可以更新跨区域聚合配置以更改当前聚合区域的链接区域。您还可以更改是否自动汇总来自新区域的调查结果、见解、控制状态和安全分数。

当您停止聚合来自链接区域的数据时，Security Hub 不会从聚合区域中删除任何现有的聚合数据。

您不能使用更新过程来更改聚合区域。要更改聚合

1. 停止跨区域聚合。请参阅 [the section called “停止跨区域聚合” \(p. 55\)](#)。
2. 将更改为您要作为新聚合区域的区域。

3. 启用跨区域聚合。请参阅 [the section called “启用跨区域聚合” \(p. 52\)](#)。

更新跨区域聚合配置 (控制台)

您必须从当前聚合区域更新跨区域聚合配置。

在聚合区域以外的区域中，调查结果面板会显示一条消息，提示您必须编辑聚合区域中的配置。选择此消息可显示定位至聚合区域的链接。

更改当前聚合区域的链接区域

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>。
2. 更改为当前聚合区域。
3. 在Security Hub设置，然后选择区域。
4. UN调查结果，选择编辑。
5. UN已关联区域，更新选定的链接区域。
6. 如果需要，请更改链接future 区域已Select。此设置确定 Security Hub 在添加对新区域的支持以及您选择加入这些区域时是否自动链接新区域。
7. 选择Save (保存)。

更新跨区域聚合配置 (Security Hub API、Amazon CLI)

您可以使用Security Hub API 或Amazon CLI更新跨区域聚合配置。您必须从当前聚合区域更新跨区域聚合。

您可以更改 Regificate (区域链接)。如果链接模式是ALL_REGIONS_EXCEPT_SPECIFIED要么SPECIFIED_REGIONS，您可以更改 certificate (排除或包含区域)。

当您更改已排除或包含的区域列表时，必须提供完整列表和更新。例如，假定您目前正在汇总美国东部 (俄亥俄) 的调查结果，并且还要汇总美国西部 (俄勒冈) 的调查结果。当您打电话的时候[UpdateFindingAggregator](#)，您提供一个Regions同时包含美国东部 (弗吉尼亚北部) 和美国西部 (弗吉尼亚北部)。

要更新跨区域聚合 (Security Hub API)，Amazon CLI)

- Security Hub 使用 [UpdateFindingAggregator](#) API 操作。要标识查找聚合器，您必须提供查找聚合器 ARN。要获取查找聚合器 ARN，请使用[ListFindingAggregators](#)。

您提供区域链接模式和已排除或包含的区域的更新列表。

- Amazon CLI：在命令行处，运行[update-finding-aggregator](#)命令。

```
aws securityhub update-finding-aggregator --region <aggregation Region> --finding-aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
```

在以下示例中，跨区域聚合配置更改为选定区域的聚合。该命令从当前的聚合区域 (即美国东部 (弗吉尼亚北部) 中运行。关联的区域是美国西部 (加利福尼亚北部) 和美国西部 (俄勒冈)。

```
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

如果您不想再聚合数据或想要更改聚合区域，请停止跨区域聚合。

当您停止跨区域聚合时，Security Hub 将停止聚合数据。它不会从聚合区域中删除任何现有的聚合数据。

停止跨区域聚合（控制台）

您必须停止当前聚合区域的跨区域聚合。

在聚合区域以外的区域中，调查结果面板会显示一条消息，提示您必须编辑聚合区域中的配置。选择此消息可显示切换到聚合区域的链接。

停止跨区域聚合

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 更改为当前聚合区域。
3. 在Security Hub设置，然后选择区域。
4. 单击调查结果，选择编辑。
5. 单击聚合区域，选择没有聚合区域。
6. 选择Save（保存）。
7. 在确认对话框的确认字段中，键入**Confirm**。
8. 选择 Confirm（确认）。

停止跨区域聚合（Security Hub API、Amazon CLI）

您可以使用Security Hub API 停止跨区域聚合。您必须停止聚合区域的跨区域聚合。

要停止跨区域聚合（Security Hub API），Amazon CLI）

- Security Hub 使用[DeleteFindingAggregator](#)operation. 要标识要删除的查找聚合器，您需要提供查找聚合器 ARN。要获取查找聚合器 ARN，请使用[ListFindingAggregators](#)。
- Amazon CLI：在命令行处，运行[delete-finding-aggregator](#)命令。

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --region <aggregation Region>
```

Amazon Security Hub 中的发现

Amazon Security Hub 消除了处理来自多个提供商的大量发现的复杂性。它减少了管理和提高所有 Amazon 账户、资源和工作负载的安全性所需的工作量。

Security Hub 从以下来源接收调查结果。

- 与您启用的 Amazon 安全服务集成。请参阅 [the section called “Amazon 服务集成” \(p. 211\)](#)。
- 与您启用的第三方产品集成。请参阅 [the section called “第三方产品集成” \(p. 221\)](#)。
- 您配置的自定义集成。请参阅 [the section called “使用自定义产品集成” \(p. 241\)](#)。
- Security Hub 检查已启用的控件。请参阅 [the section called “生成和更新控制结果” \(p. 245\)](#)。

Security Hub 使用一种称为 Amazon 安全查找结果格式的标准发现结果格式来使用调查结果。有关结果格式的更多信息，请参阅 [the section called “结果格式” \(p. 68\)](#)。

Security Hub 将集成产品的发现关联起来，优先考虑最重要的产品。

结果提供商可以更新结果，以反映结果的其他实例。您可以更新结果以提供有关调查及其结果的详细信息。

Security Hub 还允许您汇总各个区域的调查结果，以便您可以从一个地方查看所有发现。请参阅 [跨区域聚合 \(p. 50\)](#)。

主题

- [在中创建和更新调查结果 Amazon Security Hub \(p. 56\)](#)
- [查看按严重程度划分的跨区域发现结果摘要 \(p. 62\)](#)
- [在中查看查找结果列表和详细信息 Amazon Security Hub \(p. 63\)](#)
- [对结果采取措施 Amazon Security Hub \(p. 66\)](#)
- [Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)

在中创建和更新调查结果 Amazon Security Hub

在 Amazon Security Hub 中，结果可以来自以下类型的结果提供商之一。

- 与其他 Amazon 服务的启用集成
- 与第三方提供商的启用集成
- Security Hub 中启用控件

创建结果后，可以由结果提供商或客户进行更新。

- 结果提供商使用 [BatchImportFindings](#) API 操作更新有关结果的一般信息。结果提供商只能更新他们创建的结果。
- 客户使用 [BatchUpdateFindings](#) API 操作来反映调查结果的状态。[BatchUpdateFindings](#) 也可以由代表客户的票证、事件管理、协调、补救或 SIEM 工具使用。

在 Security Hub 控制台中，客户可以管理发现结果的工作流状态并将发现结果发送到自定义操作。请参阅 [the section called “对结果采取措施” \(p. 66\)](#)。

Security Hub 还会自动更新和删除发现结果。

如果在过去 90 天内未更新所有查找结果，则会自动删除这些结果。

如果您启用跨区域聚合，则 Security Hub 会自动将来自关联区域的新发现聚合到聚合区域。Security Hub 还会复制调查结果的更新。在链接区域中发生的更新将复制到聚合区域。聚合区域中发生的更新将复制到原始链接区域。有关跨区域聚合的更多信息，请参阅[跨区域聚合 \(p. 50\)](#)。

主题

- [使用 BatchImportFindings 创建和更新结果 \(p. 57\)](#)
- [使用 BatchUpdateFindings 更新结果 \(p. 59\)](#)

使用 BatchImportFindings 创建和更新结果

结果提供商使用 [BatchImportFindings](#) API 操作创建新结果，并更新他们所创建结果的相关信息。他们无法更新他们没有创建的结果。

客户、SIEMS、票证工具和 SOAR 工具使用 [BatchUpdateFindings](#) 进行与处理结果提供商的结果相关的更新。请参阅 [the section called “使用 BatchUpdateFindings” \(p. 59\)](#)。

每当 Amazon Security Hub 收到创建或更新调查结果的 [BatchImportFindings](#) 请求时，它都会自动在亚马逊中生成一个 Security Hub Findings - Imported 事件 EventBridge。请参阅 [自动响应和补救 \(p. 500\)](#)。

对账户和批量大小的要求

[BatchImportFindings](#) 必须由以下任一方法调用：

- 与结果相关的账户。关联账户的标识符是调查结果的 `AwsAccountId` 属性的值。
- 已列入允许进行官方 Security Hub 合作伙伴集成的账户。

Security Hub 只能接受已启用 Security Hub 账户的查找更新。还必须启用结果提供商。如果 Security Hub 被禁用或未启用查找提供程序集成，则将在 `FailedFindings` 列表中返回查找结果，但 `InvalidAccess` 会出现错误。

[BatchImportFindings](#) 每批最多接受 100 个搜索结果，每个查找结果最多 240 KB，每批最多接受 6 MB 的搜索结果。限制速率限制为每个区域每个账户 10 TPS，突增速率为 30 TPS。

确定是创建还是更新结果

要确定是创建还是更新调查结果，Security Hub 会检查该 ID 字段。如果 ID 的值与现有结果不匹配，则会创建一个新结果。

如果 ID 确实与现有查找结果相匹配，则 Security Hub 会检查该 `UpdatedAt` 字段是否有更新。

- 如果更新 `UpdatedAt` 时与现有查找结果匹配或之前发生过 `UpdatedAt`，则更新将被忽略。
- 如果更新的 `UpdatedAt` 出现在现有结果的 `UpdatedAt` 之后，则更新现有结果。

的受限属性 BatchImportFindings

对于现有发现，查找提供者不能 [BatchImportFindings](#) 用于更新以下属性和对象。只能使用更新这些属性 [BatchUpdateFindings](#)。

- `Note`
- `UserDefinedFields`
- `VerificationState`

- Workflow

Security Hub 会忽略这些属性和对象中的 [BatchImportFindings](#) 任何内容。客户或代表他们行事的其他提供商使用 [BatchUpdateFindings](#) 来更新它们。

使用 FindingProviderFields

查找提供者也不应 [BatchImportFindings](#) 用于更新以下属性。

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

相反，查找提供者使用 [FindingProviderFields \(p. 121\)](#) 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 会按以下方式处理顶级属性和中的 [FindingProviderFields \(p. 121\)](#) 值。

(首选) 为中的属性 [BatchImportFindings](#) 提供值 [FindingProviderFields \(p. 121\)](#)，但不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 更新中属性的值 [FindingProviderFields \(p. 121\)](#)。

仅当顶级属性尚未更新时，它才会将该值复制到顶级属性 [BatchUpdateFindings](#)。

[BatchImportFindings](#) 为顶级属性提供值，但未提供中相应属性的值 [FindingProviderFields \(p. 121\)](#)。

例如，[BatchImportFindings](#) 提供 `Confidence`，但不提供 `FindingProviderFields.Confidence`。

Security Hub 使用该值更新中的属性 [FindingProviderFields \(p. 121\)](#)。它会覆盖任何现有值。

只有当顶级属性尚未更新时，Security Hub 才会更新该属性 [BatchUpdateFindings](#)。

[BatchImportFindings](#) 为顶级属性和中的相应属性提供值 [FindingProviderFields \(p. 121\)](#)。

例如，同时 [BatchImportFindings](#) 提供 Confidence 和 FindingProviderFields.Confidence。

对于新的查找结果，Security Hub 使用中的值 [FindingProviderFields \(p. 121\)](#) 来填充中的顶级属性和相应的属性 [FindingProviderFields \(p. 121\)](#)。它不使用提供的顶级属性值。

对于现有查找结果，Security Hub 使用这两个值。但是，只有当该属性尚未更新时，它才会更新顶级属性值 [BatchUpdateFindings](#)。

使用来自的 batch-import-findings 命令 Amazon CLI

在中 Amazon Command Line Interface，您可以使用 [batch-import-findings](#) 命令创建或更新调查结果。

您以 JSON 对象的形式提供每个结果作为 JSON 对象提供。

示例

```
aws securityhub batch-import-findings --findings '[
  {
    "AwsAccountId": "123456789012",
    "CreatedAt": "2019-08-07T17:05:54.832Z",
    "Description": "Vulnerability in a CloudTrail trail",
    "FindingProviderFields": {
      "Severity": {
        "Label": "INFORMATIONAL",
        "Original": "0"
      },
      "Types": [
        "Software and Configuration Checks/Vulnerabilities/CVE"
      ]
    },
    "GeneratorId": "TestGeneratorId",
    "Id": "Id1",
    "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/default",
    "Resources": [
      {
        "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
        "Partition": "aws",
        "Region": "us-west-1",
        "Type": "AwsCloudTrailTrail"
      }
    ],
    "SchemaVersion": "2018-10-08",
    "Title": "CloudTrail trail vulnerability",
    "UpdatedAt": "2020-06-02T16:05:54.832Z"
  }
]'
```

使用 BatchUpdateFindings 更新结果

[BatchUpdateFindings](#) 用于更新与客户处理来自查找提供商的调查结果相关的信息。它可以由客户使用，也可以由代表客户工作的 SIEM、票证、事件管理或 SOAR 工具使用。[BatchUpdateFindings](#) 不能用于创建新发现。它可以用来一次更新多达 100 个结果。

每当 Security Hub 收到更新调查结果的 [BatchUpdateFindings](#) 请求时，它都会自动在亚马逊中生成一个 Security Hub Findings - Imported 事件 EventBridge。请参阅 [自动响应和补救 \(p. 500\)](#)。

[BatchUpdateFindings](#) 不会更改结果的 UpdatedAt 字段。UpdatedAt 仅反映来自结果提供商的最新更新。

的可用字段BatchUpdateFindings

管理员帐户可以使用更新[BatchUpdateFindings](#)其帐户或其成员帐户的搜索结果。成员帐户可以使用[BatchUpdateFindings](#)来更新其帐户的调查结果。

客户只能[BatchUpdateFindings](#)使用更新以下字段和对象。

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

默认情况下，管理员和成员帐户有权访问上述所有字段和字段值。Security Hub 还提供上下文密钥，允许您限制对字段和字段值的访问。

例如，您可能只允许成员帐户设置Workflow.Status为RESOLVED。或者您可能不想允许更改成员帐户Severity.Label。

配置对的访问权限BatchUpdateFindings

您可以配置 IAM 策略以限制访问权限 [BatchUpdateFindings](#)，使用更新字段和字段值。

在限制访问的语句中 [BatchUpdateFindings](#)，使用以下值。

- Action 是 securityhub:BatchUpdateFindings
- Effect 是 Deny
- 对于Condition，您可以基于以下理由拒绝[BatchUpdateFindings](#)请求：
 - 该发现包括一个特定的字段。
 - 该发现包括一个特定的字段值。

条件键

这些是限制访问的条件键[BatchUpdateFindings](#)。

ASFF 字段

ASFF 字段的条件键如下所示。

```
securityhub:ASFFSyntaxPath/<fieldName>
```

<fieldName>替换为 ASFF 字段。

例如，要限制对该Workflow.Status字段的访问权限，请使用 securityhub:ASFFSyntaxPath/Workflow.Status。

不允许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 workflow 状态。

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "Null": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
    }
  }
}
```

禁用特定字段值

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](#)不能用于设置 Workflow.Status 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列表。

```
"Condition": {
  "ForAnyValue:StringEquals": {
    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
    "<fieldValue2>", "<fieldValuen>" ]
  }
}
```

例如，以下语句表示[BatchUpdateFindings](#)不能用于将设置 Workflow.Status 为 RESOLVED 或 SUPPRESSED。

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
```

```
"Condition": {
  "ForAnyValue:StringEquals": {
    "securityhub:ASFFSyntaxPath/Workflow.Status": [
      "RESOLVED",
      "NOTIFIED"
    ]
  }
}
```

使用来自的 `batch-update-findings` 命令 Amazon CLI

在中 Amazon Command Line Interface，您可以使用 `batch-update-findings` 命令更新调查结果。

对于要更新的每个调查结果，您需要提供调查结果 ID 和生成调查结果的产品的 ARN。

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
ID="<findingID2>",ProductArn="<productARN2>"
```

当您提供要更新的属性时，可以使用 JSON 格式或快捷方式格式。

以下是使用 JSON 格式的 Note 对象更新的示例：

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

以下是使用快捷方式格式的同更新：

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

Amazon CLI 命令参考为每个字段提供了 JSON 和快捷方式语法。

以下 `batch-update-findings` 示例更新了两个发现结果以添加注释、更改严重性标签并解决这些问题。

```
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-2::product/aws/securityhub"
Id="arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status": "RESOLVED"}'
```

这是相同的示例，但使用快捷方式而不是 JSON。

```
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"
Id="arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --note Text="Known issue that is not a risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

查看按严重程度划分的跨区域发现结果摘要

在“摘要”页面上，“按区域划分的调查结果”汇总了各区域中每种严重程度的有效发现数量。计数仅包括工作流状态为 NEW 或的调查结果 NOTIFIED。

在启用跨区域聚合之前，按区域划分的调查结果仅汇总当前区域的调查结果。它提供了配置跨区域聚合的链接。

启用跨区域聚合后，“按区域划分的调查结果”仅显示在聚合区域中。它不显示在链接的区域中。该小组总结了所有关联区域的调查结果。

默认情况下，该列表仅显示具有匹配结果的链接区域。要显示所有关联区域，包括没有匹配结果的关联区域，请选择所有关联区域。要仅显示具有匹配结果的关联区域，请选择具有搜索结果的关联区域。

当您为区域选择严重性值时，将显示调查结果列表。该列表按选定的区域和严重性进行筛选。还会对列表进行筛选，以显示工作流程状态为NEW或的活跃发现NOTIFIED。

在中查看查找结果列表和详细信息Amazon Security Hub

在 Amazon Security Hub 导航窗格中，Findings (结果) 显示来自所有已启用的产品集成和控制的结果列表。

通过 Integrations (集成)，您可以显示启用的集成生成的结果列表。请参阅 [the section called “查看来自集成的结果” \(p. 210\)](#)。

从 Insights (见解) 中，您可以显示匹配的见解结果的调查结果列表。请参阅 [the section called “查看见解结果和调查结果” \(p. 195\)](#)。

根据 Security standards (安全标准)，您可以显示从所选控制生成的结果列表。请参阅 [the section called “查看控制结果并采取相应措施” \(p. 261\)](#)。

您还可以使用 [GetFindings](#) API 操作检索筛选的结果列表。

如果您启用查找聚合，则可以查看来自各个区域的调查结果。在聚合区域中，调查结果和见解页面包含来自聚合区域和关联区域的发现。在其他地区，这些页面仅包含该地区的调查结果。有关如何配置查找聚合的信息，请参阅 [跨区域聚合 \(p. 50\)](#)。

主题

- [对发现结果进行筛选和分组（控制台） \(p. 63\)](#)
- [查看结果详细信息（控制台） \(p. 65\)](#)
- [检索查找详情（Security Hub API，Amazon CLI） \(p. 66\)](#)

对发现结果进行筛选和分组（控制台）

当您显示调查结果页面、集成页面或 Insights 页面中的发现结果列表时，该列表将始终根据记录状态和工作流状态进行筛选。这是对用于洞察或整合的过滤器的补充。

记录状态指示结果处于活动状态还是存档状态。查找结果可由结果提供商存档。如果删除了关联的资源，Amazon Security Hub 还会自动存档控件的查找结果。默认情况下，结果列表仅显示活动结果。

工作流程状态指示对结果进行调查的状态。工作流程状态只能由 Security Hub 客户或代表客户运行的系统更新。默认情况下，结果列表仅显示工作流程状态为 NEW 或 NOTIFIED 的结果。控制的默认结果列表还包括 RESOLVED 结果。

如果您启用了查找聚合，则在“调查结果和见解”页面上，您可以按地区筛选发现。

有关使用控件的查找列表的信息，请参阅 [the section called “筛选和排序组件” \(p. 261\)](#)。

添加筛选器

要更改列表的范围，您可以向列表添加筛选器。

您最多可以按 10 个属性进行筛选。对于每个属性，您最多可以提供 20 个筛选值。

筛选查找结果列表时，Security Hub 会将 AND 逻辑应用于筛选器集。换句话说，仅在结果符合所有提供的筛选条件时才被视为匹配的结果。例如，如果您添加 GuardDuty 为产品名称的筛选条件和 AwsS3Bucket 资源类型的筛选条件，则匹配的查找结果必须匹配这两个标准。

但是，Security Hub 会将 OR 逻辑应用于使用相同属性但值不同的筛选器。例如，您将 GuardDuty 和 Amazon Inspector 添加为产品名称的筛选值。在这种情况下，如果发现结果是由 Amazon Inspector 生成的，则匹配结果。GuardDuty

向结果列表添加筛选器

1. 通过 <https://console.aws.amazon.com/securityhub/> 打开 Amazon Security Hub 控制台。
2. 要显示结果列表，请执行以下操作之一：
 - 在 Security Hub 导航窗格中，选择查找结果。
 - 在 Security Hub 导航窗格中，选择 Insights。选择洞察力。然后在结果列表中，选择一个洞察结果。
 - 在 Security Hub 导航窗格中，选择集成。选择“查看调查结果”以进行集成。
3. 选中“添加筛选器”框。
4. 在菜单的“筛选器”下，选择一个过滤器。

请注意，当您按公司名称或产品名称进行筛选时，Security Hub 使用顶级 CompanyName 和 ProductName 字段。API 使用中的值 ProductFields。

5. 选择筛选器匹配类型。

对于字符串过滤器，可以从以下比较选项中进行选择：

- 是 — 查找与筛选器值完全匹配的值。
- 开头为 — 找到一个以过滤器值开头的值。
- 不是 — 查找与筛选器值不匹配的值。
- 不以此开头 — 查找一个不是以过滤器值开头的值。

对于数字筛选器，您可以选择是提供单个数字（简单）还是数字范围（范围）。

对于日期或时间筛选器，您可以选择是提供自当前日期和时间（滚动窗口）起的时间长度，还是提供特定日期范围（固定范围）的时间长度。

添加多个过滤器具有以下交互作用：

- 是和开头的过滤器由 OR 连接。如果一个值包含任何筛选器值，则该值匹配。例如，如果您将严重性标签指定为“严重”，“严重性”标签为“高”，则结果将包括“严重”和“高”两个严重性发现结果。
- 不是且不以此开头的过滤器由 AND 连接。只有当一个值不包含任何这些筛选值时，该值才匹配。例如，如果您指定严重性标签不是“低”，“严重性”标签不是“中”，则结果不包括严重性低或中等严重性结果。

如果在某个字段上有 is 筛选器，则不能在同一个字段上使用 is not 或 a 不以此开头的筛选器。

6. 指定筛选器值。

请注意，对于字符串过滤器，过滤器值区分大小写。

例如，对于来自 Security Hub 的调查结果，产品名称为 Security Hub。如果您使用 EQUALS 运算符来查看来自 Security Hub 的搜索结果，则必须输入 **Security Hub** 作为筛选器值。如果输入 **security hub**，则不会显示任何结果。

同样，如果您使用 PREFIX 运算符并输入 **Sec**，则会显示 Security Hub 查找结果。如果输入 **sec**，则不会显示任何 Security Hub 查找结果。

7. 选择 Apply（应用）。

对结果进行分组

除了更改筛选器外，您还可以根据选定属性的值对发现结果进行分组。

对发现结果进行分组时，发现结果列表将替换为匹配结果中选定属性的值列表。对于每个值，列表显示与其他筛选条件相匹配的发现数目。

例如，如果您按 Amazon 账户 ID 对结果进行分组，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。

请注意，Security Hub 只能显示 100 个值。如果分组值超过 100 个，则只能看到前 100 个。

选择属性值时，将显示该值的匹配结果列表。

将结果分组到结果列表中

1. 在查找结果列表上，选中“添加筛选器”框。
2. 在菜单中的 Grouping (分组) 下，选择 Group by (分组依据)。
3. 在列表中，选择用于分组的属性。
4. 选择 Apply (应用)。

更改筛选值或分组属性

对于现有筛选器，您可以更改筛选器值。您也可以更改分组属性。

例如，您可以更改 Record state (记录状态) 筛选器以查找 ARCHIVED 结果而不是查找 ACTIVE 结果。

编辑筛选器或分组属性

1. 在筛选的查找结果列表上，选择筛选器或分组属性。
2. 对于“分组依据”，选择新属性，然后选择“应用”。
3. 对于筛选器，选择新值，然后选择 Apply (应用)。

删除筛选器或分组属性

要删除筛选器或分组属性，请选择 x 图标。

列表会自动更新以反映更改。移除分组属性后，列表将从字段值列表变回发现结果列表。

查看结果详细信息 (控制台)

在查找结果列表中，可以显示调查结果的详细信息窗格。

查看结果详细信息窗格中的查看结果详细信息

1. 通过 <https://console.aws.amazon.com/securityhub/> 打开 Amazon Security Hub 控制台。
2. 要显示结果列表，请执行以下操作之一：
 - 在 Security Hub 导航窗格中，选择查找结果。
 - 在 Security Hub 导航窗格中，选择 Insights。选择洞察力。然后在结果列表中，选择一个洞察结果。
 - 在 Security Hub 导航窗格中，选择集成。选择“查看调查结果”以进行集成。
3. 选择搜索结果标题。

查找结果详细信息窗格的顶部包含有关调查结果的概述信息，包括帐户、严重性、日期和状态。如果该账户是组织成员账户，则该信息包括账户名称。对于手动邀请的账户，该信息仅包括账户 ID。

类型和相关查找结果包含有关查找结果类型的信息。

资源包含有关受影响资源的信息。

显示控制结果的@@ 补救措施。它提供了修复触发调查结果的问题的说明的链接。

查找提供者字段显示来自查找结果提供方的置信度、重要性、相关调查结果、严重程度和查找结果类型的值。

在查找详细信息窗格中，您可以查看更多详细信息并将字段值添加到筛选器中。

- 要显示调查结果的完整 JSON，请选择调查结果 ID。从 Finding JSON (查找 JSON) 中，可以将结果 JSON 下载到一个文件。
- 要将字段值添加到查找结果列表筛选器中，请选择该字段旁边的搜索图标。
- 对于基于 Amazon Config 规则的结果，要显示适用规则的列表，请选择 Rules (规则)。

检索查找详情 (Security Hub API , Amazon CLI)

要以编程方式检索选定发现的详细信息，您可以使用 API 调用或 Amazon Command Line Interface。

请注意，当您按 CompanyName 或筛选时 ProductName，Security Hub 使用中的值 ProductFields。它不使用顶级 CompanyName 和 ProductName 字段。

检索结果的列表 (Security Hub API , Amazon CLI)

- Security Hub API—使用 [GetFindings](#) API 操作。
- Amazon CLI— 在命令行运行 [get-findings](#) 命令。

```
get-findings --filters <filter criteria JSON> --sort-criteria <sort criteria> --page-size <findings per page> --max-items <maximum number of results>
```

示例

```
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
```

对结果采取措施 Amazon Security Hub

Amazon Security Hub 允许您跟踪结果的调查状态。

您也可以将发现结果发送到自定义操作进行处理。

主题

- [设置结果的工作流状态 \(p. 66\)](#)
- [将结果发送到自定义操作 \(p. 68\)](#)

设置结果的工作流状态

对于结果，工作流程状态跟踪对结果的调查进度。工作流程状态特定于单个调查结果。它不会影响新结果的产生。例如，将工作流程状态设置为 SUPPRESSED 或 RESOLVED 不会阻止对同一问题进行新发现。

工作流状态有以下值：

NEW

查看结果的初始状态，然后查看结果的初始状态。

在以下情况下，Security Hub 还会RESOLVED将NEW工作流状态从NOTIFIED或重置为：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status从更改PASSED为FAILEDWARNING、或NOT_AVAILABLE。

这些变化意味着需要进一步调查。

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，工作流状态将自动从更改NOTIFIED为NEW：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status从更改PASSED为FAILEDWARNING、或NOT_AVAILABLE。

SUPPRESSED

表示您查看了调查结果，认为不需要采取任何行动。

如果从ARCHIVED更改为，则SUPPRESSED调查结果的工作流状态不会RecordState改变ACTIVE。

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。

除非出现以下情况之一，RESOLVED否则结果将停留不变，除非出现以下情况之一，

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status从更改PASSED为FAILEDWARNING、或NOT_AVAILABLE。

在这些情况下，工作流状态会自动重置为NEW。

对于来自控制的发现，如果Compliance.Status是PASSED，则 Security Hub 会自动将工作流状态设置为RESOLVED。

设置工作流状态（控制台）

要在查找结果详细信息窗格中设置工作流状态，请从工作流状态中选择状态。

您还可以在查找结果列表中为多个选定发现结果设置工作流状态。

为多个发现设置工作流状态（控制台）

1. 通过 <https://console.aws.amazon.com/securityhub/> 打开Amazon Security Hub控制台。
2. 要显示结果列表，请执行以下操作之一：
 - 在 Security Hub 导航窗格中，选择查找结果。
 - 在Security Hub 导航窗格中，选择 Insights。选择洞察力。然后在结果列表中，选择一个洞察结果。
 - 在 Security Hub 导航窗格中，选择集成。选择“查看调查结果”以进行集成。
 - 在 Security Hub 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. 在结果列表中，选中要更新的每个结果对应的复选框。
4. 在列表顶部的“工作流状态”中，选择状态。

设置 workflow 状态 (Security Hub API , Amazon CLI)

要设置 workflow 状态，您可以使用 API 调用或 Amazon Command Line Interface。

设置查找结果的 workflow 状态 (Security Hub API , Amazon CLI)

- S@ security Hub API- 使用 [BatchUpdateFindings](#) 操作。要确定要更新的调查结果，您必须提供调查结果 ID 和生成调查结果的产品的 ARN。
- Amazon CLI— 在命令行运行 [batch-update-findings](#) 命令。

```
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"
```

将结果发送到自定义操作

您可以创建 Amazon Security Hub 自定义操作以使用亚马逊自动执行 Security Hub EventBridge。对于自定义操作，事件类型为 Security Hub Findings - Custom Action。

有关创建自定义操作的更多信息和详细步骤，请参阅 [自动响应和补救 \(p. 500\)](#)。

设置自定义操作后，您可以向其发送结果。

将结果发送到自定义操作

1. 通过 <https://console.aws.amazon.com/securityhub/> 打开 Amazon Security Hub 控制台。
2. 要显示结果列表，请执行以下操作之一：
 - 在 Security Hub 导航窗格中，选择查找结果。
 - 在 Security Hub 导航窗格中，选择 Insights。选择洞察力。然后在结果列表中，选择一个洞察结果。
 - 在 Security Hub 导航窗格中，选择集成。选择“查看调查结果”以进行集成。
 - 在 Security Hub 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. 在结果列表中，选中要发送到自定义操作的每个结果对应的复选框。

您一次最多可以发送 20 个结果。
4. 在“操作”中，选择自定义操作。

Amazon Security Finding 格式 (ASFF)

Amazon Security Hub 使用、汇总、整理来自 Amazon 安全服务和第三方产品集成的发现，并对其进行优先排序。Security Hub 使用称为 Amazon 安全查找结果格式 (ASFF) 的标准发现结果格式处理这些发现，从而无需耗时的数据转换工作。然后，它将从各个产品提取的结果进行关联，以确定最重要问题的优先级。

主题

- [Amazon Security Finding 格式 \(ASFF\) 语法 \(p. 69\)](#)
- [ASFF 示例 \(p. 113\)](#)

AmazonSecurity Finding 格式 (ASFF) 语法

以下是Amazon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](#)。选择链接对象名称以查看该对象的示例查找结果。您可以将您的 Security Hub 发现结果与此处显示的资源 and 示例进行比较，以帮助解释您的发现。

要查看必需 ASFF 属性的描述，请参阅the section called “必需的属性” (p. 114)。

要查看其他顶级 ASFF 属性的描述，请参阅[the section called “可选的顶级属性” \(p. 119\)](#)。

```
"Findings": [
  {
    "Action \(p. 119\)": {
      "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",
"CompanyName": "string",
"Compliance (p. 120)": {
  "RelatedRequirements": ["string"],
  "Status": "string",
  "StatusReasons": [{
    "Description": "string",
    "ReasonCode": "string"
  }]
},
"Confidence": "number",
"CreatedAt": "string",

```

```

"Criticality": "number",
>Description": "string",
"FindingProviderFields \(p. 121\)": {
  "Confidence": "number",
  "Criticality": "number",
  "RelatedFindings": [{
    "ProductArn": "string",
    "Id": "string"
  }],
  "Severity": {
    "Label": "string",
    "Original": "string"
  },
  "Types": ["string"]
},
"FirstObservedAt": "string",
"GeneratorId": "string",
"Id": "string",
"LastObservedAt": "string",
"Malware \(p. 122\)": [{
  "Name": "string",
  "Path": "string",
  "State": "string",
  "Type": "string"
}],
"Network \(p. 123\)": {
  "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 \(p. 123\)": [{
  "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 \(p. 124\)": {
    "Text": "string",
    "UpdatedAt": "string",
    "UpdatedBy": "string"
},
"PatchSummary \(p. 124\)": {
    "FailedCount": "number",
    "Id": "string",
    "InstalledCount": "number",
    "InstalledOtherCount": "number",
    "InstalledPendingReboot": "number",
    "InstalledRejectedCount": "number",
    "MissingCount": "number",
    "Operation": "string",
    "OperationEndTime": "string",
    "OperationStartTime": "string",
    "RebootOption": "string"
},
"Process \(p. 124\)": {
    "LaunchedAt": "string",
    "Name": "string",
    "ParentPid": "number",
    "Path": "string",
    "Pid": "number",
    "TerminatedAt": "string"
},
"ProductArn": "string",
"ProductFields": {
    "string": "string"
},
"ProductName": "string",
"RecordState": "string",
"Region": "string",
"RelatedFindings \(p. 126\)": [{
    "Id": "string",
    "ProductArn": "string"
}],
"Remediation \(p. 126\)": {
    "Recommendation": {
        "Text": "string",
        "Url": "string"
    }
},
"Resources \(p. 129\)": [{
    "DataClassification \(p. 130\)": {
        "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": {
  "AwsApiGatewayRestApi \(p. 134\)": {
    "ApiKeySource": "string",
    "BinaryMediaTypes": ["string"],
    "CreateDate": "string",
    "Description": "string",
    "EndpointConfiguration": {
      "Types": ["string"]
    },
  },
  "Id": "string",
  "MinimumCompressionSize": "number",
  "Name": "string",
  "Version": "string"
},
  "AwsApiGatewayStage \(p. 135\)": {
    "AccessLogSettings": {
      "DestinationArn": "string",
      "Format": "string"
    },
  },
  "CacheClusterEnabled": "boolean",
  "CacheClusterSize": "string",
  "CacheClusterStatus": "string",
  "CanarySettings": {
    "DeploymentId": "string",
    "PercentTraffic": "number",
    "StageVariableOverrides": [{
      "string": "string"
    }],
  },
  "UseStageCache": "boolean"
},
  "ClientCertificateId": "string",
  "CreateDate": "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 (p. 136)": {
    "ApiEndpoint": "string",
    "ApiId": "string",
    "ApiKeySelectionExpression": "string",
    "CorsConfiguration": {
        "AllowCredentials": "boolean",
        "AllowHeaders": ["string"],
        "AllowMethods": ["string"],
        "AllowOrigins": ["string"],
        "ExposeHeaders": ["string"],
        "MaxAge": "number"
    },
    "CreateDate": "string",
    "Description": "string",
    "Name": "string",
    "ProtocolType": "string",
    "RouteSelectionExpression": "string",
    "Version": "string"
},
"AwsApiGatewayV2Stage (p. 136)": {
    "AccessLogSettings": {
        "DestinationArn": "string",
        "Format": "string"
    },
    "ApiGatewayManaged": "boolean",
    "AutoDeploy": "boolean",
    "ClientCertificateId": "string",
    "CreateDate": "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"
    }]
},

```

```

"AwsRdsDbSecurityGroup \(p. 181\)": {
  "DbSecurityGroupArn": "string",
  "DbSecurityGroupDescription": "string",
  "DbSecurityGroupName": "string",
  "Ec2SecurityGroups": [{
    "Ec2SecurityGroupArn": "string",
    "Ec2SecurityGroupName": "string",
    "Ec2SecurityGroupOwnerId": "string",
    "Status": "string"
  }],
  "IpRanges": [{
    "CidrIp": "string",
    "Status": "string"
  }],
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsAutoScalingAutoScalingGroup \(p. 137\)": {
  "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 \(p. 138\)": {
  "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 \(p. 139\)": {
    "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 \(p. 140\)": {
    "AccessPolicy": {
        "Statement": [{
            "Action": ["string"],
            "Effect": "string",
            "Principal": {
                "Amazon": "string"
            }
        }]
    }
}

```

```

    },
    "Resource": "string"
  ]],
  "Version": "string"
},
"BackupVaultArn": "string",
"BackupVaultName": "string",
"EncryptionKeyArn": "string",
"Notifications": {
  "BackupVaultEvents": ["string"],
  "SNSTopicArn": "string"
}
},
"AwsBackupRecoveryPoint \(p. 141\)": {
  "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 \(p. 142\)": {
  "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 \(p. 143\)": {
    "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 \(p. 144\)": {
    "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 (p. 145)": {
  "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 \(p. 146\)": {
    "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 \(p. 147\)": {
    "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"]
  }
},
"AwsDynamoDbTable \(p. 148\)": {
  "AttributeDefinitions": [{
    "AttributeName": "string",
    "AttributeType": "string"
  }],
  "BillingModeSummary": {
    "BillingMode": "string",
    "LastUpdateToPayPerRequestDateTime": "string"
  },
  "CreationDateTime": "string",
  "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"
  },
  "AwsEc2Eip (p. 150)": {
    "AllocationId": "string",

```

```

"AssociationId": "string",
"Domain": "string",
"InstanceId": "string",
"NetworkBorderGroup": "string",
"NetworkInterfaceId": "string",
"NetworkInterfaceOwnerId": "string",
"PrivateIpAddress": "string",
"PublicIp": "string",
"PublicIpv4Pool": "string"
},
"AwsEc2Instance (p. 151)": {
  "IamInstanceProfileArn": "string",
  "ImageId": "string",
  "IPv4Addresses": ["string"],
  "IPv6Addresses": ["string"],
  "KeyName": "string",
  "LaunchedAt": "string",
  "MetadataOptions": {
    "HttpEndpoint": "string",
    "HttpProtocolIpv6": "string",
    "HttpPutResponseHopLimit": "number",
    "HttpTokens": "string",
    "InstanceMetadataTags": "string",
  },
  "NetworkInterfaces": [{
    "NetworkInterfaceId": "string"
  }],
  "SubnetId": "string",
  "Type": "string",
  "VirtualizationType": "string",
  "VpcId": "string"
},
"AwsEc2NetworkAcl (p. 151)": {
  "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 (p. 152)": {
  "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"
},
"AwsEc2SecurityGroup \(p. 152\)": {
  "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 \(p. 153\)": {
    "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 \(p. 153\)": {
    "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 \(p. 154\)": {
    "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 \(p. 154\)": {
    "CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlock": "string",
      "CidrBlockState": "string"
    }],
    "DhcpOptionsId": "string",
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlockState": "string",
      "Ipv6CidrBlock": "string"
    }],
  },

```

```

    "State": "string"
  },
  "AwsEc2VpcEndpointService \(p. 155\)": {
    "AcceptanceRequired": "boolean",
    "AvailabilityZones": ["string"],
    "BaseEndpointDnsNames": ["string"],
    "ManagesVpcEndpoints": "boolean",
    "GatewayLoadBalancerArns": ["string"],
    "NetworkLoadBalancerArns": ["string"],
    "PrivateDnsName": "string",
    "ServiceId": "string",
    "ServiceName": "string",
    "ServiceState": "string",
    "ServiceType": [{
      "ServiceType": "string"
    }]
  },
  "AwsEc2VpcPeeringConnection \(p. 155\)": {
    "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"
  },
  "AwsEc2VpnConnection \(p. 156\)": {
    "Category": "string",
    "CustomerGatewayConfiguration": "string",
    "CustomerGatewayId": "string",
    "Options": {
      "StaticRoutesOnly": "boolean",
      "TunnelOptions": [{

```

```

        "DpdTimeoutSeconds": "number",
        "IkeVersions": ["string"],
        "OutsideIpAddress": "string",
        "Phase1DhGroupNumbers": ["number"],
        "Phase1EncryptionAlgorithms": ["string"],
        "Phase1IntegrityAlgorithms": ["string"],
        "Phase1LifetimeSeconds": "number",
        "Phase2DhGroupNumbers": ["number"],
        "Phase2EncryptionAlgorithms": ["string"],
        "Phase2IntegrityAlgorithms": ["string"],
        "Phase2LifetimeSeconds": "number",
        "PreSharedKey": "string",
        "RekeyFuzzPercentage": "number",
        "RekeyMarginTimeSeconds": "number",
        "ReplayWindowSize": "number",
        "TunnelInsideCidr": "string"
    }]
},
"Routes": [{
    "DestinationCidrBlock": "string",
    "State": "string"
}],
"State": "string",
"TransitGatewayId": "string",
"Type": "string",
"VgwTelemetry": [{
    "AcceptedRouteCount": "number",
    "CertificateArn": "string",
    "LastStatusChange": "string",
    "OutsideIpAddress": "string",
    "Status": "string",
    "StatusMessage": "string"
}],
"VpnConnectionId": "string",
"VpnGatewayId": "string"
},
"AwsEcrContainerImage \(p. 157\)": {
    "Architecture": "string",
    "ImageDigest": "string",
    "ImagePublishedAt": "string",
    "ImageTags": ["string"],
    "RegistryId": "string",
    "RepositoryName": "string"
},
"AwsEcrRepository \(p. 157\)": {
    "Arn": "string",
    "ImageScanningConfiguration": {
        "ScanOnPush": "boolean"
    },
    "ImageTagMutability": "string",
    "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
    },
    "RepositoryName": "string",
    "RepositoryPolicyText": "string"
},
"AwsEcsCluster \(p. 158\)": {
    "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 (p. 158)": {
  "Image": "string",
  "MountPoints": [{
    "ContainerPath": "string",
    "SourceVolume": "string"
  }],
  "Name": "string",
  "Privileged": "boolean"
},
"AwsEcsService (p. 159)": {
  "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 \(p. 160\)": {
  "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 \(p. 161\)": {
  "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"],
"TaskRoleArn": "string",
"Status": "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 (p. 162)": {
    "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 (p. 162)": {
    "Arn": "string",
    "CertificateAuthorityData": "string",
    "ClusterStatus": "string",
    "Endpoint": "string",
    "Logging": {
        "ClusterLogging": [{
            "Enabled": "boolean",
            "Types": ["string"]
        }]
    },
    "Name": "string",
    "ResourcesVpcConfig": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
    },
    "RoleArn": "string",
    "Version": "string"
},
"AwsElasticBeanstalkEnvironment (p. 163)": {
    "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 \(p. 164\)": {
    "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 \(p. 165\)": {
  "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 (p. 167)": {
  "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"
},
"AwsIamAccessKey (p. 167)": {
  "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 (p. 168)": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupId": "string",
  "GroupName": "string",
  "GroupPolicyList": [{
    "PolicyName": "string"
  }],
  "Path": "string"
},
"AwsIamPolicy (p. 168)": {
  "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 (p. 169)": {
  "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 \(p. 170\)": {
    "AttachedManagedPolicies": [{
      "PolicyArn": "string",
      "PolicyName": "string"
    }],
    "CreateDate": "string",
    "GroupList": ["string"],
    "Path": "string",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "string",
      "PermissionsBoundaryType": "string"
    },
    "UserId": "string",
    "UserName": "string",
    "UserPolicyList": [{
      "PolicyName": "string"
    }]
  },
  "AwsKinesisStream \(p. 170\)": {
    "Arn": "string",
    "Name": "string",
    "RetentionPeriodHours": "number",
    "ShardCount": "number",
    "StreamEncryption": {
      "EncryptionType": "string",
      "KeyId": "string"
    }
  },
  "AwsKmsKey \(p. 171\)": {
    "AWSAccountId": "string",
    "CreationDate": "string",
    "Description": "string",
    "KeyId": "string",
    "KeyManager": "string",
    "KeyRotationStatus": "boolean",
    "KeyState": "string",
    "Origin": "string"
  },
  "AwsLambdaFunction \(p. 171\)": {
    "Code": {
      "S3Bucket": "string",
      "S3Key": "string",
      "S3ObjectVersion": "string",
      "ZipFile": "string"
    },
    "CodeSha256": "string",
    "DeadLetterConfig": {
      "TargetArn": "string"
    },
    "Environment": {
      "Variables": {
        "string": "string"
      }
    }
  },

```

```

    "Error": {
      "ErrorCode": "string",
      "Message": "string"
    }
  },
  "FunctionName": "string",
  "Handler": "string",
  "KmsKeyArn": "string",
  "LastModified": "string",
  "Layers": {
    "Arn": "string",
    "CodeSize": "number"
  },
  "RevisionId": "string",
  "Role": "string",
  "Runtime": "string",
  "Timeout": "integer",
  "TracingConfig": {
    "Mode": "string"
  },
  "Version": "string",
  "VpcConfig": {
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
  "MasterArn": "string",
  "MemorySize": "number"
},
"AwsLambdaLayerVersion (p. 172)": {
  "CompatibleRuntimes": [
    "string"
  ],
  "CreateDate": "string",
  "Version": "number"
},
"AwsNetworkFirewallFirewall (p. 172)": {
  "DeleteProtection": "boolean",
  "Description": "string",
  "FirewallArn": "string",
  "FirewallId": "string",
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": "boolean",
  "SubnetChangeProtection": "boolean",
  "SubnetMappings": [{
    "SubnetId": "string"
  }],
  "VpcId": "string"
},
"AwsNetworkFirewallFirewallPolicy (p. 173)": {
  "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 \(p. 173\)": {
  "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"
              }]
            }
          }
        }],
        "Sources": [{
          "AddressDefinition": "string"
        }],
        "Targets": ["string"],
        "TargetTypes": ["string"]
      }
    }
  }
}

```

```

    }],
    "TcpFlags": [{
      "Flags": ["string"],
      "Masks": ["string"]
    }]
  }
}
}],
"RuleVariables": {
  "IpSets": {
    "Definition": ["string"]
  },
  "PortSets": {
    "Definition": ["string"]
  }
},
"RuleGroupArn": "string",
"RuleGroupId": "string",
"RuleGroupName": "string",
"Type": "string"
},
"AwsOpenSearchServiceDomain (p. 175)": {
  "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 \(p. 177\)": {
  "ActivityStreamStatus": "string",
  "AllocatedStorage": "number",
  "AssociatedRoles": [{
    "RoleArn": "string",
    "Status": "string"
  }],
  "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 \(p. 178\)": {
  "AllocatedStorage": "integer",
  "AvailabilityZones": ["string"],
  "ClusterCreateTime": "string",
  "DbClusterIdentifier": "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 \(p. 179\)": {
  "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"
  }]
},
"AwsRdsDbSnapshot \(p. 181\)": {
  "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 \(p. 182\)": {
    "CustomerAwsId": "string",
    "CustSubscriptionId": "string",
    "Enabled": "boolean",
    "EventCategoriesList": ["string"],
    "EventSubscriptionArn": "string",
    "SnsTopicArn": "string",
    "SourceIdsList": ["string"],
    "SourceType": "string",
    "Status": "string",
    "SubscriptionCreationTime": "string"
  },
  "AwsRedshiftCluster \(p. 182\)": {
    "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"
  }]
},
"AwsS3AccountPublicAccessBlock (p. 185)": {

```

```

"BlockPublicAcls": "boolean",
"BlockPublicPolicy": "boolean",
"IgnorePublicAcls": "boolean",
"RestrictPublicBuckets": "boolean"
},
"AwsS3Bucket (p. 186)": {
  "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"
},
"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",
"OwnerAccountId": "string",
"OwnerId": "string",
"OwnerName": "string",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": "boolean",
  "BlockPublicPolicy": "boolean",
  "IgnorePublicAcls": "boolean",
  "RestrictPublicBuckets": "boolean"
},
"ServerSideEncryptionConfiguration": {
  "Rules": [{
    "ApplyServerSideEncryptionByDefault": {
      "KMSEncryption": "string",
      "SSEAlgorithm": "string"
    }
  }]
},
"AwsS3Object \(p. 187\)": {
  "ContentType": "string",
  "ETag": "string",
  "LastModified": "string",
  "ServerSideEncryption": "string",
  "SSEKMSKeyId": "string",
  "VersionId": "string"
},
"AwsSecretsManagerSecret \(p. 187\)": {
  "Deleted": "boolean",
  "Description": "string",
  "KmsKeyId": "string",
  "Name": "string",
  "RotationEnabled": "boolean",
  "RotationLambdaArn": "string",
  "RotationOccurredWithinFrequency": "boolean",
  "RotationRules": {
    "AutomaticallyAfterDays": "integer"
  }
},
"AwsSnsTopic \(p. 188\)": {
  "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 \(p. 188\)": {
  "DeadLetterTargetArn": "string",
  "KmsDataKeyReusePeriodSeconds": "number",
  "KmsMasterKeyId": "string",
  "QueueName": "string"
},
"AwsSsmPatchCompliance \(p. 189\)": {
  "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"
    }
  }
},
"AwsWafRateBasedRule \(p. 189\)": {
  "MatchPredicates": [{
    "DataId": "string",
    "Negated": "boolean",
    "Type": "string"
  }],
  "MetricName": "string",
  "Name": "string",
  "RateKey": "string",
  "RateLimit": "number",
  "RuleId": "string"
},
"AwsWafRegionalRateBasedRule \(p. 190\)": {
  "MatchPredicates": [{
    "DataId": "string",
    "Negated": "boolean",
    "Type": "string"
  }],
  "MetricName": "string",
  "Name": "string",
  "RateKey": "string",
  "RateLimit": "number",

```

```

"RuleId": "string"
},
"AwsWafRegionalRule \(p. 190\)": {
  "MetricName": "string",
  "Name": "string",
  "RuleId": "string",
  "PredicateList": [{
    "DataId": "string",
    "Negated": "boolean",
    "Type": "string"
  }]
},
"AwsWafRegionalRuleGroup \(p. 191\)": {
  "MetricName": "string",
  "Name": "string",
  "RuleGroupId": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "Priority": "number",
    "RuleId": "string",
    "Type": "string"
  }]
},
"AwsWafRegionalWebAcl \(p. 191\)": {
  "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 \(p. 192\)": {
  "MetricName": "string",
  "Name": "string",
  "PredicateList": [{
    "DataId": "string",
    "Negated": "boolean",
    "Type": "string"
  }],
  "RuleId": "string"
},
"AwsWafRuleGroup \(p. 192\)": {
  "MetricName": "string",
  "Name": "string",
  "RuleGroupId": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "Priority": "number",
    "RuleId": "string",

```

```

    "Type": "string"
  }],
},
"AwsWafWebAcl \(p. 192\)": {
  "DefaultAction": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "ExcludedRules": [{
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    },
    "Priority": "number",
    "RuleId": "string",
    "Type": "string"
  }],
  "WebAclId": "string"
},
"AwsXrayEncryptionConfig \(p. 193\)": {
  "KeyId": "string",
  "Status": "string",
  "Type": "string"
},
"Container \(p. 193\)": {
  "ContainerRuntime": "string",
  "ImageId": "string",
  "ImageName": "string",
  "LaunchedAt": "string",
  "Name": "string",
  "Privileged": "boolean",
  "VolumeMounts": [{
    "Name": "string",
    "MountPath": "string"
  }],
},
"Other \(p. 194\)": {
  "string": "string"
},
  "Id": "string",
  "Partition": "string",
  "Region": "string",
  "ResourceRole": "string",
  "Tags": {
    "string": "string"
  },
  "Type": "string"
}],
"SchemaVersion": "string",
"Severity \(p. 116\)": {
  "Label": "string",
  "Normalized": "number",
  "Original": "string",
  "Product": "number"
},
"Sample": "boolean",
"SourceUrl": "string",
"Threats \(p. 127\)": [{
  "FilePaths": [{
    "FileName": "string",
    "FilePath": "string",
    "Hash": "string",
    "ResourceId": "string",

```

```
    },
    "ItemCount": "number",
    "Name": "string",
    "Severity": "string"
  }],
  "ThreatIntelIndicators \(p. 127\)": [{
    "Category": "string",
    "LastObservedAt": "string",
    "Source": "string",
    "SourceUrl": "string",
    "Type": "string",
    "Value": "string"
  }],
  "Title": "string",
  "Types": ["string"],
  "UpdatedAt": "string",
  "UserDefinedFields": {
    "string": "string"
  },
  "VerificationState": "string",
  "Vulnerabilities \(p. 128\)": [{
    "Cvss": [{
      "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
      }],
      "BaseScore": "number",
      "BaseVector": "string",
      "Source": "string",
      "Version": "string"
    }],
    "FixAvailable": "string",
    "Id": "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",
      "Version": "string"
    }],
    "Workflow": {
      "Status": "string"
    },
    "WorkflowState": "string"
  }
]
```

ASFF 示例

以下部分包含Amazon安全查找格式 (ASFF) 中必填和可选属性的示例，以及 ASFF 支持的每种资源的示例。

主题

- [必需的属性 \(p. 114\)](#)
- [可选的顶级属性 \(p. 119\)](#)
- [Resources \(p. 129\)](#)

必需的属性

Security Hub 中的所有结果都需要以下属性。有关这些必填属性的更多信息，请参阅 Amazon Security HubAPI 参考[AwsSecurityFinding](#)中的。

AwsAccountId

应用查找结果的 Amazon 账户 ID。

示例

```
"AwsAccountId": "111111111111"
```

CreatedAt

表示调查结果捕获的潜在安全问题的创建时间。

示例

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Note

Security Hub 在最近更新后 90 天或创建后 90 天或创建后 90 天（如果未发生更新）后。要将发现的存储时间超过 90 天，您可以在 Amazon 中配置一条规则 EventBridge，将发现结果路由到您的 S3 存储桶。

描述

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。

示例

```
"Description": "The version of openssl found on instance i-abcd1234 is known to contain a vulnerability."
```

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。

示例

```
"GeneratorId": "acme-vuln-9ab348"
```

Id

结果的特定于产品的标识符。

示例

```
"Id": "us-west-2/111111111111/98aebb2207407c87f51e89943f12b1ef"
```

ProductArn

由 Security Hub 生成的亚马逊资源名称 (ARN)，用于在第三方发现产品注册到 Security Hub 后唯一标识该产品。

此字段的格式为 `arn:partition:securityhub:region:account-id:product/company-id/product-id`。

- 对于与 Security Hub 集成的 Amazon 服务，company-id 必须为 `aws`，并且 product-id 必须是 Amazon 公共服务名称。由于 Amazon 产品和服务未与账户关联，因此 ARN 的 account-id 部分为空。Amazon 尚未与 Security Hub 集成的服务被视为第三方产品。
- 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

该 [Resources \(p. 129\)](#) 对象提供了一组资源数据类型，Amazon 用于描述调查结果所引用的资源。

示例

```
"Resources": [
  {
    "Type": "AwsEc2Instance",
    "Id": "arn:aws:ec2:us-west-2:111122223333:instance/i-1234567890abcdef0",
    "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 Amazon 确定的官方发布版本之一。在当前版本中，Amazon Security Finding 格式架构版本为 2018-10-08。

示例

```
"SchemaVersion": "2018-10-08"
```

严重性

定义调查结果的重要性。有关此对象的详细信息，请参阅 Amazon Security Hub API 参考 [Severity](#) 中的。

要指定严重性，调查结果中必须填充 Label 或 Normalized 字段。Label 是首选属性。如果两个属性均未填充，则该查找结果无效。

要提供严重性信息，查找提供者应在发出 [BatchImportFindings](#) API 请求 FindingProviderFields 时使用下方的 Severity 对象。如果 BatchImportFindings 请求新查找结果仅提供 Label 或仅提供 Normalized，则 Security Hub 会自动填充另一个字段的值。

调查结果的 Severity 对象值只能通过 [BatchUpdateFindings](#) API 操作更新。

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，与关键任务应用程序关联的资源比与非生产测试相关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。

我们建议在将调查结果的原生严重性分数转换为 ASFFSeverity.Label 中的值时使用以下指南。

- INFORMATIONAL— 此类别可能包括对 PASSEDWARNING、或 NOT AVAILABLE 支票的调查结果或敏感数据识别。
- LOW— 可能导致 future 妥协的发现。例如，此类别可能包括漏洞、配置缺陷和暴露的密码。
- MEDIUM— 调查结果表明存在积极的妥协，但没有迹象表明对手完成了目标。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 — 表明对手已完成其目标的调查结果，例如主动数据丢失或泄露或拒绝服务。

示例

```
"Severity": {
  "Label": "CRITICAL",
  "Original": "8.3"
}
```

Title

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。

示例

```
"Title": "S3.13 S3 buckets should have lifecycle policies configured"
```

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。有关命名空间、分类器和类别的列表，请参阅[TypesASFF 的分类法 \(p. 117\)](#)。

Types 应仅使用更新 [BatchUpdateFindings](#)。

查找想要为提供值的提供者 Types 应使用下面的 Types 属性 [FindingProviderFields](#)。

示例

```
"Types": [  
  "Software and Configuration Checks/Vulnerabilities/CVE"  
]
```

UpdatedAt

指示查找条件提供者上次更新查找结果记录的时间。

此时间戳反映了上次或最近更新查找记录的时间。因此，它可能不同于 LastObservedAt 时间戳，后者反映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。创建查找记录后，CreatedAt 和 UpdatedAt 时间戳必须相同。更新查找结果记录后，此字段的值必须比它包含的所有先前值都要新。

请注意，UpdatedAt 无法使用 [BatchUpdateFindings](#) API 操作进行更新。您只能使用对其进行更新 [BatchImportFindings](#)。

示例

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Note

Security Hub 在最近更新后 90 天或创建后 90 天或创建后 90 天（如果未发生更新）后。要将发现的存储时间超过 90 天，您可以在 Amazon 中配置一条规则 EventBridge，将发现结果路由到您的 S3 存储桶。

TypesASFF 的分类法

以下信息介绍 Types 路径的前三个级别。在列表中，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。我们建议查找提供者使用定义的命名空间来帮助对发现的结果进行排序和分组。也可以使用已定义类别和分类器，但不是必需的。只有软件和配置检查命名空间定义了分类器。

- 命名空间
 - 类别
 - 分类器

查找提供者可以为命名空间/类别/分类器定义部分路径。例如，以下结果类型均有效：

- TTP
- TTP/Defense Evasion
- ttps/防御逃避/CloudTrailStopped

以下列表中的战术、技巧和程序类别与 MITRE ATT&CK MatrixTM 一致。异常行为反映了一般的异常行为，例如一般的统计异常，与特定的 TTP 不一致。但是，您可以使用异常行为和 TTP 查找类型对发现进行分类。

- Software and Configuration Checks
 - 漏洞
 - CVE
 - Amazon 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
 - Amazon 基础安全最佳实践
 - CIS 主机强化基准
 - CIS Amazon 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
 - 执行
 - 持久性
 - 权限提升
 - 躲避防御系统
 - 凭证访问
 - 发现
 - 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
 - 容器
 - Serverless (无服务器)
 - 过程
 - 数据库。
 - 数据
- 敏感数据识别
 - PII
 - 密码
 - 法律条款
 - 财务
 - 安全性
 - 业务

可选的顶级属性

这些顶级属性在Amazon安全查找格式中是可选的。有关这些属性的更多信息，请参阅 Amazon Security Hub API 参考 [AwsSecurityFinding](#) 中的。

操作

该 [Action](#) 对象提供有关影响资源或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
}
```

CompanyName

生成调查结果的产品的公司名称。对于基于控制的发现，该公司是Amazon。

Security Hub 会自动为每个查找结果填充此属性。您无法使用[BatchImportFindings](#)或对其进行更新[BatchUpdateFindings](#)。例外情况是当您使用自定义集成时。请参阅 [the section called “使用自定义产品集成” \(p. 241\)](#)。

当您使用 Security Hub 控制台按公司名称筛选发现结果时，应使用此属性。当您使用 Security Hub API 按公司名称筛选发现结果时，请使用下面的aws/securityhub/CompanyName属性ProductFields。Security Hub 不同步这两个属性。

示例

```
"CompanyName": "Amazon"
```

Compliance

该[Compliance](#)对象提供查找与控件相关的详细信息。只有从 Security Hub 控件生成的发现结果才会返回此属性。

示例

```
"Compliance": {
  "RelatedRequirements": ["Req1", "Req2"],
  "Status": "PASSED",
  "StatusReasons": [
    {
      "ReasonCode": "CLOUDWATCH_ALARMS_NOT_PRESENT",
      "Description": "CloudWatch alarms do not exist in the account"
    }
  ]
}
```

信心

调查结果准确识别其要识别的行为或问题的可能性。

Confidence应仅使用更新[BatchUpdateFindings](#)。

查找想要为提供值的提供者Confidence应使用下面的Confidence属性FindingProviderFields。请参阅 [the section called “使用 FindingProviderFields” \(p. 58\)](#)。

Confidence使用比率等级以 0—100 为基础进行评分。0 表示 0% 的置信度，100 表示 100% 的置信度。例如，基于网络流量统计偏差的数据泄露检测的置信度很低，因为实际的泄露尚未得到验证。

示例

```
"Confidence": 42
```

临界性

分配给与调查结果相关的资源的重要性级别。

Criticality只能通过调用 [BatchUpdateFindings](#) API 操作进行更新。不要用更新这个对象[BatchImportFindings](#)。

查找想要为提供值的提供者Criticality应使用下面的Criticality属性FindingProviderFields。请参阅 [the section called “使用 FindingProviderFields” \(p. 58\)](#)。

Criticality使用仅支持全整数的比率等级，以 0—100 为基础进行评分。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，在分配时要考虑以下几点Criticality：

- 受影响的资源是否包含敏感数据（例如，带有 PII 的 S3 存储桶）？
- 受影响的资源是否使攻击者能够加深其访问权限或扩展其能力以进行其他恶意活动（例如，被盗的 sysadmin 帐户）？
- 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：

- 为关键任务系统提供支持或包含高度敏感数据的资源可以在 75—100 范围内进行评分。
- 为重要（但不是关键系统）提供动力或包含中等重要数据的资源可以在25—74的范围内进行评分。
- 为不重要系统供电或包含非敏感数据的资源应在 0—24 范围内进行评分。

示例

```
"Criticality": 99
```

FindingProviderFields

FindingProviderFields包含以下属性：

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

您可以使用 [BatchImportFindings](#) API 操作进行更新FindingProviderFields。您无法使用对其进行更新[BatchUpdateFindings](#)。

有关 Security Hub 如何处理来自 [BatchImportFindings](#) 对应顶级属性的更新 `FindingProviderFields` 和对应顶级属性的更新的详细信息，请参阅 [the section called “使用 FindingProviderFields” \(p. 58\)](#)。

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

表示首次观察到调查结果发现的潜在安全问题的时间。

该时间戳反映了首次观察到事件或漏洞的时间。因此，它可能不同于 `CreatedAt` 时间戳，后者反映了创建此查找记录的时间。

此时间戳在两次更新查找记录之间应该是不可变的，但是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

表示安全发现产品最近观察到调查结果发现的潜在安全问题的时间。

该时间戳反映了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，时间戳反映了此发现记录的最后更新时间或最近更新时间。

您可以提供此时间戳，但在首次观察时不是必需的。如果您在第一次观察时提供此字段，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](#) 对象提供与结果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)

该[Network](#)对象提供有关调查结果的网络相关信息。

此对象将停用。要提供这些数据，您可以将数据映射到中的资源Resources，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

该[NetworkPath](#)对象提供与调查结果相关的网络路径的相关信息。中的每个条目NetworkPath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" ]
    }
}
]

```

注意

该[Note](#)对象指定了用户定义的注释，您可以将其添加到调查结果中。

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。您只能使用更新笔记[BatchUpdateFindings](#)。

示例

```

"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}

```

PatchSummary

该[PatchSummary](#)对象根据选定的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"
}

```

过程

该[Process](#)对象提供与查找结果相关的流程相关详细信息。

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"  
}
```

ProductFields

一种数据类型，其中安全发现产品可以包含其他特定于解决方案的详细信息，这些详细信息不属于已定义 Amazon 的安全调查结果格式。

对于由 Security Hub 控件生成的调查结果，ProductFields 包括有关控件的信息。请参阅 [the section called “生成和更新控制结果” \(p. 245\)](#)。

该字段不应包含冗余数据，并且不能包含与 Amazon Security Finding 格式字段冲突的数据。

“aws/” 前缀仅代表 Amazon 产品和服务的保留命名空间，不得与第三方集成的结果一起提交。

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。

示例

```
"ProductFields": {  
  "API", "DeleteTrail",  
  "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

提供生成调查结果的产品的名称。对于基于控制的发现，产品名称为 Security Hub。

Security Hub 会自动为每个查找结果填充此属性。您无法使用 [BatchImportFindings](#) 或对其进行更新 [BatchUpdateFindings](#)。例外情况是当您使用自定义集成时。请参阅 [the section called “使用自定义产品集成” \(p. 241\)](#)。

当您使用 Security Hub 控制台按产品名称筛选查找结果时，应使用此属性。

当您使用 Security Hub API 按产品名称筛选发现结果时，请使用下面的 aws/securityhub/ ProductName 属性 ProductFields。

Security Hub 不同步这两个属性。

RecordState

提供调查结果的记录状态。

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。已存档的查找结果不会立即删除。您可以对它们进行搜索、查看和报告。如果关联资源被删除、资源不存在或控件被禁用，Security Hub 会自动存档基于控制的调查结果。

RecordState 旨在寻找提供商，只能由更新 [BatchImportFindings](#)。您无法使用对其进行更新 [BatchUpdateFindings](#)。

要跟踪调查结果的状态，请使用 [Workflow \(p. 128\)](#) 而不是 RecordState。

如果记录状态从 ARCHIVED 更改为 ACTIVE，并且查找结果的工作流状态为 NOTIFIED 或 RESOLVED，则 Security Hub 会自动将工作流状态设置为 NEW。

示例

```
"RecordState": "ACTIVE"
```

区域

指定Amazon Web Services 区域生成查找结果的来源。

Security Hub 会自动为每个查找结果填充此属性。您无法使用[BatchImportFindings](#)或对其进行更新[BatchUpdateFindings](#)。

示例

```
"Region": "us-west-2"
```

RelatedFindings

提供与当前调查结果相关的发现结果列表。

RelatedFindings应仅[BatchUpdateFindings](#)通过 API 操作进行更新。你不应该用更新这个对象[BatchImportFindings](#)。

对于[BatchImportFindings](#)请求，查找提供者应使用下方的RelatedFindings对象[FindingProviderFields \(p. 121\)](#)。

要查看RelatedFindings属性的描述，请参阅 Amazon Security HubAPI 参考[RelatedFinding](#)中的。

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" }
]
```

修复

[Remediation](#) 对象提供有关为解决结果问题而建议的修复步骤的信息。

示例

```
"Remediation": {
  "Recommendation": {
    "Text": "Run sudo yum update and cross your fingers and toes.",
    "Url": "http://myfp.com/recommendations/dangerous_things_and_how_to_fix_them.html"
  }
}
```

示例

指定该调查结果是否为样本调查结果。

```
"Sample": true
```

SourceUrl

该SourceUrl对象提供一个 URL，该网址链接到有关查找产品中当前发现的页面。

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

该[ThreatIntelIndicator](#)对象提供与调查结果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

该[Threats](#)对象提供有关调查结果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

提供与结果关联的名称-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。这些字段可以通过您的特定配置自动生成。

查找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Amazon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

提供调查结果真实性。调查结果产品可以UNKNOWN为该字段提供值。如果发现产品的系统中存在有意义的类似物，则发现产品应为该字段提供值。此字段通常由用户调查结果后的决定或操作填充。

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。您只能使用更新此属性 [BatchUpdateFindings](#)。

```
"VerificationState": "Confirmed"
```

漏洞

该 [Vulnerabilities](#) 对象提供与调查结果相关的漏洞列表。

示例

```
"Vulnerabilities" : [
  {
    "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"
      }
    ],
    "FixAvailable": "YES",
    "Id": "CVE-2020-12345",
    "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",
        "Version": "1.0.2k"
      }
    ]
  }
]
```

工作流程

[Workflow](#) 对象提供有关结果调查状态的信息。

此字段供客户与补救、协调和票务工具一起使用。它不适用于结果提供商。

您只能使用更新该 Workflow 字段 [BatchUpdateFindings](#)。客户还可以从控制台更新它。请参阅 [the section called “设置结果的工作流状态” \(p. 66\)](#)。

示例

```
"Workflow": {
  "Status": "NEW"
}
```

WorkflowState (已退休)

此对象已停用，已被该Workflow对象的Status字段所取代。

此字段提供查找结果的工作流状态。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"
```

Resources

Resources 对象提供有关结果中涉及的资源的信息。

它包含一个最多包含 32 个资源对象的数组。

示例

```
"Resources": [
  {
    "Type": "AwsEc2Instance",
    "Id": "arn:aws:ec2:us-west-2:111122223333:instance/i-1234567890abcdef0",
    "Partition": "aws",
    "Region": "us-west-2",
    "ResourceRole": "Target",
    "Tags": {
      "billingCode": "Lotus-1-2-3",
      "needsPatching": "true"
    },
    "Details": {
      "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IPv4Addresses": [ "string" ],
        "IPv6Addresses": [ "string" ],
        "KeyName": "string",
        "LaunchedAt": "string",
        "NetworkInterfaces": [
          {
            "NetworkInterfaceId": "string"
          }
        ],
        "SubnetId": "string",
        "Type": "string",
        "VpcId": "string"
      }
    }
  }
]
```

主题

- [资源属性 \(p. 130\)](#)
- [AwsApiGateway \(p. 134\)](#)

- [AwsAutoScaling \(p. 137\)](#)
- [AwsBackup \(p. 139\)](#)
- [AwsCertificateManager \(p. 142\)](#)
- [AwsCloudFormation \(p. 143\)](#)
- [AwsCloudFront \(p. 144\)](#)
- [AwsCloudTrail \(p. 145\)](#)
- [AwsCloudWatch \(p. 146\)](#)
- [AwsCodeBuild \(p. 147\)](#)
- [AwsDynamoDB \(p. 148\)](#)
- [AwsEc2 \(p. 150\)](#)
- [AwsEcr \(p. 157\)](#)
- [AwsEcs \(p. 158\)](#)
- [AwsEfs \(p. 161\)](#)
- [AwsEks \(p. 162\)](#)
- [AwsElasticBeanstalk \(p. 163\)](#)
- [AwsElasticSearch \(p. 164\)](#)
- [AwsElb \(p. 165\)](#)
- [AwsIam \(p. 167\)](#)
- [AwsKinesis \(p. 170\)](#)
- [AwsKms \(p. 171\)](#)
- [AwsLambda \(p. 171\)](#)
- [AwsNetworkFirewall \(p. 172\)](#)
- [AwsOpenSearchService \(p. 175\)](#)
- [AwsRds \(p. 177\)](#)
- [AwsRedshift \(p. 182\)](#)
- [AwsS3 \(p. 185\)](#)
- [AwsSecretsManager \(p. 187\)](#)
- [AwsSns \(p. 188\)](#)
- [AwsSqs \(p. 188\)](#)
- [AwsSsm \(p. 189\)](#)
- [AwsWaf \(p. 189\)](#)
- [AwsXray \(p. 193\)](#)
- [Container \(p. 193\)](#)
- [Other \(p. 194\)](#)

资源属性

以下是Amazon Security Finding 格式 (ASFF) 中对Resources对象的描述和示例。要查看Resources对象的属性，请参阅 Amazon Security HubAPI 参考[Resource](#)中的。

DataClassification

该[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
}
}
}

```

详细信息

该 [Details](#) 字段使用相应对象提供有关单个资源的更多信息。每个资源都必须在对象中的单独资源 [Resources](#) 对象中提供。

请注意，如果查找结果大小超过最大值 240 KB，则该 [Details](#) 对象将从查找结果中删除。对于使用 Amazon Config 规则的控制发现，可以在 Amazon Config 控制台上查看资源详细信息。

Security Hub 为其支持的资源类型提供了一组可用资源详细信息。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，则将资源设置 [Type](#) 为 [AwsS3Bucket](#) 并在 [AwsS3Bucket \(p. 186\)](#) 对象中提供资源详细信息。

该 [Other \(p. 194\)](#) 对象允许您提供自定义字段和值。您可以在以下情况下使用该 [Other](#) 对象：

- 资源类型（资源的值 [Type](#)）没有相应的详细信息对象。要提供资源的详细信息，请使用 [Other \(p. 194\)](#) 对象。
- 资源类型的对象不包含要填充的所有字段。在这种情况下，使用资源类型的详细信息对象来填充可用字段。使用该 [Other](#) 对象填充不在特定类型对象中的字段。
- 资源类型不是提供的类型之一。在这种情况下，设置 `Resource.Type` 为 `Other`，然后使用 [Other](#) 对象填充细节。

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": "da4d66eac431652a4d44d490a00500bde52c97d235b7b4752f9f688566fe6de",
  "OwnerName": "acmes3bucketowner"
},
"Other": { "LightPen": "blinky", "SerialNo": "1234abcd" }
}
```

Id

给定资源类型的标识符。

对于Amazon由亚马逊资源名称 (ARN) 标识的资源，这是 ARN。

对于缺少 ARNAmazon 的资源，这是创建资源的Amazon服务定义的标识符。

对于非Amazon资源，这是与资源关联的唯一标识符。

示例

```
"Id": "arn:aws:s3:::example-bucket"
```

分区

资源所在的分区。分区是一组Amazon区域。每个 Amazon 账户的作用域为一个分区。

支持以下分区：

- aws – Amazon 区域
- aws-cn – 中国区域
- aws-us-gov – Amazon GovCloud (US) Region

示例

```
"Partition": "aws"
```

区域

此资源所在Amazon区域的代码。有关区域代码的列表，请参阅区域终端节点，请参阅[区域终端节点](#)。

示例

```
"Region": "us-west-2"
```

ResourceRole

确定资源在调查结果中的作用。资源要么是查找活动的目标，要么是执行该活动的参与者。

示例

```
"ResourceRole": "target"
```

标签

处理调查结果时与资源相关的Amazon标签列表。您只能为具有关联标签的资源添加该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。

下面是适用于标签的基本限制：

- 您只能在此字段中提供Amazon资源上存在的标签。要提供未在Amazon安全查找结果格式中定义的数据，请使用Other详细信息子字段。
- 值仅限于以下字符：A-Z、a-z、0-9、空格和.:+ = @ _/ - (连字符)。
- 值限制为Amazon标签值最长 256 个字符。

示例

```
"Tags": {  
  "billingCode": "Lotus-1-2-3",  
  "needsPatching": "true"  
}
```

类型

您正在提供详细信息的资源类型。

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都不匹配，则将资源设置Type为Other，并使用Other详细信息子字段填充详细信息。

支持的值列在 [“资源 \(p. 129\)”](#) 下。

示例

```
"Type": "AwsS3Bucket"
```

AwsApiGateway

以下是AwsApiGateway资源Amazon的安全查找格式的示例。

AwsApiGatewayRestApi

该AwsApiGatewayRestApi对象包含有关亚马逊 API Gateway 版本 1 中的 REST API 的信息。

以下是Security FAwsApiGatewayRestApi indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsApiGatewayRestApi属性的描述，请参阅 Amazon Security HubAPI 参考[AwsApiGatewayRestApiDetails](#)中的。

示例

```
AwsApiGatewayRestApi: {  
  "Id": "exampleapi",
```



```
\": \"$context.integrationStatus\", \"$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,
"CreateDate": "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

该AwsApiGatewayV2Api对象包含有关 Amazon API Gateway 中的版本 2 API 的信息。

以下是Security FAwsApiGatewayV2Api indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsApiGatewayV2Api属性的描述，请参阅 Amazon Security HubAPI 参考ApiDetails中的[AwsApiGatewayV2](#)。

示例

```
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
  "ApiId": "a1b2c3d4",
  "ApiKeySelectionExpression": "$request.header.x-api-key",
  "CreateDate": "2020-03-28T00:32:37Z",
  "Description": "ApiGatewayV2 Api",
  "Version": "string",
  "Name": "my-api",
  "ProtocolType": "HTTP",
  "RouteSelectionExpression": "$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 版本 2 阶段的信息。

以下是Security FAwsApiGatewayV2Stage indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsApiGatewayV2Stage属性的描述，请参阅 Amazon Security HubAPI 参考StageDetails中的[AwsApiGatewayV2](#)。

示例

```

"AwsApiGatewayV2Stage": {
  "CreateDate": "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,
}

```

AwsAutoScaling

以下是AwsAutoScaling资源Amazon的安全查找格式的示例。

AwsAutoScalingAutoScalingGroup

该AwsAutoScalingAutoScalingGroup对象提供有关自动伸缩组的详细信息。

以下是Security FAwsAutoScalingAutoScalingGroup indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsAutoScalingAutoScalingGroup属性的描述，请参阅 Amazon Security HubAPI 参考[AwsAutoScalingAutoScalingGroupDetails](#)中的。

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

该AwsAutoScalingLaunchConfiguration对象提供有关启动配置的详细信息。

以下是Security FAwsAutoScalingLaunchConfiguration indingAmazon 格式 (ASFF) 中的结果示例。

要查看AwsAutoScalingLaunchConfiguration属性的描述，请参阅 Amazon Security HubAPI 参考[AwsAutoScalingLaunchConfigurationDetails](#)中的。

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

以下是AwsBackup资源Amazon的安全查找格式的示例。

AwsBackupBackupPlan

该AwsBackupBackupPlan对象提供有关Amazon Backup备份计划的信息。Amazon Backup备份计划是一种策略表达式，它定义了您希望何时以及如何备份Amazon资源。

以下示例显示AwsBackupBackupPlan对象Amazon的安全结果格式 (ASFF)。要查看AwsBackupBackupPlan属性的描述，请参阅 Amazon Security HubAPI 参考[AwsBackupBackupPlan](#)中的。

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

该AwsBackupBackupVault对象提供有关Amazon Backup备份保管库的信息。Amazon Backup备份保管库是存储和组织备份的容器。

以下示例显示AwsBackupBackupVault对象Amazon的安全结果格式 (ASFF)。要查看AwsBackupBackupVault属性的描述，请参阅 Amazon Security Hub API 参考 [AwsBackupBackupVault](#) 中的。

示例

```

"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [
      {
        "Action": [
          "backup:DeleteBackupVault",
          "backup:DeleteBackupVaultAccessPolicy",

```

```

        "backup:DeleteRecoveryPoint",
        "backup:StartCopyJob",
        "backup:StartRestoreJob",
        "backup:UpdateRecoveryPointLifecycle"
    ],
    "Effect": "Deny",
    "Principal": {
        "Amazon": "*"
    },
    "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",
"EncryptionKeyArn": "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

该AwsBackupRecoveryPoint对象提供有关Amazon Backup备份的信息，也称为恢复点。Amazon Backup恢复点表示资源在指定时间的内容。

以下示例显示AwsBackupRecoveryPoint对象Amazon的安全结果格式 (ASFF)。要查看AwsBackupBackupVault属性的描述，请参阅 Amazon Security HubAPI 参考[AwsBackupRecoveryPoint](#)中的。

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

以下是AwsCertificateManager资源Amazon的安全查找格式的示例。

AwsCertificateManagerCertificate

该AwsCertificateManagerCertificate对象提供有关Amazon Certificate Manager (ACM) 证书的详细信息。

以下是Security F AwsCertificateManagerCertificate indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsCertificateManagerCertificate属性的描述，请参阅 Amazon Security HubAPI 参考[AwsCertificateManagerCertificateDetails](#)中的。

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_ENCRYPTMENT",
}
],
"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

以下是AwsCloudFormation资源Amazon的安全查找格式的示例。

AwsCloudFormationStack

AwsCloudFormationStack对象提供有关在顶层模板中作为Amazon CloudFormation资源进行嵌套，作为资源进行嵌套。

以下示例显示AwsCloudFormationStack对象Amazon的安全结果格式 (ASFF)。要查看AwsCloudFormationStack属性的描述，请参阅 Amazon Security HubAPI 参考[AwsCloudFormationStackDetails](#)中的。

示例

```
"AwsCloudFormationStack": {
  "Capabilities": [
    "CAPABILITY_IAM",
    "CAPABILITY_NAMED_IAM"
  ],
  "CreationTime": "2022-02-18T15:31:53.161Z",
  "Description": "Amazon 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

以下是AwsCloudFront资源Amazon的安全查找格式的示例。

AwsCloudFrontDistribution

该AwsCloudFrontDistribution对象提供有关亚马逊 CloudFront 分发配置的详细信息。

以下是Security FAwsCloudFrontDistribution indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsCloudFrontDistribution属性的描述，请参阅 Amazon Security HubAPI 参考[AwsCloudFrontDistributionDetails](#)中的。

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": "my-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

以下是AwsCloudTrail资源Amazon的安全查找格式的示例。

AwsCloudTrailTrail

该AwsCloudTrailTrail对象提供有关Amazon CloudTrail跟踪的详细信息。

以下是Security FAwsCloudTrailTrail indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsCloudTrailTrail属性的描述，请参阅 Amazon Security HubAPI 参考[AwsCloudTrailTrailDetails](#)中的。

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

以下是AwsCloudWatch资源Amazon的安全查找格式的示例。

AwsCloudWatchAlarm

该AwsCloudWatchAlarm对象提供有关 Amazon CloudWatch 警报的详细信息，这些警报用于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AwsCloudWatchAlarm对象Amazon的安全结果格式 (ASFF)。要查看AwsCloudWatchAlarm属性的描述，请参阅 Amazon Security HubAPI 参考[AwsCloudWatchAlarmDetails](#)中的。

示例

```
"AwsCloudWatchAlarm": {
  "ActonsEnabled": 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

以下是AwsCodeBuild资源Amazon的安全查找格式的示例。

AwsCodeBuildProject

AwsCodeBuildProject 对象提供有关 Amazon CodeBuild 项目的信息。

以下是Security F AwsCodeBuildProject indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsCodeBuildProject属性的描述，请参阅 Amazon Security HubAPI 参考[AwsCodeBuildProjectDetails](#)中的。

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"]
}
}
```

AwsDynamoDB

以下是AwsDynamoDB资源Amazon的安全查找格式的示例。

AwsDynamoDbTable

该AwsDynamoDbTable对象提供有关Amazon DynamoDB 表的详细信息。

以下是Security FAwsDynamoDbTable indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsDynamoDbTable属性的描述，请参阅 Amazon Security HubAPI 参考[AwsDynamoDbTableDetails](#)中的。

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",
  "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

以下是AwsEc2资源Amazon的安全查找格式的示例。

AwsEc2Eip

该AwsEc2Eip对象提供弹性 IP 地址的相关信息。

以下示例显示AwsEc2Eip对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2Eip属性的描述，请参阅 Amazon Security HubAPI 参考EipDetails中的 [AwsEc2](#)。

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

该AwsEc2Instance对象可提供有关 Amazon EC2 实例的详细信息。

以下示例显示AwsEc2Instance对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2Instance属性的描述，请参阅 Amazon Security HubAPI 参考InstanceDetails中的 [AwsEc2](#)。

示例

```
"AwsEc2Instance": {  
  "IamInstanceProfileArn": "string",  
  "ImageId": "string",  
  "IPv4Addresses": [ "string" ],  
  "IPv6Addresses": [ "string" ],  
  "KeyName": "string",  
  "LaunchedAt": "string",  
  "NetworkInterfaces": [  
    {  
      "NetworkInterfaceId": "string"  
    }  
  ],  
  "SubnetId": "string",  
  "Type": "string",  
  "VpcId": "string"  
}
```

AwsEc2NetworkAcl

该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AwsEc2NetworkAcl对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2NetworkAcl属性的描述，请参阅 Amazon Security HubAPI 参考NetworkAclDetails中的 [AwsEc2](#)。

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

该AwsEc2NetworkInterface对象提供有关 Amazon EC2 网络接口的信息。

以下示例显示AwsEc2NetworkInterface对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2NetworkInterface属性的描述，请参阅 Amazon Security HubAPI 参考NetworkInterfaceDetails中的 [AwsEc2](#)。

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  
}
```

AwsEc2SecurityGroup

AwsEc2SecurityGroup对象描述了一个Amazon EC2 安全组。

以下示例显示AwsEc2SecurityGroup对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2SecurityGroup属性的描述，请参阅 Amazon Security HubAPI 参考SecurityGroupDetails中的 [AwsEc2](#)。

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

该AwsEc2Subnet对象提供有关 Amazon EC2 中子网的信息。

以下示例显示AwsEc2Subnet对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2Subnet属性的描述，请参阅 Amazon Security HubAPI 参考SubnetDetails中的 [AwsEc2](#)。

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 Amazon EC2 中转网关的详细信息，用于互连 Virtual Private Cloud (VPC) 和本地网络。

以下是Security FAwsEc2TransitGateway indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsEc2TransitGateway属性的描述，请参阅 Amazon Security HubAPI 参考TransitGatewayDetails中的 [AwsEc2](#)。

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

该AwsEc2Volume对象提供有关Amazon EC2 卷的详细信息。

以下示例显示AwsEc2Volume对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2Volume属性的描述，请参阅 Amazon Security HubAPI 参考VolumeDetails中的 [AwsEc2](#)。

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/wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Size": 80,
  "SnapshotId": "",
  "Status": "available"
}
```

AwsEc2Vpc

该AwsEc2Vpc对象提供有关Amazon EC2 VPC 的详细信息。

以下示例显示AwsEc2Vpc对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2Vpc属性的描述，请参阅 Amazon Security HubAPI 参考VpcDetails中的 [AwsEc2](#)。

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

该AwsEc2VpcEndpointService对象包含有关 VPC 终端节点服务的配置服务的详细信息。

以下示例显示AwsEc2VpcEndpointService对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2VpcEndpointService属性的描述，请参阅 Amazon Security HubAPI 参考 VpcEndpointServiceDetails中的 [AwsEc2](#)。

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

该AwsEc2VpcPeeringConnection对象提供有关两个 VPC 之间的网络连接的详细信息。

以下示例显示AwsEc2VpcPeeringConnection对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2VpcPeeringConnection属性的描述，请参阅 Amazon Security HubAPI 参考 VpcPeeringConnectionDetails中的 [AwsEc2](#)。

示例

```
"AwsEc2VpcPeeringConnection": {  
  "AcceptorVpcInfo": {  
    "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"
}
}
```

AwsEc2VpnConnection

该AwsEc2VpnConnection对象提供有关Amazon EC2 VPN 连接的详细信息。

以下示例显示AwsEc2VpnConnection对象Amazon的安全结果格式 (ASFF)。要查看AwsEc2VpnConnection属性的描述，请参阅 Amazon Security Hub API 参考VpnConnectionDetails中的[AwsEc2](#)。

示例

```
"AwsEc2VpnConnection": {
  "VpnConnectionId": "vpn-205e4f41",
  "State": "available",
  "CustomerGatewayConfiguration": "",
  "CustomerGatewayId": "cgw-5699703f",
  "Type": "ipsec.1",
  "VpnGatewayId": "vgw-2ccb2245",
  "Category": "VPN",
  "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
  "VgwTelemetry": [
    {
      "OutsideIpAddress": "92.0.2.11",
      "Status": "DOWN",
      "LastStatusChange": "2016-11-11T23:09:32.000Z",
      "StatusMessage": "IPSEC IS DOWN",
      "AcceptedRouteCount": 0
    },
    {
      "OutsideIpAddress": "92.0.2.12",
      "Status": "DOWN",
      "LastStatusChange": "2016-11-11T23:10:51.000Z",
      "StatusMessage": "IPSEC IS DOWN",
      "AcceptedRouteCount": 0
    }
  ]
},
```

```

    "Routes": [{
      "DestinationCidrBlock": "10.24.34.0/24",
      "State": "available"
    }],
    "Options": {
      "StaticRoutesOnly": true
      "TunnelOptions": [{
        "DpdTimeoutSeconds": 30,
        "IkeVersions": ["ikev1", "ikev2"],
        "Phase1DhGroupNumbers": [14, 15, 16, 17, 18],
        "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
        "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
        "Phase1LifetimeSeconds": 28800,
        "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
        "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
        "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
        "Phase2LifetimeSeconds": 28800,
        "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkKSDLyGJoe1QEWeGxqkQ=",
        "RekeyFuzzPercentage": 100,
        "RekeyMarginTimeSeconds": 540,
        "ReplayWindowSize": 1024,
        "TunnelInsideCidr": "10.24.34.0/23"
      }]
    }
  }
}

```

AwsEcr

以下是AwsEcr资源Amazon的安全查找格式的示例。

AwsEcrContainerImage

该AwsEcrContainerImage对象可提供有关 Amazon ECR 映像的信息。

以下示例显示AwsEcrContainerImage对象Amazon的安全结果格式 (ASFF)。要查看AwsEcrContainerImage属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcrContainerImageDetails](#)中的。

示例

```

"AwsEcrContainerImage": {
  "RegistryId": "123456789012",
  "RepositoryName": "repository-name",
  "Architecture": "amd64"
  "ImageDigest":
  "sha256:a568e5c7a953fbaaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["00000000-0000-0000-0000-000000000000"],
  "ImagePublishedAt": "2019-10-01T20:06:12Z"
}

```

AwsEcrRepository

该AwsEcrRepository对象提供有关亚马逊弹性容器注册存储库的信息。

以下示例显示AwsEcrRepository对象Amazon的安全结果格式 (ASFF)。要查看AwsEcrRepository属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcrRepositoryDetails](#)中的。

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

以下是AwsEcs资源Amazon的安全查找格式的示例。

AwsEcsCluster

该AwsEcsCluster对象提供有关 Amazon Elastic Container Service

以下示例显示AwsEcsCluster对象Amazon的安全结果格式 (ASFF)。要查看AwsEcsCluster属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcsClusterDetails](#)中的。

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

该AwsEcsContainer对象包含有关 Amazon ECS 容器的详细信息。

以下示例显示AwsEcsContainer对象Amazon的安全结果格式 (ASFF)。要查看AwsEcsContainer属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcsContainerDetails](#)中的。

示例

```
{
  "AwsEcsContainer": {
```

```

    "Image": "1111111/knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
      "ContainerPath": "/mnt/etc",
      "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
  }

```

AwsEcsService

该AwsEcsService对象提供有关 Amazon ECS Service Service 的详细信息。

以下示例显示AwsEcsService对象Amazon的安全结果格式 (ASFF)。要查看AwsEcsService属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcsServiceDetails](#)中的。

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

该AwsEcsTask对象提供有关 Amazon ECS 任务的详细信息。

以下示例显示AwsEcsTask对象Amazon的安全结果格式 (ASFF)。要查看AwsEcsTask属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcsTask](#)中的。

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AwsEcsTaskDefinition对象Amazon的安全结果格式 (ASFF)。要查看AwsEcsTaskDefinition属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEcsTaskDefinitionDetails](#)中的。

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"],  
  "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",  
}
```

AwsEfs

以下是AwsEfs资源Amazon的安全查找格式的示例。

AwsEfsAccessPoint

该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AwsEfsAccessPoint对象Amazon的安全结果格式 (ASFF)。要查看AwsEfsAccessPoint属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEfsAccessPointDetails](#)中的。

示例

```
"AwsEfsAccessPoint": {
  "AccessPointId": "fsap-05c4c0e79ba0b118a",
  "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/fsap-05c4c0e79ba0b118a",
  "ClientToken": "AccessPointCompliant-ASK06ZZSxSp",
  "FileSystemId": "fs-0f8137f731cb32146",
  "PosixUser": {
    "Gid": "1000",
    "SecondaryGids": ["0", "4294967295"],
    "Uid": "1234"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "1000",
      "OwnerUid": "1234",
      "Permissions": "777"
    },
    "Path": "/tmp/example"
  }
}
```

AwsEks

以下是AwsEks资源Amazon的安全查找格式的示例。

AwsEksCluster

该AwsEksCluster对象可提供有关 Amazon EKS 集群的详细信息。

以下示例显示AwsEksCluster对象Amazon的安全结果格式 (ASFF)。要查看AwsEksCluster属性的描述，请参阅 Amazon Security HubAPI 参考[AwsEksClusterDetails](#)中的。

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": {
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {

```

```

        "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
        ],
        "Enabled": true
    }
}
},
"Status": "CREATING",
"CertificateAuthorityData": {},
}
}

```

AwsElasticBeanstalk

以下是AwsElasticBeanstalk资源Amazon的安全查找格式的示例。

AwsElasticBeanstalkEnvironment

该AwsElasticBeanstalkEnvironment对象包含有关Amazon Elastic Beanstalk环境的详细信息。

以下示例显示AwsElasticBeanstalkEnvironment对象Amazon的安全结果格式 (ASFF)。要查看AwsElasticBeanstalkEnvironment属性的描述，请参阅 Amazon Security Hub API 参考[AwsElasticBeanstalkEnvironmentDetails](#)中的。

示例

```

"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Name": "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

以下是AwsElasticSearch资源Amazon的安全查找格式的示例。

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AwsElasticSearchDomain对象Amazon的安全结果格式 (ASFF)。要查看AwsElasticSearchDomain属性的描述，请参阅 Amazon Security HubAPI 参考[AwsElasticSearchDomainDetails](#)中的。

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

以下是AwsElb资源Amazon的安全查找格式的示例。

AwsElbLoadBalancer

该AwsElbLoadBalancer对象包含有关Classic Load Balancer 详细信息。

以下示例显示AwsElbLoadBalancer对象Amazon的安全结果格式 (ASFF)。要查看AwsElbLoadBalancer属性的描述，请参阅 Amazon Security HubAPI 参考[AwsElbLoadBalancerDetails](#)中的。

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": "doc-example-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AwsElbv2LoadBalancer对象Amazon的安全结果格式 (ASFF)。要查看AwsElbv2LoadBalancer属性的描述，请参阅 Amazon Security HubAPI 参考LoadBalancerDetails中的 [AwsElbv2](#)。

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"
}

```

AwsIam

以下是AwsIam资源Amazon的安全查找格式的示例。

AwsIamAccessKey

该AwsIamAccessKey对象包含与调查结果相关的 IAM 访问密钥的详细信息。

以下示例显示AwsIamAccessKey对象Amazon的安全结果格式 (ASFF)。要查看AwsIamAccessKey属性的描述，请参阅 Amazon Security HubAPI 参考[AwsIamAccessKeyDetails](#)中的。

示例

```
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
  "PrincipalName": "string",
  "PrincipalType": "string",
  "SessionContext": {
    "Attributes": {
      "CreateDate": "string",
      "MfaAuthenticated": boolean
    },
    "SessionIssuer": {
      "AccountId": "string",
      "Arn": "string",
      "PrincipalId": "string",
      "Type": "string",
      "UserName": "string"
    }
  },
  "Status": "string"
}
```

AwsIamGroup

该AwsIamGroup对象包含有关 IAM 群组的详细信息。

以下示例显示AwsIamGroup对象Amazon的安全结果格式 (ASFF)。要查看AwsIamGroup属性的描述，请参阅 Amazon Security HubAPI 参考[AwsIamGroupDetails](#)中的。

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

该AwsIamPolicy对象表示 IAM 权限策略。

以下示例显示AwsIamPolicy对象Amazon的安全结果格式 (ASFF)。要查看AwsIamPolicy属性的描述，请参阅 Amazon Security HubAPI 参考[AwsIamPolicyDetails](#)中的。

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

该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AwsIamRole对象Amazon的安全结果格式 (ASFF)。要查看AwsIamRole属性的描述，请参阅Amazon Security HubAPI 参考[AwsIamRoleDetails](#)中的。

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": "AR0AJ520TH4H7LEXAMPLE",
          "RoleName": "example-role",
          "AssumeRolePolicyDocument": ""
        }
      ]
    }
  ]
}
```



```

    ],
    "MaxSessionDuration": 3600,
    "Path": "/",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "ARO4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
      {
        "PolicyName": "Example role policy"
      }
    ]
  }
}

```

AwsIamUser

该AwsIamUser对象提供有关 IAM 用户的信息。

以下示例显示AwsIamUser对象Amazon的安全结果格式 (ASFF)。要查看AwsIamUser属性的描述，请参阅 Amazon Security HubAPI 参考[AwsIamUserDetails](#)中的。

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

以下是AwsKinesis资源Amazon的安全查找格式的示例。

AwsKinesisStream

该AwsKinesisStream对象可提供有关 Amazon Kinesis Data Streams 的详细信息。

以下示例显示AwsKinesisStream对象Amazon的安全结果格式 (ASFF)。要查看AwsKinesisStream属性的描述，请参阅 Amazon Security HubAPI 参考[AwsKinesisStreamDetails](#)中的。

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

以下是AwsKms资源Amazon的安全查找格式的示例。

AwsKmsKey

该AwsKmsKey对象提供有关的详细信息Amazon KMS key。

以下示例显示AwsKmsKey对象Amazon的安全结果格式 (ASFF)。要查看AwsKmsKey属性的描述，请参阅 Amazon Security HubAPI 参考[AwsKmsKeyDetails](#)中的。

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Amazon的安全查找格式的示例。

AwsLambdaFunction

该AwsLambdaFunction对象提供有关 Lambda 函数的配置的详细信息。

以下示例显示AwsLambdaFunction对象Amazon的安全结果格式 (ASFF)。要查看AwsLambdaFunction属性的描述，请参阅 Amazon Security HubAPI 参考[AwsLambdaFunctionDetails](#)中的。

示例

```
"AwsLambdaFunction": {
  "Code": {
    "S3Bucket": "string",
    "S3Key": "string",
    "S3ObjectVersion": "string",
    "ZipFile": "string"
  },
  "CodeSha256": "string",
  "DeadLetterConfig": {
    "TargetArn": "string"
  },
  "Environment": {
    "Variables": {
      "string": "string"
    }
  }
}
```

```

        "Error": {
            "ErrorCode": "string",
            "Message": "string"
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
            "Arn": "string",
            "CodeSize": number
        },
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": "integer",
        "TracingConfig": {
            "Mode": "string"
        },
        "Version": "string",
        "VpcConfig": {
            "SecurityGroupIds": [ "string" ],
            "SubnetIds": [ "string" ]
        },
        "MasterArn": "string",
        "MemorySize": number
    }

```

AwsLambdaLayerVersion

该AwsLambdaLayerVersion对象提供有关 Lambda 层版本的详细信息。

以下示例显示AwsLambdaLayerVersion对象Amazon的安全结果格式 (ASFF)。要查看AwsLambdaLayerVersion属性的描述，请参阅 Amazon Security HubAPI 参考[AwsLambdaLayerVersionDetails](#)中的。

示例

```

"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreateDate": "2019-10-09T22:02:00.274+0000"
}

```

AwsNetworkFirewall

以下是AwsNetworkFirewall资源Amazon的安全查找格式的示例。

AwsNetworkFirewallFirewall

该AwsNetworkFirewallFirewall对象包含有关Amazon Network Firewall防火墙的详细信息。

以下示例显示AwsNetworkFirewallFirewall对象Amazon的安全结果格式 (ASFF)。要查看AwsNetworkFirewallFirewall属性的描述，请参阅 Amazon Security HubAPI 参考[AwsNetworkFirewallFirewallDetails](#)中的。

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

该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AwsNetworkFirewallFirewallPolicy对象Amazon的安全结果格式 (ASFF)。要查看AwsNetworkFirewallFirewallPolicy属性的描述，请参阅 Amazon Security Hub API 参考[AwsNetworkFirewallFirewallPolicyDetails](#)中的。

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

该AwsNetworkFirewallRuleGroup对象提供有关Amazon 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单个数据包。有状态规则组适用于数据包的流量上下文中的数据。

防火墙策略中引用了规则组。

以下示例显示AwsNetworkFirewallRuleGroup对象Amazon的安全结果格式 (ASFF)。要查看AwsNetworkFirewallRuleGroup属性的描述，请参阅 Amazon Security HubAPI 参考[AwsNetworkFirewallRuleGroupDetails](#)中的。

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

以下是AwsOpenSearchService资源Amazon的安全查找格式的示例。

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AwsOpenSearchServiceDomain对象Amazon的安全结果格式 (ASFF)。要查看AwsOpenSearchServiceDomain属性的描述，请参阅 Amazon Security Hub API 参考 [AwsOpenSearchServiceDomainDetails](#) 中的。

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

以下是AwsRds资源Amazon的安全查找格式的示例。

AwsRdsDbCluster

该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AwsRdsDbCluster对象Amazon的安全结果格式 (ASFF)。要查看AwsRdsDbCluster属性的描述，请参阅 Amazon Security Hub API 参考 [AwsRdsDbClusterDetails](#) 中的。

Example

```

"AwsRdsDbCluster": {
  "AllocatedStorage": 1,
  "AvailabilityZones": [
    "us-east-1c",
    "us-east-1e",
    "us-east-1a"
  ],
  "BackupRetentionPeriod": 1,
  "DatabaseName": "",
  "Status": "modifying",
  "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
  "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
  "CustomEndpoints": [],
  "MultiAz": false,
  "Engine": "aurora-mysql",
  "EngineVersion": "5.7.mysql_aurora.2.03.4",
  "Port": 3306,
  "MasterUsername": "admin",
  "PreferredBackupWindow": "04:52-05:22",
  "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
  "ReadReplicaIdentifiers": [],
  "VpcSecurityGroups": [
    {
      "VpcSecurityGroupId": "sg-example-1",
      "Status": "active"
    }
  ],
  "HostedZoneId": "ZONE1",
  "StorageEncrypted": true,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "DbClusterResourceId": "cluster-example",

```



```

    "AssociatedRoles": [
      {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
        "Status": "PENDING"
      }
    ],
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "EnabledCloudwatchLogsExports": [
      "audit",
      "error",
      "general",
      "slowquery"
    ],
    "EngineMode": "provisioned",
    "DeletionProtection": false,
    "HttpEndpointEnabled": false,
    "ActivityStreamStatus": "stopped",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "DomainMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbSubnetGroup": "subnet-group",
    "DbClusterOptionGroupMemberships": [],
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
      {
        "IsClusterWriter": true,
        "PromotionTier": 1,
        "DbInstanceIdentifier": "database-3-instance-1",
        "DbClusterParameterGroupStatus": "in-sync"
      }
    ],
    "IamDatabaseAuthenticationEnabled": false
  }
}

```

AwsRdsDbClusterSnapshot

该AwsRdsDbClusterSnapshot对象包含有关 Amazon RDS DB Securite Service S

以下示例显示AwsRdsDbClusterSnapshot对象Amazon的安全结果格式 (ASFF)。要查看AwsRdsDbClusterSnapshot属性的描述，请参阅 Amazon Security HubAPI 参考[AwsRdsDbClusterSnapshotDetails](#)中的。

示例

```

"AwsRdsDbClusterSnapshot": {
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1d",
    "us-east-1e"
  ],
  "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
  "Engine": "aurora",
  "AllocatedStorage": 0,
  "Status": "available",
  "Port": 0,
  "VpcId": "vpc-faf7e380",
  "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
  "MasterUsername": "admin",
  "EngineVersion": "5.6.10a",
  "LicenseModel": "aurora",
  "SnapshotType": "automated",
  "PercentProgress": 100,

```

```

    "StorageEncrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "IamDatabaseAuthenticationEnabled": false
  }

```

AwsRdsDbInstance

该AwsRdsDbInstance对象可提供有关 Amazon RDS 数据库实例的详细信息。

以下示例显示AwsRdsDbInstance对象Amazon的安全结果格式 (ASFF)。要查看AwsRdsDbInstance属性的描述，请参阅 Amazon Security HubAPI 参考[AwsRdsDbInstanceDetails](#)中的。

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

该AwsRdsDbSecurityGroup对象包含有关 Amazon Relational Database Ser

以下示例显示AwsRdsDbSecurityGroup对象Amazon的安全结果格式 (ASFF)。要查看AwsRdsDbSecurityGroup属性的描述，请参阅 Amazon Security HubAPI 参考[AwsRdsDbSecurityGroupDetails](#)中的。

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

该AwsRdsDbSnapshot对象包含有关 Amazon RDS 数据库集群快照的详细信息。

以下示例显示AwsRdsDbSnapshot对象Amazon的安全结果格式 (ASFF)。要查看AwsRdsDbSnapshot属性的描述，请参阅 Amazon Security HubAPI 参考[AwsRdsDbSnapshotDetails](#)中的。

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 AwsRdsEventSubscription 对象 Amazon 的安全结果格式 (ASFF)。要查看 AwsRdsEventSubscription 属性的描述，请参阅 Amazon Security Hub API 参考 [AwsRdsEventSubscriptionDetails](#) 中的。

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

以下是 AwsRedshift 资源 Amazon 的安全查找格式的示例。

AwsRedshiftCluster

该 AwsRedshiftCluster 对象包含有关 Amazon Redshift 集群的详细信息。

以下示例显示 AwsRedshiftCluster 对象 Amazon 的安全结果格式 (ASFF)。要查看 AwsRedshiftCluster 属性的描述，请参阅 Amazon Security Hub API 参考 [AwsRedshiftClusterDetails](#) 中的。

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": "Ja1rXUtnFEMI/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": "test-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"
        }
    ]
}

```

AwsS3

以下是AwsS3资源Amazon的安全查找格式的示例。

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock提供了有关 Amazon S3 公有访问块配置的信息。

以下示例显示AwsS3AccountPublicAccessBlock对象Amazon的安全结果格式 (ASFF)。要查看AwsS3AccountPublicAccessBlock属性的描述，请参阅 Amazon Security HubAPI 参考 AccountPublicAccessBlockDetails中的 [AWSS3](#)。

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AwsS3Bucket对象Amazon的安全结果格式 (ASFF)。要查看AwsS3Bucket属性的描述，请参阅 Amazon Security HubAPI 参考BucketDetails中的 [AWSS3](#)。

示例

```
"AwsS3Bucket": {
  "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
  "OwnerName": "s3bucketowner",
  "CreatedAt": "2007-11-30T01:46:56.000Z",
  "ServerSideEncryptionConfiguration": {
    "Rules": [
      {
        "ApplyServerSideEncryptionByDefault": {
          "SSEAlgorithm": "AES256",
          "KMSEMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
        }
      }
    ]
  },
  "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"
            }
        ]
    }
}
},
"PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true,
}
}

```

AwsS3Object

该AwsS3Object对象提供有关 Amazon S3 对象的信息。

以下示例显示AwsS3Object对象Amazon的安全结果格式 (ASFF)。要查看AwsS3Object属性的描述，请参阅 Amazon Security HubAPI 参考ObjectDetails中的 [AWSS3](#)。

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": "ws310urg00jH_HH1lIxPE35P.MELYaYh"
}

```

AwsSecretsManager

以下是AwsSecretsManager资源Amazon的安全查找格式的示例。

AwsSecretsManagerSecret

该AwsSecretsManagerSecret对象提供有关 Secrets Manager 密钥的详细信息。

以下示例显示AwsSecretsManagerSecret对象Amazon的安全结果格式 (ASFF)。要查看AwsSecretsManagerSecret属性的描述，请参阅 Amazon Security HubAPI 参考[AwsSecretsManagerSecretDetails](#)中的。

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

以下是AwsSns资源Amazon的安全查找格式的示例。

AwsSnsTopic

该AwsSnsTopic对象包含有关Amazon Simple Notifice Service 主题的

以下示例显示AwsSnsTopic对象Amazon的安全结果格式 (ASFF)。要查看AwsSnsTopic属性的描述，请参阅 Amazon Security HubAPI 参考[AwsSnsTopicDetails](#)中的。

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

以下是AwsSqs资源Amazon的安全查找格式的示例。

AwsSqsQueue

该AwsSqsQueue对象包含有关Amazon Simple Service 队列的信息。

以下示例显示AwsSqsQueue对象Amazon的安全结果格式 (ASFF)。要查看AwsSqsQueue属性的描述，请参阅 Amazon Security HubAPI 参考[AwsSqsQueueDetails](#)中的。

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

以下是AwsSsm资源Amazon的安全查找格式的示例。

AwsSsmPatchCompliance

该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AwsSsmPatchCompliance对象Amazon的安全结果格式 (ASFF)。要查看AwsSsmPatchCompliance属性的描述，请参阅 Amazon Security Hub API 参考[AwsSsmPatchComplianceDetails](#)中的。

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"
    }
  }
}
```

AwsWaf

以下是AwsWaf资源Amazon的安全查找格式的示例。

AwsWafRateBasedRule

该AwsWafRateBasedRule对象包含有关全球资源Amazon WAF基于速率的规则的信息。Amazon WAF基于速率的规则提供设置，用于指示何时允许、阻止或计数请求。基于速率的规则包括在时间段内到达的请求数量。

以下示例显示AwsWafRateBasedRule对象Amazon的安全结果格式 (ASFF)。要查看AwsWafRateBasedRule属性的描述，请参阅 Amazon Security Hub API 参考[AwsWafRateBasedRuleDetails](#)中的。

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

该AwsWafRegionalRateBasedRule对象包含有关区域资源基于费率的规则的详细信息。基于速率的规则提供设置以指示何时允许、阻止或计数请求。基于速率的规则包括在时间段内到达的请求数量。

以下示例显示AwsWafRegionalRateBasedRule对象Amazon的安全结果格式 (ASFF)。要查看AwsWafRegionalRateBasedRule属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafRegionalRateBasedRuleDetails](#)中的。

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Amazon WAF区域规则的详细信息。此规则可识别要允许、阻止或计数的 Web 请求。

以下示例显示AwsWafRegionalRule对象Amazon的安全结果格式 (ASFF)。要查看AwsWafRegionalRule属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafRegionalRuleDetails](#)中的。

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

该AwsWafRegionalRuleGroup对象提供有关Amazon WAF区域规则组的详细信息。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。

以下示例显示AwsWafRegionalRuleGroup对象Amazon的安全结果格式 (ASFF)。要查看AwsWafRegionalRuleGroup属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafRegionalRuleGroupDetails](#)中的。

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Amazon WAF区域 Web 访问控制列表 (Web ACL) 的详细信息。Web ACL 包含用于标识要允许、阻止或计数的请求的规则。

以下是Security FAwsWafRegionalWebAcl indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsApiGatewayV2Stage属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafRegionalWebAclDetails](#)中的。

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Amazon WAF规则的信息。Amazon WAF规则可识别要允许、阻止或计数的 Web 请求。

以下是Security FAwsWafRule indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsApiGatewayV2Stage属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafRuleDetails](#)中的。

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提供有关Amazon WAF规则组的信息。Amazon WAF规则组是您添加到 Web 访问控制列表 (Web ACL) 中的预定义规则进行嵌套。

以下是Security FAwsWafRuleGroup indingAmazon 格式 (ASFF) 中的结果示例。要查看AwsApiGatewayV2Stage属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafRuleGroupDetails](#)中的。

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"
  }]
}
```

AwsWafWebAcl

该AwsWafWebAcl对象提供有关Amazon WAF Web ACL 的详细信息。

以下示例显示AwsWafWebAcl对象Amazon的安全结果格式 (ASFF)。要查看AwsWafWebAcl属性的描述，请参阅 Amazon Security HubAPI 参考[AwsWafWebAclDetails](#)中的。

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"
  }
}
```

AwsXray

以下是AwsXray资源Amazon的安全查找格式的示例。

AwsXrayEncryptionConfig

该AwsXrayEncryptionConfig对象包含有关加密配置的信息Amazon X-Ray。

以下示例显示AwsXrayEncryptionConfig对象Amazon的安全结果格式 (ASFF)。要查看AwsXrayEncryptionConfig属性的描述，请参阅 Amazon Security HubAPI 参考[AwsXrayEncryptionConfigDetails](#)中的。

示例

```
"AwsXRayEncryptionConfig":{
  "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
  "Status": "UPDATING",
  "Type":"KMS"
}
```

Container

与结果相关的容器详细信息。

以下示例显示Container对象Amazon的安全结果格式 (ASFF)。要查看Container属性的描述，请参阅 Amazon Security HubAPI 参考[ContainerDetails](#)中的。

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"
  }]
}
```


Other

该Other对象允许您提供自定义字段和值。您可以在以下情况下使用该Other对象。

- 资源类型没有对应的Details对象。要提供资源的详细信息，请使用Other对象。
- 资源类型的Details对象不包含您要填充的所有属性。在这种情况下，使用资源类型的Details对象来填充可用属性。使用该Other对象填充不在特定类型对象中的属性。
- 资源类型不是提供的类型之一。在这种情况下，您可以Resource.Type将设置为Other，然后使用Other对象填充详细信息。

类型：最多包含 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。

中的见解AmazonSecurity Hub

网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的AmazonSecurity Hub 见解是相关结果的集合。它确定了需要注意和干预的安全区域。例如，洞察可能会指出 EC2 实例是检测不良安全做法的调查结果的主题。见解汇集了来自各个结果提供商的结果。

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结果进行分组，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进行分组，则见解将生成资源标识符的列表。可选的筛选条件将标识见解的匹配结果。例如，您可能希望仅查看来自特定提供商的结果或与特定类型的资源相关的结果。

Security Hub 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 Amazon 环境和使用情况独有的安全问题，您可以使用自定义见解。

仅在启用了集成或标准来生成匹配的结果时，见解才返回结果。例如，托管见解 29. Top resources by counts of failed CIS checks (按失败 CIS 检查数排列的顶级资源) 只有在启用 CIS 的情况下才返回结果 Amazon 标准。

主题

- [查看和筛选洞察列表 \(p. 195\)](#)
- [查看见解结果和调查结果并采取相应措施 \(p. 195\)](#)
- [托管见解 \(p. 197\)](#)
- [自定义见解 \(p. 204\)](#)

查看和筛选洞察列表

这些区域有：见解页面显示可用见解的列表。

默认情况下，该列表显示托管和自定义见解。要根据见解类型筛选见解列表，请从筛选器字段旁边的下拉菜单中选择见解类型。

- 要显示所有可用见解，请选择所有见解。这是默认选项。
- 要仅显示托管见解，请选择托管见解 Security Hub。
- 要仅显示自定义见解，请选择自定义见解。

您还可以根据洞察名称中的文本筛选洞察列表。

在“Filter”字段中，键入要用于筛选列表的文本。此筛选条件不区分大小写。筛选器会查找包含洞察名称中任意位置文本的见解。

查看见解结果和调查结果并采取相应措施

对于每一个洞察力，AmazonSecurity Hub 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。

从见解控制台页面中，您可以查看结果和调查结果并采取相应措施。

如果启用跨区域聚合, 则在聚合区域中, 托管见解的结果包括来自聚合区域和链接区域的结果。对于自定义洞察结果, 如果洞察不按区域进行筛选, 则结果将包括来自聚合区域和链接区域的调查结果。

在其他地区, 洞察结果仅适用于该地区。

有关如何配置跨区域聚合的信息, 请参阅[跨区域聚合 \(p. 50\)](#)。

查看见解结果并采取相应措施 (控制台)

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结果数。

请注意, 如果调查结果按资源标识符或资源类型分组, 则结果将包括匹配结果中的所有资源。这包括类型与筛选条件中指定的资源类型不同的资源。例如, 洞察可以识别与 S3 存储桶关联的发现。如果匹配发现同时包含 S3 存储桶资源和 IAM 访问密钥资源, 则见解结果将列出这两个资源。

结果列表的排序方式为: 从匹配率最高的结果到匹配率最低的结果。

Security Hub 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结果数。

- Severity label— 每个严重性标签的结果数
- Amazon 账户 ID— 匹配结果的前 5 个账户 ID
- 资源类型— 匹配结果的前 5 个资源类型
- Resource ID (资源 ID)— 匹配结果的前 5 个资源 ID
- 产品名称-匹配结果的前 5 个结果提供商

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。操作必须与 CloudWatch 规则 Security Hub Insight Results 事件类型。请参阅[自动响应和补救 \(p. 500\)](#)。

如果您尚未配置自定义操作, 则操作菜单已禁用。

显示见解结果列表并采取相应措施

1. 打开 Amazon 在 Security Hub 控制台<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 Actions (操作) 菜单中, 选择自定义操作。

查看见解结果 (Security Hub API , Amazon CLI)

要查看见解结果, 您可以使用 API 调用或 Amazon Command Line Interface。

要查看见解结果 (Security Hub API) , Amazon CLI)

- Security Hub API— 使用 [GetInsightResults](#) operation。要确定要返回结果的见解, 您需要洞察 ARN。要获取洞察 ARN 以获取自定义见解, 请使用 [GetInsights](#) operation。
- Amazon CLI— 在命令行处, 运行 [get-insight-results](#) 命令。

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

例如:

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

查看见解结果的结果 (控制台)

从见解结果列表中，您可以显示每个结果的调查结果列表。

显示见解结果并采取相应措施

1. 打开Amazon在 Security Hub 控制台<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。

调查结果列表显示了工作流程状态为 NEW 或 NOTIFIED 的所选见解结果的活动调查结果。

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 \(p. 63\)](#)
- [查看单个结果的详细信息 \(p. 65\)](#)
- [更新结果的工作流程状态 \(p. 66\)](#)
- [将结果发送到自定义操作 \(p. 68\)](#)

托管见解

AmazonSecurity Hub 提供了多个托管见解。

您无法编辑或删除 Security Hub 托管见解。您可以[查看见解结果和调查结果并采取措施 \(p. 195\)](#)。您还可以[将托管见解用作新的自定义见解的基础 \(p. 206\)](#)。

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结果时，托管见解才返回结果。

对于按资源标识符分组的见解，结果包括匹配结果中所有资源的标识符。这包括类型与筛选条件中的资源类型不同的资源。例如，见解 2 确定了与 S3 存储桶关联的调查结果。如果匹配发现同时包含 S3 存储桶资源和 IAM 访问密钥资源，则洞察结果包括两种资源。

在当前版本中，Security Hub 提供了以下托管见解：

1. 具有最多结果的 Amazon 资源

ARN : arn:aws:securityhub:::insight/securityhub/default/1

分组方式：资源标识符

结果筛选条件：

- 记录状态为 ACTIVE
- 工作流程状态为 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

Game by (分组依 资源标识符

结果筛选条件：

- 类型以 Effects/Data Exposure 开头
- 资源类型为 AwsS3Bucket
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

3. AMIs that are generating the most findings (生成最多结果的 AMI)

ARN : arn:aws:securityhub:::insight/securityhub/default/3

Game by (分组依 EC2 instance image ID

结果筛选条件：

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

4. 涉及已知战术、技术和过程 (TTP) 的 EC2 实例

ARN : arn:aws:securityhub:::insight/securityhub/default/14

Game by (分组依 资源 ID

结果筛选条件：

- 类型以 TTPs 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

5. Amazon 有可疑访问密钥活动的委托人

ARN : arn:aws:securityhub:::insight/securityhub/default/9

分组方式：IAM 访问密钥委托人名称

结果筛选条件：

- 资源类型为 AwsIamAccessKey
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

6. 不符合安全标准/最佳实践的 Amazon 资源实例

ARN : arn:aws:securityhub:::insight/securityhub/default/6

分组方式：资源 ID

结果筛选条件：

- 类型为 Software and Configuration Checks/Industry and Regulatory Standards/Amazon Security Best Practices
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

7. 与潜在数据泄露相关的 Amazon 资源

ARN : arn:aws:securityhub:::insight/securityhub/default/7

分组方式：：资源 ID

结果筛选条件：

- 类型以 Effects/Data Exfiltration/ 开头
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

8. 与未经授权的资源使用相关的 Amazon 资源

ARN : arn:aws:securityhub:::insight/securityhub/default/8

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 Effects/Resource Consumption 开头
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

9. S3 buckets that don't meet security standards / best practice (不符合安全标准/最佳实践的 S3 存储桶)

ARN : arn:aws:securityhub:::insight/securityhub/default/11

分组方式 : 资源 ID

结果筛选条件 :

- 资源类型为 AwsS3Bucket
- 类型为 Software and Configuration Checks/Industry and Regulatory Standards/Amazon Security Best Practices
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

10. 具有敏感数据的 S3 存储桶

ARN : arn:aws:securityhub:::insight/securityhub/default/12

分组方式 : 资源 ID

结果筛选条件 :

- 资源类型为 AwsS3Bucket
- 类型以 Sensitive Data Identifications/ 开头
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

11. Credentials that may have leaked (可能泄露的凭证)

ARN : arn:aws:securityhub:::insight/securityhub/default/13

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 Sensitive Data Identifications/Passwords/ 开头
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

12. 缺少重要漏洞安全补丁的 EC2 实例

ARN : arn:aws:securityhub:::insight/securityhub/default/16

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 Software and Configuration Checks/Vulnerabilities/CVE 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

13. 具有一般异常行为的 EC2 实例

ARN : arn:aws:securityhub:::insight/securityhub/default/17

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 Unusual Behaviors 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED。

14. EC2 instances that have ports accessible from the Internet (具有可从 Internet 访问的端口的 EC2 实例)

ARN : arn:aws:securityhub:::insight/securityhub/default/18

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 Software and Configuration Checks/Amazon Security Best Practices/Network Reachability 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

15. EC2 instances that don't meet security standards / best practices (不符合安全标准/最佳实践的 EC2 实例)

ARN : arn:aws:securityhub:::insight/securityhub/default/19

分组方式 : 资源 ID

结果筛选条件 :

- 类型以下列某个项开头 :
 - Software and Configuration Checks/Industry and Regulatory Standards/
 - Software and Configuration Checks/Amazon Security Best Practices
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

16. EC2 instances that are open to the Internet (对 Internet 开放的 EC2 实例)

ARN : arn:aws:securityhub:::insight/securityhub/default/21

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 Software and Configuration Checks/Amazon Security Best Practices/Network Reachability 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE

- 工作流程状态为 NEW 或 NOTIFIED

17. 与攻击者侦测相关的 EC2 实例

ARN : arn:aws:securityhub:::insight/securityhub/default/22

分组方式 : 资源 ID

结果筛选条件 :

- 类型以 TTPs/Discovery/Recon 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

18. 与恶意软件相关的 Amazon 资源

ARN : arn:aws:securityhub:::insight/securityhub/default/23

Game by (分组依 资源 ID

结果筛选条件 :

- 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
- 工作流程状态为 NEW 或 NOTIFIED

19. 与加密货币问题相关的 Amazon 资源

ARN : arn:aws:securityhub:::insight/securityhub/default/24

Game by (分组依 资源 ID

结果筛选条件 :

- 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
- 工作流程状态为 NEW 或 NOTIFIED

20. 具有未经授权的访问尝试的 Amazon 资源

ARN : arn:aws:securityhub:::insight/securityhub/default/25

Game by (分组依 资源 ID

结果筛选条件 :

- 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
- 工作流程状态为 NEW 或 NOTIFIED

21. Threat Intel indicators with the most hits in the last week (上周命中次数最多的威胁情报指标)

ARN : arn:aws:securityhub:::insight/securityhub/default/26

结果筛选条件 :

- 已在过去 7 天内创建

22. Top accounts by counts of findings (按结果数排列的顶级账户)

ARN : arn:aws:securityhub:::insight/securityhub/default/27

Game by (分组依 Amazon 账户 ID)

结果筛选条件 :

- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

23. Top products by counts of findings (按结果数排列的顶级产品)

ARN : arn:aws:securityhub:::insight/securityhub/default/28

Game by (分组依 产品名称)

结果筛选条件 :

- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

24. Severity by counts of findings (按结果数排列的严重性)

ARN : arn:aws:securityhub:::insight/securityhub/default/29

Game by (分组依 Severity label)

结果筛选条件 :

- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

25. Top S3 buckets by counts of findings (按结果数排列的顶级 S3 存储桶)

ARN : arn:aws:securityhub:::insight/securityhub/default/30

Game by (分组依 资源 ID)

结果筛选条件 :

- 资源类型为 AwsS3Bucket
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

26. Top EC2 instances by counts of findings (按结果数排列的顶级 EC2 实例)

ARN : arn:aws:securityhub:::insight/securityhub/default/31

Game by (分组依 资源 ID)

结果筛选条件 :

- 资源类型为 AwsEc2Instance

- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

27. Top AMIs by counts of findings (按结果数排列的顶级 AMI)

ARN : `arn:aws:securityhub:::insight/securityhub/default/32`

Game by (分组依 EC2 instance image ID)

结果筛选条件 :

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

28. Top IAM users by counts of findings(按结果数排列的顶级 IAM 用户)

ARN : `arn:aws:securityhub:::insight/securityhub/default/33`

Game by (分组依 IAM access key user name)

结果筛选条件 :

- 资源类型为 AwsIamAccessKey
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

29. Top resources by counts of failed CIS checks (按失败 CIS 检查数排列的顶级资源)

ARN : `arn:aws:securityhub:::insight/securityhub/default/34`

Game by (分组依 资源 ID)

结果筛选条件 :

- 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
- 工作流程状态为 NEW 或 NOTIFIED

30. Top integrations by counts of findings (按结果数排列的顶级集成)

ARN : `arn:aws:securityhub:::insight/securityhub/default/35`

Game by (分组依 产品 ARN)

结果筛选条件 :

- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

31. 安全检查失败最多的资源

ARN : `arn:aws:securityhub:::insight/securityhub/default/36`

Game by (分组依 资源 ID)

结果筛选条件 :

- 已在最后一天更新
- 合规性状态为 FAILED

- ### 32. 有可疑活动的 IAM 用户

Game by (分组依 IAM 用户名)

- 资源类型为 `AwsIamUser`
- 记录状态为 `ACTIVE`
- 工作流程状态为 `NEW` 或 `NOTIFIED`

以下是一些可能对设置有用的自定义见解的示例：

- 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。

- 分组— 分组属性确定了见解结果列表中显示的项目。例如，如果分组属性为产品名称，则则则则则则则则则则则则将显示与每个结果提供商关联的结果数。
- 可选筛选条件— 筛选条件将缩小见解的匹配结果的范围。

不过，Security Hub 会对使用的属性相同但值不同的筛选条件应用布尔 OR 逻辑。例如，如果筛选条件为“产品名称为 GuardDuty和“产品名称是 Amazon Inspector”，则则则仅在结果由以下任一方生成时才被视为匹配的结果 GuardDuty 或Amazon Inspector

创建自定义见解（控制台）

创建自定义见解

-
- 204

3. 选择 Create insight (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条件选项。
 - b. 选择 Group by (分组依据)。
 - c. 选择要用于对该见解关联的结果进行分组的属性。
 - d. 选择 Apply (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 Apply。
6. 选择 Create insight (创建见解)。
7. 输入 Insight name (见解名称)，然后选择 Create insight (创建见解)。

创建自定义见解 (Security Hub) Amazon CLI)

要创建自定义见解，可以使用 API 调用或 Amazon Command Line Interface。

要创建自定义见解 (Security Hub API)，Amazon CLI)

- Security Hub—[CreateInsight](#) operation. 创建自定义洞察时，必须提供名称、筛选器和分组属性。
- Amazon CLI在命令行处，运行[create-insight](#)命令。

```
aws securityhub create-insight --name <insight name> --filters <filter values> --group-by-attribute <attribute name>
```

示例

```
aws securityhub create-insight --filters '{"ResourceType": [{"Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-attribute "ResourceId" --name "Critical role findings"
```

修改自定义见解 (控制台)

您可以修改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。

修改见解

1. 打开 Amazon Security Hub <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
 - 要更改用于对见解中的结果进行分组的属性，请执行以下操作：
 - a. 要删除现有分组，请选择 X 旁边 Group by (分组依据) 设置。
 - b. 选择搜索框。
 - c. 选择要用于分组的属性。
 - d. 选择 Apply (应用)。
 - 要从见解中删除筛选条件，请选择带圆圈的 X 在过滤器旁边。
 - 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 Apply (应用)。
5. 完成更新后，请选择 Save insight (保存见解)。
6. 在出现提示时，执行下列操作之一：
 - 要更新现有见解以反映您的更改，请选择 Update **<Insight_Name>** (更新 <Insight_Name>)，然后选择 Save insight (保存见解)。
 - 要使用更新创建新的见解，请选择 Save new insight (保存新见解)。输入 Insight name (见解名称)，然后选择 Save insight (保存见解)。

修改自定义见解 (Security HubAmazon CLI)

要修改自定义见解，可以使用 API 调用或 Amazon Command Line Interface。

要修改自定义见解 (Security Hub API)，Amazon CLI)

- Security Hub—[UpdateInsight](#) operation. 要识别自定义洞察，您需要提供见解 ARN。要获取自定义见解的洞察 ARN，请使用 [GetInsights](#) operation. 然后，您可以更新名称、筛选器和分组值。
- Amazon CLI 在命令行处，运行 [update-insight](#) 命令。

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

示例

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111" --filters '{"ResourceType": [{"Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --name "High severity role findings"
```

从托管见解创建新的自定义见解 (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。您可以将托管见解用作新的自定义见解的基础。

从托管见解创建新的自定义见解

1. 打开 Amazon Security Hub <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
 - 要更改用于对见解中的结果进行分组的属性，请执行以下操作：
 - a. 要删除现有分组，请选择 X 旁边 Group by (分组依据) 设置。
 - b. 选择搜索框。
 - c. 选择要用于分组的属性。
 - d. 选择 Apply (应用)。
 - 要从见解中删除筛选条件，请选择带圆圈的 X 在过滤器旁边。
 - 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 Apply (应用)。
5. 更新完成后, 请选择 Create insight (创建见解)。
6. 出现提示时, 请输入见解名称, 然后选择创建见解。

删除自定义见解 (控制台)

当您不再需要自定义见解时, 可以将其删除。您无法删除托管见解。

删除自定义见解

1. 打开AmazonSecurity Hub<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 Delete (删除)。

删除自定义见解 (Security HubAmazon CLI)

要删除自定义见解, 可以使用 API 调用或Amazon Command Line Interface。

删除自定义见解 (Security Hub) Amazon CLI)

- Security Hub—[DeleteInsight](#)operation. 要确定要删除的自定义洞察, 请提供见解 ARN。要获取自定义见解的洞察 ARN, 请使用[GetInsights](#)operation。
- Amazon CLI在命令行处, 运行[delete-insight](#)命令。

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

示例

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

中的产品集成AmazonSecurity Hub

AmazonSecurity Hub 可以聚合来自多个安全查找数据Amazon支持的服务和支持的Amazon合作伙伴网络 (APN) 安全解决方案。这一聚合提供了整个您的安全性和合规性的全面视图。Amazon环境。

您还可以发送从您自己的自定义安全产品生成的结果。

Important

来自受支持的Amazon以及合作伙伴产品集成，Security Hub 仅接收和合并您在中启用 Security Hub 后生成的结果。Amazon账户。

该服务不会以追溯方式接收和合并启用 Security Hub 前生成的安全结果。

有关 Security Hub 如何对提取结果收费的详细信息，请参阅[Security Hub 定价](#)。

主题

- [管理产品集成 \(p. 208\)](#)
- [可用的 Amazon 服务集成 \(p. 211\)](#)
- [可用的第三方合作伙伴产品集成 \(p. 221\)](#)
- [使用自定义产品集成将结果发送到AmazonSecurity Hub \(p. 241\)](#)

管理产品集成

这些区域有：集成中的页面Amazon Web Services Management Console提供对所有可用的Amazon和第三方产品集成。这些区域有：AmazonSecurity Hub API 还提供了可用于管理集成的操作。

Note

某些集成并非在所有区域都可用。如果当前区域不支持某个集成，则不会在集成页。

另请参阅 [the section called “中国（北京）和中国（宁夏）支持的集成” \(p. 517\)](#) 和 [the section called “Amazon GovCloud（美国东部）和Amazon GovCloud（美国西部）中支持的集成” \(p. 517\)](#)。

查看和筛选集成列表（控制台）

从 Integrations (集成) 页面中，您可以查看和筛选集成列表。

查看集成列表

1. 打开Amazon在 Security Hub 控制台<https://console.aws.amazon.com/securityhub/>。
2. 在 Security Hub 导航窗格中，选择集成。

在 Integrations (集成) 页面上，依次列出了与其他 Amazon 服务的集成和与第三方产品的集成。

对于每个集成，Integrations (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

您可以通过输入以下字段中的文本来筛选列表。

- 公司名称
- 产品名称
- 集成描述
- 类别

查看有关产品集成的信息 (Security Hub API , Amazon CLI)

要查看有关产品集成的信息，您可以使用 API 调用或 Amazon Command Line Interface。您可以显示有关所有产品集成的信息，或者有关已启用的产品集成的信息。

要查看有关所有可用产品集成的信息 (Security Hub API) , Amazon CLI)

- Security Hub API— 使用 [DescribeProducts](#) operation。要确定要退货的特定产品集成，请使用 `ProductArn` 参数来提供集成 ARN。
- Amazon CLI— 在命令行处，运行 [describe-products](#) 命令。要确定要返回的特定产品集成，请提供集成 ARN。

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

示例

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

要查看有关您已启用的产品集成的信息 (Security Hub API , Amazon CLI)

- Security Hub API— 使用 [ListEnabledProductsForImport](#) operation。
- Amazon CLI— 在命令行处，运行 [list-enabled-products-for-import](#) 命令。

```
aws securityhub list-enabled-products-for-import
```

启用集成

在 Integrations (集成) 页面上，每个集成均提供了自身的必需启用步骤。

对于与其他 Amazon 服务的大多数集成，唯一必需的步骤是启用另一项服务。集成信息包含指向服务主页的链接。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 能够收到来自服务的结果。

对于第三方产品集成，您可能需要从 Amazon Web Services Marketplace 中购买集成，然后配置该集成。集成信息提供了用于执行这些任务的链接。

如果 Amazon Web Services Marketplace 中有产品的多个版本，请选择要订阅的版本，然后选择 Continue to Subscribe (继续订阅)。例如，某些产品提供标准版本和 Amazon 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。该资源策略定义 Security Hub 需要的权限，从而使能够收到来自该产品的结果。

禁用和启用来自集成的结果流 (控制台)

在存储库的集成页面，对于发送调查结果的集成，状态信息表明您目前是否接受调查结果。

要停止接受结果，请选择 Stop accepting findings (停止接受结果)。

要恢复接受结果，请选择 Accept findings (接受结果)。

禁用来自集成的结果流 (Security Hub API , Amazon CLI)

要禁用来自集成的结果流，您可以使用 API 调用或使用 Amazon Command Line Interface。

要禁用来自集成 (Security Hub API ,) 的结果流 Amazon CLI)

- Security Hub API— 使用 [DisableImportFindingsForProduct](#) operation. 要确定要禁用的集成，您需要订阅的 ARN。要获取启用的集成的订阅 ARN，请使用 [ListEnabledProductsForImport](#) operation.
- Amazon CLI— 在命令行处，运行 [disable-import-findings-for-product](#) 命令。

```
aws securityhub disable-import-findings-for-product --product-subscription-arn <subscription ARN>
```

示例

```
aws securityhub disable-import-findings-for-product --product-subscription-arn "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/crowdstrike-falcon"
```

启用来自集成的结果流 (Security Hub API , Amazon CLI)

要启用来自集成的结果流，您可以使用 API 调用或 Amazon Command Line Interface。

要启用来自集成的结果流 (Security Hub API , Amazon CLI)

- Security Hub API— 使用 [EnableImportFindingsForProduct](#) operation. 要使 Security Hub 能够收到来自集成的结果，您需要产品 ARN。要获取可用集成的 ARN，请使用 [DescribeProducts](#) operation.
- Amazon CLI：在命令行处，运行 [enable-import-findings-for-product](#) 命令。

```
aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
```

示例

```
aws securityhub enable-import-findings-for-product --product-arn "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

查看来自集成的结果

对于您接受调查结果的集成 (状态是接受结果)，要查看结果列表，请选择查看发现。

结果列表显示了工作流程状态为 NEW 或 NOTIFIED 的所选集成的活动结果。

如果启用跨区域聚合，则在聚合区域中，列表将包括来自聚合区域和启用集成的链接区域的结果。Security Hub 不会根据跨区域聚合配置自动启用集成。

在其他区域中，集成的查找结果列表仅包含来自当前区域的调查结果。

有关如何配置跨区域聚合的信息，请参阅[跨区域聚合 \(p. 50\)](#)。

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 \(p. 63\)](#)
- [查看单个结果的详细信息 \(p. 65\)](#)
- [更新结果的工作流程状态 \(p. 66\)](#)
- [将结果发送到自定义操作 \(p. 68\)](#)

可用的 Amazon 服务集成

Amazon Security Hub 支持与多种 Amazon 服务的集成。

Note

某些集成仅在部分地区可用。

如果不支持集成，则不会在 Security Hub 控制台的集成页面上列出该集成。

另请参阅[中国（北京）和中国（宁夏）支持的集成 \(p. 517\)](#)和[Amazon GovCloud（美国东部）和 Amazon GovCloud（美国西部）中支持的集成 \(p. 517\)](#)。

除了从 Amazon Macie 中发现的敏感数据外，您会自动选择与 Security Hub 进行所有其他 Amazon 服务集成。如果您已开启 Security Hub 和其他服务，则无需采取其他步骤即可激活这两个服务之间的集成。

与 Security Hub 的 Amazon 服务集成概述

以下是向 Security Hub 发送调查结果或从 Security Hub 接收发现结果的 Amazon 服务的概述。

综合 Amazon 服务	Direction	
Amazon Config	发送结果	
Amazon Firewall Manager	发送结果	
亚马 GuardDuty	发送结果	
Amazon Health	发送结果	
Amazon Identity and Access Management Access Analyzer	发送结果	
Amazon Inspector	发送结果	
Amazon Macie	发送结果	
Amazon Systems Manager Patch Manager	发送结果	
Amazon Audit Manager	接收结果	
Amazon Chatbot	接收结果	

综合Amazon服务	Direction	
Amazon Detective	接收结果	
Amazon Systems Manager探险家和 OpsCenter	接收和更新调查结果	
Amazon Trusted Advisor	接收结果	

Amazon将结果发送到 Security Hub 的服务

以下Amazon服务通过将发现结果发送到Security Hub 来与 Security Hub 集成。Security Hub 将调查结果转换为[Amazon安全调查结果格式 \(p. 69\)](#)。

Amazon Config (发送调查结果)

Amazon Config是一项服务，允许您评估、审计和评估Amazon资源配置。Amazon Config持续监控和记录您的Amazon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Amazon Config，您可以在 Security Hub 中将Amazon Config托管和自定义规则评估的结果视为 Security Hub 中的调查结果。这些发现可以与其他 Security Hub 调查结果一起查看，从而全面概述您的安全状况。

Amazon Config使用亚马逊 EventBridge 向Security Hub 发送Amazon Config规则评估。Security Hub 将规则评估转换为遵循[Amazon安全调查结果格式的调查 \(p. 68\)](#)结果。然后，Security Hub 通过获取有关受影响资源的更多信息，例如亚马逊资源名称 (ARN) 和创建日期，尽最大努力丰富调查结果。

有关此整合的更多信息，请参阅以下部分：

Amazon Config 将结果发送到 Security Hub 的方式

Security Hub 中的所有结果都使用标准的 JSON 格式。ASFF 包括有关结果起源、受影响资源以及结果当前状态的详细信息。Amazon Config通过将托管和自定义规则评估发送到 Security Hub EventBridge。Security Hub 将规则评估转换为遵循 ASFF 的结果，并在尽最大努力的基础上丰富调查结果。

Amazon Config发送到 Security Hub 的结果类型

激活集成后，Amazon Config将所有Amazon Config托管规则和自定义规则的评估发送到 Security Hub。仅排除来自[服务相关Amazon Config规则 \(p. 244\)](#)的评估，例如用于对安全控制进行检查的评估。

向 Security Hub 发送Amazon Config结果

激活集成后，Security Hub 将自动分配从中接收调查结果所需的权限Amazon Config。Security Hub 使用 service-to-service 级别权限，为您提供安全的方式来激活此集成并Amazon Config通过亚马逊导入调查结果 EventBridge。

发送结果的延迟

Amazon Config创建新查找结果时，您通常可以在五分钟内在 Security Hub 中查看该查找结果。

Security Hub 不可用时重试

Amazon Config尽最大努力将结果发送到 Security Hub EventBridge。如果事件未成功传送到 Security Hub，则 EventBridge重试投递最多 24 小时或 185 次，以先到者为准。

更新 Security Hub 中的现有Amazon Config结果

将结果Amazon Config发送到 Security Hub 之后，它可以将对同一结果发送到 Security Hub 中，以反映对查找活动的其他观测结果到 Security Hub 中。

存在Amazon Config调查结果的地区

Amazon Config调查结果是以区域为基础的。Amazon Config将发现结果发送到发现结果所在区域或区域的 Security Hub。

查看Amazon Config结果

要查看您的Amazon Config发现，请从 Security Hub 导航窗格中选择调查结果。要筛选搜索结果以仅显示搜索Amazon 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。

解释 SAmazon Config ecurity Hub 中的名称

Security Hub 将Amazon Config规则评估转换为后续结果[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。Amazon Config与 ASFF 相比，规则评估使用不同的事件模式。下表将Amazon Config规则评估字段与 Security Hub 中显示的 ASFF 对应字段映射到 Security Hub 中。

Config 规则评估查找类型	ASFF 结果类型	硬编码值
详细信息。awsAccountId	AwsAccountId	
详细信息。 newEvaluationResult. resultRecordedTime	CreatedAt	
详细信息。 newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	"arn:: securityHub<partition>::<region>: product/aws/c
	ProductName	"Config
	CompanyName	"Amazon"
	区域	"euuu-central-1
configRuleArn	GeneratorId, ProductFields	
详细信息。ConfigRulearn/ Finding/Hash	Id	
详细信息。configRuleName	标题， ProductFields	
详细信息。configRuleName	描述	"此发现是为更改配置 规则的资源合规性而创 建\${detail.ConfigRuleName}的："
配置项目“ARN”或Security Hub 计算的 ARN	资源 [i] .id	
详情。资源类型	资源 [i] .Type	"AwsS3Bucket"
	资源 [i] .分区	"aws"
	资源 [i] .Region	"euuu-central-1
配置项目“配置”	资源 [i]。详情	
	SchemaVersion	"2018-10-08"

Config 规则评估查找类型	ASFF 结果类型	硬编码值
	严重性.Label	请参阅下面的“解释严重性标签”
	类型	["软件和配置检查"]
详细信息。newEvaluationResult. 合规性类型	合规性。状态	“失败”、“不可用”、“已通过”或“警告”
	工作流程。状态	如果生成的Amazon Config调查结果的合规性状态为“已通过”，或者合规性状态从“失败”更改为“已通过”，则为“已解决”。否则，Workflow.Status 将为“新建”。您可以通过 BatchUpdateFindings API 操作更改此值。

解析严重性标签

在 ASFF 中，所有Amazon Config规则评估结果的默认严重性标签均为 MEDIUM。您可以使用 [BatchUpdateFindings](#) API 操作更新调查结果的严重性标签。

来自 Amazon Config 的典型结果

Security Hub 将Amazon Config规则评估转换为 ASFF 之后的调查结果。以下是 ASFF 典型结果Amazon Config的示例。

Note

如果描述超过 1024 个字符，它将被截断为 1024 个字符，最后会显示“(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:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
    "AwsS3Bucket": {
      "OwnerId": "4edbbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
      "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

要使用与 Security Hub 的集Amazon Config成，必须设置这两项服务，并在中添加至少一个托管或自定义规则Amazon Config。有关如何设置的信息Amazon Config，请参阅Amazon Config开发者指南中的[入门](#)。有关如何设置 Security Hub 的信息，请参阅[设置AmazonSecurity Hub \(p. 10\)](#)。

设置Amazon Config和 Security Hub 之后，集成将自动激活。Amazon Config立即开始将结果发送到 Security Hub。

停止向 Security Hub 发布结果

要停止向 Security Hub 发送结果，您可以使用 Security Hub 控制台、Security Hub API 或Amazon CLI。

请参阅[禁用和启用来自集成的结果流（控制台）\(p. 210\)](#)或[禁用来自集成的结果流（Security Hub API, Amazon CLI）\(p. 210\)](#)。

Amazon Firewall Manager（发送调查结果）

当资源的 Web 应用程序防火墙 (WAF) 策略或 Web 访问控制列表 (Web ACL) 规则不合规时，Firewall Manager 会发送结果到 Security Hub 中。Firewall Manager 还会在未保护资源或发现攻击时发送调查结果。Amazon Shield Advanced

如果您已经在使用Firewall Manager，Security Hub 会自动启用此集成。您不需要执行任何其他操作即可开始接收来自 Firewall Manager 的结果到 Firewall Manager 中。

要了解有关集成的更多信息，请查看 Security Hub 控制台中的集成页面。

要了解有关Firewall Manager 更多信息，请参阅[Amazon WAF开发者指南](#)。

亚马逊 GuardDuty (发送调查结果)

GuardDuty 将所有支持的查找条件类型的发现结果发送到 Security Hub。

来自 GuardDuty 的新发现将在五分钟内发送到 Security Hub。对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 示例发现结果时，Security Hub 会收到样本发现结果并在查找结果类型[Sample]中省略前缀。例如，中的样本查找结果类型在 Security HubRecon:IAMUser/ResourcePermissions 中显示 GuardDuty [SAMPLE] Recon:IAMUser/ResourcePermissions为。

有关 GuardDuty 集成的更多信息，请参阅亚马逊 GuardDuty 用户指南中的[与 SAmazon ecurity Hub 集成](#)。

Amazon Health (发送调查结果)

Amazon Health让您可以持续了解您的资源性能以及Amazon服务和账户的可用性。您可以使用Amazon Health事件来了解服务和资源更改会如何影响运行的应用程序Amazon。

与的集成Amazon Health不使用BatchImportFindings。相反，Amazon Health使用 service-to-service 事件消息将结果发送到 Security Hub。

有关整合的更多信息，请参阅以下部分：

Amazon Health 将结果发送到 Security Hub 的方式

在 Security Hub 中，安全问题按结果进行跟踪。一些发现结果来自其他 Amazon 服务或第三方合作伙伴检测到的问题。Security Hub 还有一套用于检测安全问题和生成结果的规则。

Security Hub 提供了管理来自所有这些来源的结果的工具。您可以查看和筛选结果列表，并查看结果的详细信息。请参阅 [在中查看查找结果列表和详细信息Amazon Security Hub \(p. 63\)](#)。您还可以跟踪结果的调查状态。请参阅 [对结果采取措施Amazon Security Hub \(p. 66\)](#)。

Security Hub 中的所有结果都使用标准的 JSON 格式，称为[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。ASFF 包括有关问题根源、受影响资源以及结果当前状态的详细信息。

Amazon Health是将结果发送到Amazon Security Hub。

Amazon Health发送到 Security Hub 的结果类型

启用集成后，将其生成的所有与安全相关的发现Amazon Health发送到 Security Hub。使用将发现结果发送到Security Hub[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。与安全相关的发现定义如下：

- 与Amazon安全服务相关的任何发现
- 在security TAmazon Health ypeCodecertificate 中找到任何带有abuse、或
- 发现Amazon Health服务在哪里risk或abuse

向 Security Hub 发送Amazon Health结果

当您选择接受来自的发现时Amazon Health，Security Hub 将自动分配从中接收调查结果所需的权限Amazon Health。Security Hub 使用 service-to-service 级别权限为您提供安全、简便的方法来启用此集成并EventBridge 代表您Amazon Health通过亚马逊导入调查结果。选择“接受调查结果”会授予 Security Hub 使用来自的结果的权限Amazon Health。

发送结果的延迟

Amazon Health创建新结果时，通常会在五分钟内将结果发送到 Security Hub。

Security Hub 不可用时重试

Amazon Health尽最大努力将结果发送到 Security Hub EventBridge。当事件未成功传送到 Security Hub 时，会在 24 小时内 EventBridge重试发送该事件。

更新 Security Hub 中的现有结果

将结果Amazon Health发送到 Security Hub 之后，它可以发送反映对查找活动的其他观测结果到 Security Hub 中。

存在调查结果的地区

对于全球事件，Amazon Health将调查结果发送到 us-east-1 (Amazon分区)、cn-northwest-1 (中国分区) 和 gov-us-west -1 (分区) 中的Security Hub。GovCloud Amazon Health将特定区域的事件发送到事件发生地相同的一个或多个区域中的 Security Hub。

查看Amazon Health结果

要在 Security Hub 中查看您的Amazon Health发现，请从导航面板中选择查找结果。要筛选发现结果以仅显示调查Amazon Health结果，请从“产品名称”字段中选择“Health”。

解释 SAmazon Health ecurity Hub 中的名称

Amazon Health使用 Security Hub 发送结果[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。Amazon Health与 Security Hub ASFF 格式相比，查找使用了不同的事件模式。下表详细列出了所有Amazon Health查找字段及其在 Security Hub 中出现的 ASFF 对应字段。

Health 结果类型	ASFF 结果类型	硬编码值
账户	AwsAccountId	
详情。startTime	CreatedAt	
detail.eventDescription.最新描述	描述	
详细信息。eventTypeCode	GeneratorId	
detail.eventarn (包括账户) + detail.startTime 的哈希	Id	
“arn: aws: securityHub:<region>:: product/aws/	ProductArn	
账户或 resourceId	资源 [i] .id	
	资源 [i] .Type	“其他”
	SchemaVersion	“2018-10-08”
	严重性.Label	请参阅下面的“解释严重性标签”
“Amazon Health-” 细节。eventTypeCode	Title	
-	类型	["软件和配置检查"]
event.time	UpdatedAt	
Health 控制台上事件的 URL	SourceUrl	

解析严重性标签

ASFF 调查结果中的严重性标签是使用以下逻辑确定的：

- 严重程度严重，如果：
 - Amazon Health调查结果中的service字段的值为Risk

- Amazon Health调查结果中的typeCode字段的值为AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
- Amazon Health调查结果中的typeCode字段的值为AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK
- Amazon Health调查结果中的typeCode字段的值为AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES

严重性为高，如果：

- Amazon Health调查结果中的service字段的值为Abuse
- Amazon Health调查结果中的typeCode字段包含该值SECURITY_NOTIFICATION
- Amazon Health调查结果中的typeCode字段包含该值ABUSE_DETECTION

严重程度为中等，如果：

- 调查结果中的service字段是以下任意字段：ACMARTIFACT、AUDITMANAGER、BACKUP、CLOUDENDURE、CLOUDHSM、CLOUDTRAILCLOUDWATCH、CODE或WAF
- Amazon Health调查结果中的 TypeCode 字段包含该值CERTIFICATE
- Amazon Health调查结果中的 TypeCode 字段包含该值END_OF_SUPPORT

来自 Amazon Health 的典型结果

Amazon Health使用结果发送到 Security Hub[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。以下是典型结果的示例Amazon Health。

Note

如果描述超过 1024 个字符，它将被截断为 1024 个字符，最后会说（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 Amazon Region US East (N. Virginia).\n\nYou can now use this MAIL FROM
domain with cmf.pinpoint.sysmon-iaadzel.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 Amazon 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": "Amazon"
    },
    "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

设置 Security Hub 时，会自动激活与Amazon Health Security Hub 的集成。Amazon Health立即开始将结果发送到 Security Hub。

停止向 Security Hub 发布结果

要停止向 Security Hub 发送结果，您可以使用 Security Hub 控制台、Security Hub API 或Amazon CLI。

请参阅[禁用和启用来自集成的结果流（控制台）](#) (p. 210)或[禁用来自集成的结果流（Security Hub API, Amazon CLI）](#) (p. 210)。

Amazon Identity and Access Management Access Analyzer (发送调查结果)

使用 IAM 访问分析器，所有发现结果都将发送到Security Hub。

IAM Access Analyzer 使用基于逻辑的推理来分析应用于您账户中支持资源的基于资源的策略。IAM Access Analyzer 在检测到允许外部委托人访问您账户中资源的策略语句时生成一个结果。

要了解更多信息，请参阅 IAM 用户指南中的[与Amazon security Hub 集成](#)。

Amazon Inspector (发送调查结果)

Amazon Inspector 是一项漏洞管理服务，可持续扫描您的Amazon工作负载是否存在漏洞。Amazon Inspector 会自动发现并扫描 Amazon EC2 实例和驻留在 Amazon Elastic Container 扫描结果会查找软件漏洞和意外网络暴露。

当您同时启用 Amazon Inspector 和 Security Hub 时，集成将自动启用。Amazon Inspector 开始将结果发送到 Security Hub。Amazon Inspector 将其生成的所有调查结果发送到Security Hub。

有关集成的更多信息，请参阅 Amazon InspAmazon ector 用户指南中的与Sec [urity Hub 集成](#)。

Security Hub 还可以接收来自亚马逊 Inspector Classic 的调查结果。Amazon Inspector Classic 将调查结果发送到 Security Hub，这些结果是通过对所有支持的规则包进行评估而生成的。

有关集成的更多信息，请参阅 Amazon Inspector Classic 用户指南中的与 Amazon Security Hub 集成。

Amazon Inspector 和 Amazon Inspector Classic 的 Amazon Inspector 的调查结果中有以下条目 ProductFields：

```
"aws/inspector/ProductVersion": "2",
```

Amazon Macie (发送调查结果)

来自 Macie 的结果可能表明存在潜在的政策违规行为，或者组织在 Amazon S3 中存储的数据中存在敏感数据 (PII)。

默认情况下，Mace 仅向 Security Hub 发送结果。您可以将集成配置为将敏感数据发现结果发送到 Security Hub。

在 Security Hub 中，策略或敏感数据查找结果的查找类型更改为与 ASFF 兼容的值。例如，Macie 中的 Policy: IAMUser/S3BucketPublic 查找结果类型在 “Security Hub” Effects/Data Exposure/ Policy: IAMUser-S3BucketPublic 中显示为。

Mace 还向 Security Hub 发送生成的示例发现结果。对于样本发现，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 Amazon Macie 与 Amazon Security Hub 的集成](#)。

Amazon Systems Manager 补丁管理器 (发送调查结果)

Amazon Systems Manager 当客户队列中的实例不符合其补丁合规性标准时，Patch Manager 会将发现结果发送到 Security Hub。

Patch Manager 可以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。

有关使用补丁管理器的更多信息，请参阅 Amazon Systems Manager 用户指南中的 [Amazon Systems Manager 补丁管理器](#)。

Amazon接收来自 Security Hub 的结果的服务

以下 Amazon 服务与 Security Hub 集成并接收来自 Security Hub 调查结果。如有说明，综合服务也可能更新调查结果。在这种情况下，查找您在集成服务中所做的更新也会反映在 Security Hub 中。

Amazon Audit Manager (接收调查结果)

Amazon Audit Manager 接收来自 Security Hub 的结果。这些发现可帮助 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《Aud [Amazonit Manager 用户指南](#)》。 [Amazon 支持的 Security Hub 检查 Amazon Audit Manager](#) 列出了 Security Hub 将调查结果发送给 Audit Manager 的控件。

Amazon Chatbot (接收调查结果)

Amazon Chatbot 是一个互动代理，可帮助您监控 Slack 频道和 Amazon Chime 聊天室中的 Amazon 资源并与之互动。

Amazon Chatbot 接收来自 Security Hub 的结果。

要了解有关与 Security Hub 集 Amazon Chatbot 成的更多信息，请参阅《Amazon Chatbot 管理员指南》中的 [Security Hub 集成概述](#)。

亚马逊Detective (接收调查结果)

Detective 会自动从您的Amazon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可视化并进行更快、更高效的安全调查。

Security Hub 与 Detective 的集成允许你从 Security Hub 中的亚马逊 GuardDuty 发现转向Detective。然后，您可以使用Detective 工具和可视化效果来调查它们。集成不需要在 Security Hub 或 Detective 中进行任何额外配置。

要 GuardDuty 查找类型，查找详细信息包括“在Detective 中调查”小节。该小节包含指向Detective 的链接。请参阅《亚马逊Detective 用户指南》中的“转到实体简介 GuardDuty 或从亚马逊或Amazon Security Hub 查找概述”。

如果启用了跨区域聚合，则当您从聚合区域进行透视时，Detective 会在发现结果产生的区域中打开 Detective。

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 Systems ManagerExplorer 和 OpsCenter (接收和更新调查结果)

Amazon Systems Manager浏览并从 Security Hub OpsCenter 接收调查结果，然后在 Security Hub 中更新这些发现。

Explorer 为您提供可自定义的仪表板，提供有关Amazon环境运行状况和性能的关键见解和分析。

OpsCenter 为您提供了查看、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《Amazon Systems Manager用户指南》中的[操作管理](#)。

Amazon Trusted Advisor (接收调查结果)

Trusted Advisor 凝聚了从为数十万 Amazon 客户提供服务中总结的最佳实践。Trusted Advisor 可检查您的 Amazon 环境，然后在有可能节省开支、提高系统可用性和性能或弥补安全漏洞时为您提供建议。

当您同时启用Trusted Advisor和 Security Hub 时，集成将自动更新。

Security Hub 将其“Amazon基础安全最佳实践”检查结果发送给Trusted Advisor。

有关 Security Hub 与集成的更多信息Trusted Advisor，请参阅《Support 用户指南》Amazon Trusted Advisor中的查看 SAmazon securitAmazon y [Hub 控件](#)。

可用的第三方合作伙伴产品集成

AmazonSecurity Hub 已与以下第三方产品集成。对于每个提供商，该列表显示了集成与发现结果的交互方式。集成可以执行以下操作：

- 将其生成的发现发送到Security Hub。
- 接收来自 Security Hub 的结果。
- 更新 Security Hub 中的检查结果。从 Security Hub 接收发现结果的集成也可能会更新这些发现。

所有将结果发送到 Security Hub 的集成，都有一个Amazon 资源名称 (ARN)。

Note

某些集成并非在所有区域都可用。

如果不支持集成，则不在集成Security Hub 控制台的页面。

另请参阅 [the section called “中国（北京）和中国（宁夏）支持的集成” \(p. 517\)](#) 和 [the section called “Amazon GovCloud（美国东部）和Amazon GovCloud（美国西部）中支持的集成” \(p. 517\)](#)。

如果您有安全解决方案并且有兴趣成为 Security Hub 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 [Amazon Security Hub 合作伙伴集成指南](#)。

第三方与 Security Hub 集成的概述

以下是将发现结果发送到 Security Hub 或从 Security Hub 接收发现结果的第三方集成的概述。

集成	Direction	ARN (如果适用)
3CORESec – 3CORESec NTA	发送结果	arn:aws:securityhub:<REGION>::product/3coresec-nta
Alert Logic – SIEMless Threat Management	发送结果	arn:aws:securityhub:<REGION>::product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	发送结果	arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	发送结果	arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench
Armor – Armor Anywhere	发送结果	arn:aws:securityhub:<REGION>::product/armordefense/armoranywhere
AttackIQ – AttackIQ	发送结果	arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	发送结果结果结果	arn:aws:securityhub:<REGION>::product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	发送结果	arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon for Amazon	发送结果	arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws
Capitis Solutions – C2VS	发送结果	arn:aws:securityhub:<REGION>::product/capitis/c2vs
Check Point – CloudGuard IaaS	发送结果	arn:aws:securityhub:<REGION>::product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	发送结果	arn:aws:securityhub:<REGION>::product/checkpoint/dome9-arc
Cloud Storage Security–Antivirus forAmazon S3	发送结果	arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3

集成	Direction	ARN (如果适用)
CrowdStrike – CrowdStrike Falcon	发送结果	arn:aws:securityhub:<REGION>::product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	发送结果	arn:aws:securityhub:<REGION>::product/cyberark/cyberark-pta
Data Theorem – Data Theorem	发送结果	arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure
Forcepoint – Forcepoint CASB	发送结果	arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	发送结果	arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	发送结果	arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	发送结果	arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-ngfw
Fugue – Fugue	发送结果	arn:aws:securityhub:<REGION>::product/fugue/fugue
Guardicore – Centra 4.0	发送结果	arn:aws:securityhub:<REGION>::product/guardicore/guardicore
Guardicore – Infection Monkey	发送结果	arn:aws:securityhub:<REGION>::product/guardicore/aws-infection-monkey
HackerOne – Vulnerability Intelligence	发送结果	arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	发送结果	arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	发送结果	arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	发送结果	arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer
Lacework – Lacework	发送结果	arn:aws:securityhub:<REGION>::product/lacework/lacework

集成	Direction	ARN (如果适用)
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	发送结果	arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	发送结果	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Palo Alto Networks – Prisma Cloud Compute	发送结果	arn:aws:securityhub:<REGION>::product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	发送结果	arn:aws:securityhub:<REGION>::product/paloaltonetworks/redlock
Prowler – Prowler	发送结果	arn:aws:securityhub:<REGION>::product/prowler/prowler
Qualys – Vulnerability Management	发送结果	arn:aws:securityhub:<REGION>::product/qualys/qualys-vm
Rapid7 – InsightVM	发送结果	arn:aws:securityhub:<REGION>::product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	发送结果	arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb
SentinelOne – SentinelOne	发送结果	arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection
Sonrai Security – Sonrai Dig	发送结果	arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig
Sophos – Server Protection	发送结果	arn:aws:securityhub:<REGION>::product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	发送结果	arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	发送结果	arn:aws:securityhub:<REGION>::product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	发送结果	arn:aws:securityhub:<REGION>::product/symantec-corp/symantec-cwp
Sysdig – Sysdig Secure for cloud	发送结果	arn:aws:securityhub:<REGION>::product/sysdig/sysdig-secure-for-cloud

集成	Direction	ARN (如果适用)
Tenable – Tenable.io	发送结果	arn:aws:securityhub:<REGION>::product/tenable/tenable-io
Vectra Detect	发送结果	arn:aws:securityhub:<REGION>::product/vectra-ai/cognito-detect
Atlassian - Jira Service Management	接收和更新调查结果	不适用
Atlassian – Opsgenie	对结果	不适用
FireEye – FireEye Helix	对结果	不适用
Fortinet – FortiCNP	对结果	不适用
Helecloud – Managed Security	对结果	不适用
IBM – QRadar	对结果	不适用
Logz.io Cloud SIEM	对结果	不适用
MicroFocus – MicroFocus Arcsight	对结果	不适用
PagerDuty – PagerDuty	对结果	不适用
Palo Alto Networks – Cortex XSOAR	对结果	不适用
Palo Alto Networks – VM-Series	对结果	不适用
Rackspace Technology – Cloud Native Security	对结果	不适用
Rapid7 – InsightConnect	对结果	不适用
RSA – RSA Archer	对结果	不适用
ServiceNow – ITSM	接收和更新调查结果	不适用
Slack – Slack	接收结果	不适用
Splunk – Splunk Enterprise	接收结果	不适用
Splunk – Splunk Phantom	接收结果	不适用
ThreatModeler	接收结果	不适用
Caveonix – Caveonix Cloud	发送和接收调查结果	arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	发送和接收调查结果	arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian
cloudtamer.io – cloudtamer.io	发送和接收调查结果	arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio

集成	Direction	ARN (如果适用)
DisruptOps, Inc. – DisruptOPS	发送和接收调查结果	arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops
Turbot – Turbot	发送和接收调查结果	arn:aws:securityhub:<REGION>::product/turbot/turbot

将结果发送到 Security Hub 的第三方集成

以下第三方合作伙伴产品集成将结果发送到 Security Hub。Security Hub 将发现结果转化为[Amazon安全调查格式 \(p. 69\)](#)。

3CORESec – 3CORESec NTA

集成类型：发送

产品代码产品ARN ub arn:aws:securityhub:<REGION>::product/3coresec/3coresec

3CORESec为本地和本地提供托管检测服务Amazon系统。它们与 Security Hub 的集成允许查看恶意软件、权限升级、横向移动和不正确的网络分段等威胁。

[产品链接](#)

[合作伙伴文档](#)

Alert Logic – SIEMless Threat Management

集成类型：发送

产品代码产品ARN ub arn:aws:securityhub:<REGION>::product/alertlogic/althreatmanagement

获得适当的覆盖范围：漏洞和资产可见性、威胁检测和事件管理，Amazon WAF，并分配了 SOC 分析师选项。

[产品链接](#)

[合作伙伴文档](#)

Aqua Security – Aqua Cloud Native Security Platform

集成类型：发送

产品代码产品ARN ub 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 CI/CD 管道到运行时生产环境）提供完整的生命周期安全。

[产品链接](#)

[合作伙伴文档](#)

Aqua Security – Kube-bench

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`
Kube-bench是一个开源工具，可针对您的环境运行 Center for Internet Security (Center) Kubernetes 基准。

[产品链接](#)

[合作伙伴文档](#)

Armor – Armor Anywhere

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/armordefense/armoranywhere`

Armor Anywhere提供托管的安全性和合规性Amazon.

[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模拟符合 MITRE ATT&CK 框架的真实对抗行为，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>::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移至公共云时保持安全。

[AmazonMarketplace I](#)

[产品链接](#)

BigID – BigID Enterprise

集成类型：发送

产品ARN：`arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

这些区域有：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](#)

Blue Hexagon – Blue Hexagon forAmazon

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的威胁，包括恶意软件和网络异常。

[产品链接](#)

[合作伙伴文档](#)

Capitis Solutions – C2VS

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/capitis/c2vs

C2VS是一种可定制的合规性解决方案，旨在自动识别您的应用程序特定的错误配置及其根本原因。

[产品链接](#)

[合作伙伴文档](#)

Check Point – CloudGuard IaaS

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/checkpoint/cloudguard-iaas

Check Point CloudGuard可以轻松地将全面的威胁防御安全扩展到Amazon同时保护云端资产。

[产品链接](#)

[合作伙伴文档](#)

Check Point – CloudGuard Posture Management

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/checkpoint/dome9-arc

一个 SaaS 平台，可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](#)

Cloud Storage Security–Antivirus forAmazon 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 对象提供云原生反恶意软件和防病毒扫描。

Antivirus for Amazon S3 提供对 Amazon S3 中的对象和文件的实时和定时扫描，以查找恶意软件和威胁。它为问题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](#)

CrowdStrike – CrowdStrike Falcon

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/crowdstrike/crowdstrike-falcon

这些区域有：CrowdStrike Falcon单一轻量级传感器将下一代防病毒、端点检测和响应以及全天候管理的云端搜寻功能统一起来。

[产品链接](#)

[合作伙伴文档](#)

CyberArk – Privileged Threat Analytics

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/cyberark/cyberark-pta

Privileged Threat Analytics收集、检测、提醒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](#)

Data Theorem – Data Theorem

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，以寻找安全漏洞和数据隐私漏洞，以防止 AppSec 数据泄露。

[产品链接](#)

[合作伙伴文档](#)

Forcepoint – Forcepoint CASB

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::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 – Forcepoint Cloud Security Gateway

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway

Forcepoint Cloud Security Gateway是一项聚合云安全服务，无论用户和数据位于何处，均可为其提供可见性、控制和威胁防护。

[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>::product/forcepoint/forcepoint-dlp

Forcepoint DLP无论您的员工在哪里工作，无论数据位于何处，都能通过可见性和控制来解决以人为本的风险。

[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>::product/forcepoint/forcepoint-ngfw

Forcepoint NGFW让你连接你的Amazon环境融入企业网络，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](#)

Fugue – Fugue

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，可自动进行持续验证 infrastructure-as-code 和使用相同策略的云运行时环境。

[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、微分段和漏洞检测。

[产品链接](#)

[合作伙伴文档](#)

Guardicore – Infection Monkey

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/guardicore/aws-infection-monkey

Infection Monkey是一种攻击模拟工具，旨在测试网络免受攻击者的攻击。

[产品链接](#)

[合作伙伴文档](#)

HackerOne – Vulnerability Intelligence

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence

这些区域有：HackerOne平台与全球黑客社区合作，发现最相关的安全问题。Vulnerability Intelligence使您的组织能够超越自动扫描的范围。它共享的漏洞有HackerOne道德黑客已经验证并提供了复制步骤。

[产品链接](#)

[合作伙伴文档](#)

JFrog – Xray

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray

JFrog Xray是一种通用的应用程序安全软件组合分析 (SCA) 工具，它持续扫描二进制文件中是否存在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。

[AmazonMarketplace |](#)

[合作伙伴文档](#)

Juniper Networks – vSRX Next Generation Firewall

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall

Juniper Networks vSRX 虚拟下一代防火墙提供基于云的完整虚拟防火墙，具有高级安全性、安全 SD-WAN、强大的网络和内置自动化功能。

[AmazonMarketplace |](#)

[合作伙伴文档](#)

[产品链接](#)

k9 Security – Access Analyzer

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer

k9 Security在您的访问权限发生重要更改时通知您Amazon Identity and Access Management账户。与k9 Security，你可以理解每个 IAM 用户和角色对关键角色的访问权限Amazon服务和您的数据。

k9 Security专为持续交付而构建，允许您通过可操作的访问审核和简单的策略自动化来实现 IAMAmazon CDK和 Terraform。

[产品链接](#)

[合作伙伴文档](#)

Lacework – Lacework

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 可大规模自动执行云安全，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 Cloud Native Application Protection Platform (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)为您提供云安全状态管理 (CSPM) 和云工作负载保护平台 (CWPP)Amazon环境。

[产品链接](#)

[合作伙伴文档](#)

NETSCOUT – NETSCOUT Cyber Investigator

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](#)

Palo Alto Networks – Prisma Cloud Compute

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/twistlock/twistlock-enterprise

Prisma Cloud Compute是一个云原生网络安全平台，用于保护虚拟机、容器和无服务器平台。

[产品链接](#)

[合作伙伴文档](#)

Palo Alto Networks – Prisma Cloud Enterprise

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/paloaltonetworks/redlock

通过云安全分析、高级威胁检测和合规性监控保护您的 Amazon 部署。

[产品链接](#)

[合作伙伴文档](#)

Prowler – Prowler

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::product/prowler/prowler

Prowler是一个可以执行的开源安全工具Amazon与安全最佳实践、强化和持续监控相关的检查。

[产品链接](#)

[合作伙伴文档](#)

Qualys – Vulnerability Management

集成类型：发送

产品ARN：arn:aws:securityhub:<REGION>::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

产品代码产品ARN ub arn:aws:securityhub:<REGION>::product/rapid7/insightvm

Rapid7 InsightVM 为现代环境提供漏洞管理，使您能够高效地发现漏洞、确定漏洞的优先级和修复漏洞。

[产品链接](#)

[合作伙伴文档](#)

SecureCloudDB – SecureCloudDB

集成类型：发送

产品代码产品ARN ub arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb

SecureCloudDB是一款云原生数据库安全工具，可全面了解内部和外部安全态势和活动。它会标记安全违规行为，并对可利用的数据库漏洞提供补救措施。

[产品链接](#)

[合作伙伴文档](#)

SentinelOne – SentinelOne

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne是一个自主的扩展检测和响应 (XDR) 平台，涵盖基于人工智能的跨端点、容器、云工作负载和 IoT 设备的预防、检测、响应和搜寻。

[AmazonMarketplace I](#)

[合作伙伴文档](#)

[产品链接](#)

Sonrai Security – Sonrai Dig

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig监控和修复云配置错误和策略违规行为，因此您可以改善安全与合规状况。

[产品链接](#)

[合作伙伴文档](#)

Sophos – Server Protection

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/sophos/sophos-server-protection`

Sophos Server Protection使用全面的保护组织核心的关键应用程序和数据 defense-in-depth 方法。

[产品链接](#)

[合作伙伴文档](#)

StackRox – StackRox Kubernetes Security

集成类型：发送

产品代码产品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

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/sumologicinc/sumologic-mda`

Sumo Logic是一个安全的机器数据分析平台，它使开发和安全运营团队能够构建、运行和保护他们的 Amazon 应用程序

[产品链接](#)

[合作伙伴文档](#)

Symantec – Cloud Workload Protection

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::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 实例提供全面保护。

[产品链接](#)

[合作伙伴文档](#)

Sysdig – Sysdig Secure for cloud

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/sysdig/sysdig-secure-for-cloud`

Sysdig Secure for cloud支持资产发现、风险管理、云安全状态管理 (CSPM)、合规性、Amazon Elastic Container Registry (ECR) 和 Fargate 的自动漏洞扫描，以及基于 CloudTrail。您可以将所有这些部署为单个安全平台。

[产品链接](#)

[合作伙伴文档](#)

Tenable – Tenable.io

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/tenable/tenable-io`

准确识别、调查漏洞并确定其优先级。在云中管理。

[产品链接](#)

[合作伙伴文档](#)

Vectra Detect

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/vectra-ai/cognito-detect`

Vectra正在通过应用先进的人工智能在隐藏的网络攻击者窃取或造成损害之前对其进行检测和响应，从而改变网络安全。

[AmazonMarketplace |](#)

[合作伙伴文档](#)

接收来自 Security Hub 结果的第三方集成

以下第三方合作伙伴产品集成接收来自 Security Hub 的调查结果。如有说明，这些产品还可能更新调查结果。在这种情况下，查找您在合作伙伴产品中所做的更新也会反映在 Security Hub 中。

Atlassian-Jira Service Management (接收和更新调查结果)

集成类型：接收和更新

这些区域有：Amazon的服务管理连接器Jira将来自 Security Hub 的结果Jira.Jira问题是根据调查结果产生的。当Jira问题已更新，相应的发现已在 Security Hub 中更新。

该集成仅支持 Jira 服务器和 Jira 数据中心。

[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对服务中断进行规划，并在事故发生时保持控制。

与 Security Hub 集成可确保将与安全相关的关键任务事件转发给相应的团队，以便立即解决。

[产品链接](#)

[合作伙伴文档](#)

FireEye – FireEye Helix

集成类型：接收

FireEye Helix是一个云托管的安全运营平台，允许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](#)

Fortinet – FortiCNP

集成类型：接收

FortiCNP是一款 Cloud Native Protection 产品，它将安全发现汇总为可操作的见解，并根据风险评分对安全洞察进行优先排序，以减少警报疲劳并加速修复。

[AmazonMarketplace |](#)

[合作伙伴文档](#)

Helecloud – Managed Security

集成类型：接收

HeleCloud是一家Managed Services 提供商，负责照顾您的Amazon基础架构，这样您就可以专注于核心业务。

[产品链接](#)

IBM – QRadar

集成类型：接收

IBM QRadarSIEM 使安全团队能够快速、准确地检测、确定威胁的优先级、调查和应对威胁。

[产品链接](#)

[合作伙伴文档](#)

Logz.io Cloud SIEM

集成类型：接收

Logz.io是提供Cloud SIEM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、分析和响应安全威胁。

[产品链接](#)

[合作伙伴文档](#)

MicroFocus – MicroFocus Arcsight

集成类型：接收

ArcSight加速有效的威胁检测和实时响应，将事件关联以及监督和非监督分析与响应自动化和协调相集成。

[产品链接](#)

[合作伙伴文档](#)

PagerDuty – PagerDuty

集成类型：接收

这些区域有：PagerDuty数字运营管理平台通过自动将任何信号转化为正确的见解和行动，使团队能够主动缓解影响客户的问题。

Amazon用户可以使用PagerDuty套装Amazon整合以扩大他们的规模Amazon以及充满信心的混合环境。

当与 Security Hub 聚合和组织安全警报相结合时，PagerDuty允许团队自动执行威胁响应流程，并快速设置自定义操作以防止潜在问题。

PagerDuty正在执行云迁移项目的用户可以快速移动，同时减少在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是一个安全编排、自动化和响应 (SOAR) 平台，可与您的整个安全产品堆栈集成，以加速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 集成可收集威胁情报并将其发送到VM-Series下一代防火墙作为自动安全策略更新，可阻止恶意 IP 地址活动。

[产品链接](#)

[合作伙伴文档](#)

Rackspace Technology – Cloud Native Security

集成类型：接收

Rackspace Technology 在本机基础上提供托管安全服务Amazon用于全天候监控的安全产品 RackspaceSOC、高级分析和威胁补救。

[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，使您的团队能够在几乎不使用代码的情况下优化 SOC 操作。

[产品链接](#)

[合作伙伴文档](#)

RSA – RSA Archer

集成类型：接收

RSA ArcherIT 和安全风险管理允许您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 (接收和更新调查结果)

集成类型：接收和更新

这些区域有：ServiceNow与 Security Hub 集成允许在其中查看来自Security Hub 调查结果ServiceNow ITSM. 还可以配置ServiceNow在收到 Security Hub 的调查结果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 中的发现更新。

[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个层，它将人员、数据和应用程序汇集在一起。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 CloudWatch Security Hub 结果的使用者。将您的数据发送到Splunk用于高级安全分析和 SIEM。

[产品链接](#)

[合作伙伴文档](#)

Splunk – Splunk Phantom

集成类型：接收

使用Splunk Phantom对结果进行存位AmazonSecurity Hub，调查结果将发送至Phantom使用其他威胁情报信息自动丰富上下文或执行自动响应操作。

[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，用于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](#)

向 Security Hub 发送调查结果和从安全中心接收发现结果的第三方集成

以下第三方合作伙伴产品集成将调查结果发送到 Security Hub 并从 Security Hub 接收调查结果。

Caveonix – Caveonix Cloud

集成类型：发送和接收

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix Cloud是一个 SaaS 风险缓解平台，可提供自动合规性和混合云安全态势管理，以提供全面的工作负载保护。

[产品链接](#)

[合作伙伴文档](#)

Cloud Custodian – Cloud Custodian

集成类型：发送和接收

产品代码产品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，从而实现安全且成本优化的管理良好的云基础架构。

[产品链接](#)

[合作伙伴文档](#)

Cloud Storage Security–Antivirus forAmazon S3 (发送调查结果)

集成类型：发送

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security为 Amazon S3 对象提供云原生反恶意软件和防病毒扫描。

Antivirus for Amazon S3 提供对 Amazon S3 中的对象和文件的实时和定时扫描，以查找恶意软件和威胁。它为问题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](#)

Kion (发送和接收调查结果)

集成类型：发送和接收

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion (以前是 cloudtamer.io) 是一款完整的云治理解决方案Amazon.Kion让利益相关者了解云运营，帮助云用户管理账户、控制预算和成本，并确保持续合规。

[产品链接](#)

[合作伙伴文档](#)

DisruptOps, Inc. – DisruptOPS

集成类型：发送和接收

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

这些区域有：DisruptOpsSecurity Operations Platform 通过使用自动护栏帮助组织在云中维护最佳安全实践。

[产品链接](#)

[合作伙伴文档](#)

Turbot – Turbot

集成类型：发送和接收

产品代码产品ARN `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot确保您的云基础设施安全、合规、可扩展和成本优化。

[产品链接](#)

[合作伙伴文档](#)

使用自定义产品集成将结果发送到AmazonSecurity Hub

除了由综合产生的调查结果Amazon服务和第三方产品，Security Hub 还可以使用由您可能使用的其他自定义安全产品生成的结果。

您可 Security Hub 用[BatchImportFindings](#)API 操作。

设置自定义集成时，请使用[指南和清单](#)在中提供Security Hub 合作伙伴集成指南。

从自定义安全产品发送结果的要求和建议

在成功调用[BatchImportFindings](#)启用 API 操作，您必须启用 Security Hub。

您必须使用 [the section called “结果格式” \(p. 68\)](#) 提供结果详细信息。对于来自自定义集成的结果，请使用以下要求和建议。

设置产品 ARN

启用 Security Hub 时，会在当前账户中生成一个默认的产品 Amazon 资源名称 (ARN)。

此产品 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`。

使用此产品 ARN 作为[ProductArn](#)调用时的属性BatchImportFindingsAPI 操作。

定义公司和产品名称

您可以使用BatchImportFindings为向 Security Hub 发送调查结果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 控制台和每个查找结果的 JSON 中。请参阅 [使用 BatchImportFindings 创建和更新结果 \(p. 57\)](#)。

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。

每个新结果必须具有唯一的 `ResultId`。

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。

从发送结果 Chef InSpec 扫描到 Security Hub

您可以创建 Amazon CloudFormation 运行 `Chef InSpec` 合规性扫描，然后将结果发送到 Security Hub。

有关更多详细信息，请参阅 [使用持续监控合规 Chef InSpec 和 Amazon Security Hub](#)。

发送检测到的容器漏洞 Trivy 到 Security Hub

您可以创建 Amazon CloudFormation 使用的模板 `AquaSecurity Trivy` 扫描容器中的漏洞，然后将这些漏洞发现发送到 Security Hub。

有关更多详细信息，请参阅 [如何使用构建用于容器漏洞扫描的 CI/CD 管道 Trivy 和 Amazon Security Hub](#)。

中的安全标准和控制AmazonSecurity Hub

AmazonSecurity Hub 使用、汇总和分析来自各种支持的各个安全结果Amazon和第三方产品。

Security Hub 还会生成自己的结果，针对一组支持的安全标准中的规则运行的自动连续检查，以生成自己的结果 这些规则决定了标准内的控制是否得到遵守。这些检查提供了就绪分数，并指定了需要引起注意的特定账户和资源。

Security Hub 提供以下标准的控制。

- [CISAmazonFunations \(p. 263\)](#)
- [支付卡行业数据安全标准 \(PCI DSS\) \(p. 310\)](#)
- [Amazon 基础安全最佳实践 \(p. 361\)](#)

有关进行安全检查的 Security Hub 定价的信息，请参阅[Security Hub 定价](#)。

主题

- [的工作原理Amazon Security Hub运行并使用安全检查 \(p. 243\)](#)
- [查看和管理安全标准 \(p. 251\)](#)
- [查看和管理控件 \(p. 257\)](#)
- [中的中可用安全标准Amazon Security Hub \(p. 263\)](#)

的工作原理Amazon Security Hub运行并使用安全检查

对于每个启用的控件，Amazon Security Hub运行 vacum 检查。安全检查可确定您的资源是否符合控制要求。

有些检查定期运行。其他检查仅在资源状态发生变化时运行。请参阅 [the section called “有关运行安全检查的计划” \(p. 244\)](#)。

许多安全检查使用Amazon Config管理或自定义规则，以建立合规性要求。要进行这些检查，你必须 Amazon Config已启用。请参阅 [the section called “Security Hub 如何使用Amazon Config运行安全检查的规则” \(p. 244\)](#)。其他人则使用自定义 Lambda 函数，这些函数由Security Hub 管理，客户看不到这些函数。

对于每项检查，Security Hub 都会创建或更新调查结果。请参阅 [the section called “生成和更新控制结果” \(p. 245\)](#)。

Security Hub 使用调查结果来评估每项控制措施和整个标准的安全状况。请参阅[the section called “确定控制状态” \(p. 250\)](#)和[the section called “确定标准安全分数” \(p. 251\)](#)。

主题

- [Security Hub 如何使用Amazon Config运行安全检查的规则 \(p. 244\)](#)
- [有关运行安全检查的计划 \(p. 244\)](#)
- [生成和更新控制结果 \(p. 245\)](#)
- [从结果中确定控制的总体状态 \(p. 250\)](#)
- [确定安全标准的安全分数 \(p. 251\)](#)

Security Hub 如何使用Amazon Config运行安全规则的规则

要对环境的资源运行安全检查，Amazon Security Hub使用标准指定的步骤，或使用特定Amazon Config规则。有些规则是托管规则，由Amazon Config. 其他规则是 Security Hub 开发的自定义规则。

Amazon ConfigSecurity Hub 用于控制的规则称为服务相关规则，因为它们是由Security Hub 服务启用和控制的。

启用对这些的检查Amazon Config规则，每个启用了 Security Hub 的账户都必须先启用Amazon Config，并启用所有资源的资源记录。请参阅 [the section called “启用 Amazon Config” \(p. 7\)](#)。

Security Hub 如何生成服务相关规则

对于每个使用Amazon Config服务相关规则，Security Hub 在您的Amazon环境。

这些服务相关规则特定于 Security Hub。即使已存在相同规则的其他实例，它也会创建这些服务相关规则。服务关联规则添加了securityhub在原始规则名称之前，以及规则名称后面的唯一标识符。例如，对于原来的Amazon Config托管规则vpc-flow-logs-enabled，则服务关联规则名称将类似于securityhub-vpc-flow-logs-enabled-12345。

Amazon ConfigHas[托管规则数量的配额](#)每区域每账户。服务相关的Amazon ConfigSecurity Hub 创建的规则不计入该配额。即使您已达到Amazon Config账户中托管规则的限制。对于服务相关规则，每区域每账户的配额为 250 个规则。这是对Amazon Config托管规则的配额。

查看有关Amazon Config控制规则

对于使用的控件Amazon Config托管规则，控制说明中包含指向Amazon Config关联的规则详细信息Amazon Config规则。请参阅[CISAmazon 基金会基准控制 \(p. 264\)](#)、[the section called “PCI DSS 控制” \(p. 311\)](#)和[the section called “所需的 Amazon Config 资源” \(p. 361\)](#)。自定义规则未与控件描述链接。

对于从这些控件生成的查找结果，查找结果详细信息包括指向关联的Amazon Config规则。请注意，要导航到Amazon Config规则以查找详细信息，您还必须在选定账户中具有 IAM 权限才能导航到Amazon Config。

发现的详细信息在结果页. 见解页. 集成页面包含一个Rule链接到Amazon Config规则详细信息。请参阅 [the section called “查看结果详细信息 \(控制台\)” \(p. 65\)](#)。

在控件详细信息页面上，调查查找结果列表的列包含指向Amazon Config规则详细信息。请参阅 [the section called “查看Amazon Config结果资源的规则” \(p. 262\)](#)。

有关运行安全计划的计划

在启用安全标准后，Amazon Security Hub在两小时内开始运行所有检查。大多数检查在 25 分钟内开始运行。在控制完成第一次检查前，其状态为没有数据。

在初始检查后，每个控制的计划可能是定期的，也可能是触发更改的。

- 在最近一次运行后的 12 小时内，将自动运行定期检查。您无法更改周期。
- 在关联的资源更改状态时，将运行更改触发的检查。即使资源没有更改状态，更改触发的检查的更新时间也将每 18 小时刷新一次。这有助于指明控件仍处于启用状态。

通常，Security Hub 尽可能使用更改触发的规则。要使资源使用更改触发的规则，必须支持Amazon Config配置项目。

对于基于托管的控件Amazon Config规则，控制描述包含指向中的规则描述的链接。Amazon Config开发人员指南. 该描述包括规则是由更改触发的还是定期的。

使用 Security Hub 自定义 Lambda 函数的检查始终是定期的。

生成和更新控制结果

Amazon Security Hub通过对安全控制中的规则运行检查来生成调查结果。这些结果使用 Amazon Security Finding 格式 (ASFF)。请注意，如果查找结果大小超过最大值 240 KB，则Resource.Details对象被移除。对于使用以下方法的控件的调查结果Amazon Config规则，您可以在上查看资源详情Amazon Config控制台。

Security Hub 通常对控制的每项安全检查收费。但是，如果多个控件使用相同的控件Amazon Config规则，那么 Security Hub 对每张支票只收取一次费用Amazon Config规则。它根据检查结果为每个对照生成单独的调查结果。

例如，Amazon Config规则iam-password-policy由互联网安全中心 (CIS) 的多个控件使用Amazon基金会基准测试和 IAM.7 在Amazon基础安全最佳实践 (FSBP) 标准。每次 Security Hub 都会对此进行检查Amazon Config规则，它将为每个相关控件生成单独的调查结果，但只对支票收取一次费用。

Compliance控制结果的详细信息

对于通过控制措施安全检查得出的结果，[Compliance \(p. 120\)](#)字段中返回的子位置类型AmazonSecy Fity F) 包含与控制相关的结果的详细信息。[Compliance \(p. 120\)](#) 字段包含以下信息。

RelatedRequirements

控件的相关要求列表。这些要求来自第三方控制安全框架，例如支付卡行业数据安全标准。

Status

Security Hub 针对给定控件运行的最新检查结果。之前检查的结果将保持存档状态 90 天。

StatusReasons

包含值的原因列表Compliance.Status. 对于每个原因，StatusReasons 包括原因代码和说明。

下表列出了可用的状态原因代码和描述。原因代码的补救步骤取决于哪个控件使用原因代码生成了调查结果。您可以在以下网址查看 FSBP 控制的补救措施[the section called "Amazon 基础安全最佳实践控件" \(p. 362\)](#).

原因代码	Compliance.Status	描述
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	多区域不存在指标筛选条件 CloudTrail 跟踪。
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	该账户没有多区域 CloudTrail 使用所需的配置进行跟踪。
CLOUDTRAIL_REGION_INVALID	WARNING	多区域 CloudTrail 跟踪不在当前区域中返回的子位置类型。
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。
CONFIG_ACCESS_DENIED	NOT_AVAILABLE	Amazon Config 拒绝访问
	Amazon Config 状态为 ConfigError	验证 Amazon Config 是否已启用并已授予足够的权限。

原因代码	Compliance.Status	描述
CONFIG_EVALUATIONS_EMPTY	PASSED	Amazon Config根据规则评估了您的资源。 规则不适用于其范围内的 Amazon 资源，指定的资源已删除，或者评估规则已删除。
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	合规状态为NOT_AVAILABLE因为 Amazon Config返回的状态为不适用。 Amazon Config没有提供该状态的原因。以下是一些可能的原因不适用状态： - 该资源已从作用域中移除Amazon Config规则。 - 这些区域有：Amazon Config规则已删除。 - 资源已删除。 - 这些区域有：Amazon Config规则逻辑可以产生不适用状态。
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE Amazon Config 状态为 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。 错误的类型可能是以下值之一： - 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 Amazon 订阅。 - 评估时出现一般超时。 - 账户暂停。
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE Amazon Config 状态为 ConfigError	这些区域有：Amazon Config规则正在创建过程中。
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	出现未知错误。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	NOT_AVAILABLE	Security Hub 无法对自定义 Lambda 运行时执行检查。

原因代码	Compliance.Status	描述
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	该结果在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	这些区域有：CloudWatch 日志指标筛选条件没有有效的 Amazon SNS 订阅。
SNS_TOPIC_CROSS_ACCOUNT	WARNING	该结果在WARNING状态。 与此规则关联的 SS 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sns:ListSubscriptionsByTopic主题的权限。
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	该结果在WARNING状态是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

这些区域有：ProductFieldsASFF 中的属性包括有关控制安全检查生成的发现的其他详细信息。

对于安全检查生成的调查结果，ProductFields包含以下字段：

StandardsGuideArn 或者 StandardsArn

与控件关联的标准 ARN。

对于独联体来说Amazon基金会基准标准，该领域是StandardsGuideArn.

适用于 PCI DS 和Amazon基础安全最佳实践标准，该字段是StandardsArn.

StandardsGuideSubscriptionArn 或者 StandardsSubscriptionArn

该账户订阅标准的 ARN。

对于独联体来说Amazon基金会基准标准，该领域是StandardsGuideSubscriptionArn.

对于 PCI DSS 和Amazon基础安全最佳实践标准，该字段是StandardsSubscriptionArn.

RuleId 或者 ControlId

控件的标识符。

对于独联体来说Amazon基金会基准标准，该领域是RuleId.

对于 PCI DSS 和Amazon基础安全最佳实践标准，该字段是ControlId.
RecommendationUrl

控件修复信息的 URL。

RelatedAWSResources:0/name

与结果关联的资源名称。

RelatedAWSResource:0/type

与控件关联的资源类型。

StandardsControlArn

控件的 ARN。

aws/securityhub/ProductName

对于基于控制的发现，产品名称为 Security Hub。

aws/securityhub/CompanyName

对于基于控制的调查结果，公司名称为Amazon.

aws/securityhub/annotation

对控件发现的问题的描述。

aws/securityhub/FindingId

调查结果的标识符。

为控制结果分配严重性

分配给 Security Hub 控件的严重性确定了该控件的重要性。对照的严重性决定了分配给控制结果的严重性标签。

严重性标准

对照的严重程度是根据对以下标准的评估来确定的：

- 威胁参与者利用与控制相关的配置缺陷有多困难？

难度取决于利用弱点实施威胁情景所需的复杂程度或复杂程度。

- 这种弱点会导致你的妥协的可能性有多大Amazon账户还是资源？

你的妥协Amazon账户或资源意味着您的数据的机密性、完整性或可用性，或Amazon基础设施在某种程度上受到了破坏。

入侵的可能性表明威胁情景导致您的中断或违规的可能性有多大Amazon服务或资源。

例如，考虑以下配置缺陷：

- IAM 用户访问密钥不会每 90 天轮换一次。
- IAM 根访问密钥存在。

这两个弱点同样难以被对手利用。在这两种情况下，对手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，如果威胁参与者获得根用户访问密钥，则入侵的可能性要高得多，因为根密钥为他们提供了更大的访问权限。因此，root 用户密钥漏洞的严重性更高。

严重性没有考虑到底层资源的重要程度。重要性是与调查结果相关的资源的重要级别。例如，与关键任务应用程序关联的资源比与非生产测试相关的资源更为重要。要捕获资源重要性信息，请使用Criticality的子位置类型AmazonSecy Fy F)。

下表列出了漏洞利用的难度和安全标签被泄露的可能性。

	极有可能妥协	可能妥协	不太可能妥协	妥协的可能性极小
很容易被利用	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，以避免其升级。

例如，开放的 S3 存储桶被视为具有“严重”严重性的结果。由于有太多参与者扫描打开的 S3 存储桶，暴露的 S3 存储桶中的数据很可能会被其他人发现和访问。

通常，可公开访问的资源被视为关键安全问题。你应该以最紧迫的态度对待关键发现。您还应该考虑资源的重要性。

高 — 必须将该问题作为近期优先事项加以解决。

例如，如果默认 VPC 安全组对入站和出站流量开放，则将其视为高严重性。威胁参与者使用这种方法入侵 VPC 有点容易。威胁参与者也有可能资源进入 VPC 后破坏或窃取资源。

Security Hub 建议您将严重程度高的发现视为近期优先事项。你应该立即采取补救措施。您还应该考虑资源的重要性。

中度 — 应将该问题作为中期优先事项加以解决。

例如，对传输中的数据缺乏加密被视为中等严重性发现。它需要复杂的 man-in-the-middle 攻击以利用这个弱点。换句话说，这有点困难。如果威胁情景成功，某些数据很可能会遭到泄露。

Security Hub 建议您尽早调查相关资源。您还应该考虑资源的重要性。

低-该问题不需要单独采取行动。

例如，未能收集取证信息被视为低严重性。这种控制有助于防止future 出现妥协，但缺乏取证并不能直接导致妥协。

您无需立即对严重程度较低地发现采取行动，但是当您将它们与其他问题关联时，它们可以提供背景信息。

信息-未发现配置漏洞。

换句话说，状态是PASSED,WARNING，或NOT AVAILABLE。

没有建议的操作。信息性结果可帮助客户证明其处于合规状态。

更新控制结果的规则

随后对给定规则的检查可能会生成新的结果。例如，“避免使用 root 账户”的状态可能会从FAILED到PASSED. 在这种情况下，将生成一个包含最新结果的新发现。

如果根据给定规则进行的后续检查生成与当前结果相同的结果，则更新现有结果。不会生成新结果。

如果关联资源被删除、资源不存在或控件被禁用，Security Hub 会自动归档控件中的发现。资源可能已不存在，因为当前未使用关联的服务。结果将根据以下条件之一自动存档：

- 调查结果在三到五天内没有更新（请注意，这是尽力而为，不能保证）。
- 关联的 Amazon Config 评估返回了 NOT_APPLICABLE。

从结果中确定控制的总体状态

Security Hub 使用 `Compliance.Status` 根据每个对照的调查结果得出的值来确定总体控制状态。总体状态显示在标准的控制列表和控制详细信息页面上。

对于管理员帐户，控制状态反映了管理员帐户和所有成员帐户的聚合状态。如果您设置了聚合区域，则聚合区域中的控制状态会反映所有关联区域的控制状态。具体而言，控件的总体状态显示为已失败如果该控件在至少一个帐户和一个关联区域中有一个或多个不合格发现。

Security Hub 通常会在您首次访问 Security Hub 后的 30 分钟内生成初始控制状态摘要页面或 Security Hub 控制台上的页面。状态仅适用于在您访问这些页面时启用的控件。使用 [UpdateStandardsControl](#) 用于启用或禁用控件的 API 操作。另请参阅 Amazon Config 必须配置资源记录才能显示控制状态。首次生成控制状态后，Security Hub 会根据过去 24 小时的调查结果每 24 小时更新一次控制状态。在控件详细信息页面上，Security Hub 显示时间戳以指示控件状态的最后更新时间。

Note

启用控件后，最多可能需要 24 小时才能在中国区域生成首次控制状态；Amazon GovCloud (US) Region。

的值 `Compliance.Status`

这些区域有：`Compliance.Status` 为每项求解结果分配以下任一值。

- PASSED— 自动设置 `Security Hub Workflow.Status` 到 RESOLVED。

如果 `Compliance.Status` 为 PASSED 到 FAILED, WARNING, 或 NOT_AVAILABLE；以及 `Workflow.Status` 或者 NOTIFIED 要么 RESOLVED；然后 Security Hub 会自动设置 `Workflow.Status` 到 NEW。

- FAILED— 表示该控件未通过此发现的安全检查。
- WARNING— 表示检查已完成，但 Security Hub 无法确定资源是否在 PASSED 要么 FAILED 状态。
- NOT_AVAILABLE— 表示无法完成检查的原因是服务器出现故障、资源被删除或是服务器出现故障 Amazon Config 求解是 NOT_APPLICABLE。

如果 Amazon Config 求解结果为 NOT_APPLICABLE，然后 Security Hub 会自动存档调查结果。

控制状态的值

Security Hub 使用控制结果的合规性状态来计算总体控制状态。在计算总体控制状态时，Security Hub 会忽略具有以下特征的调查结果 `Workflow.Status` 的 SUPPRESSED。

总体控制状态的可用值如下：

- 通过— 表示所有发现都有 `Compliance.Status` 的 PASSED。
- 已失败— 表示至少有一项调查结果具有 `Compliance.Status` 的 FAILED。
- Unknown— 表示至少有一项调查结果具有 `Compliance.Status` 的 WARNING 要么 NOT_AVAILABLE。任何结果都不为 FAILED。

- 没有数据— 表示没有对照的发现。例如，新控件在开始生成发现结果之前一直处于此状态。如果所有发现结果都是，则控件也具有此状态SUPPRESSED。
- Disabled— 表示当前账户和区域中的控件已停用。这意味着目前没有对这个控制权进行安全检查，就是这个账户和区域。但是，禁用的控件的值可能为Compliance.Status禁用后最多 24 小时。

确定安全标准的安全分数

在存储库的安全标准页面上，Security Hub 为每个启用的标准显示一个介于 0-100% 之间的安全分数。这些区域有：摘要页面还会显示所有已启用的标准的总体安全分数。

启用 Security Hub 后，Security Hub 会在您首次访问摘要页或安全标准页面位于Security Hub 控制台上。只有在您访问这些页面时启用的标准才会生成分数。要查看当前启用的标准列表，请使用[GetEnabledStandards](#) API 操作。此外，Amazon Config必须配置资源记录才能显示分数。总体安全分数是标准安全分数的平均值。

首次生成分数后，Security Hub 每 24 小时更新一次安全分数。Security Hub 会显示一个时间戳，以指示上次更新安全分数的时间。

Note

在中国区域，最长可能需要 24 小时才能生成首次安全分数Amazon GovCloud (US) Region.

如何计算安全分数

安全分数代表的比例Passed控件到已启用的控制。此分数以百分比形式显示。例如，如果为一个标准启用了 10 个控件，其中 7 个控件处于一个控件中Passedstate，则该标准的安全分数为 70%。

如果您的账户是管理员账户，则安全评分会考虑所有成员账户中的控制结果。

如果您设置了聚合区域，则总体安全分数是一个汇总分数，它考虑了所有关联区域的调查结果。同样，每个标准的安全分数是一个汇总分数，它考虑了所有关联区域中与该标准相关的调查结果。请注意，如果您的账户是管理员账户，则安全评分适用于所有成员账户和所有区域。

安全分数计算会忽略没有任何发现结果的已启用控件（总体状态为没有数据）。例如，一个标准启用了 12 个控件。其中六个控件位于Passed状态。两个控件没有数据。由于计算忽略了没有数据的控件，因此安全分数为 60%。

管理员帐户的安全分数

对于管理员账户，总体安全分数和特定标准的安全分数是管理员账户和所有成员账户的汇总分数。

如果您设置了聚合区域，则安全分数

如果您设置了聚合区域，则总体安全分数和每个标准的安全分数会反映来自所有关联区域的调查结果。如果您的账户是管理员账户，则安全分数也适用于所有成员账户。

在 Summary (摘要) 页面上，

在存储库的摘要页，的安全标准卡显示每个已启用标准的安全分数。它还显示一个综合安全分数，表示所有已启用标准中的已通过控件与已启用控件的比例。

查看和管理安全标准

安全标准提供了一套相关控制措施，以确定是否符合监管框架、行业最佳实践或公司政策。

对于 Security Hub 中的标准，您可以查看控件列表并确定是为您的帐户启用还是禁用标准。您还可看到该标准的总体安全评分。

管理员帐户可以在其成员帐户中查看汇总的安全分数和控制状态。如果您正在查看聚合区域的标准，则标准的安全分数将包括所有关联区域的控制措施的合规性状态。

有关可用标准及其控件的列表，请参阅[the section called “可用标准” \(p. 263\)](#)。

有关如何管理标准中的各个控件的信息，请参阅[the section called “查看和管理控件” \(p. 257\)](#)。

主题

- [禁用或启用安全标准 \(p. 252\)](#)
- [查看有关标准的详细信息 \(p. 254\)](#)

禁用或启用安全标准

您可以在 Security Hub 中禁用或启用每种支持的安全标准。默认情况下，某些安全标准处于启用状态，但您可以选择退出自动启用的标准。

Security Hub 是区域性的。启用或禁用安全标准时，仅在当前区域或您指定的区域中启用或禁用该标准。

在您禁用 Security 标准时，会发生以下情况：

- 不再对其控制进行检查。
- 没有为其控制生成其他调查结果。
- 现有发现将在三到五天后自动存档（请注意，这是尽力而为，不能保证）。
- 相关的 Amazon Config Security Hub 创建的规则已被删除。

这通常在您禁用标准后的几分钟内发生，但可能需要更长的时间。

如果第一次请求删除 Amazon Config 规则失败，然后 Security Hub 每 12 小时重试一次。但是，如果您禁用了 Security Hub 或者没有启用任何其他标准，则 Security Hub 将无法重试请求，这意味着它无法删除 Amazon Config 规则。如果发生这种情况，您需要 Amazon Config 规则已删除，联系 Amazon Web Services Support。

在启用任何 Security 标准之前，请确保您已启用 Amazon Config 并配置了资源记录。请参阅 [the section called “启用 Amazon Config” \(p. 7\)](#)。

在启用安全标准时，将默认启用该标准的所有控制。然后，您可以禁用各个控制。请参阅 [the section called “禁用和启用各项控制” \(p. 258\)](#)。

启用 Security Hub 后，Security Hub 会在您首次访问标准后的 30 分钟内计算出标准的初始安全分数摘要页面或保安标准 Security Hub 控制台上的页面。只有在您访问这些页面时启用的标准才会生成分数。此外，Amazon Config 必须配置资源录制才能显示分数。首次生成分数后，Security Hub 每 24 小时更新一次安全分数。Security Hub 显示时间戳以指示上次更新安全分数的时间。要查看当前启用的标准列表，请使用 [GetEnabledStandards](#) API 操作。

Note

在中国区域，生成首次 Security security security ef (中国区域) 最长可能需要 24 小时才能生成 Amazon GovCloud (US) Region。

自动启用的安全标准

Security Hub 会自动为新帐户启用默认安全标准。此外，如果您使用集成 Amazon Organizations，Security Hub 会自动为新成员帐户启用默认安全标准。您可以选择自动启用的标准。

目前，自动启用的默认安全标准是 Amazon 基础安全最佳实践 (FSBP) 标准和互联网安全中心 (CIS) v1.2.0 Amazon 基金会基准测试。

选择退出自动启用的标准

以下退出步骤仅在您使用与集成时才适用 Amazon Organizations。如果您不使用此集成，则可以在首次启用 Security Hub 时选择退出默认标准，也可以按照以下步骤操作 [禁用标准 \(p. 253\)](#)。

选择退出自动启用标准（控制台）

1. 打开 Amazon Security Hub 控制台位于 <https://console.aws.amazon.com/securityhub/>。
2. 登录到管理员账户。
3. 在 Security Hub 中，选择设置。
4. 在账户选项卡，关闭自动使能。

要选择退出自动启用的标准（Security Hub API），Amazon CLI）

- SSecurity Hub— 使用 [UpdateOrganizationConfiguration](#) 操作来自 Security Hub 操作。的默认值 `AutoEnabledStandards` 参数等于 `DEFAULT`。要在新成员账户中选择不使用自动启用的标准，请设置 `AutoEnableStandards` 等于 `NONE`。
- Amazon CLI— 在命令行处，运行 `update-organization-configuration` 命令。

```
aws securityhub update-organization-configuration --auto-enable-standards
```

禁用安全标准

在 Security standards (安全标准) 页面上，每个启用的标准包含禁用该标准的选项。请按照以下步骤禁用标准。

要禁用 Security 标准（控制台）

1. 打开 Amazon Security Hub 控制台位于 <https://console.aws.amazon.com/securityhub/>。
2. 确认您正在要禁用标准的区域中使用 Security Hub。
3. 在 Security Hub 中，选择保安标准。
4. 对于要禁用的标准，请选择 Disable (禁用)。

要禁用安全标准（Security Hub API），Amazon CLI）

- SSecurity Hub— 使用 [BatchDisableStandards](#) 操作。对于要禁用的每个标准，您需要提供该标准的订阅的 ARN。要获取已启用标准的订阅 ARN，请使用 [GetEnabledStandards](#) 操作。
- Amazon CLI— 在命令行处，运行 [batch-disable-standards](#) 命令。

```
aws securityhub batch-disable-standards --standards-subscription-arns <subscription ARN>
```

示例

```
aws securityhub batch-disable-standards --standards-subscription-arns  
"arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0"
```

启用安全标准

在 Security standards (安全标准) 页面上，每个禁用的标准包含启用该标准的选项。请按照以下步骤操作以启用标准。

启用安全标准（控制台）

1. 打开Amazon Security Hub控制台位于<https://console.aws.amazon.com/securityhub/>.
2. 确认您正在要在其中启用 Security Hub。
3. 在 Security Hub 中，选择保安标准。
4. 对于要启用的标准，请选择 Enable (启用)。

要启用安全标准（Security Hub API），Amazon CLI

- SSecurity Hub— 使用[BatchEnableStandards](#)操作。要确定要启用的标准，必须提供标准 ARN。要获取标准 ARN，请使用[DescribeStandards](#)操作。
- Amazon CLI— 在命令行处，运行[batch-enable-standards](#)命令。

```
aws securityhub batch-enable-standards --standards-subscription-requests  
'{"StandardsArn": "<standard ARN>"}
```

示例

```
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"}'
```

查看有关标准的详细信息

标准的详细信息页面包含标准中的控件列表。它还显示了标准赛的总体得分。

您可以查看和筛选控制列表，并执行以下操作：

- [启用或禁用控制 \(p. 258\)](#)
- [查看有关控制件的详细信息 \(p. 257\)](#)。控制详细信息页面包括控制结果列表。请参阅 [the section called “查看控制结果并采取相应措施” \(p. 261\)](#)。

显示已启用的标准的详细信息页面（控制台）

从安全标准页面上，您可以显示标准的详细信息页面。您只能显示已启用的标准的详细信息。您无法显示禁用标准的详细信息。

这也适用于管理员帐户。未为其个人账户启用标准的管理员帐户无法查看该标准的详细信息。他们无法查看已启用标准的成员账户的汇总安全分数和状态信息。

显示启用的标准（控制台）的控制列表

1. 打开Amazon Security Hub控制台在<https://console.aws.amazon.com/securityhub/>.
2. 在 Security Hub 导航窗格中，选择安全标准。
3. 对于要显示其详细信息的标准，选择查看结果。

标准详情页面上的信息

详细信息页面顶部是标准的总体得分。分数是传递的控件相对于具有数据的标准的已启用控件数量的百分比。Security Hub 通常会在您首次访问后的 30 分钟内计算出初始安全分数摘要页面或安全标准页面位于 Security Hub 控制台上。只有在您访问这些页面时启用的标准才会生成分数。要查看当前启用的标准列表，

请使用[GetEnabledStandardsAPI](#) 操作。此外，Amazon Config必须配置资源记录才能显示分数。首次生成分数后，Security Hub 每 24 小时更新一次安全分数。Security Hub 会显示一个时间戳，以指示上次更新安全分数的时间。请参阅 [the section called “确定标准安全分数” \(p. 251\)](#)。

Note

在中国区域中，首次生成安全分数最长可能需要 24 小时才能生成。Amazon GovCloud (US) Region.

总分旁边是一个汇总控制状态的图表。该图表显示了失败和通过的控件的百分比。当您在图表上暂停时，弹出窗口将显示以下内容：

- 每个严重性的失败控件数
- 状态为的控件的数量Unknown
- 传递的控件数量

详细信息页面底部是标准的控制列表。控制列表根据控件的当前总体状态和分配给每个控件的严重性进行组织和排序。Security Hub 每 24 小时更新一次控制状态。每个选项卡上的时间戳表示控件状态最近更新的时间。请参阅 [the section called “确定控制状态” \(p. 250\)](#)。

对于管理员帐户，分数和状态在管理员账户和所有成员账户中汇总。

上面的所有数据安全标准除非您设置了聚合区域，否则详细信息页面特定于当前区域。如果您设置了聚合区域，则安全分数是跨区域的，并考虑了所有关联区域的调查结果。标准详情页面上控制措施的合规性状态也反映了来自关联区域的调查结果，安全检查的数量包括来自关联区域的调查结果。

对控件进行筛选和排序

标准的控制列表使用选项卡根据控件状态为列表提供内置筛选。您还可以根据 ID、标题和严重程度来筛选列表。

这些区域有：所有已启用的选项卡列出了标准版的所有已启用的控件。对于管理员帐户，所有已启用的包含在其账户或任何成员账户中启用的控件。

在存储库的已失败、Unknown、没有数据、和Passed选项卡，来自所有已启用的选项卡被筛选为仅包含具有该状态的控件。

这些区域有：Disabled选项卡包含已禁用控件的列表。对于管理员帐户，Disabled选项卡列出了未在其账户或任何成员账户中启用的控件。

对于独立账户和成员账户，启用和禁用的控件列表会实时更新，以反映启用和禁用的控件。每个控件的整体状态以及通过和失败的检查次数每 24 小时更新一次。

对于管理员帐户，包括列表在内的所有信息每隔 24 小时更新一次。

对于每个控制，控制列表包含以下信息：

- 控件的总体状态 (请参阅[the section called “确定控制状态” \(p. 250\)](#))
- 分配给控件的严重性
- 控制标识符和标题
- 失败的活动查找结果的数量和活动查找结果的总数。如果适用，检查失败列还列出了状态为的查找结果的数目Unknown.

除了每个选项卡上的内置筛选器外，您还可以使用以下字段中的值筛选列表：

- 状态

- 严重性
- ID
- 职务

您可以使用任意列对每个列表进行排序。默认为所有已启用的选项卡进行排序，以便失败的控制件列在列表顶部。这有助于您立即关注需要补救的问题。

默认情况下，在每个状态和其余选项卡上，控件按严重性降序排序。换句话说，关键控制首先是严重性控制，其次是高，然后是中等严重性控制，然后是低严重性控制。

管理员帐户的其他选项卡

对于管理员帐户，前六个选项卡上的列表包含管理员帐户及其成员帐户的汇总信息。例如，一个控件列在所有已启用的选项卡（如果至少有一个帐户启用了该控件）。控件列在Disabled选项卡，仅当所有帐户均未启用该控件时。

这些选项卡上的所有信息每 24 小时更新一次。

管理员帐户还会看到以下附加选项卡：

- 已启用此帐户的控件列出了为管理员帐户启用的控件。
- 已禁用此帐户的控件列出了管理员帐户禁用的控件。

这些列表会实时更新，以反映管理员帐户已启用或禁用的控件。

下载控制列表

您可以将控制列表的当前页面下载到.csv文件。

如果您筛选了控制列表，则下载的文件仅包含与筛选器匹配的控件。

如果您从列表中选择了特定控件，则下载的文件仅包含该控件。

要下载控制列表的当前页面或当前选定的控件，请选择下载。

查看启用的标准的控制 (Security Hub API、Amazon CLI)

要显示有关已启用标准的控件的信息，您可以使用 API 调用或Amazon Command Line Interface。

要显示启用的标准 (Security Hub API) 的控制，Amazon CLI)

- SSecurity Hub— 使用[DescribeStandardsControls](#)operation. 要确定要显示控制件的标准，您需要提供控制件订阅的 ARN。要获取启用的标准的订阅 ARN，请使用[GetEnabledStandards](#)operation.
- Amazon CLI— 在命令行处，运行[describe-standards-controls](#)命令。

```
aws securityhub describe-standards-controls --standards-subscription-arn <subscription ARN>
```

示例

```
aws securityhub describe-standards-controls --standards-subscription-arn  
"arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0"
```

查看和管理控件

控件是针对特定资源的安全检查。从 Security Hub，您可以查看控制详细信息。控件详细信息包括控制状态以及为每个控件生成的调查结果。

您可以启用或禁用账户的控件。您还可以查看控件生成的调查结果的详细信息并对其进行采取措施。

对于管理员帐户，控件详细信息显示所有成员账户的状态和调查结果。如果您设置了聚合区域，则控件详细信息将反映所有关联区域的调查结果。

主题

- [查看控制的详细信息 \(p. 257\)](#)
- [自动启用新控件 \(p. 258\)](#)
- [禁用和启用各项控制 \(p. 258\)](#)
- [查看控制结果并采取相应措施 \(p. 261\)](#)

查看控制的详细信息

对于每个控制，您可以显示有用详细信息的页面。

显示控件的详细信息

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. [显示启用的标准的控制。 \(p. 254\)](#)
3. 从控制列表中，选择控制名称。

控制详细信息页面顶部提供了控件的概述，包括其启用状态和整体控制状态。

- 启用状态— 启用状态告诉您控件当前是否已激活。如果您登录到管理员帐户，状态将显示为Enabled (已启用)如果至少在一个成员账户中激活了控件。如果您设置了聚合区域，则状态显示为Enabled (已启用)如果至少在一个区域中激活了控件。
- 控制状态— 控制状态根据控制结果的合规性状态汇总控件的性能。Security Hub 通常在您首次访问摘要页面或安全标准Security Hub 控制台上的页面。状态仅适用于访问这些页面时启用的控件。使用[UpdateStandardsControl](#)用于启用或禁用控件的 API 操作。此外，Amazon Config必须配置资源录制才能显示控制状态。首次生成控制状态后，Security Hub 会根据前 24 小时的调查结果每 24 小时更新一次控制状态。在标准详细信息页面和控制详细信息页面上，Security Hub 显示时间戳以指示上次更新状态的时间。管理员帐户可以在管理员帐户和成员帐户中看到聚合控制状态。如果您设置了聚合区域，则控制状态会记录所有关联区域的查找结果。有关控制状态的更多信息，请参阅[the section called “确定控制状态” \(p. 250\)](#).

Note

启用对在中国地区生成首次控制状态的控制权后，最长可能需要 24 小时，Amazon GovCloud (US) Region.

有关支付卡行业数据安全标准 (PCI DSS) 和 CIS 的控制Amazon“基金会标准”相关要求选项卡列出了框架内的相关要求。

在详细信息页面中，您可以禁用或启用控件。请参阅 [the section called “禁用和启用各项控制” \(p. 258\)](#)。

详细信息页面底部包含有关控制的活动结果的信息。控制结果是通过对照控件进行的安全检查生成的。控件查找结果列表不包括存档的调查结果。

查找结果列表使用显示列表中不同子集的选项卡。在大多数选项卡中，结果列表显示了工作流程状态为NEW、NOTIFIED，或者RESOLVED。显示一个单独的标签SUPPRESSED结果。

对于每个查找结果，该列表都可以访问其合规性状态以及有关查找结果和关联资源的详细信息。您还可以设置每个结果的工作流程状态，以及将结果发送到自定义操作。

请参阅 [the section called “查看控制结果并采取相应措施” \(p. 261\)](#)。

自动启用新控件

Amazon Security Hub定期为标准添加新的控制措施。当您第一次启用 Security Hub 时，它会在添加新控件时自动启用它们。这仅适用于启用的标准。当将新控件添加到您禁用的标准中时，Security Hub 不会启用这些控件。

可以选择是否自动启用新控件。如果不自动启用新控件，则必须手动启用它们。请参阅 [the section called “禁用和启用各项控制” \(p. 258\)](#)。

选择是否自动启用新控件（控制台）

这些区域有：普通的“”选项卡设置页面包含用于控制是否自动启用新控件的设置。

选择是否为启用的标准启用新控制

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>。
2. 在导航窗格中，选择设置，然后选择普通的选项卡。
3. UDLE自动启用新控制，选择编辑。
4. Toggle在我启用的标准中自动启用新控件。
5. 选择保存。

选择是否自动启用新控件（Security Hub API，Amazon CLI）

要配置是否自动启用新控件，可以使用 API 调用或Amazon Command Line Interface。

要配置是否自动启用新控件（Security Hub API），Amazon CLI）

- Security Hub— 使用[UpdateSecurityHubConfiguration](#)operation. 要自动启用控件，请设置AutoEnableControls到true. 要不自动启用控件，请设置AutoEnableControls为 false。
- Amazon CLI— 在命令行处，运行[update-security-hub-configuration](#)命令。要自动启用新控件，请指定--auto-enable-controls. 要不启用新控件，请指定--no-auto-enable-controls.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

示例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

禁用和启用各项控制

在启用标准时，将默认启用该标准的所有控制。然后，您可以在启用的标准中禁用和启用特定的控制。

在禁用控制时，将发生以下情况：

- 不再执行该控制的检查。
- 不会为该控制生成任何其他结果。
- 现有的调查结果会在三到五天后自动存档（请注意，这是最大努力，不能保证）。
- 相关Amazon Config删除 Security Hub 创建的规则。

禁用针对与您的环境不相关的控件的安全检查可能会很有用。例如，您可能更喜欢使用亚马逊 GuardDuty 而不是 CloudWatch 要监控的警报是否与您的关联的异常活动Amazon CloudTrail日志。然后，您可以禁用 CISAmazon基金会基准测试控制 3.1-3.14，其重点是 CloudWatch 警报。

禁用不相关的控制会减少不相关的结果数量。它还会从相关标准的安全分数中删除失败的检查。

请记住，Security Hub 是区域性的。在禁用或启用控制时，仅在当前区域或您在 API 请求中指定的区域中禁用该控制。

此外，在禁用整个标准时，Security Hub 不会跟踪禁用了哪些控制。如果随后再次启用该标准，则会启用所有控制。有关更多信息，请参阅 [the section called “禁用或启用安全标准” \(p. 252\)](#)。

Note

启用和禁用控件 region-by-region 基础通过 Security Hub 控制台、API 或 CLI 进行。如果您设置了聚合区域，则可以看到来自所有链接区域的控件。如果控件在链接区域中可用，但在聚合区域中不可用，则无法从聚合区域启用或禁用该控件。有关多账户和多区域控制禁用脚本，请参阅[在多账户环境中禁用 Security Hub 控件](#)

禁用控制（控制台）

在 Security Hub 控制台中，您可以从标准详细信息页面上的控件列表或控件详细信息页面禁用控件。

禁用控制（控制台）

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>。
2. 确认您要在禁用控制的区域中使用 Security Hub。
3. 在 Security Hub 导航窗格中，选择安全标准。
4. 对于要禁用控制的标准，请选择查看结果。
5. 如果你是管理员帐户，请选择已启用此帐户。

其他账户可以从除了Disabled选项卡。

6. 请执行下列操作之一：
 - 在控件列表中，选择要禁用的控件。然后选择 。禁用。
 - 选择控件标题。然后，在控制详细信息页面上，选择禁用。
7. 输入禁用控制的原因。这可以帮助组织中的其他人了解禁用控制的原因。
8. 选择 Disable（禁用 Amazon Macie）。

禁用控件（Security Hub API，Amazon CLI）

要禁用控件，您可以使用 API 调用或Amazon Command Line Interface。

要禁用控件（Security Hub API），Amazon CLI）

- Security Hub API— 使用[UpdateStandardsControl](#)operation. 要确定要禁用的控件，请提供控制 ARN。要检索标准中控件的 ARN，请使用[DescribeStandardsControl](#)soperation.
- Amazon CLI— 在命令行处，运行[update-standards-control](#)命令。

```
aws securityhub update-standards-control --standards-control-arn <control ARN> --control-status "DISABLED" --disabled-reason <description of reason to disable>
```

示例

```
aws securityhub update-standards-control --standards-control-arn "arn:aws:securityhub:us-east-1:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/ACM.1" --control-status "DISABLED" --disabled-reason "Not applicable for my service"
```

启用控制 (控制台)

在标准详细信息页面上，禁用的控件显示在Disabled选项卡。

对于管理员帐户，Disabled选项卡包含跨账户的汇总列表。单个管理员帐户的禁用控件显示在已禁用此帐户选项卡。

您可以从控件列表中启用控件Disabled选项卡，或者从控件详细信息页面中。

启用禁用控制 (控制台)

1. 打开Amazon Security Hub控制台<https://console.aws.amazon.com/securityhub/>.
2. 确认您要在禁用控制的区域中使用 Security Hub。
3. 在 Security Hub 导航窗格中，选择安全标准。
4. 对于要启用控制的标准，请选择。查看结果。
5. 显示已禁用控件的列表。

对于成员账户或独立账户，请选择Disabled。

对于管理员账户，请选择已禁用此账户。

6. 请执行下列操作之一：
 - 在控制列表中Disabled要么已禁用此帐户选项卡中，选择要启用的控制。然后选择 Enable。
 - 选择控件标题。然后，在控制详细信息页面上，选择启用。

启用控件 (Security Hub API , Amazon CLI)

要启用控件，您可以使用 API 调用或Amazon Command Line Interface。

要启用控件 (Security Hub API) , Amazon CLI)

- Security Hub API— 使用[UpdateStandardsControl](#)operation. 要确定要启用的控件，请提供控制 ARN。要检索标准中控件的 ARN，请使用[DescribeStandardsControls](#)operation.
- Amazon CLI— 在命令行处，运行[update-standards-control](#)命令。

```
aws securityhub update-standards-control--standards-control-arn <control ARN> --control-status "ENABLED"
```

示例

```
aws securityhub update-standards-control --standards-control-arn "arn:aws:securityhub:us-east-1:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/ACM.1" --control-status "ENABLED"
```

查看控制结果并采取相应措施

控制详细信息页面包含控制的活动结果的列表。该列表不包括存档的调查结果。

控制详细信息页面不支持跨区域聚合。控制详细信息页面仅显示来自当前区域的查找结果。

该列表提供了筛选和排序查找结果的工具，以便您可以首先关注更紧急的查找结果。每个查找结果都可以在相关服务控制台中包含指向资源详细信息的链接。对于基于Amazon Config规则，您可以查看有关规则和配置时间表的详细信息。

您也可以使用Amazon Security Hub用于检索结果的列表。请参阅 [the section called “检索查找详情 \(Security Hub API , Amazon CLI \) ” \(p. 66\)](#)。

主题

- [筛选、排序和下载控制结果列表 \(p. 261\)](#)
- [查看有关控件查找和查找资源的详细信息 \(p. 262\)](#)
- [对控制结果采取行动 \(p. 263\)](#)

筛选、排序和下载控制结果列表

控件查找结果列表使用选项卡根据查找状态为列表提供内置过滤。您还可以根据其他查找结果值筛选列表，并从列表中下载查找结果。

对控件查找列表进行筛选和排序

这些区域有：所有检查选项卡列出了 workflow 状态为的所有活动查找结果NEW、NOTIFIED，或者RESOLVED。默认情况下，列表的顶部会显示失败的结果排在列表的顶部。这种排序顺序提请注意需要解决的调查结果。

上面的名单已失败、Unknown, 和Passed选项卡根据的值进行过滤Compliance.Status. 这些列表还仅包括 workflow 状态为的活动查找结果NEW、NOTIFIED，或者RESOLVED。

这些区域有：黑名单选项卡包含 workflow 状态为“已禁止”的活动查找结果的列表。

除了每个选项卡上的内置筛选器外，您还可以使用以下字段中的值来筛选列表：

- 账户 ID
- 工作流程状态
- 合规性状态
- 资源 ID
- 资源类型

您可以使用任一列对每个列表进行排序。

下载对照调查结果列表

如果你导航到安全标准然后选择一个标准，你会看到该标准的控件列表。从列表中选择控件会转到控件详细信息页面。您可以从此处将控制结果的当前页面下载到 .csv 文件中。

如果您筛选了查找结果列表，则下载内容仅包含与筛选器匹配的控件。

如果您从列表中选择了特定的查找结果，则下载内容将仅包含选定的查找结果。

要下载列表的当前页面或选定的搜索结果，请选择下载。

查看有关控件查找和查找资源的详细信息

对于每个发现，Amazon Security Hub提供对详细信息的访问权限，以帮助您调查调查结果。

您可以显示有关查找资源和相关配置规则的详细信息。

您还可以查看添加到查找结果中的任何注释。

查看完整的 .json 以查找结果

您可以显示和下载完整的 .json 一个发现。

显示 .json，在查找 .json 列上，选择图标。

在存储库的查找 JSON 面板，以下载 .json，选择下载。

查看有关结果资源的信息

这些区域有：资源列包含资源类型和资源标识符。

要显示有关资源的信息，请选择资源标识符。适用于 Amazon 账户，如果该账户是组织成员账户，则信息包括账户 ID 和账户名。对于手动邀请的账户，信息仅包含账户 ID。

如果您有权在资源的原始服务中查看资源，则资源标识符会显示指向该服务的链接。例如，对于 Amazon 用户，则资源详细信息提供指向 IAM 中查看用户详细信息的链接。

如果资源位于其他帐户中，Security Hub 会显示一条消息，通知您。

查看查找资源的配置时间表

调查的一个途径是资源的配置时间表 Amazon Config。

如果您有权查看查找资源的配置时间表，则查找结果列表会提供指向该时间轴的链接。

如果资源位于其他帐户中，Security Hub 会显示一条消息，通知您。

要导航到中的配置时间轴 Amazon Config

1. 在调查列上，选择图标。
2. 在菜单上，选择配置时间表。如果您无权访问配置时间线，则不会显示链接。

查看 Amazon Config 结果资源的规则

如果控制基于 Amazon Config 规则，则可能还想查看有关的详细信息 Amazon Config 规则。这些区域有：Amazon Config 规则信息可以帮助您更好地了解检查通过或失败的原因。

如果您有权查看 Amazon Config 控件的规则，则查找结果列表会提供指向 Amazon Config 统治 Amazon Config。

如果资源位于其他帐户中，Security Hub 会显示一条消息，通知您。

导航到 Amazon Config 规则

1. 在调查列上，选择图标。
2. 在菜单上，选择 Config 规则。如果您无权访问 Amazon Config 规则 Config 规则未链接。

查看发现结果的注释

如果发现结果具有关联的注释，那么 Updated 列显示备注图标。

显示与查找结果关联的注解

在Updated列上，选择附注图标。

对控制结果采取行动

要反映调查的当前状态，请设置工作流程状态。请参阅 [the section called “设置结果的工作流状态” \(p. 66\)](#)。

Amazon Security Hub还允许您将选定的调查结果发送到亚马逊的自定义操作 EventBridge。请参阅 [the section called “将结果发送到自定义操作” \(p. 68\)](#)。

中的中可用安全标准Amazon Security Hub

安全标准提供了一套相关控制措施，以确定是否符合监管框架、行业最佳实践或公司政策。

每个标准的信息都包括该标准中的控件列表。每个控件包含以下信息：

- 控件所属的安全类别
- 控件适用的资源
- 如果适用，Amazon Config用于控件的规则
- 控件使用的任何参数
- 对控件及其检查内容的描述
- 对于与监管框架相关的标准，该框架中的适用要求
- 有关如何修复失败的支票的信息。例如，您可能需要更改资源的配置。

Amazon Security Hub支持下面列出的安全标准。如果你正在使用集成Amazon Organizations，默认情况下，在新成员账户中自动启用 CIS 和基础安全最佳实践标准。有关自动启用标准的更多信息，请参阅[自动启用的安全标准 \(p. 252\)](#)。

主题

- [CISAmazon 基金会基准标准 \(p. 263\)](#)
- [支付卡行业数据安全标准 \(PCI DSS\) \(p. 310\)](#)
- [Amazon 基础安全最佳实践标准 \(p. 361\)](#)

CISAmazon 基金会基准标准

Security Hub 支持互联网安全中心 (CIS)Amazon 基础基准标准。有关更多信息，请参阅 CIS 网站的[Amazon Web Service 安全](#)。

AmazonSecurity Hub 已满足 CIS 安全软件认证的要求，并已获得以下 CIS 基准测试的 CIS 安全软件认证：

- CIS Amazon Web Services 基金会基准测试基准，v1.2.0，第 1 级
- CIS Amazon Web Services 基金会基准测试基准，v1.2.0，第 2 级

主题

- [CIS 控制所需的 Amazon Config 资源 \(p. 264\)](#)
- [CISAmazon 基金会基准控制 \(p. 264\)](#)
- [您可能要禁用的 CISAmazon 基础基准测试控件 \(p. 310\)](#)
- [CISAmazon Foundations Security Hub 不支持的安全检查 \(p. 310\)](#)

CIS 控制所需的 Amazon Config 资源

要对环境资源上已启用的控件进行安全检查，Security Hub 要么执行[保护 Amazon Web Services](#) 中为检查规定的确切审计步骤，要么使用特定的 Amazon Config 托管规则。

如果您没有在 Amazon Config 中启用所有资源，则会为控件[2.5 — 确保 Amazon Config 已启用 \(p. 277\)](#)生成一个结果。对于其他 CIS 控件，要使 Security Hub 准确报告发现结果，必须在中启用对以下资源的记录 Amazon Config。

- AWS::CloudTrail::Trail
- AWS::EC2::SecurityGroup
- AWS::EC2::VPC
- AWS::IAM::Policy
- AWS::IAM::User
- AWS::KMS::Key
- AWS::S3::Bucket

如果调查结果是由基于 Amazon Config 规则的安全检查生成的，则调查结果详细信息包括用于打开关联规则的 Amazon Config 规则链接。要导航到 Amazon Config 规则，您还必须在所选账户中拥有 IAM 权限才能导航到该规则 Amazon Config。

CIS Amazon 基金会基准控制

对于 CIS Amazon 基础标准，Security Hub 支持以下控件。对于每个控制，该信息包括所需的 Amazon Config 规则和修复步骤。

1.1 — 避免使用根用户

严重性：低

Amazon Config 规则：无（自定义 Security Hub 规则）

时间表类型：定期

根 Amazon 账户中的所有服务和资源具有不受限制的访问权限。我们强烈建议您避免使用 root 用户执行日常任务。尽量减少 root 用户的使用并采用最小权限原则进行访问管理，可降低意外更改和意外泄露高权限凭证的风险。

作为最佳做法，请仅在需要时使用 root 用户凭[证访问](#)。将 IAM 策略直接应用于群组 and 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 用户指南中的创建您的第一个 IAM 管理员用户[和群组](#)

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CIS Amazon Foundations Benchmark v1.2](#) 中为控制 3.3 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查 FAILED 结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 `ListSubscriptionsByTopic`。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：

- a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
 7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后，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. 选中筛选的复选框。选择 Create alarm (创建警报)。

10. 在 **Connet** (指定指标和条件) 下, 执行以下操作 :
 - a. 在 “条件” 下, 为 “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 **Next** (下一步) 。
11. 在配置操作下, 执行以下操作 :
 - a. 在 “警报状态触发器” 下, 选择 “警报中”。
 - b. 在 **Select an SNS topic** (选择 SNS 主题) 下, 选择 **Select an existing SNS topic** (选择现有的 SNS 主题)。
 - c. 对于 **Sname** (向发送通知), 输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 **Next** (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 **Create alarm** (创建警报)。

1.2 — 确保为具有控制台密码的所有 IAM 用户启用多重验证 (MFA)

严重性：中

Amazon Config 规则：[mfa-enabled-for-iam-console-access](#)

时间表类型：定期

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 Amazon 网站时, 系统会提示他们输入用户名和密码以及 Amazon MFA 设备的验证码。

CIS 建议您为所有拥有控制台密码的账户启用 MFA。MFA 为控制台访问提供更高的安全保护。它要求身份验证负责人拥有一台发出时间敏感密钥的设备并知道证书。

Important

用于该检查的 Amazon Config 规则最多可能需要 4 个小时才能准确报告 MFA 的结果。在启用 CIS 安全检查后的前 4 小时内生成的任何发现都可能不准确。修复此问题后, 最多可能需要 4 个小时才能通过检查。

Note

Amazon Config 应在您使用 Security Security Hub p 的所有区域中启用。但是, 可以在单个区域中启用全局资源记录。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[Amazon 中的使用多重身份验证 \(MFA\)](#)。

1.3 — 确保禁用 90 天或更长时间未使用的证书

严重性：中

Amazon Config 规则：[iam-user-unused-credentials-check](#)

时间表类型：定期

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 Amazon 资源。

CIS 建议您删除或停用在 90 天或更长时间内未使用的所有证书。禁用或删除不必要的凭证可减少他人使用遭盗账户或已弃用账户的关联凭证的风险。

此控件的 Amazon Config 规则使用 [GetCredentialReport](#) 和 [GenerateCredentialReport](#) API 操作，这些操作每四小时才更新一次。对 IAM 用户所做的更改最多可能需要四个小时才能被该控件看到。

Note

Amazon Config 应在您使用 Security Security Hub p 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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

要获取监控账户是否有过期证书所需的一些信息，请使用 IAM 控制台。例如，当您查看账户中的用户时，会显示 Access key age (访问密钥使用期限)、Password age (密码使用期限) 和 Last activity (上次活动时间)。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账户和识别 90 天或更长时间没有活动的账户。您可以从 IAM 控制台下载 .csv 格式的证书报告。有关凭证报告的更多信息，请参阅[获取您 Amazon 账户的凭证报告](#)。

确定非活动账户或未使用的凭证后，请使用以下步骤禁用它们。

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Users (用户)。
3. 选择凭证超过 90 天的用户的名称。
4. 选择 Security credentials (安全凭证)，然后为 90 天或更长时间未使用的所有登录凭证和访问密钥选择转为非活跃。

1.4 — 确保每隔 90 天或更短时间轮换一次访问密钥

严重性：中

Amazon Config 规则：[access-keys-rotated](#)

时间表类型：定期

访问密钥包含访问密钥 ID 和秘密访问密钥，用于签署对发出的编程请求 Amazon。Amazon 用户需要自己的访问密钥才能 Amazon 从 Amazon Command Line Interface (Amazon CLI)、Windows 工具、Amazon SDK 进行编程调用 PowerShell，或者使用单个 Amazon 服务的 API 进行直接 HTTP 调用。

定期轮换访问密钥时，可以减少使用与泄漏或终止账户相关的访问密钥的可能性。轮换访问密钥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。

Note

非洲（开普敦）或欧洲（米兰）不支持此控件。

Amazon Config 应在您使用 Security Security Hub p 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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

确保访问密钥的使用时长不超过 90 天

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Users (用户)。
3. 对于显示 Access key age (访问密钥使用期限) 超出 90 天的每个用户，选择用户名来打开该用户的设置。

4. 选择 Security credentials (安全凭证)。
5. 为用户创建新的密钥：
 - a. 选择创建访问密钥。
 - b. 要保存密钥内容，请下载秘密访问密钥，或者选择 Show (显示)，然后从页面中复制该密钥。
 - c. 将密钥存储在安全位置以提供给用户。
 - d. 选择 Close (关闭)。
6. 更新使用上一个密钥的所有应用程序以使用新密钥。
7. 对于上一个密钥，请选择 Make inactive (转为非活跃) 来使访问密钥转为非活动状态。现在，用户无法使用该密钥发出请求。
8. 确认使用新密钥的所有应用程序都能按预期工作。
9. 确认所有应用程序都使用新密钥后，删除以前的密钥。访问密钥一经删除，就无法恢复。

要删除上一个密钥，请在行末尾选择 X，然后选择 Delete (删除)。

1.5 — 确保 IAM 密码策略要求至少一个大写字母

严重性：中

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码使用不同的字符集。

CIS 建议密码策略至少要求一个大写字母。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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Account settings (账户设置)。
3. 选择至少需要一个大写字母，然后选择 Apply password policy (应用密码策略)。

1.6 — 确保 IAM 密码策略要求至少一个小写字母

严重性：中

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码使用不同的字符集。CIS 建议密码策略至少要求一个小写字母。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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Account settings (账户设置)。
3. 选择至少需要一个小写字母 (Requires at least one lowercase letter)，然后选择 Apply password policy (应用密码策略)。

1.7 — 确保 IAM 密码策略要求至少一个符号

严重性：中

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码使用不同的字符集。

CIS 建议密码策略至少要求一个符号。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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Account settings (账户设置)。
3. 选择 Require at least one non-alphanumeric character (至少需要一个非字母数字字符)，然后选择 Apply password policy (应用密码策略)。

1.8 — 确保 IAM 密码策略要求至少一个数字

严重性：中

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码使用不同的字符集。

CIS 建议密码策略至少要求一个数字。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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Account settings (账户设置)。
3. 选择 Requires at least one number (至少需要一个数字)，然后选择 Apply password policy (应用密码策略)。

1.9 — 确保 IAM 密码策略要求的最小长度为 14 或更长

严重性：中

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码的长度至少为给定长度。

CIS 建议密码策略要求最小密码长度为 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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。

2. 选择 Account settings (账户设置)。
3. 在 最短密码长度 (Minimum password length) 字段中，输入 **14**，然后选择 Apply password policy (应用密码策略)。

1.10 — 确保 IAM 密码策略防止密码重复使用

严重性：低

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

此控件检查要记住的密码数量是否设置为 24。如果值不是 24，则控制失败。

IAM 密码策略可以防止同一个用户重复使用给定密码。

CIS 建议密码策略防止重复使用密码。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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Account settings (账户设置)。
3. 选择“防止重复使用密码”，然后输入 **24** “要记住的密码数量”。
4. 选择 Apply password policy (应用密码策略)。

1.11 — 确保 IAM 密码策略在 90 天或更短时间内使密码过期

严重性：低

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

IAM 密码策略可以要求密码在给定天数后轮换或过期。

CIS 建议密码策略在 90 天或更短时间后过期。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 过滤器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

修改密码策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Account settings (账户设置)。
3. 选择“启用密码过期时间”，然后输入“密码有效期（以天**90**为单位）”。
4. 选择 Apply password policy (应用密码策略)。

1.12 — 确保不存在根用户访问密钥

严重性：重大

Amazon Config 规则：[iam-root-access-key-check](#)

时间表类型：定期

根账户具有对 Amazon 账户中所有服务和资源的完全访问权限。Amazon 访问密钥提供对给定账户的编程访问权限。

CIS 建议删除所有与 root 用户关联的访问密钥。移除与 root 用户关联的访问密钥限制了账户可能被入侵的矢量。移除 root 用户访问密钥还会鼓励创建和使用权限最低的基于角色的账户。

Note

亚太地区（大阪）不支持此控件。

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](#)。

1.13 — 确保为根用户启用 MFA

严重性：重大

Amazon Config 规则：[root-account-mfa-enabled](#)

时间表类型：定期

根账户具有对 Amazon 账户中所有服务和资源的完全访问权限。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 Amazon 网站时，系统会提示他们输入用户名和密码以及 Amazon MFA 设备的验证码。

当您为 root 用户使用虚拟 MFA 时，CIS 建议使用的设备不是个人设备。请改用与任何个人设备分开付费和保护的专用移动设备（平板电脑或手机）。这可降低因设备丢失、设备换购或拥有设备的个人离开公司而导致无法访问 MFA 的风险。

Note

以下区域不支持此控制。

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）。

修复

要将 MFA 添加到根用户，请参阅 IAM 用户指南中的[在中使用 Multi-Factor Authentication \(MFA\)](#)。

1.14 — 确保为根用户启用硬件 MFA

严重性：重大

Amazon Config 规则：[root-account-hardware-mfa-enabled](#)

时间表类型：定期

根账户具有对 Amazon 账户中所有服务和资源的完全访问权限。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 Amazon 网站时，系统会提示他们输入用户名和密码以及 Amazon MFA 设备的验证码。

对于级别 2，CIS 建议您使用硬件 MFA 保护根用户证书。硬件 MFA 的攻击面小于虚拟 MFA。例如，硬件 MFA 不受虚拟 MFA 所在的移动智能手机引入的攻击面影响。

对大量账户使用硬件 MFA 可能会产生物流设备管理问题。如果发生这种情况，请考虑有选择性地对安全性最高的账户实施此第 2 级别的建议。然后，您可以将第 1 级别的建议应用于其余账户。

基于时间的一次性密码 (TOTP) 和通用第二要素 (U2F) 令牌均可作为硬件 MFA 选项。

Note

以下区域不支持此控制。

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)。

修复

要为根用户添加硬件 MFA 设备，请参阅 IAM 用户指南中的[为 Amazon 账户根用户启用硬件 MFA 设备 \(控制台\)](#)。

1.16 — 确保 IAM 策略仅附加到群组或角色

严重性：低

Amazon Config 规则：[iam-user-no-policies-check](#)

时间表类型：触触触触更改

默认情况下，IAM 用户、组和角色没有对 Amazon 资源的访问权限。IAM policy 是向用户、组或角色授予权限的方式。

CIS 建议您将 IAM 策略直接应用于群组和角色，但不适用于用户。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

由亚马逊简单电子邮件服务创建的 IAM 用户是使用内联策略自动创建的。Security Hub 会自动免除这些用户的此控制。

Amazon Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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

要解决此问题，[请创建 IAM 群组](#)并将策略附加到该群组。然后，[将用户添加到群组中](#)。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](#)。

1.20 - 确保已创建支持角色来管理与 Amazon Support 相关的事件

严重性：低

Amazon Config 规则：[iam-policy-in-use](#)

时间表类型：定期

Amazon 提供了可用于事件通知和响应的支持中心，以及技术支持和客户服务。

创建 IAM 角色以允许授权用户通过 SupportAmazon 管理事件。通过实现访问控制的最小权限，IAM 角色将需要适当的 IAM 策略来允许 Support 中心访问，以便管理 Amazon 支持人员的事件。

Note

以下区域不支持此控制。

- 非洲（开普敦）
- 亚太地区（大阪）
- 欧洲（米兰）

修复

要纠正此问题，请创建一个角色以允许授权用户管理 Amazon Support 事件。

创建要用于 Amazon Support 访问的角色

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
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 Amazon 账户”。
4. 对于 Account ID (账户 ID)，输入您希望向其授予对资源的访问权限的 Amazon 账户的 Amazon 账户 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 IAM 用户授予担任该角色的权限。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 Next: Permissions (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 Next: 标签。
9. (可选) 要向角色添加元数据，请以键值对的形式附加标签。

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 Next: 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 Amazon 账户内必须是唯一的。它们不区分大小写。

12. (可选) 对于 Role description (角色描述)，输入新角色的描述。
13. 检查该角色，然后选择 Create role (创建角色)。

1.22 — 确保未创建允许完全 “*: *” 管理权限的 IAM 策略

严重性：高

Amazon Config 规则：[iam-policy-no-statements-with-admin-access](#)

时间表类型：触触触触更改

此控件通过添加带“Effect”: “Allow”有 over 的语句来检查默认版本的 IAM 策略（也称为客户托管策略）是否具有管理员访问权限“Resource”: “*”。 “Action”: “*”如果您的 IAM 策略包含此类语句，则控制会失败。

该控制仅检查您创建的客户托管策略。它不检查内联和Amazon托管策略。

IAM 策略定义了授予用户、群组或角色的一组权限。建议遵循标准安全建议来授予最小权限，即仅授予执行任务所需的权限。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。

应先尽量授予一组具有最小许可的许可，然后根据需要授予额外许可，而不应先授予过于宽松的许可，而后再试图收紧。提供完全管理权限而不是限制用户执行任务所需的最小权限集会将资源暴露给可能有害的操作。

您应该删除带"Effect": "Allow"有 over 语句的 IAM 策略"Resource": "*"。"Action": "*"

Note

Amazon Config应在您使用 Security Security Hub p 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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

要修改您的 IAM 策略使其不允许完整的 "*" 管理权限，请参阅 [IAM 用户指南中的编辑 IAM 策略](#)。

2.1 — 确保 CloudTrail 在所有区域均已启用

严重性：高

Amazon Config 规则：[multi-region-cloudtrail-enabled](#)

时间表类型：定期

此控件检查是否存在至少一条多区域 CloudTrail 跟踪。它还会检查其中至少一条跟踪的ExcludeManagementEventSources参数是否为空。

CloudTrail 是一项服务，用于记录您的账户Amazon的 API 调用并将日志文件传送给您。记录的信息包括 API 调用者的身份、API 调用的时间、API 调用方的源 IP 地址、请求参数和Amazon服务返回的响应元素。CloudTrail 提供账户的Amazon API 调用历史记录，包括通过、Amazon SDKAmazon Web Services Management Console、命令行工具和更高级别的Amazon服务（例如Amazon CloudFormation）进行的 API 调用。

生成的Amazon 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。此外：

- 确保存在多区域跟踪可确保检测到在其他未使用区域中发生的意外活动
- 确保存在多区域跟踪可确保默认情况下为跟踪启用全局服务日志记录，以捕获在 Amazon 全局服务上生成的事件的记录
- 对于多区域跟踪，确保为所有类型的读取/写入配置管理事件可确保记录对 Amazon 账户中的所有资源执行的管理操作

默认情况下，使用创建的 CloudTrail 跟踪Amazon Web Services Management Console是多区域跟踪。

修复

要在中创建新路线 CloudTrail

1. 登录Amazon Web Services Management Console并通过 <https://console.aws.amazon.com/cloudtrail/> 打开主 CloudTrail 机。
2. 如果您 CloudTrail 之前没有使用过，请选择“立即开始”。
3. 选择 Trails (跟踪)，然后选择 Create trail (创建跟踪)。
4. 输入跟踪的名称。

5. 在 Storage location (存储位置) 下, 执行下列操作之一:
 - 要为 CloudTrail 日志创建新的 S3 存储桶, 请选择创建新的 S3 存储桶, 然后输入存储桶的名称。
 - 选择使用现有 S3 存储桶, 然后选择要使用的存储桶。
6. 选择“其他设置”, 然后在“日志文件验证”中选择“启用”即可通过[2.2 — 确保启用 CloudTrail 日志文件验证 \(p. 275\)](#)。
7. 要通过[the section called “2.4 — 确保 CloudTrail 跟踪与亚马逊 CloudWatch 日志集成” \(p. 276\)](#), 必须启用 CloudWatch 日志。
 - a. 在“CloudWatch 日志”下, 选中“启用”复选框。
 - b. 对于日志组, 请执行以下操作之一:
 - 要使用现有的日志组, 请选择 Existing (现有), 然后输入要使用的日志组的名称。
 - 要创建新的日志组, 请选择 New (新建), 然后输入要创建的日志组的名称。
 - c. 对于 IAM role (IAM 角色), 执行以下操作之一:
 - 要使用现有角色, 请选择 Existing (现有), 然后从下拉列表中选择角色。
 - 要创建新角色, 请选择新建, 然后输入要创建的角色名称。将为新角色分配一个策略以授予所需的权限。

要查看授予该角色的权限, 请展开策略文档。
8. 选择 Create (创建)。

要在中更新现有跟踪, 请执行以下操作 CloudTrail

1. 登录 Amazon Web Services Management Console 并通过 <https://console.aws.amazon.com/cloudtrail/> 打开主 CloudTrail 控制台。
2. 选择 Trails (跟踪)。
3. 在 Name (名称) 列中选择跟踪的名称。
4. 根据需要更新跟踪配置。

要更新特定部分中的配置, 请执行以下操作:

 - a. 为该分区选择“编辑”。
 - b. 对配置进行必要的更新。
 - c. 选择 Save changes (保存更改)。

2.2 — 确保启用 CloudTrail 日志文件验证

严重性: 中

Amazon Config 规则: [cloud-trail-log-file-validation-enabled](#)

时间表类型: 定期

CloudTrail 日志文件验证会创建一个数字签名的摘要文件, 其中包含 CloudTrail 写入 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 提交后是否已更改、删除或未更改, 可以确定日志文件是否已更改、删除或未更改。

CIS 建议您在所有路径上启用文件验证。启用日志文件验证可对 CloudTrail 日志进行额外的完整性检查。

修复

启用 CloudTrail 日志文件验证

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。

- ## 2.3 — 确保上传到的 S3 存储桶 CloudTrail 日志不可公开访问

Amazon Config规则：无（自定义Security Hub规则）

CloudTrail 记录您账户中每次 API 调用的记录。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攻击者识别受影响账户的使用或配置中的弱点。

如果您将日志聚合到单个集中式 S3 存储桶中，则 Security Hub 仅对集中式 S3 存储桶所在的账户和区域运行检查。对于其他账户和区域，控制状态为无数据。

如果存储桶可以公开访问，则检查会生成一个失败的调查结果。

删除对于 Amazon S3 存储桶的公有访问权限

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 请选择存放您的 CloudTrail 存储桶的存储桶存储桶存储桶存储桶存储桶存储桶存储桶存储桶存储桶
3. 选择 Permissions (权限)，然后选择 Public access settings (公有访问权限) 设置。
4. 选择 Edit (编辑)，选择所有四个选项，然后选择 Save (保存)。
5. 如果出现提示，输入 **confirm**，然后选择 Confirm (确认)。

严重性：低

Amazon Config 规则: `cloud-trail-cloud-watch-logs-enabled`

CloudTrail 是一项 Web 服务，Amazon 用于记录在给定账户中进行的 API 调用。记录的信息包括 API 调用者的身份、API 调用的时间、API 调用者的源 IP 地址、请求参数以及 Amazon 服务返回的响应元素。

CloudTrail 使用 Amazon S3 进行日志文件存储和传输，因此日志文件可以持久存储。除了在指定的 Amazon S3 存储桶中捕获 CloudTrail 日志以进行长期分析外，您还可以通过配置将日志发送 CloudTrail 到 CloudWatch 日志来执行实时分析。

对于在账户的所有区域中启用的跟踪，CloudTrail 将来自所有这些区域的日志文件发送到 CloudWatch 日志日志组。

CIS 建议您将 CloudTrail 日志发送到 CloudWatch 日志。

Note

本建议的目的是确保账户活动得到捕获、监控和适当的警报。CloudWatch 日志是使用 Amazon 服务实现此目的的本机方法，但不排除使用替代解决方案。

将 CloudTrail 日志发送到 CloudWatch 日志有助于根据用户、API、资源和 IP 地址记录实时和历史活动。它提供了为异常或敏感账户活动建立警报和通知的机会。

修复

确保 CloudTrail 跟踪与 CloudWatch 日志集成

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
 2. 选择 Trails (跟踪)。
 3. 在“日志CloudWatch日志”组列中选择没有值的跟踪。
 4. 向下滚动到“日CloudWatch志”部分，然后选择“编辑”。
 5. 选中 Enabled (启用) 复选框。
 6. 对于日志组，请执行以下操作之一：
 - 要使用现有的日志组，请选择 Existing (现有)，然后输入要使用的日志组的名称。
 - 要创建新的日志组，请选择 New (新建)，然后输入要创建的日志组的名称。
 7. 对于 IAM role (IAM 角色)，执行以下操作之一：
 - 要使用现有角色，请选择 Existing (现有)，然后从下拉列表中选择角色。
 - 要创建新角色，请选择新建，然后输入要创建的角色名称。将为新角色分配一个策略以授予所需的权限。
- 要查看授予该角色的权限，请展开策略文档。
8. 选择 Save changes (保存更改)。

有关更多信息，请参阅 [《Amazon CloudTrail用户指南》中的使用控制台配置 CloudWatch 日志监控](#)。

2.5 — 确保Amazon Config已启用

严重性：中

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

Amazon Config 是一种 Web 服务，可对您账户中支持的 Amazon 资源执行配置管理，并为您提供日志文件。记录的信息包括配置项 (Amazon 资源)、配置项之间的关系 (Amazon 资源) 以及资源之间的任何配置更改。

CIS 建议您在所有区域Amazon Config中启用。Amazon Config 捕获的 Amazon 配置项历史记录可用于安全分析、资源更改跟踪和合规性审计。

Note

CIS 2.5 要求Amazon Config在您使用Security Hub 的所有区域中启用该功能。

由于 Security Hub 是一项区域服务，因此对此控制执行的检查仅检查该账户的当前区域。它不会检查所有区域。

您还必须记录全局资源，以便能在每个区域中检查针对全局资源的安全检查。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。

您也可以考虑在未启用全球资源记录的区域禁用这些 IAM 控件 (CIS 1.2、CIS 1.3、CIS 1.4、CIS 1.16、CIS 1.22)。由于 IAM 是一项全球服务，因此 IAM 资源将仅记录在启用全球资源记录的区域中。

要运行此检查，Security Hub 会执行自定义逻辑，以执行 [CISAmazon Foundations Benchmark v1.2](#) 中为其规定的审计步骤。Security Hub 还要求在每个区域记录全球资源，因为 Security Hub 是一项区域性服务，会逐个区域执行安全检查。

修复

配置 Amazon Config 设置

1. 通过以下网址打开 Amazon Config 控制台：<https://console.aws.amazon.com/config/>。
2. 选择要在其中配置 Amazon Config 的区域。
3. 如果您 Amazon Config 之前没有使用过，请参阅 Amazon Config 开发者指南中的 [入门](#)。
4. 从菜单导航到“设置”页面，然后执行以下操作：
 - 选择 Edit (编辑)。
 - 在“要记录的资源类型”下，选择“记录该区域支持的所有资源”和“包括全球资源”(例如 Amazon IAM 资源)。
 - 在“数据保留期”下，选择 Amazon Config 数据的默认保留期，或指定自定义保留期。
 - 在“Amazon Config 角色”下，选择“创建 Amazon Config 服务相关角色”或“从账户中选择一个角色”，然后选择要使用的角色。
 - 在 Amazon S3 bucket (Amazon S3 存储桶) 下面，指定要使用的存储桶，或者创建存储桶并包括前缀 (可选)。
 - 在 Amazon SNS 主题，从账户中选择一个 Amazon SNS 主题，或创建一个。有关 Amazon SNS 的更多信息，请参阅 [Amazon Simple Notification Service 入门指南](#)。
5. 选择 Save (保存)。

有关使用 from Amazon Config 的更多信息 Amazon Command Line Interface，请参阅 Amazon Config 开发者指南 Amazon Config 中的 [开启](#)。

您还可以使用 Amazon CloudFormation 模板自动执行这一过程。有关更多信息，请参阅 Amazon CloudFormation 用户指南中的 [Amazon CloudFormation StackSets 示例模板](#)。

2.6 — 确保在 S3 存储桶上启用 CloudTrail S3 存储区访问日志记录

严重性：低

Amazon Config 规则：无 (自定义 Security Hub 规则)

时间表类型：定期

Amazon S3 存储桶访问日志会生成一个日志，其中包含对您的 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 CloudTrail S3 存储桶上启用存储区访问日志记录。

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 首先使用自定义逻辑来查找存储 CloudTrail 日志的存储桶，然后使用 Amazon Config 托管规则检查日志记录是否已启用。

如果您将日志聚合到单个集中式 S3 存储桶中，则 Security Hub 仅对集中式 S3 存储桶所在的账户和区域运行检查。对于其他账户和区域，控制状态为无数据。

如果存储桶可以公开访问，则检查会生成一个失败的调查结果。

修复

启用 S3 存储桶访问日志记录

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 选择用于的存储桶 CloudTrail。
3. 请选择属性。
4. 选择 Server access logging (服务器访问日志记录)，然后选择启用日志记录。
5. 从 Target bucket (目标存储桶) 列表选择一个存储桶 (并可选择输入前缀)。
6. 选择 Save (保存)。

2.7 — 确保使用静态加密 CloudTrail 日志 Amazon KMS keys

严重性：中

Amazon Config 规则：[cloud-trail-encryption-enabled](#)

时间表类型：定期

CloudTrail 是一项 Web 服务，用于记录账户的 Amazon API 调用，并根据 IAM 策略将这些日志提供给用户和资源。Amazon Key Management Service (Amazon KMS) 是一项托管服务，可帮助创建和控制用于加密账户数据的加密密钥，并使用硬件安全模块 (HSM) 来保护加密密钥的安全。

您可以配置 CloudTrail 日志以利用服务器端加密 (SSE) 和 KMS 密钥来进一步保护 CloudTrail 日志。

CIS 建议您将配置 CloudTrail 为使用 SSE-KMS。

配置 CloudTrail 为使用 SSE-KMS 可对日志数据提供额外的机密性控制，因为给定用户必须对相应的日志存储桶拥有 S3 读取权限，并且必须获得 KMS 密钥策略的解密权限。

Note

如果您正在使用 Amazon Control Tower，则可以使用加密您的 CloudTrail 日志 Amazon KMS key。有关更多信息，请参阅《Amazon Control Tower 用户指南》Amazon KMS keys 中的 [可选配置](#)

修复

启用 CloudTrail 日志加密

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
2. 选择 Trails (跟踪)。
3. 选择要更新的跟踪。
4. 在 Storage location (存储位置) 下，选择铅笔图标以编辑设置。
5. 对于 Encrypt log files with SSE-KMS (使用 SSE-KMS 加密日志文件)，选择 Yes (是)。
6. 对于 Create a new KMS key (创建新的 KMS 密钥)，执行以下操作之一：
 - 要创建密钥，请选择 Yes (是)，然后在 KMS key (KMS 密钥) 字段中输入密钥的别名。密钥在与存储桶相同的区域中创建。
 - 要使用现有密钥，请选择 No (否)，然后从 KMS key (KMS 密钥) 列表中选择密钥。

Note

Amazon KMS 密钥和 S3 存储桶必须位于同一区域。

7. 选择 Save (保存)。

您可能需要修改的策略 CloudTrail 才能成功与您的 KMS 密钥交互。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用[Amazon KMS 托管式密钥 \(SSE-KMS\) 加密 CloudTrail 日志文件](#)。

2.8 — 确保启用客户创建的 KMS 密钥的轮换

严重性：中

Amazon Config 规则：[cmk-backing-key-rotation-enabled](#)

时间表类型：定期

Amazon KMS 允许客户轮换备用密钥，后备密钥是存储在中的 Amazon KMS 密钥材料，与 KMS 密钥的密钥 ID 绑定。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

启用 KMS 密钥轮换

1. 在 Amazon KMS <https://console.aws.amazon.com/kms> 打开 控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector (区域选择器)。
3. 选择 Customer managed keys (客户托管密钥)。
4. 在 Alias (别名) 列中选择要更新的密钥的别名。
5. 选择 Key rotation (密钥轮换)。
6. 选择 L 每年自动轮换此 KMS 密钥，然后选择 Save (保存)。

2.9 — 确保在所有 VPC 中启用 VPC 流量记录

严重性：中

Amazon Config 规则：[vpc-flow-logs-enabled](#)

时间表类型：定期

利用 VPC 流日志这项功能，您可以捕获有关传入和传出您的 VPC 中网络接口的 IP 流量的信息。创建流日志后，您可以在 CloudWatch 日志中查看和检索其数据。

CIS 建议您为 VPC 的数据包拒绝启用流量记录。流日志提供对穿过 VPC 的网络流量的可见性，并可在安全工作流程中检测异常流量或见解。

修复

启用 VPC 流日志记录

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 选择 Your VPCs (您的 VPC)。
3. 选择要更新的 VPC。
4. 选择页面底部的 Flow Logs (流日志) 选项卡。
5. 选择 Create flow log (创建流日志)。
6. 对于 Filter (筛选条件)，选择 Reject (拒绝)。
7. 对于 Destination log group (目标日志组)，选择要使用的日志组。
8. 对于 IAAAAAAM 角色，选择要使用的 IAAAAAAA
9. 选择 Create (创建)。

3.1 — 确保针对未授权的 API 调用存在日志指标筛选条件和警报

严重性：低

Amazon Config规则：无（自定义Security Hub 规则）

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。

CIS 建议您创建指标筛选器并对未经授权的 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 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。

2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.errorCode="*UnauthorizedOperation") || ($.errorCode="AccessDenied*") }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标s。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选条件，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onget (指定指标和条件) 下，执行以下操作：
 - a. 在“指标”下，在“统计数据”中，选择“平均值”。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入**1**。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.1-UnauthorizedAPICalls**。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 Create alarm (创建警报)。

3.2 — 确保在没有 MFA 的情况下 Amazon Web Services Management Console 登录时存在日志指标筛选条件和警报

严重性：低

Amazon Config规则：无 (自定义 Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 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 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查 FAILED 结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 `ListSubscriptionsByTopic`。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。

5. 在定义模式下，执行以下操作：

- a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes")  
  && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin =  
    "Success") }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。

- c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标s。
d. 对于 Metric value (指标值)，输入 **1**。
e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选条件，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。

10. 在 C onget (指定指标和条件) 下，执行以下操作：

- a. 在 Metails (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
b. 在“条件”下，为“阈值”选择静态。
c. 对于“定义警报条件”，选择“大于/等于”。
d. 在定义阈值中，输入**1**。
e. 选择 Next (下一步)。

11. 在配置操作下，执行以下操作：

- a. 在“警报状态触发器”下，选择“警报中”。
b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
d. 选择 Next (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-3.2-ConsoleSigninWithoutMFA**。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 Create alarm (创建警报)。

3.3 — 确保存在使用根用户的日志指标筛选条件和警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

您可以实时监控 API 调用，将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报。

CIS 建议您为 root 用户登录尝试创建指标筛选条件和警报。通过监控 root 用户的登录，可以了解完全特权账户的使用情况，并有机会减少该账户的使用。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.3 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。

在以下情况下，检查 FAILED 结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 ListSubscriptionsByTopic。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标s。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选条件，请选中右上方的复选框。
9. 选择 Create Alarm (创建告警)。
10. 在 C onget (指定指标和条件) 下，执行以下操作：
 - a. 在 Metails (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入**1**。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 Next (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，**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 Create alarm (创建警报)。

3.4 — 确保存在针对 IAM 策略更改的日志指标筛选条件和警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。

CIS 建议您为 IAM 策略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。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.4 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

请注意，警报按名称检查特定的 API 操作。其中一项操作是DeletePolicy。警报不检查呼叫是否来自 IAM。因此，在 Auto Scaling 调用时也会触发警报DeletePolicy。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#)中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=DeleteGroupPolicy) || ($.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)}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onget (指定指标和条件) 下，执行以下操作：
 - a. 在“指标”下，在“统计数据”中，选择“平均值”。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入**1**。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.4-IAMPolicyChanges**。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 Create alarm (创建警报)。

3.5 — 确保存在日志指标筛选条件和 CloudTrail 配置更改警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。

CIS 建议您为 CloudTrail配置设置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账户中活动的持续可见性。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.5 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查 FAILED 结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 `ListSubscriptionsByTopic`。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=CreateTrail) || ($.eventName=UpdateTrail) ||  
  ($.eventName>DeleteTrail) || ($.eventName=StartLogging) ||  
  ($.eventName=StopLogging) }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。

- c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。

10. 在 Onget (指定指标和条件) 下，执行以下操作：

- a. 在 Metrics (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的 [统计数据](#)。
- b. 在“条件”下，为“阈值”选择静态。
- c. 对于“定义警报条件”，选择“大于/等于”。
- d. 在定义阈值中，输入 **1**。
- e. 选择 Next (下一步)。

11. 在配置操作下，执行以下操作：

- a. 在“警报状态触发器”下，选择“警报中”。
- b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
- c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
- d. 选择 Next (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-3.5-CloudTrailChanges**。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 Create alarm (创建警报)。

3.6 — 确保存在日志指标筛选条件和 Amazon Web Services Management Console 身份验证失败警报

严重性：低

Amazon Config 规则：无 (自定义 Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 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 使用自定义逻辑来执行 [CIS Amazon Foundations Benchmark v1.2](#) 中为控制 3.6 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查 FAILED 结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 ListSubscriptionsByTopic。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{(($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication"))}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。

- c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 1。
 - e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 Onget (指定指标和条件) 下，执行以下操作：
 - a. 在 Metrics (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入 1。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.6-ConsoleAuthenticationFailure**。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 Create alarm (创建警报)。

3.7 — 确保存在禁用或计划删除客户管理密钥的日志指标筛选器和警报

严重性：低

Amazon Config规则：无 (自定义 Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。

CIS 建议您为状态已更改为禁用或计划删除的客户管理的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 使用自定义逻辑来执行 [CIS Amazon Foundations Benchmark v1.2](#) 中为控制 3.7 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，则控件也会失败 kms.amazonaws.com。

Note

当 Security Hub 对此控件执行检查时，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。多区域路线也可能位于不同的区域。

在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#)中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) ||  
  ($.eventName=ScheduleKeyDeletion)) }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。

- c. 对于 Metric name (指标名称) , 为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值) , 输入 **1**。
 - e. 选择 Next (下一步) 。
7. 在“查看并创建”下, 验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡, 然后选择刚创建的指标筛选器。

要选择指标筛选器, 请选中右上方的复选框。
 9. 选择 Create Alarm (创建告警) 。
 10. 在 C onfig (指定指标和条件) 下, 执行以下操作 :
 - a. 在 Metrics (指标算法) 保留默认值。有关可用统计数据的更多信息, 请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下, 为“阈值”选择静态。
 - c. 对于“定义警报条件”, 选择“大于/等于”。
 - d. 在定义阈值中, 输入**1**。
 - e. 选择 Next (下一步) 。
 11. 在配置操作下, 执行以下操作 :
 - a. 在“警报状态触发器”下, 选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下, 选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Sname (向发送通知) , 输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.7-DisableOrDeleteCMK**。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 Create alarm (创建警报)。

3.8 — 确保存在针对 S3 存储桶策略更改的日志指标筛选条件和警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报, 您可以对 API 调用进行实时监控。

CIS 建议您为 S3 存储桶策略的更改创建指标筛选条件和警报。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 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.8 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 对此控件执行检查时, 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。多区域路线也可能位于不同的区域。
在以下情况下, 检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 `ListSubscriptionsByTopic`。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventSource=s3.amazonaws.com) && (( $.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) || ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) || ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) || ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) || ($.eventName=DeleteBucketReplication)) }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。

- c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
- d. 对于 Metric value (指标值)，输入 **1**。
- e. 选择 Next (下一步)。

7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onfig (指定指标和条件) 下，执行以下操作：
 - a. 在“指标”下，在“统计数据”中，选择“平均值”。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入1。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Sname (向发送通知)，输入您在上一流程中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.8-S3BucketPolicyChanges**。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 Create alarm (创建警报)。

3.9 — 确保存在日志指标筛选条件和Amazon Config配置更改警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。

CIS 建议您为 Amazon Config 配置设置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账户中配置项的持续可见性。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CIS Amazon Foundations Benchmark v1.2](#) 中为控制 3.9 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查 FAILED 结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限 `ListSubscriptionsByTopic`。否则，Security Hub 会生成控件的 WARNING 调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：

- a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{(($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) || ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder)))}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
 7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onget (指定指标和条件) 下，执行以下操作：
 - a. 在 Metails (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入1。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Send to (发送通知)，请输入您在上一步中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.9-AmazonConfigChanges**。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 Create alarm (创建警报)。

3.10 — 确保存在日志指标筛选条件和安全组更改警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 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不会意外公开 资源和服务。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.10 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。

在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=AuthorizeSecurityGroupIngress) || ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) || ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) || ($.eventName>DeleteSecurityGroup) }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
 7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。
 9. 选择 Create Alarm (创建告警)。
 10. 在 Configure (指定指标和条件) 下，执行以下操作：
 - a. 在 Metrics (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的 [统计数据](#)。

- b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入1。
 - e. 选择 Next (下一步) 。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Send to (发送通知) ，请输入您在上一步中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.10-SecurityGroupChanges**。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 Create alarm (创建警报)。

3.11 — 确保存在网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。NACL 用作无状态的数据包筛选器，可用于控制 VPC 中子网的传入和传出流量。

CIS 建议您创建指标筛选器并针对 NACL 的更改发出警报。监控此类更改有助于确保不会意外公开 Amazon 资源和服务。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.11 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。
在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#)中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：

- a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=CreateNetworkAcl) || ($.eventName=CreateNetworkAclEntry) || ($.eventName>DeleteNetworkAcl) || ($.eventName>DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) || ($.eventName=ReplaceNetworkAclAssociation) }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。

 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
 7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 Onget (指定指标和条件) 下，执行以下操作：
 - a. 在 Metails (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入 **1**。

- e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Send to (发送通知)，请输入您在上一步中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.11-NetworkACLChanges**。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 Create alarm (创建警报)。

3.12 — 确保存在日志指标筛选条件和网络网关变更警报

严重性：低

Amazon Config规则：无 (自定义Security Hub 规则)

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 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 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.12 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。

在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。

2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#)中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=CreateCustomerGateway) || ($.eventName>DeleteCustomerGateway) ||  
  ($.eventName=AttachInternetGateway) || ($.eventName>CreateInternetGateway) ||  
  ($.eventName>DeleteInternetGateway) || ($.eventName=DetachInternetGateway) }
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onget (指定指标和条件) 下，执行以下操作：
 - a. 在 Metails (指标算法) 保留默认值。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入**1**。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。

- b. 在 Select an SNS topic (选择 SNS 主题) 下, 选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Send to (发送通知), 请输入您在上一步中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.12-NetworkGatewayChanges**。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 Create alarm (创建警报)。

3.13 — 确保存在路由表更改的日志指标筛选条件和警报

严重性：低

Amazon Config规则：无（自定义Security Hub 规则）

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报, 您可以对 API 调用进行实时监控。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所有 VPC 流量都流经预期路径。

为了运行此检查, Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.13 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 对此控件执行检查时, 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。多区域路线也可能位于不同的区域。
在以下情况下, 检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下, 检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报, 当前账户必须拥有引用的 Amazon SNS 主题, 或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则, Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#)中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：
 - a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) ||  
  ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation)  
  || ($.eventName>DeleteRouteTable) || ($.eventName>DeleteRoute) ||  
  ($.eventName=DisassociateRouteTable)}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
 7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onfig (指定指标和条件) 下，执行以下操作：
 - a. 在“指标”下，在“统计数据”中，选择“平均值”。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入 **1**。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Send to (发送通知)，请输入您在上一步中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.13-RouteTableChanges**。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 Create alarm (创建警报)。

3.14 — 确保 VPC 更改存在日志指标筛选条件和警报

严重性：低

Amazon Config规则：无（自定义Security Hub 规则）

时间表类型：定期

通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选条件和警报，您可以对 API 调用进行实时监控。您可以在一个账户中拥有多个 VPC，并在两个 VPC 之间创建对等连接，从而使网络流量能够在 VPC 之间路由。

CIS 建议您为 VPC 的变化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。

为了运行此检查，Security Hub 使用自定义逻辑来执行 [CISAmazon Foundations Benchmark v1.2](#) 中为控制 3.14 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 对此控件执行检查时，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。多区域路线也可能位于不同的区域。

在以下情况下，检查FAILED结果是不明的：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

在以下情况下，检查会导致控制状态为：NO_DATA

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用获得对 Amazon SNS 主题的访问权限ListSubscriptionsByTopic。否则，Security Hub 会生成控件的WARNING调查结果。

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条件警报。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题接收所有 CIAmazon 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，设置适用于所有地区的活动 CloudTrail。为此，请按照[the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#)中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您可以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. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Log groups (日志组)。
3. 选中与您创建的 CloudTrail 跟踪关联的 CloudWatch 日志日志组对应的复选框。
4. 在操作中，选择创建指标筛选条件。
5. 在定义模式下，执行以下操作：

- a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

```
{ ($.eventName=CreateVpc) || ($.eventName>DeleteVpc) ||  
  ($.eventName=ModifyVpcAttribute) || ($.eventName=AcceptVpcPeeringConnection)  
  || ($.eventName=CreateVpcPeeringConnection)  
  || ($.eventName>DeleteVpcPeeringConnection) ||  
  ($.eventName=RejectVpcPeeringConnection) || ($.eventName=AttachClassicLinkVpc)  
  || ($.eventName=DetachClassicLinkVpc) || ($.eventName=DisableVpcClassicLink) ||  
  ($.eventName=EnableVpcClassicLink)}
```

- b. 选择 Next (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 日志指标筛选器使用相同的命名空间，则所有 CIS Benchmark 指标将组合在一起。
 - c. 对于 Metric name (指标名称)，为其输入指标名称。记住指标的名称。您需要在创建警报时选择指标。
 - d. 对于 Metric value (指标值)，输入 **1**。
 - e. 选择 Next (下一步)。
 7. 在“查看并创建”下，验证您为新指标筛选条件提供的信息。然后选择创建指标筛选条件。
 8. 选择 Metrics (指标筛选器) 选项卡，然后选择刚创建的指标筛选器。

要选择指标筛选器，请选中右上方的复选框。

9. 选择 Create Alarm (创建告警)。
10. 在 C onfig (指定指标和条件) 下，执行以下操作：
 - a. 在“指标”下，在“统计数据”中，选择“平均值”。有关可用统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的[统计数据](#)。
 - b. 在“条件”下，为“阈值”选择静态。
 - c. 对于“定义警报条件”，选择“大于/等于”。
 - d. 在定义阈值中，输入 **1**。
 - e. 选择 Next (下一步)。
11. 在配置操作下，执行以下操作：
 - a. 在“警报状态触发器”下，选择“警报中”。
 - b. 在 Select an SNS topic (选择 SNS 主题) 下，选择 Select an existing SNS topic (选择现有的 SNS 主题)。
 - c. 对于 Send to (发送通知)，请输入您在上一步中创建的 SNS 主题名称。
 - d. 选择 Next (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-3.14-VPCHanges**。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 Create alarm (创建警报)。

4.1 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 22

严重性：高

Amazon Config 规则：[restricted-ssh](#)

时间表类型：触触触触更改

安全组为 Amazon 资源提供传入和传出网络流量的有状态筛选。

CIS 建议任何安全组都不允许对端口 22 进行不受限制的入口访问。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。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

修复

对与 VPC 关联的每个安全组执行以下步骤。

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在左侧窗格中，选择安全组。
3. 选择一个安全组。
4. 在页面底部，选择 Inbound Rules (入站规则) 选项卡。
5. 选择 Edit rules (编辑规则)。
6. 确定允许通过端口 22 进行访问的规则，然后选择 X 将其删除。
7. 选择 Save rules (保存规则)。

4.2 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 3389

严重性：高

Amazon Config 规则：[restricted-common-ports](#)

时间表类型：触触触触更改

关联的 Amazon Config 托管规则的名称是 restricted-common-ports。但是，创建的规则使用名称 restricted-rdp。

安全组为 Amazon 资源提供传入和传出网络流量的有状态筛选。

CIS 建议任何安全组都不允许对端口 3389 进行不受限制的入口访问。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。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

修复

对与 VPC 关联的每个安全组执行以下步骤。

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在左侧窗格中，选择安全组。
3. 选择一个安全组。
4. 在页面底部，选择 Inbound Rules (入站规则) 选项卡。
5. 选择 Edit rules (编辑规则)。
6. 确定允许通过端口 3389 进行访问的规则，然后选择 X 将其删除。
7. 选择 Save rules (保存规则)。

4.3 — 确保每个 VPC 的默认安全组限制所有流量

严重性：高

Amazon Config 规则：[vpc-default-security-group-closed](#)

时间表类型：触触触触更改

VPC 会生成默认安全组，它的初始设置将拒绝所有入站数据流、允许所有出站数据流、以及允许在分配到您的安全组的实例间的所有数据流。如果您在启动实例时未指定安全组，实例将自动关联到默认安全组。安全组为 Amazon 资源提供传入和传出网络流量的有状态筛选。

CIS 建议默认安全组限制所有流量。

更新要确保合规的每个区域中默认 VPC 的默认安全组。任何新的 VPC 都自动包含默认安全组，您需要对该默认安全组进行修复，以遵守此建议。

Note

在实施此建议时，您可以使用启用的 VPC 流量日志来确定系统正常运行所需的最低权限端口访问权限。[the section called “2.9 — 确保在所有 VPC 中启用 VPC 流量记录” \(p. 280\)](#) VPC 流量记录可以记录当前安全组下发生的所有数据包接受和拒绝。

将所有 VPC 默认安全组配置为限制所有流量，鼓励开发最低权限安全组并谨慎地将 Amazon 资源放入安全组。这反过来又减少了这些资源的暴露量。

修复

更新默认安全组以限制所有访问

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 查看默认安全组详细信息以了解分配给它们的资源。
3. 为资源创建一组最小权限安全组。
4. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
5. 在 Amazon EC2 控制台上，将使用默认安全组的资源的安全组更改为您创建的最低权限安全组。
6. 对于每个默认安全组，请选择 Inbound (入站) 选项卡并删除所有入站规则。
7. 对于每个默认安全组，请选择 Outbound (出站) 选项卡并删除所有出站规则。

有关更多信息，请参阅 Amazon VPC 用户指南中的[使用安全组](#)。

您可能要禁用的 CISAmazon 基础基准测试控件

对于 CIS Foundation Benchmark 标准，以下是您可能希望禁用的一些特定控件。

CISAmazon 基金会基准 2.7 控制

此控件涉及使用 Amazon KMS 加密 CloudTrail 跟踪日志。如果您在集中式日志账户中记录这些跟踪，则只需要在进行集中记录的账户和区域中运行此控件。

CISAmazon 基金会基准 1.1.14、1.20 和 2.5 控制

要节省 Amazon Config 的成本，您可以禁用所有区域（有一个区域除外）中的全局资源的记录，然后禁用处理所有区域（运行全局记录的区域除外）中的全局资源的这些控件。

如果您禁用这些 1.x 控件并禁用特定区域中的全局资源记录，则还应禁用 2.5。这是因为 2.5 需要全局资源记录才能通过。

独联体 Amazon 基金会基准 1.1、3.1-3.14

您可能更喜欢使用亚马逊 GuardDuty 进行异常检测，而不是 CloudWatch 警报，因为警报可能会很吵。

如果是，则可以禁用这些控件，这些控件侧重于 CloudWatch 警报。

CISAmazon Foundations Security Hub 不支持的安全检查

Security Hub 中的 CIS Foundations Benchmark 标准不支持以下规则，因为它们无法以自动方式进行评估。Security Hub 侧重于自动安全检查。

- 1.15 — 确保 Amazon 账户中已注册安全问题
- 1.17 — 保留当前的联系方式
- 1.18 — 确保安全联系人信息已注册
- 1.19 — 确保使用 IAM 实例角色从实例访问 Amazon 资源
- 1.21 — 在初始用户设置期间，请勿为所有拥有控制台密码的 IAM 用户设置访问密钥
- 4.4 — 确保 VPC 对等的路由表是“最低访问权限”

支付卡行业数据安全标准 (PCI DSS)

Security Hub 中的支付卡行业数据安全标准 (PCI DSS) 由一组组成 Amazon 安全最佳实践控制。每个控制适用于特定的 Amazon 资源，并与一个或多个 PCI DSS 3.2.1 版要求相关。PCI DSS 要求可能与多个控制相关。每个 PCI DSS 控制的详细信息页面列出了与该控制相关的特定 PCI DSS 要求。请参阅 [the section called “查看有关标准的详细信息” \(p. 254\)](#)。

Security Hub 中的 PCI DSS 合规性标准旨在帮助您完成正在进行的 PCI DSS 安全活动。这些控制无法验证您的系统是否符合 PCI DSS 标准。它们既不能替代内部工作，也无法保证您会通过 PCI DSS 评估。Security Hub 不会检查需要手动收集证据的过程控制。

目前，Security Hub 将控制范围限定在账户级别。建议您在所有具有存储、处理和/或传输持卡人数据的资源的账户中启用这些控制。

该标准已通过验证 Amazon 安全保障服务有限责任公司 (AmazonSAS)，这是一个由合格安全评估员 (QSA) 组成的团队，经认证可提供 PCI DSS 安全标准委员会 (PCI SSC) 的 PCI DSS 指导和评估。AmazonSAS 已确认自动检查可以帮助客户为 PCI DSS 评估做准备。

目录

- [PCI DSS 控制所需的 Amazon Config 资源 \(p. 311\)](#)
- [PCI DSS 控制 \(p. 311\)](#)
- [您可能希望禁用的 PCI DSS 控件 \(p. 360\)](#)

PCI DSS 控制所需的 Amazon Config 资源

PCI DSS 控制对以下资源进行检查。对于 Amazon Security Hub 要准确报告所有控制措施的调查结果，您必须在中启用对这些资源的记录 Amazon Config。

- 拥有 Amazon 账户
- AWS::AutoScaling::AutoScalingGroup
- AWS::CloudTrail::Trail
- AWS::CodeBuild::Project
- AWS::DMS::ReplicationInstance
- AWS::EC2::EIP
- AWS::EC2::Instance
- AWS::EC2::SecurityGroup
- AWS::EC2::Volume
- AWS::EC2::VPC
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::IAM::Policy
- AWS::IAM::User
- AWS::KMS::Key
- AWS::Lambda::Function
- AWS::RDS::DBInstance
- AWS::RDS::DBSnapshot
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::SageMaker::NotebookInstance
- AWS::SSM::AssociationCompliance
- AWS::SSM::PatchCompliance

PCI DSS 控制

Security Hub 中的 PCI DSS 支持以下控件。对于每个控制，该信息包括严重性、资源类型、Amazon Config 规则和修复步骤。

[PCI。AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用运行状况检查

严重性：低

资源类型：AWS::AutoScaling::AutoScalingGroup

Amazon Config 规则：[autoscaling-group-elb-healthcheck-required](#)

Schedule 类型：已触发更改

参数：None (无)

此控件检查与负载均衡器关联的 Auto Scaling 组是否正在使用 Elastic Load Balancing 运行状况检查。

PCI DSS 不需要使用负载均衡或高可用性配置。不过，该检查符合 Amazon 最佳实践。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 2.2：为所有系统组件制定配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。

使用负载均衡复制系统可以提供高可用性，并且是一种减轻 DDoS 事件影响的方法。

这是一种用于实施系统强化配置的方法。

修复

启用 Elastic Load Balancing 运行状况检查

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格的 Auto Scaling 下，选择 Auto Scaling 组。
3. 要从列表中选择群组，请选择右边的复选框。
4. 从 Actions (操作) 中，选择 Edit (编辑)。
5. 对于运行状况检查类型，请选择 ELB。
6. 对于运行状况检查宽限期，输入 **300**。
7. 选择 Save (保存)。

有关在 Auto Scaling 组中使用负载均衡器的更多信息，请参阅[Amazon EC2 Auto Scaling 用户指南](#)。

[PCI。CloudTrail1] CloudTrail 日志应使用静态加密Amazon KMS keys

合规性严重性 中

资源类型：AWS::CloudTrail::Trail

Amazon Config 规则：[cloud-trail-encryption-enabled](#)

Schedule 类型：定期

参数：None (无)

此控件检查是否 Amazon CloudTrail 配置为使用服务器端加密 (SSE) Amazon KMS key 加密。

如果仅使用默认加密选项，您可以选择禁用该检查。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 3.4：无论存储在何处（包括便携式数字媒体、备份媒体和日志），主账号 (PAN) 都无法读取。

如果您正使用 Amazon 处理和存储 PAN 的服务，您的 CloudTrail 日志应该在静态时加密。加密日志可确保如果日志捕获 PAN，则 PAN 受到保护。

默认情况下，由传送的日志文件 CloudTrail 使用具有 Amazon S3 托管加密密钥 (SSE-S3) 的 Amazon 服务器端加密对您的 S3 存储桶进行加密。请参阅[Amazon Service 用户指南](#)。

您可以配置 CloudTrail 日志利用客户管理的密钥来进一步保护 CloudTrail 日志。

这些是用于使 PAN 不可读的方法。

修复

要修复此问题，请为您的启用加密 CloudTrail 日志文件。

有关如何加密的详细信息，CloudTrail 使用以下方式记录文件 Amazon KMS 托管密钥 (SSE-KMS)，请参阅[加密 CloudTrail 使用以下方式记录文件 Amazon KMS—托管密钥 \(SSE-KMS\)](#)在 Amazon CloudTrail 用户指南。

[PCI。CloudTrail2] CloudTrail 应启用

合规性严重性 高

资源类型：Amazon 帐户

Amazon Config 规则：[cloudtrail-enabled](#)

类型：Schedule 定期

参数：None (无)

此控件检查是否 CloudTrail 已在您的中启用 Amazon 帐户。

不过，某些 Amazon 服务不会为所有 API 和事件启用日志记录。除了 CloudTrail 并在中查看每项服务的文档[CloudTrail 支持的服务和集成](#)。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求关联：

PCI DSS 10.1：实施审计跟踪，将对系统组件的所有访问权限链接到每个单独的用户。

通过启用 CloudTrail，Event History 为您提供 90 天随时可用的事件和审计记录，供每个用户访问系统组件。

您可以在中找到用户的身份 `eventSource` 部分 CloudTrail 日志。

PCI DSS 10.2.1：对所有系统组件实施自动审计跟踪，以重建以下事件：所有个人用户均可访问持卡人数据

根据持卡人数据的存储位置，可以在以下位置找到个人用户对持卡人数据的访问权限 `userIdentity`、`eventSource`、`eventName`，或 `responseElements` 的部分 CloudTrail 日志。

PCI DSS 10.2.2：对所有系统组件实施自动审计跟踪，以重建以下事件：任何具有 root 权限或管理权限的个人采取的所有操作

根用户标识位于日志的 `userIdentity` 部分中。

PCI DSS 10.2.3：对所有系统组件实施自动审计跟踪，以重建以下事件：访问所有审计记录

可以在日志的 `eventSource`、`eventName` 或 `responseElements` 部分中找到对审核跟踪的访问。

PCI DSS 10.2.4：对所有系统组件实施自动审计跟踪，以重建以下事件：逻辑访问尝试无效

您可以在以下位置找到无效的逻辑访问尝试 CloudTrail 日志。例如：`responseElements`：
"`ConsoleLogin`" 和 `responseElements`：`"Failure"`。

PCI DSS 10.2.5：对所有系统组件实施自动审计跟踪，以重建以下事件：识别和身份验证机制的使用和变更（包括但不限于创建新帐户和权限提升）以及对具有 root 权限或管理员权限的帐户进行的所有更改、添加或删除

可以在日志的 `userAgent`、`eventName` 或 `responseElements` 部分中找到使用和更改标识和身份验证机制的操作。

PCI DSS 10.2.6：对所有系统组件实施自动审计跟踪，以重建以下事件：初始化、停止或暂停审计日志启动和停止日志记录在 CloudTrail 日志。

审计日志启动和停止的示例如下所示 CloudTrail 日志：eventName：
"StopLogging"和eventName："StartLogging"

PCI DSS 10.2.7：对所有系统组件实施自动审计跟踪，以重建以下事件：创建和删除系统级对象

系统级对象的创建和删除捕获在 CloudTrail 日志。一个系统级对象示例是 Amazon Lambda 函数。

CloudTrail 捕获createFunction和deleteFunctionAPI 调用，如中所述[Amazon Lambda开发人员指南](#)。

PCI DSS 10.3.1：至少记录每个事件的所有系统组件的以下审计追踪条目：用户确定

您可以在 CloudTrail 日志的 userIdentity 部分中找到用户标识。

PCI DSS 10.3.2：至少记录每个事件的所有系统组件的以下审计追踪条目：事件类型

您可以在 CloudTrail 日志的 eventName 部分中找到事件类型。

PCI DSS 10.3.3：至少记录每个事件的所有系统组件的以下审计追踪条目：日期和时间

您可以在以下位置找到事件的日期和时间eventTime部分 CloudTrail 日志。

PCI DSS 10.3.4：至少记录每个事件的所有系统组件的以下审计追踪条目：成功或失败指示

您可以在以下位置找到成功或失败的指示responseElements部分 CloudTrail 日志。

PCI DSS 10.3.5：至少记录每个事件的所有系统组件的以下审计追踪条目：事件的起源

您可以在以下位置找到事件的起源userAgent要么sourceIPAddress部分 CloudTrail 日志。

PCI DSS 10.3.6：至少记录每个事件的所有系统组件的以下审计追踪条目：受影响数据、系统组件或资源的身份或名称。

您可以在中找到资源的身份eventSource部分 CloudTrail 日志。

修复

在 CloudTrail

1. 登录Amazon Web Services Management Console使用您为其配置的 IAM 用户 CloudTrail管理。
2. 打开 CloudTrail 控制台为<https://console.aws.amazon.com/cloudtrail/>。
3. 在 Region (区域) 选择器中，选择要在其中创建跟踪的 Amazon 区域。这是跟踪的主区域。

主区域是一个唯一的 Amazon 区域，在此区域中，您可以在创建跟踪之后查看和更新跟踪，即使此跟踪记录所有 Amazon 区域中的事件也不例外。

4. 在导航窗格中，选择 Trails (跟踪记录)。
5. 在 Trails (跟踪) 页面上，选择 Get Started Now (立即开始使用)。如果您没有看到该选项，请选择 Create Trail (创建跟踪)。
6. 在 Trail name (跟踪名称) 中，指定跟踪的名称，例如 **My-Management-Events-Trail**。

作为最佳实践，请使用可快速识别跟踪用途的名称。在这种情况下，您正在创建的跟踪将记录管理事件。

7. 在 Management Events (管理事件) 中，确保 Read/Write events (读/写事件) 设置为 All (全部)。
8. 在 Data Events (数据事件) 中，请勿进行任何更改。此跟踪不会记录任何数据事件。
9. 为日志创建新的 S3 存储桶：
 - a. 在存储位置中，在创建新的 S3 存储桶中选择是。

- b. 在 S3 bucket (S3 存储桶) 中, 指定存储桶的名称, 例如 **my-bucket-for-storing-cloudtrail-logs**。

S3 存储桶的名称必须是全局唯一的。有关 S3 存储桶命名要求的更多信息, 请参阅 [Amazon CloudTrail 用户指南](#)。

- c. 下面高级, 选择是两者兼得使用 SSE-KMS 加密日志文件和启用日志文件验证。

10. 选择 Create (创建)。

有关更多详细信息, 请参阅中的教程[Amazon CloudTrail 用户指南](#)。

[PCI。CloudTrail.3] CloudTrail 应启用日志文件验证

合规性严重性 低

资源类型 : AWS::CloudTrail::Trail

Amazon Config 规则 : [cloud-trail-log-file-validation-enabled](#)

Schchule 结构 : 定期

参数 : None (无)

此控件检查是否 CloudTrail 日志文件验证已启用。

它不会检查何时修改了配置。

要监控日志文件更改并发出警报, 您可以使用 Amazon EventBridge 要么 CloudWatch 指标筛选条件。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关 :

PCI DSS 10.5.2 : 保护审计追踪文件免遭未经授权的修改。

CloudTrail 日志文件验证会创建一个数字签名的摘要文件, 其中包含每个日志的哈希值 CloudTrail 写入 Amazon S3。

您可以使用这些摘要文件来确定日志文件之后是否已更改、删除或未更改 CloudTrail 已发送日志。

这是一种有助于保护审核跟踪文件以免受到未经授权的修改的方法。

PCI DSS 10.5.5 : 在日志上使用文件完整性监控或更改检测软件, 确保在不生成警报的情况下无法更改现有日志数据。

CloudTrail 日志文件验证会创建一个数字签名的摘要文件, 其中包含每个日志的哈希值 CloudTrail 写入 Amazon S3。

您可以使用这些摘要文件来确定日志文件之后是否已更改、删除或未更改 CloudTrail 已发送日志。

这是一种有助于确保对日志使用文件完整性监控或更改检测软件的方法。

修复

启用 CloudTrail 日志文件验证

1. 打开 CloudTrail 控制台 <https://console.aws.amazon.com/cloudtrail/>。
2. 选择 Trails (跟踪)。
3. 在 Name (名称) 列中, 选择要编辑的跟踪的名称。

4. 下面一般详细信息，选择编辑。
5. 下面其他设置，对于日志文件验证，selectEnabled。
6. 选择 Save (保存)。

[PCI。CloudTrail.4] CloudTrail 步道应与 CloudWatch 日志

严重性：低

资源类型：AWS::CloudTrail::Trail

Amazon Config 规则：[cloud-trail-cloud-watch-logs-enabled](#)

Schedule 类型：定期

参数：None (无)

此控件检查是否 CloudTrail 跟踪配置为将日志发送到 CloudWatch 日志。

它不会检查修改日志或日志组的用户权限。您应该创建特定的 CloudWatch 在何时提醒的规则 CloudTrail 日志已更改。

此控件也不会检查除此之外的任何其他审计日志来源 CloudTrail被发送到 a CloudWatch 日志组。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 10.5.3：及时将审计跟踪文件备份到集中式日志服务器或难以更改的介质上。

CloudTrail 使用 Amazon S3 进行日志文件存储和传输，因此日志文件是永久存储的。

CloudWatch 日志是一种快速备份审计追踪文件的原生方法。

修复

为了确保 CloudTrail 步道与 CloudWatch 日志

1. 打开 CloudTrail 控制台<https://console.aws.amazon.com/cloudtrail/>。
2. 选择 Trails (跟踪)。
3. 选择一条没有价值的路线CloudWatch 日志日志组列。
4. 向下滚动到CloudWatch 日志部分，然后选择编辑。
5. 对于日志组字段，执行以下操作之一：
 - 要使用默认日志组，请保持名称不变。
 - 要使用现有日志组，请选择现有然后输入要使用的日志组的名称。
 - 要创建新的日志组，请选择new然后输入要创建的日志组的名称。
6. 选择 Continue (继续)。
7. 对于 IAM role (IAM 角色)，执行以下操作之一：
 - 要使用现有角色，请选择现有然后从下拉列表中选择角色。
 - 要创建新角色，请选择new然后输入要创建的角色名称。

将为新角色分配一个策略以授予所需的权限。

要查看授予该角色的权限，请展开策略文档。

8. 选择 Save changes (保存更改)。

有关配置的更多信息 CloudWatch 使用控制台监控日志，请参阅[Amazon CloudTrail用户指南](#)。

[PCI。CodeBuild1] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth

严重性：重大

资源类型：AWS::CodeBuild::Project

Amazon Config 规则：[codebuild-project-source-repo-url-check](#)

Schedule 类型：已触发更改

参数：None (无)

此控件检查是否 GitHub 或 Bitbucket 源存储库 URL 包含个人访问令牌或用户名和密码。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 8.2.1 使用强加密技术，在传输和存储所有系统组件的过程中，使所有身份验证凭证（例如密码/短语）不可读。

您可以使用 CodeBuild 在 PCI DSS 环境中编译源代码，运行单元测试，或生成可供部署的构件。否则，您的身份验证凭证不应以明文形式存储或传输，也不得出现在存储库 URL 中。

您应该使用 OAuth 代替个人访问令牌或用户名和密码来授予访问权限 GitHub 或 Bitbucket 存储库。这是一种使用强大加密技术使身份验证凭证不可读的方法。

修复

删除基本身份验证/(GitHub) 个人访问令牌来自 CodeBuild 项目来源

1. 打开 CodeBuild 控制台<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 Build 项目。
3. 从 Edit (编辑) 中，选择 Source (源)。
4. 选择断开连接 GitHub /Bitbucket。
5. 选择使用 OAuth 进行Connect然后选择连接到 GitHub /Bitbucket。
6. 在源提供商显示的消息中，进行相应的授权。
7. 根据需要，重新配置 Repository URL (存储库 URL) 和 additional configuration (其他配置) 设置。
8. 选择 Update source (更新源)。

SELECT CodeBuild 使用基于案例的示例，请参阅[Amazon CodeBuild用户指南](#)。

[PCI。CodeBuild2] CodeBuild 项目环境变量不应包含明文证书

严重性：重大

资源类型：AWS::CodeBuild::Project

Amazon Config 规则：[codebuild-project-envvar-awscred-check](#)

计划：已触发更改

参数：None (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。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 8.2.1 使用强加密技术，在传输和存储所有系统组件的过程中，使所有身份验证凭据（例如密码/短语）不可读。

您可以使用 CodeBuild 在 PCI DSS 环境中编译源代码，运行单元测试，或生成可供部署的构件。如果您这样做，切勿存储身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY 以明文表示。

使用环境变量将凭证存储在您的 CodeBuild 项目可能违反使用强加密的要求以使身份验证凭证不可读。

修复

要在中引用敏感数据 CodeBuild 运行时使用环境变量，使用以下步骤。

删除环境变量

1. 打开 CodeBuild 控制台<https://console.aws.amazon.com/codebuild/>。
2. 展开 Build (构建)，选择 Build project (构建项目)，然后选择包含明文凭证的构建项目。
3. 从 Edit (编辑) 中，选择 Environment (环境)。
4. 展开 Additional configuration (其他配置)，然后滚动到 Environment variables (环境变量)。
5. 选择环境变量旁边的 Remove (删除)。
6. 选择 Update environment (更新环境)。

将敏感值存储在 Amazon EC2 Systems Manager 参数存储库中，然后从您的构建规范中检索它们

1. 打开 CodeBuild 控制台<https://console.aws.amazon.com/codebuild/>。
2. 展开 Build (构建)，选择 Build project (构建项目)，然后选择包含明文凭证的构建项目。

3. 从 Edit (编辑) 中, 选择 Environment (环境)。
4. 展开 Additional configuration (其他配置), 然后滚动到 Environment variables (环境变量)。
5. 在 Amazon Systems Manager 中, 创建一个包含您的敏感数据的 Systems Manager 参数。有关如何执行此操作的说明, 请参阅教程 [Amazon Systems Manager 用户指南](#)。
6. 在创建参数后, 复制参数名称。
7. 回到 CodeBuild 控制台, 选择创建环境变量。
8. 对于 name (名称), 输入在构建规范中显示的变量名称。
9. 对于 value (值), 粘贴参数名称。
10. 从 type (类型) 中, 选择 Parameter (参数)。
11. 选择删除在包含纯文本凭证的不合规环境变量旁边。
12. 选择 Update environment (更新环境)。

有关构建环境中环境变量的信息, 请参阅 [Amazon CodeBuild 用户指南](#)。

[PCI.Config.1] 应启用 Amazon Config

严重性: 中

资源类型: Amazon 帐户

Amazon Config 规则: 无。要运行此检查, Security Hub 会运行中为其规定的审核步骤 [保护 Amazon Web Services](#)。不会在您的 Amazon 环境中为该检查创建任何 Amazon Config 托管规则。

Schedule 类型: 定期

参数: None (无)

该控制检查是否已在帐户中为本地区域启用了 Amazon Config, 并记录所有资源。

它不会检查所有关键系统文件和内容文件的更改检测, 因为 Amazon Config 仅支持一部分资源类型。

Amazon Config 服务对您帐户中支持的 Amazon 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 (Amazon 资源)、配置项之间的关系以及资源之间的任何配置更改。

Security Hub 建议您启用 Amazon Config 在所有区域。Amazon Config 捕获的 Amazon 配置项历史记录可用于安全分析、资源更改跟踪和合规性审计。

Note

由于 Security Hub 是一项区域服务, 因此对此控制执行的检查仅检查该帐户的当前区域。它不会检查所有区域。

要允许针对每个区域中的全局资源进行安全检查, 您还必须记录全局资源。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。

有关更多信息, 请参见 [Amazon Config 开发人员指南](#)。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关:

PCI DSS 10.5.2: 保护审计追踪文件免遭未经授权的修改。

Amazon Config 持续监控、跟踪和评估 [Amazon 资源配置](#) 以获取所需的设置, 并每 6 小时生成一次配置更改历史记录文件。

您应该启用 Amazon Config 以保护审核跟踪文件, 以免受到未经授权的修改。

PCI DSS 11.5：部署变更检测机制，提醒人员注意关键系统文件、配置文件或内容文件遭到未经授权的修改；并将软件配置为至少每周进行一次关键文件比较。

Amazon Config 持续监控、跟踪和评估 [Amazon 资源配置](#) 以获取所需的设置，并每 6 小时生成一次配置更改历史记录文件。

您应该启用 Amazon Config 以确保部署了更改检测机制，并将其配置为至少每周执行一次关键文件比较。

修复

配置 Amazon Config 设置

1. 通过以下网址打开 Amazon Config 控制台：<https://console.aws.amazon.com/config/>。
2. 选择要在其中配置 Amazon Config 的区域。
3. 如果你还没用过 Amazon Config 以前，请参阅[开始使用](#)在 Amazon Config 开发人员指南。
4. 从菜单导航到“设置”页面，然后执行以下操作：
 - 选择 Edit (编辑) 。
 - 下面要记录的资源类型，select 记录该地区支持的所有资源和包括全球资源 (例如 Amazon IAM 资源) 。
 - 下面数据保留期，请选择默认的保留期 Amazon Config 数据，或者指定自定义保留期。
 - 下面 Amazon Config 角色，要么选择 Create Amazon Config 服务相关角色或者选择从您的账户中选择一个角色然后选择要使用的角色。
 - 在 Amazon S3 bucket (Amazon S3 存储桶) 下面，指定要使用的存储桶，或者创建存储桶并包括前缀 (可选) 。
 - 下面 Amazon SNS 主题，从您的账户中选择一个 Amazon SNS 主题或创建一个。有关 Amazon SNS 的更多信息，请参阅[Amazon Service 入门指南](#)。
5. 选择 Save (保存) 。

有关使用的更多信息 Amazon Config 来自 的 Amazon CLI，请参阅[Amazon Config 开发人员指南](#)。

您还可以使用 Amazon CloudFormation 模板自动执行这一过程。有关更多信息，请参阅 [Amazon CloudFormation 用户指南](#)。

[PCI.CW.1] 应具有有关“根”用户使用的日志指标筛选器和警报

严重性：重大

资源类型：Amazon 帐户

Amazon Config 规则：无。Security Hub 无需创建 Amazon Config 您的托管规则 Amazon 记下这张支票。

Schedule 类型：定期

参数：None (无)

此控件会检查 CloudWatch 指标筛选条件使用以下模式：

```
{ $.userIdentity.type = "Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent" }
```

它检查以下内容：

- 日志组名称已配置为与活跃的多区域一起使用 CloudTrail。

- 跟踪具有至少一个事件选择器，将 `IncludeManagementEvents` 设置为 `true` 并将 `ReadWriteType` 设置为 `All`。
- 至少有一个与警报相关的 Amazon SNS 主题的活跃订阅者。

Note

当 Security Hub 对此控件执行检查时，它会查找 CloudTrail 当前账户使用的线索。这些跟踪可能是属于另一个账户的组织跟踪。多区域路线也可能位于不同的区域。
检查结果为 `FAILED` 在以下案例中的发现：

- 未配置任何跟踪。
- 当前区域内且由往来账户拥有的可用跟踪不符合控制要求。

检查得出的控制状态为 `NO_DATA` 在以下情况下：

- 多区域路线位于不同的区域。Security Hub 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 只能为拥有跟踪的账户生成调查结果。

对于警报，当前账户必须拥有引用的 Amazon SNS 主题，或者必须通过调用来获得 Amazon SNS 主题的访问权限 `ListSubscriptionsByTopic`。否则 Security Hub `WARNING` 对照调查结果。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 7.2.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

根用户是 Amazon 账户中权限最高的用户，可以不受限制地访问 Amazon 账户中的所有资源。

您应该设置日志指标筛选条件和警报，以防万一 Amazon Web Services 账户使用根用户凭证。

你还应该确保 CloudTrail 允许对任何具有 root 权限或管理权限的个人所采取的操作进行审计跟踪（参见 [the section called “\[PCI. CloudTrail2\] CloudTrail 应启用” \(p. 313\)](#)）。可以在以下位置找到 root 用户标识 `userIdentity` 部分 CloudTrail 日志。

修复

修复此问题的步骤包括设置 Amazon SNS 主题、指标筛选条件和指标筛选条件警报。

这些步骤与修复 [the section called “3.3 — 确保存在使用根用户的日志指标筛选条件和警报” \(p. 284\)](#) 结果的步骤相同。

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 创建 Amazon SNS 主题，用于接收所有 CIS 警报。

为该主题创建至少一个订阅者。

有关如何创建 Amazon SNS 主题的更多信息，请参阅 [Amazon Service 开发人员指南](#)。

3. 设置一个 `Authorize CloudTrail` 适用于所有区域的路线。

为此，请按照 [the section called “2.1 — 确保 CloudTrail 在所有区域均已启用” \(p. 274\)](#) 中的修复步骤进行操作。

记下关联的日志组名称。

创建指标筛选条件和警报

1. 打开 CloudWatch 控制台<https://console.aws.amazon.com/cloudwatch/>.
2. 选择日志，然后选择日志组。
3. 选择日志组，其中 CloudTrail 正在记录。
4. 在日志组详细信息页面上，选择指标筛选条件。
5. 选择 Create metric filter (创建指标筛选条件)。
6. 复制以下图案然后将其粘贴到筛选模式。

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

7. 选择 Next (下一步)。
8. 输入新筛选器的名称。例如，**RootAccountUsage**。
9. 确认的值指标命名空间是 LogMetrics。

这可确保将所有 CIS 基准指标分组到一起。

10. 中指标名称，输入指标的名称。
11. 中指标值，输入**1**，然后选择下一页。
12. 选择 Create metric filter (创建指标筛选条件)。
13. 接下来，设置通知。选择刚刚创建的指标筛选条件，然后选择创建警报。
14. 输入警报的阈值（例如**1**），然后选择下一页。
15. 下面选择 SNS 主题，对于发送通知到，选择电子邮件列表，然后选择下一页。
16. 输入名称和说明用于警报，例如**RootAccountUsageAlarm**，然后选择下一页。
17. 选择 Create Alarm (创建告警)。

[PCI.DMS.1]Amazon Database Migration Service复制实例不应公开

合规性严重性重大

资源类型：AWS::DMS::ReplicationInstance

Amazon Config 规则：[dms-replication-not-public](#)

Schedule 类型：定期

参数：None (无)

此控件检查是否 Amazon DMS 复制实例是公共的。为此，它会检查 PubliclyAccessible 字段中返回的子位置类型。

私有复制实例有一个私有 IP 地址，您无法在复制网络之外访问该地址。当源数据库和目标数据库位于同一个网络中，并且该网络使用 VPN 连接到复制实例的 VPC 时，复制实例应具有私有 IP 地址，Amazon Direct Connect，或 VPC 对等。要了解有关公有和私有复制实例的更多信息，请参阅[公有复制实例和私有复制实例](#)在 Amazon Database Migration Service 用户指南。

您还应确保访问您的 Amazon DMS 实例配置仅限于授权用户。为此，请限制用户的 IAM 修改权限 Amazon DMS 设置和资源。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 1.2.1-将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您将Amazon DMS在您定义的 CDE 中，设置复制实例的PubliclyAccessible字段到'false'。允许公共访问您的复制实例可能违反仅允许进出 CDE 的必要流量的要求。

PCI DSS 1.3.1-实施 DMZ，将入站流量限制为仅提供经授权的、可公开访问服务、协议和端口的系统组件。

如果您使用Amazon DMS在您定义的 CDE 中，设置复制实例的PubliclyAccessible字段到'false'。允许公共访问您的复制实例可能违反将入站流量限制为仅提供授权的、可公开访问的服务、协议和端口的系统组件的要求。

PCI DSS 1.3.2-将入站互联网流量限制为隔离区内的 IP 地址。

如果您使用Amazon DMS在您定义的 CDE 中，设置复制实例的PubliclyAccessible字段到'false'。允许对您的复制实例进行公共访问可能违反将入站流量限制在 DMZ 内 IP 地址的要求。

PCI DSS 1.3.4 不允许未经授权的出站流量从持卡人数据环境流向互联网。

如果您使用Amazon DMS在您定义的 CDE 中，设置复制实例的PubliclyAccessible字段到'false'。允许公共访问您的复制实例可能会违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 1.3.6 将存储持卡人数据的系统组件 (例如数据库) 放置在内部网络区域中，与 DMZ 和其他不可信网络隔离。

如果您将Amazon DMS在您定义的 CDE 中，要迁移存储持卡人数据的数据库，请设置复制实例的PubliclyAccessible字段到'false'。允许公共访问您的复制实例可能违反将存储持卡人数据的系统组件放置在内部网络区域中的要求，与 DMZ 和其他不可信网络隔离。

修复

请注意，一旦创建了复制实例，就无法更改公共访问设置。必须将其删除并重新创建。

配置Amazon DMS复制实例设置为不可公开访问

1. 打开 Amazon Database Migration Service 控制台 (<https://console.aws.amazon.com/dms/>)。
2. 在左侧导航窗格中，在资源管理，导航到复制实例。
3. 要删除公共实例，请选中该实例的复选框，然后选择操作，然后选择删除。
4. 选择创建复制实例。提供配置详情。
5. 要禁用公共访问权限，请确保公开访问未被选中。
6. 选择 Create (创建)。

有关更多信息，请参阅以下部分[创建复制实例](#)在Amazon Database Migration Service用户指南。

[PCI.EC2.1] 亚马逊 EBS 快照不应公开恢复

合规性严重性 重大

资源类型：AWS::EC2::Volume

Amazon Config 规则：[ebs-snapshot-public-restorable-check](#)

Schedule 类型：定期

参数：None (无)

此控制检查亚马逊弹性区块存储快照是否不可由所有人公开恢复。除非您明确允许，否则不应让所有人公开恢复 Amazon EBS 快照，以避免意外泄露贵公司的敏感数据。

您还应确保更改 Amazon EBS 配置的权限仅限于获得授权 Amazon 仅限账户。要了解有关管理 Amazon EBS 快照权限的更多信息，请参阅[适用于Linux实例的 Amazon EC2 用户指南](#)。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

Amazon EBS 快照用于在特定时间点将 Amazon EBS 卷上的数据备份到 Amazon S3。它们可用于恢复 EBS 卷以前的状态。

如果 Amazon EBS 快照存储持卡人数据，则不应让所有人都能公开恢复。这会违反以下要求：仅允许与 CDE 之间的所需流量。

PCI DSS 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

Amazon EBS 快照用于在特定时间点将 Amazon EBS 卷上的数据备份到 Amazon S3。它们可用于恢复 Amazon EBS 卷以前的状态。

如果 Amazon EBS 快照存储持卡人数据，则不应让所有人都能公开恢复。这会违反以下要求：将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。

PCI DSS 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

Amazon EBS 快照用于在特定时间点将 Amazon EBS 卷上的数据备份到 Amazon S3，并可用于恢复 EBS 卷的先前状态。

如果 Amazon EBS 快照存储持卡人数据，则不应让所有人都能公开恢复。这将违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 7.2.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

Amazon EBS 快照用于在特定时间点将 Amazon EBS 卷上的数据备份到 Amazon S3。它们可用于恢复 Amazon EBS 卷以前的状态。

如果 Amazon EBS 快照存储持卡人数据，则不应让所有人都能公开恢复。这可能会违反以下要求：确保将对系统组件的访问限制为所需的最小权限或用户需要了解的内容。

修复

将公开的 Amazon EBS 快照设为私有

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，在弹性方块存储，选择快照然后选择您的公共快照。

3. 选择 Actions (操作) , 然后选择 Modify permissions (修改权限)
4. 选择 Private (私有)
5. (可选) 添加Amazon与之共享快照的授权账户的账号。
6. 选择 Save

有关共享 Amazon EBS 快照的更多信息, 请参阅 [适用于Linux 实例的 Amazon EC2 用户指南](#)。

[PCI.EC2.2] VPC 默认安全组应禁止入站和出站流量

合规性严重性 中

资源类型 : AWS::EC2::SecurityGroup

Amazon Config 规则 : [vpc-default-security-group-closed](#)

Schedule 类型 : 已触发更改

参数 : None (无)

该控制检查 VPC 的默认安全组是否不允许入站或出站流量。

它不会检查其他非默认安全组和其他 VPC 配置的访问限制。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关 :

PCI DSS 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量, 并特别拒绝所有其他流量。

如果 PCI DSS 范围内的服务与默认安全组相关联, 则该安全组的默认规则将允许所有出站流量。规则还允许来自分配给相同安全组的网络接口 (及其关联实例) 的入站流量。

您应该更改默认的安全组规则设置以限制入站和出站流量。使用默认设置可能会违反只允许必要的流量进出 CDE 的要求。

PCI DSS 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果 PCI DSS 范围内的服务与默认安全组相关联, 则该安全组的默认规则将允许所有出站流量。规则还允许来自分配给相同安全组的网络接口 (及其关联实例) 的入站流量。

您应该更改默认的安全组规则设置, 以限制未经授权的入站和出站流量。使用默认设置可能会违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 2.1 在网络上安装系统之前, 请务必更改供应商提供的默认帐户并删除或禁用不必要的默认帐户。

如果 PCI DSS 范围内的服务与默认安全组相关联, 则该安全组的默认规则将允许所有出站流量。规则还允许来自分配给相同安全组的网络接口 (及其关联实例) 的入站流量。

您应该更改默认的安全组规则设置以限制入站和出站流量。使用默认帐户可能会违反删除或禁用不必要的默认帐户的要求。

修复

要修复此问题, 请创建新的安全组并将这些安全组分配给您的资源。为防止使用默认安全组, 请删除其入站和出站规则。

创建新的安全组并将其分配给您的资源

1. 通过以下网址打开 Amazon VPC 控制台 : <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Security groups (安全组)。查看默认安全组详细信息以了解分配给它们的资源。
3. 为资源创建一组最小权限安全组。有关如何创建安全组的详细信息，请参阅[创建安全组](#)在Amazon VPC User Guide。
4. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
5. 在 Amazon EC2 控制台上，将使用默认安全组的资源的安全组更改为您创建的最低权限安全组。请参阅[更改实例的安全组](#)在Amazon VPC User Guide。

将新安全组分配给资源后，从默认安全组中移除入站和出站规则。这样可以确保不使用默认安全组。

从默认安全组中移除规则

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security groups (安全组)。
3. 选择默认安全组，然后选择入站规则选项卡。选择 Edit inbound rules (编辑入站规则)。然后删除所有入站规则。选择 Save rules (保存规则)。
4. 对每个默认安全组重复上一步骤。
5. 选择默认安全组并选择出站规则选项卡。选择编辑出站规则。然后删除所有出站规则。选择 Save rules (保存规则)。
6. 对每个默认安全组重复上一步骤。

有关在 Amazon VPC 中使用安全组的更多信息，请参阅[Amazon VPC User Guide](#)。

[PCI.EC2.3] 应删除未使用的 EC2 安全组 (已停用)

该控件已停用。

[PCI.EC2.4] 应删除未使用的 EC2 EIP

合规性严重性 低

资源类型：AWS::EC2::EIP

Amazon Config 规则：[eip-attached](#)

Schedule 类型：已触发更改

参数：None (无)

此控制检查分配给 VPC 的弹性 IP 地址是否连接到 Amazon EC2 实例或正在使用的弹性网络接口 (ENI)。

如果发现失败，则表明您可能有未使用的 Amazon EC2 EIP。

这将帮助您在持卡人数据环境 (CDE) 中维护 EIP 的准确资产清单。

Note

此控件在非洲 (开普敦) 或欧洲 (米兰) 不支持。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 2.4：保存 PCI DSS 范围内的系统组件清单。

如果 EIP 未连接到 Amazon EC2 实例，则表明该实例已不再使用。

除非具有业务需求以保留该资源，否则，应删除未使用的资源以保留准确的系统组件清单。

修复

如果您不再需要弹性 IP 地址，Security Hub 建议您释放该地址（地址不得与实例关联）。

使用控制台释放弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的网络与安全下，选择弹性 IP。
3. 选择弹性 IP 地址，选择操作，然后选择释放弹性 IP 地址。
4. 系统提示时，选择 Release。

有关更多信息，请参阅中有关释放弹性 IP 地址的更多信息，请参阅。[适用于Linux 实例的 Amazon EC2 用户指南](#)。

[PCI.EC2.5] 安全组不应允许从 0.0.0.0/0 进入端口 22

合规性严重性 高

资源类型：AWS::EC2::SecurityGroup

Amazon Config 规则：[restricted-ssh](#)

Schedule 类型：触发变更了

参数：None (无)

此控件检查正在使用的安全组是否禁止不受限制的传入 SSH 流量。

它不评估出站流量。

请注意，安全组是有状态的。如果您从实例发送一个请求，则无论入站安全组规则如何，都将允许该请求的响应流量流入。如果是为响应已允许的入站流量，则该响应可以出站，此时可忽略出站规则。要了解有关安全组的更多信息，请参阅[您的 VPC 的安全组](#)在 Amazon VPC User Guide。

Note

以下区域不支持此控制。

- 非洲（开普敦）
- 亚太地区（大阪）
- 欧洲（米兰）

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1-将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

您可以允许 SSH 流量到您定义的 CDE 中的实例。如果是，请将从 0.0.0.0/0 (任何地方) 保留对 SSH 的无限访问权限可能违反只允许必要的流量进出 CDE 的要求。

PCI DSS 1.3.1-实施 DMZ，将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件。

您可以允许 SSH 流量到您定义的 CDE 中的实例。如果是，请将从 0.0.0.0/0 (任何地方) 保留对 SSH 的无

限制访问权限可能违反将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件的要求。

PCI DSS 2.2.2 仅启用系统功能所需的必要服务、协议、守护程序等。

您可以允许 SSH 流量到您定义的 CDE 中的实例。如果是，则根据安全组功能的要求，将入站 SSH 源从 0.0.0.0/0 (任何地方) 限制为特定 IP 地址或范围。在 CDE 中，可以将安全组视为系统组件，应对其进行适当的强化。保留对 SSH 的无限制访问权限可能违反仅启用系统功能所需的必要服务、协议、守护程序等的要求。

修复

对与 VPC 关联的每个安全组执行以下步骤。

从安全组移除对端口 22 的访问权限

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，在安全，选择安全组。
3. 选择一个安全组。
4. 在页面底部，选择入站规则。
5. 选择 Edit inbound rules (编辑入站规则)。
6. 确定允许通过端口 22 进行访问的规则，然后选择 X 将其删除。
7. 选择 Save rules (保存规则)。

[PCI.EC2.6] 应在所有 VPC 中启用 VPC 流量记录

合规性严重性 中

资源类型：AWS::EC2::VPC

Amazon Config 规则：[vpc-flow-logs-enabled](#)

Schedule 类型：定期

参数：

- trafficType – REJECT

此控件检查是否找到 VPC 流日志并启用了 VPC 流日志。流量类型设置为 REJECT。

使用 VPC 流日志，您可以捕获有关在您的 VPC 中传入和传出网络接口的 IP 地址流量的信息。在创建流日志后，您可以使用 CloudWatch 用于查看和检索日志数据的日志。

Security Hub 建议您为 VPC 的数据包拒绝启用流量记录。流日志提供了通过 VPC 的网络流量的可见性。它们可以检测异常流量并提供对安全工作流程的见解。

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[VPC 流日志](#)在 Amazon VPC User Guide。

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 10.3.3 验证日志条目中是否包含日期和时间戳。

通过为您的 VPC 启用 VPC 流日志记录，您可以识别日志条目的日期和时间。事件日期和时间记录在开始和结束字段中。这些值以 Unix 秒为单位显示。

PCI DSS 10.3.4 验证日志条目中是否包含成功或失败指示。

通过为您的 VPC 启用 VPC 流日志记录，您可以识别发生的事件的类型。事件的类型记录在操作字段中，可以是ACCEPT要么REJECT。

PCI DSS 10.3.5 验证日志条目中是否包含事件的来源。

通过为您的 VPC 启用 VPC 流日志记录，您可以验证事件的来源。事件起源记录在pkt-srcaddr,srcaddr，以及srcport字段之间没有不同。这些字段显示了流量的源 IP 地址和源端口。

PCI DSS 10.3.6 验证日志条目中是否包含受影响数据、系统组件或资源的身份或名称。

通过为您的 VPC 启用 VPC 流日志记录，您可以验证受影响数据、系统组件或资源的身份或名称。这些区域有：pkt-dstaddr,dstaddr，以及dstport字段显示流量的目标 IP 地址和目标端口。

修复

要修复此问题，请启用 VPC 流量记录。

启用 VPC 流日志记录

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，在虚拟私有云，选择您的 VPC。
3. 选择要更新的 VPC。
4. 在页面底部，选择流日志。
5. 选择 Create flow log (创建流日志)。
6. 对于 Filter (筛选条件)，选择 Reject (拒绝)。
7. 对于目标日志组，选择要使用的日志组。
8. 如果你选择了CloudWatch 日志对于您的目标日志组，对于IAM 角色，选择要使用的 IAM 角色。
9. 选择 Create (创建)。

[PCI.ELBV2.1] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS

合规性严重性 中

资源类型：AWS::ElasticLoadBalancingV2::LoadBalancer

Amazon Config 规则：[alb-http-to-https-redirection-check](#)

Schedule 类型：定期

参数：None (无)

此控件检查应用程序负载均衡器的所有 HTTP 侦听器上是否配置了 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，则控制将失败。

在开始使用Application Load Balancer 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。监听器支持 HTTP 和 HTTPS 协议。您可以使用 HTTPS 侦听器将加密和解密的工作交给负载均衡器完成。要在传输过程中强制加密，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[Application Load Balancer 的侦听器](#)在适用于应用程序负载均衡器的用户指南。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 2.3 使用强加密对所有非控制台管理访问进行加密。

如果您将应用程序负载均衡器与 HTTP 侦听器一起使用，请确保将侦听器重定向到 HTTPS 以获得任何非控制台管理访问权限。允许持卡人数据环境的管理员通过 HTTP 进行未加密的身份验证可能违反使用强加密对所有非控制台管理访问进行加密的要求。

PCI DSS 4.1 在通过开放的公共网络传输过程中，使用强大的加密和安全协议来保护敏感的持卡人数据。

如果您将应用程序负载均衡器与 HTTP 侦听器一起使用，请确保在传输持卡人数据时将侦听器重定向到 HTTPS。允许未加密传输持卡人数据可能违反在通过开放的公共网络传输过程中使用强加密和安全协议来保护敏感的持卡人数据的要求。

修复

要修复此问题，请将 HTTP 请求重定向到 HTTPS。

在 Application Load Balancer 上将 HTTP 请求重定向到 HTTPS

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，在负载均衡，选择负载均衡器。
3. 选择 Application Load Balancer。
4. 选择侦听器。
5. 选中 HTTP 侦听器 (端口 80 TCP) 的复选框，然后选择编辑。
6. 如果存在现有规则，则必须将其删除。否则，选择添加操作然后选择重定向为....
7. 选择 HTTPS，然后输入 **443**。
8. 选择圆形符号中的复选标记，然后选择 Update (更新)。

[PCI.ES.1] Elasticsearch 域应该在 VPC 中

合规性严重性 重大

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：[elasticsearch-in-vpc-only](#)

Schedule 类型：定期

参数：None (无)

此控件检查 Elasticsearch 域是否在 VPC 中。

它不会评估 VPC 子网路由配置以确定可公开访问性。

这个 Amazon 控件也不会检查是否 OpenSearch 基于服务资源的策略允许其他账户或外部实体进行公共访问。您应该确保 Elasticsearch 域未连接到公有子网。请参阅[基于资源的策略](#)在亚马逊 OpenSearch 服务开发人员指南。

您还应该确保根据建议的最佳实践配置了 VPC。请参阅[VPC 的安全最佳实践](#)在 Amazon VPC User Guide。

Note

亚太地区（大阪）不支持此控件。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果你的 OpenSearch 服务集群包含持卡人数据，OpenSearch 服务域应放在 VPC 中。这样做可以实现两者之间的安全通信 OpenSearch 您可以在 VPC 中部署 Service 和 VPN 连接端口，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

该方法用于仅允许与 CDE 之间的所需流量。

PCI DSS 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果你的 OpenSearch 服务集群包含持卡人数据，OpenSearch 服务域应放在 VPC 中。这样做可以实现两者之间的安全通信 OpenSearch 您可以在 VPC 中部署 Service 和 VPN 连接端口，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

该方法用于将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。

PCI DSS 将入站互联网流量限制为 DMZ 内的 IP 地址。

如果你的 OpenSearch 服务集群包含持卡人数据，OpenSearch 服务域应放置在 VPC 中，这样可以实现两者之间的安全通信 OpenSearch 您可以在 VPC 中部署 Service 和 VPN 连接端口，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

此方法用于将入站互联网流量限制为 DMZ 内的 IP 地址。

您还可以使用基于资源的策略，并指定 IP 条件以根据源 IP 地址限制访问。查看博客文章[如何控制对您的 Amazon 的访问 OpenSearch 服务域](#)。

PCI DSS 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果你的 OpenSearch 服务集群包含持卡人数据，OpenSearch 服务域应放置在 VPC 中，这样可以实现两者之间的安全通信 OpenSearch 您可以在 VPC 中部署 Service 和 VPN 连接端口，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

此方法用于阻止从持卡人数据环境到互联网的未经授权的出站流量。

PCI DSS 将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

如果你的 OpenSearch 服务集群包含持卡人数据，OpenSearch 服务域应放在 VPC 中。这样做可以实现两者之间的安全通信 OpenSearch 您可以在 VPC 中部署 Service 和 VPN 连接端口，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

该方法用于将存储持卡人数据的系统组件放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。

修复

如果您创建一个具有公有终端节点的域，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终端节点。您必须[创建另一个域](#)或禁用该控制。

请参阅[启动您的 Amazon OpenSearch VPC 中的服务域](#)在亚马逊 OpenSearch 服务开发人员指南。

[PCI.ES.2] Elasticsearch 域应启用静态加密

合规性严重性 中

资源类型 : AWS::Elasticsearch::Domain

Amazon Config 规则 : [elasticsearch-encrypted-at-rest](#)

Schedule 类型 : 定期

参数 : None (无)

此控件检查 Elasticsearch 域是否启用了静态加密配置。

Note

亚太地区 (大阪) 不支持此控件。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关 :

PCI DSS 3.4 : 无论存储在何处 (包括便携式数字媒体、备份媒体和日志) , 主账号 (PAN) 都无法读取。

如果您将 OpenSearch 存储信用卡主账号 (PAN) 的服务, 应通过启用来保护 PAN OpenSearch 静态服务域加密。

如果启用, 它会对域的以下方面进行加密: 索引、自动快照、OpenSearch 服务日志、交换文件以及应用程序目录中的所有其他数据。

这是一种用于使 PAN 不可读的方法。

修复

默认情况下, 域不对数据进行静态加密, 并且您无法配置现有的域以使用该功能。

要启用该功能, 您必须创建另一个域并迁移数据。有关创建域的信息, 请参阅[亚马逊 OpenSearch 服务开发人员指南](#)。

静态数据加密需要 OpenSearch 服务 5.1 或更高版本。有关加密静态数据的更多信息 OpenSearch 服务, 请参阅[亚马逊 OpenSearch 服务开发人员指南](#)。

[PCI. GuardDuty1] GuardDuty 应启用

合规性严重性 高

资源类型 : Amazon 帐户

Amazon Config 规则 : [guardduty-enabled-centralized](#)

Schedule 类型 : 定期

参数 : None (无)

此控件检查亚马逊是否 GuardDuty 已在您的中启用 Amazon 账户和区域。

而 GuardDuty 可以有效抵御入侵检测系统通常会保护的攻击, 但它可能不是适用于所有环境的完整解决方案。该规则也不会检查是否向人员生成警报。有关的更多信息 GuardDuty, 请参阅[亚马逊 GuardDuty 用户指南](#)。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Europe (Milan)
- Middle East (Bahrain)
- Amazon GovCloud (美国东部)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 11.4 使用入侵检测和/或入侵防御技术来检测和/或防止入侵网络。

GuardDuty 通过监控持卡人数据环境周边及其所有关键点的流量，可以帮助满足要求 11.4。它还可以使所有入侵检测引擎、基准和签名保持最新状态。调查结果来自 GuardDuty。您可以使用亚马逊将这些警报发送给工作人员 CloudWatch。请参阅[创建对自定义响应 GuardDuty 亚马逊的发现 CloudWatch 事件](#)在亚马逊 GuardDuty 用户指南。未启用 GuardDuty 在你的 Amazon 帐户可能违反使用入侵检测和/或防御技术来防止入侵网络的要求。

修复

要修复此问题，请启用 GuardDuty。

有关如何启用的详细信息 GuardDuty，包括如何使用 Amazon Organizations 要管理多个账户，请参阅[开始使用 GuardDuty](#)在亚马逊 GuardDuty 用户指南。

[PCI.IAM.1] IAM 根用户访问密钥不应存在

合规性严重性 重大

资源类型：Amazon 帐户

Amazon Config 规则：[iam-root-access-key-check](#)

Schedule 类型：定期

参数：None (无)

该控制检查根用户的用户访问密钥是否存在。

Note

此控件在非洲 (开普敦) 或亚太地区 (大阪) 不支持。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 2.1 在网络上安装系统之前，请务必更改供应商提供的默认帐户并删除或禁用不必要的默认帐户。

这些区域有：Amazon Web Services 帐户 root 用户是最有特权的 AmazonUSER。Amazon 访问密钥提供对给定帐户的编程访问。

不应为根用户创建访问密钥，因为这可能会违反以下要求：删除或禁用不需要的默认账户。

PCI DSS 2.2：为所有系统组件制定配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。

root 用户是最有特权的AmazonUSER。Amazon访问密钥提供对给定账户的编程访问。

不应为根用户创建访问密钥，因为这可能会违反以下要求：实施系统强化配置。

PCI DSS 7.2.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

root 用户是最有特权的AmazonUSER。Amazon访问密钥提供对给定账户的编程访问。

不应为 root 用户创建访问密钥。这样做可能违反确保对系统组件的访问仅限于必要的最低权限或用户需要知道的要求。

修复

要删除根用户访问密钥，请参阅[删除根用户的访问密钥](#)在IAM 用户指南。

[PCI.IAM.2] IAM 用户不应附加 IAM 策略

合规性严重性 低

资源类型：AWS::IAM::User

Amazon Config 规则：[iam-user-no-policies-check](#)

Schedule 类型：触发变更了

参数：None (无)

此控制可检查您的所有 IAM 用户是否都没有附加策略。IAM 用户必须继承 IAM 群组或角色的权限。

它不检查最低权限策略是否应用于 IAM 角色和群组。

Note

由亚马逊简单电子邮件服务创建的 IAM 用户是使用内联策略自动创建的。Security Hub 会自动免除这些用户的此控制。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 7.2.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

IAM 策略是向中的用户、组或角色授予权限的方式Amazon。

默认情况下，IAM 用户、组和角色无权访问Amazon在将 IAM 策略附加到资源之前。

要管理最低权限访问并降低 PCI DSS 范围内资源的访问管理的复杂性，您应该在组或角色级别而不是在用户级别分配 IAM 策略。

通过降低访问管理复杂性，可以降低委托人无意中获得或保留过多权限的可能性。

这是一种用于确保将对包含持卡人数据的系统组件的访问限制为所需的最小权限或用户需要了解的内容的方法。

修复

要解决这一问题，[创建 IAM 组](#)，并将该策略附加到组。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[添加和删除 IAM 身份权限](#)在IAM 用户指南。

[PCI.IAM.3] IAM 策略不应允许完全“*”管理权限

合规性严重性 高

资源类型：AWS::IAM::Policy

Amazon Config 规则：[iam-policy-no-statements-with-admin-access](#)

类型：Schedule 触发变更了

参数：None (无)

该控制检查 Amazon Identity and Access Management 策略 (也称为客户托管策略) 的默认版本是否没有管理员访问权限，并且语句具有 "Effect": "Allow" with "Action": "*" over "Resource": "*"。

它仅检查您创建的[客户托管策略](#)，而不检查各个服务 (例如 "S3:*") 的完全访问权限。

它不会检查[内联和Amazon托管策略](#)。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 7.2.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

提供完全管理权限而不是限制为所需的最小权限可能会违反以下要求：确保将对系统组件的访问限制为所需的最小权限或用户需要了解的内容。

修复

要修改您的 IAM 策略以使其不允许完整的 “*” 管理权限，请参阅[编辑 IAM policy](#)在IAM 用户指南。

[PCI.IAM.4] 应该为根用户启用硬件 MFA

合规性严重性 重大

资源类型 Amazon 帐户

Amazon Config 规则：[root-account-hardware-mfa-enabled](#)

类型：Schedule 定期

参数：None (无)

这个控件会检查你是否Amazon账户已启用使用多重身份验证 (MFA) 硬件设备使用根用户证书登录。

它不会检查您是否使用虚拟 MFA。

要满足 PCI DSS 要求 8.3.1，您可以在硬件 MFA (该控制) 和虚拟 MFA ([the section called "\[PCI.IAM.5\] 应该为根用户启用虚拟 MFA" \(p. 336\)](#)) 之间进行选择。

基于时间的一次性密码 (TOTP) 和通用第二重要素 (U2F) 令牌均可作为硬件 MFA 选项。

Note

以下区域不支持此控制。

- ## 相关的 PCI DSS 要求

PCI DSS 8.1 将所有非控制台访问的多因素身份验证整合到持卡人数据环境 (CDE) 中，供具有管理访问权限的人员使用。

MFA 在用户名和密码之上增加了一层额外的防护。如果具有管理权限的用户通过网络接口而不是到系统组件的直接物理连接访问持卡人数据环境，并且没有实际位于他们管理的计算机前面，则需要使用 MFA。

修复

要为根用户添加硬件 MFA 设备，请参阅[为以下启用硬件 MFA 设备Amazon账户根用户（控制台）](#)在IAM 用户指南。

合规性严重性 重大

资源类型 Amazon帐户

Amazon Config 规则 : `root-account-mfa-enabled`

类型：Schedule 定期

参数：None（无）

此控件可检查您的用户是否为Amazon账户需要多重身份验证 (MFA) 设备才能使用根用户凭证登录。

它不会检查您是否使用硬件 MFA。

要满足 PCI DSS 要求 8.3.1，您可以在虚拟 MFA（该控制）和硬件 MFA（[the section called “\[PCI.IAM.4\] 应该为根用户启用硬件 MFA” \(p. 335\)](#)）之间进行选择。

以下区域不支持此控制。

- ## 相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 8.1 将所有非控制台访问的多因素身份验证整合到持卡人数据环境 (CDE) 中，供具有管理访问权限的人员使用。

根用户是账户中权限最高的用户。

MFA 在用户名和密码之上增加了一层额外的防护。如果具有管理权限的用户访问持卡人数据环境，并且没有实际位于他们管理的计算机前面，则需要使用 MFA。

启用虚拟 MFA 是一种用于合并多重身份验证 (MFA) 的方法，用于合并所有非控制台管理访问权限。

修复

要为根用户添加虚拟 MFA，请参阅[为您的启用虚拟 MFA 设备Amazon账户根用户 \(控制台\)](#)在IAM 用户指南。

[PCI.IAM.6] 应为所有 IAM 用户启用 MFA

合规性严重性 中

资源类型 AWS::IAM::User

Amazon Config 规则：[iam-user-mfa-enabled](#)

类型：Schedule 定期

参数：None (无)

此控件会检查 IAM 用户是否启用了多重身份验证 (MFA)。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 8.1 将所有非控制台访问的多因素身份验证整合到持卡人数据环境 (CDE) 中，供具有管理访问权限的人员使用。

为所有 IAM 用户启用 MFA 是一种用于为所有非控制台管理访问合并多重验证 (MFA) 的方法。

修复

要为 IAM 用户添加 MFA，请参阅[在中使用多重身份验证 \(MFA\)Amazon](#)在IAM 用户指南。

[PCI.IAM.7] 如果在预定义的天数内未使用 IAM 用户证书，则应禁用

合规性严重性 中

资源类型 AWS::IAM::User

Amazon Config 规则：[iam-user-unused-credentials-check](#)

类型：Schedule 定期

参数：

- maxCredentialUsageAge: 90 (天)

此控件检查您的 IAM 用户是否拥有在指定天数内未使用的密码或有效访问密钥。默认值为 90 天。

Security Hub 强烈建议您不要生成和删除账户中的所有访问密钥。相反，推荐的最佳做法是创建一个或多个 IAM 角色或者使用[联合身份](#)。这些做法允许您的用户使用他们现有的公司凭证登录 Amazon Web Services Management Console 控制台和 Amazon CLI。

每种方法都有其使用案例。对于拥有现有中央目录或计划需要超出当前 IAM 用户配额的企业，Federation 通常更好。在 Amazon 环境外运行的应用程序需要访问密钥才能对 Amazon 资源进行编程访问。

但是，如果需要提供编程访问的资源在 Amazon 内部运行，则最佳做法是使用 IAM 角色。您可以使用角色授予资源访问权限，而无需在配置中部署访问密钥 ID 和秘密访问密钥。

要了解有关保护您的访问密钥和账户的更多信息，请参阅[管理的最佳实践 Amazon 访问密钥](#)在 Amazon 一般参考。另请参阅博客文章[保护您的 Amazon 使用编程访问权限时的帐户](#)。

如果您已经拥有访问密钥，我们建议您删除或停用在 90 天或更长时间内处于非活动状态的未使用用户证书。

此控件仅检查非活动密码或有效访问密钥。它不会在 90 天后禁用该帐户。客户有责任采取措施并禁用未使用的证书。

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 8.1.4 在 90 天内删除/禁用不活跃的用户帐户。

如果您使用 IAM 密码或访问密钥，请确保对其使用进行监控，如果在 90 天内未使用，则将其禁用。允许 IAM 用户账户使用未使用的证书保持活动状态可能违反在 90 天内删除/禁用不活跃用户账户的要求。

修复

要获取监控账户是否有过期证书所需的一些信息，请使用 IAM 控制台。例如，当您查看账户中的用户时，会有以下列访问密钥类型、密码期限，以及上次活动。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账户和识别 90 天或更长时间没有活动的账户。您可以在以下位置下载证书报告.csv IAM 控制台中的格式。有关凭证报告的更多信息，请参阅[获取您的凭证报告 Amazon 帐户](#)在 IAM 用户指南。

确定非活动账户或未使用的凭证后，请使用以下步骤禁用它们。

禁用不活跃账户或未使用的 IAM 证书

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 下面访问管理，选择 Users。
3. 选择凭证已超过 90 天的用户的姓名。
4. 选择 Security credentials (安全凭证)。选择设置为 `inact` 适用于 90 天或更长时间未使用的所有登录证书和访问密钥。

[PCI.IAM.8] IAM 用户的密码策略应具有强配置

合规性严重性 中

资源类型 Amazon 帐户

Amazon Config 规则：[iam-password-policy](#)

类型：Schedule 定期

参数：None (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— 密码中至少需要一个大写字符。(默认值 = true)
- RequireLowercaseCharacters— 密码中至少需要一个小写字符。(默认值 = true)
- RequireNumbers— 密码中至少需要一个数字。(默认值 = true)
- MinimumPasswordLength— 密码最小长度。(默认 = 7 或更长)
- PasswordReusePrevention— 允许重复使用之前的密码数量。(默认值 = 4)
- MaxPasswordAge — 密码到期前的天数。(默认值 = 90)

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 8.1.4：在 90 天内删除/禁用不活跃的用户帐户。

如果您有 IAM 用户 Amazon 账户，您应该适当地配置 IAM 密码策略。不保护 IAM 用户的密码可能违反在 90 天内删除或禁用不活跃用户账户的要求。默认情况下，MaxPasswordAge 参数设置为 90 天。密码过期后，IAM 用户在更改密码之前无法访问他们的账户，这会禁用该用户。

PCI DSS 8.2.1 密码/密码短语必须满足以下要求：要求最小长度至少为七个字符，并且同时包含数字和字母字符。

如果您有 IAM 用户 Amazon 账户，应适当配置 IAM 密码策略。不保护 IAM 用户的密码可能会违反密码长度至少为七个字符的要求。它还可能违反同时包含数字和字母字符的要求。默认值为 MinimumPasswordLength 是 7, RequireUppercaseCharacters 是 true，以及 RequireLowercaseCharacters 是 true。

PCI DSS 8.2.4 每 90 天至少更改一次用户密码/密码。

如果您有 IAM 用户 Amazon 账户，应适当配置 IAM 密码策略。不保护 IAM 用户的密码可能违反每隔 90 天至少更改一次用户密码或密码的要求。默认情况下，MaxPasswordAge 参数设置为 90 天。密码过期后，在更改密码之前，IAM 用户无法访问该账户。

PCI DSS 8.2.1 不要允许个人提交与他或她最近使用的四个密码/密码中的任何一个相同的新密码/密码。

如果您有 IAM 用户 Amazon 账户，应适当配置 IAM 密码策略。不保护 IAM 用户的密码可能违反不允许个人提交与之前的四个密码或密码相同的新密码或密码短语的要求。默认值为 PasswordReusePrevention 将设置为 4，它可以防止用户重复使用他们最近的四个密码。

修复

要更新您的密码策略以使用推荐的配置，请参阅 [为 IAM 用户设置账户密码策略](#) 在 IAM 用户指南。

[PCI.KMS.1] 应启用 KMS 密钥轮换

合规性严重性 中

资源类型 AWS::KMS::Key

Amazon Config 规则：[cmk-backing-key-rotation-enabled](#)

类型：Schedule 定期

参数：None (无)

此控件检查每个 KMS 密钥是否已启用密钥轮换。它不检查具有导入密钥材料的 KMS 密钥。

您应该确保密钥包含导入的材料和未存储在中的密钥Amazon KMS旋转。Amazon 托管式密钥每 3 年轮换一次。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 3.6.4：加密密钥在加密周期结束后应进行更改。

尽管 PCI DSS 没有指定加密周期的时间范围，但如果启用密钥轮换，则默认情况下每年轮换一次。

如果您使用 KMS 密钥加密持卡人数据，则应启用密钥轮换。

这是一种用于在到达加密限时更改加密密钥的方法。

修复

启用 KMS 密钥轮换

1. 在 Amazon KMS<https://console.aws.amazon.com/kms> [打开](#) 控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector (区域选择器)。
3. 选择 Customer managed keys (客户托管密钥)。
4. 在 Alias (别名) 列中，选择要更新的密钥的别名。
5. 选择 Key rotation (密钥轮换)。
6. Select每年自动轮换此 KMS 密钥然后选择Save (保存) 。

[PCI.Lambda.1] Lambda 函数应禁止公共访问

合规性严重性 重大

资源类型 AWS::Lambda::Function

Amazon Config 规则：[lambda-function-public-access-prohibited](#)

类型：Schedule 触发变更了

参数：None (无)

此控件检查 Lambda 函数基于资源的策略是否禁止公共访问。

它不检查内部委托人 (例如 IAM 角色) 对 Lambda 函数的访问权限。您应使用基于资源的最低权限 Lambda 策略，确保仅限授权委托人访问 Lambda 函数。请注意，您必须使用AWS:SourceAccount在您的 Lambda 函数策略中传递此控制。

有关使用基于资源的策略的更多信息Amazon Lambda，请参阅[Amazon Lambda开发人员指南](#)。

Note

以下区域不支持此控制。

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您使用在 PCI DSS 范围内的 Lambda 函数，则不应公开访问该函数。可公开访问的函数可能会违反以下要求：仅允许与 CDE 之间的所需流量。

PCI DSS 1.3.1 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果您使用在 PCI DSS 范围内的 Lambda 函数，则不应公开访问该函数。可公开访问的函数可能会违反以下要求：将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。

PCI DSS 1.3.2 将入站互联网流量限制为 DMZ 内的 IP 地址。

如果您使用在 PCI DSS 范围内的 Lambda 函数，则不应公开访问该函数。可公开访问的功能可能违反将入站互联网流量限制在 DMZ 内 IP 地址的要求。

PCI DSS 1.3.4 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果您使用在 PCI DSS 范围内的 Lambda 函数，则该函数不得公开访问。可公开访问的功能可能违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 7.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

如果您使用在 PCI DSS 范围内的 Lambda 函数，则不应公开访问该函数。可公开访问的函数可能会违反以下要求：确保将对包含持卡人数据的系统组件的访问限制为所需的最小权限或用户需要了解的内容。

修复

要修复此问题，请更新基于资源的策略，将可公开访问的 Lambda 函数更改为私有 Lambda 函数。

您只能为 Lambda 资源更新基于资源的策略 [AddPermission](#) 和 [AddLayerVersionPermission](#) API 操作。

您不能为您在 JSON 中的 Lambda 资源编写策略，也不能使用 CLI 或 SDK 使用没有映射到这些操作的参数的条件。

要使用 Amazon CLI 从中撤销函数使用权限 Amazon 服务或其他账户

1. 要从 Amazon CLI 中获取 GetPolicy 输出中的语句的 ID，请运行以下命令：

```
aws lambda get-policy --function-name yourfunctionname
```

此命令返回与可公开访问的 Lambda 函数关联的基于 Lambda 资源的策略字符串。

2. 从 get-policy 命令返回的策略语句中，复制 Sid 字段的字符串值。
3. 从 Amazon CLI 中，运行

```
aws lambda remove-permission --function-name yourfunctionname --statement-id youridvalue
```

使用 Lambda 控制台限制对 Lambda 函数的访问

1. 打开 Amazon Lambda 控制台，地址：<https://console.aws.amazon.com/lambda/>。
2. 导航到函数然后选择可公开访问的 Lambda 函数。
3. 在 Designer (设计器) 下面，选择左上角的钥匙图标。它具有工具提示查看权限。
4. 在 Function policy (函数策略) 下面，如果策略允许委托人元素 “*” 或 {“AWS”: “*”} 的操作，则可以公开访问该函数。

考虑添加以下 IAM 条件以限定对您账户的访问权限。

```
"Condition": {
  "StringEquals": {
    "AWS:SourceAccount": "<account_id>"
  }
}
```

有关允许您基于资源向其他账户授予使用权限的 Lambda 资源策略示例，请参阅有关使用基于资源的策略的信息。Amazon Lambda 在 [Amazon Lambda 开发人员指南](#)。

[PCI.Lambda.2] Lambda 函数应位于 VPC 中

合规性严重性 低

资源类型 AWS::Lambda::Function

Amazon Config 规则：[lambda-inside-vpc](#)

类型：Schedule 触发变更了

参数：None (无)

此控件检查 Lambda 函数是否在 VPC 中。你可能会看到 Lambda @Edge 资源的搜索结果失败。

它不会评估 VPC 子网路由配置以确定可公开访问性。

Note

以下区域不支持此控制。

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

默认情况下，Lambda 在可访问 VPC 的安全默认 VPC 中运行您的函数 Amazon 服务和互联网。

如果您使用 PCI DSS 范围内的 Lambda 函数，可以将该函数配置为使用 VPC 终端节点。这将允许您从 VPC 内连接到 Lambda 函数，而无需互联网访问权限。该方法用于仅允许与 CDE 之间的所需流量。

PCI DSS 1.3.1 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

默认情况下，Lambda 在可访问 VPC 的安全默认 VPC 中运行您的函数 Amazon 服务和互联网。

如果您使用 PCI DSS 范围内的 Lambda 函数，可以将该函数配置为使用 VPC 终端节点。这使您可以从 VPC 内连接到 Lambda 函数，而无需互联网访问权限。这种方法用于将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件。

PCI DSS 1.3.2 将入站互联网流量限制为 DMZ 内的 IP 地址。

默认情况下，Lambda 在可访问 VPC 的安全默认 VPC 中运行您的函数 Amazon 服务和互联网。

如果您使用 PCI DSS 范围内的 Lambda 函数，可以将该函数配置为使用 VPC 终端节点。这使您可以从 VPC 内连接到 Lambda 函数，而无需互联网访问权限。这是一种用于将入站互联网流量限制为 DMZ 内的 IP 地址的方法。

PCI DSS 1.3.4 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

默认情况下，Lambda 在可访问 VPC 的安全默认 VPC 中运行您的函数 Amazon 服务和互联网。

如果您使用 PCI DSS 范围内的 Lambda 函数，可以将该函数配置为使用 VPC 终端节点。这使您可以从 VPC 内连接到 Lambda 函数，而无需互联网访问权限。这是一种用于阻止从持卡人数据环境到互联网的未经授权的出站流量的方法。

修复

配置函数以连接到您的账户的 Virtual Private Cloud (VPC) 中的私有子网

1. 打开 Amazon Lambda 控制台，地址：<https://console.aws.amazon.com/lambda/>。
2. 导航到函数然后选择您的 Lambda 函数。
3. 滚动到 Network (网络)，然后选择一个符合函数连接要求的 VPC。
4. 要在高可用性模式下运行函数，Security Hub 建议您至少选择两个子网。
5. 至少选择一个符合该功能连接要求的安全组。
6. 选择 Save (保存)。

有关更多信息，请参阅中有关配置 Lambda 函数以访问 VPC 中的资源的部分。[Amazon Lambda 开发人员指南](#)。

[PCI。OpenSearch.1] 亚马逊 OpenSearch 服务域应位于 VPC 中

类别：类别：：保护 > 安全网络配置 > VPC 中的资源

合规性严重性 中

资源类型 AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-in-vpc-only](#)

类型：Schedule 触发变更了

参数：None (无)

此控件检查是否 OpenSearch 域位于 VPC 中。它不会通过评估 VPC 子网路由配置来确定公有访问权限。

您应该确保 OpenSearch 域未连接到公有子网。请参阅[基于资源的策略](#)在亚马逊 OpenSearch Service 开发人员指南。

您还应确保根据推荐的最佳实践配置您的 VPC。请参阅[VPC 的安全最佳实践](#)在 Amazon VPC 用户指南中。

OpenSearch 在 VPC 中部署的域可以通过私有域与 VPC 资源通信 Amazon 网络，无需遍历公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。VPC 提供多种网络控制来安全访问 OpenSearch 域，包括网络 ACL 和安全组。Security Hub 建议你迁移到公共位置 OpenSearch 域到 VPC 以利用这些控件。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您的 Amazon ES 集群包含持卡人数据，则应将 Amazon ES 域放在 VPC 中。这样您就可以在 Amazon ES 和 VPC 中的其他服务之间进行安全通信，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

该方法用于仅允许与 CDE 之间的所需流量。

PCI DSS 1.3.1 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果您的 Amazon ES 集群包含持卡人数据，则应将 Amazon ES 域放在 VPC 中。这样您就可以在 Amazon ES 和 VPC 中的其他服务之间进行安全通信，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

该方法用于将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。

PCI DSS 1.3.2 将入站互联网流量限制为 DMZ 内的 IP 地址。

如果你的亚马逊 OpenSearch 服务集群包含持卡人数据，亚马逊 OpenSearch 服务域应放置在 VPC 中，这样可以实现亚马逊之间的安全通信。OpenSearch 您可以在 VPC 中部署 Service 和 VPN 连接端口，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

此方法用于将入站互联网流量限制为 DMZ 内的 IP 地址。

您还可以使用基于资源的策略，并指定 IP 条件以根据源 IP 地址限制访问。查看博客文章[如何控制对 Amazon Elasticsearch Service 域的访问](#)。

PCI DSS 1.3.4 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果您的 Amazon ES 集群包含持卡人数据，则应在 Amazon ES 和 VPC 中的其他服务之间进行安全通信，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

此方法用于阻止从持卡人数据环境到互联网的未经授权的出站流量。

PCI DSS 1.3.6 将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

如果您的 Amazon ES 集群包含持卡人数据，则应将 Amazon ES 域放在 VPC 中。这样您就可以在 Amazon ES 和 VPC 中的其他服务之间进行安全通信，而无需 Internet 网关、NAT 设备或 VPN 连接端口。

该方法用于将存储持卡人数据的系统组件放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。

修复

如果您创建一个具有公有终端节点的域，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终端节点。您必须[创建另一个域](#)或禁用该控制。

请参阅[启动您的 Amazon OpenSearch VPC 中的服务域](#)在亚马逊 OpenSearch Service 开发人员指南。

[PCI。OpenSearch2] OpenSearch 域应启用静态加密

类别：类别：：保护 > 数据保护 > 静态数据加密

合规性严重性 中

资源类型 AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-encrypted-at-rest](#)

类型：Schedule 触发变更了

参数：None (无)

此控件检查亚马逊是否 OpenSearch 域有 encryption-at-rest 配置已启用。如果未启用静态加密，检查将失败。

为了给您的敏感数据增加一层安全保护 OpenSearch，你应该配置你的 OpenSearch 待静态加密的域。OpenSearch 域提供静态数据加密。该功能使用 Amazon KMS 存储和管理您的加密密钥。为执行加密，它使用具有 256 位密钥 (AES-256) 的高级加密标准算法。

了解相关更多信息 OpenSearch 静态加密，请参阅[Amazon 静态数据加密 OpenSearch 服务](#)在亚马逊 OpenSearch Service 开发人员指南。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 3.4：无论存储在何处（包括便携式数字媒体、备份媒体和日志），主账号 (PAN) 都无法读取。

如果你使用亚马逊 OpenSearch 存储信用卡主账号 (PAN) 的服务，应通过启用亚马逊来保护 PAN OpenSearch 静态服务域加密。

如果启用，它会对域的以下方面进行加密：指数、自动快照、亚马逊 OpenSearch 服务日志、交换文件以及应用程序目录中的所有其他数据。

这是一种用于使 PAN 不可读的方法。

修复

默认情况下，域不对数据进行静态加密，并且您无法配置现有的域以使用该功能。要启用该功能，您必须创建另一个域并迁移数据。

有关创建域的信息，请参阅[创建和管理 Amazon OpenSearch Schice 域](#)在亚马逊 OpenSearch Service 开发人员指南。

请参阅[启动您的 Amazon OpenSearch VPC 中的服务域](#)在亚马逊 OpenSearch Service 开发人员指南。

[PCI.RDS.1] 亚马逊 RDS 快照应禁止公共访问

合规性严重性 重大

资源类型 AWS::RDS::DBSnapshot

Amazon Config 规则：[rds-snapshots-public-prohibited](#)

类型：Schedule 触发变更了

参数：None (无)

此控制检查 Amazon RDS 数据库快照是否禁止其他账户访问。您还应确保快照的访问权限和更改 Amazon RDS 配置的权限仅限于授权委托人。

要了解有关在 Amazon RDS 中共享数据库快照的更多信息，请参阅[Amazon RDS 用户指南](#)。

请注意，如果将配置更改为允许公有访问，则 Amazon Config 规则可能在长达 12 小时内无法检测到更改。在 Amazon 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。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

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。

如果 RDS 快照存储持卡人数据，则不应与其他账户共享 RDS 快照。共享 RDS 快照将允许其他账户从快照中恢复 RDS 实例。允许这样做可能会违反只允许必要的流量进出 CDE 的要求。

PCI DSS 1.3.1 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

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。

如果 RDS 快照存储持卡人数据，则不应与其他账户共享 RDS 快照。共享 RDS 快照将允许其他账户从快照中恢复 RDS 实例。允许这样做可能会违反将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件的要求。

PCI DSS 1.3.4 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

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。

如果 RDS 快照存储持卡人数据，则不应与其他账户共享 RDS 快照。共享 RDS 快照将允许其他账户从快照中恢复 RDS 实例。允许这样做可能会违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 1.3.6 将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

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。

如果 RDS 快照存储持卡人数据，则不应与其他账户共享 RDS 快照。共享 RDS 快照将允许其他账户从快照中恢复 RDS 实例。允许这样做可能违反将存储持卡人数据的系统组件放置在内部网络区域中的要求，该区域与 DMZ 和其他不可信网络隔离。

PCI DSS 7.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

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。

如果 RDS 快照存储持卡人数据，则不应与其他账户共享 RDS 快照。共享 RDS 快照将允许其他账户从快照中恢复 RDS 实例。允许这样做可能违反确保对包含持卡人数据的系统组件的访问仅限于必要的最低权限或用户需要知道的要求。

修复

删除 Amazon RDS 快照的公有访问权限

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 导航到 Snapshots (快照)，然后选择要修改的公有快照
3. 从 Actions (操作) 列表中，选择 Share Snapshots (共享快照)
4. 从 DB snapshot visibility (数据库快照可见性) 中，选择 Private (私有)
5. 在 DB snapshot visibility (数据库快照可见性) 下面，选择 for all (用于所有)
6. 选择 Save

[PCI.RDS.2] Amazon RDS 数据库实例应禁止公共访问，由以下因素决定 PubliclyAccessible 配置

合规性严重性 重大

资源类型 AWS::RDS::DBInstance

Amazon Config 规则：[rds-instance-public-access-check](#)

类型：Schedule 触发变更了

参数：None (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 RDS 实例。publiclyAccessible 值指示是否可以公开访问数据库实例。如果可以公开访问数据库实例，则它是一个面向 Internet 的实例并具有可公开解析的 DNS 名称，该名称解析为一个公有 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。

该控制不会检查 VPC 子网路由设置或安全组规则。您还应该确保 VPC 子网路由不允许公开访问，并且与 RDS 实例关联的安全组入站规则不允许不受限制的访问 (0.0.0.0/0)。您还应该限制用户修改 RDS 实例设置和资源的 IAM 权限，以确保将对 RDS 实例配置的访问限制为仅授权的用户。

有关更多信息，请参阅 [从 Internet 隐藏 VPC 中的数据库实例](#) 在 Amazon RDS 用户指南。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您使用在 PCI DSS 范围内的 RDS 实例，则不应公开访问该 RDS 实例。允许这样做可能违反只允许必要的流量进出 CDE 的要求。

PCI DSS 1.3.1 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果您使用 RDS 实例存储持卡人数据，则不应公开访问 RDS 实例。允许这样做可能会违反将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件的要求。

PCI DSS 1.3.2 将入站互联网流量限制为 DMZ 内的 IP 地址。

如果您使用 RDS 实例存储持卡人数据，则不应公开访问 RDS 实例，因为这可能违反将入站互联网流量限制在 DMZ 内 IP 地址的要求。

PCI DSS 1.3.4 不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果您使用 RDS 实例存储持卡人数据，则不应公开访问 RDS 实例。允许这样做可能会违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 1.3.6 将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

如果您使用 RDS 实例存储持卡人数据，则不应公开访问 RDS 实例。允许这样做可能违反将存储持卡人数据的系统组件放置在内部网络区域中的要求，该区域与 DMZ 和其他不可信网络隔离。

PCI DSS 7.1 为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

如果您使用 RDS 实例存储持卡人数据，则不应公开访问 RDS 实例，因为这可能会违反以下要求：确保将对包含持卡人数据的系统组件的访问限制为所需的最小权限或用户需要了解的内容。

修复

移除对 Amazon RDS 数据库的公共访问权限

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 导航到 Databases (数据库)，然后选择公有数据库。
3. 选择 Modify (修改)。
4. Scrocro网络与安全。

5. 对于公开可用性，选择否。
6. 滚动到底部然后选择继续。
7. 下面调度修改，选择立即应用。
8. 选择修改数据库实例。

有关在 VPC 中使用数据库实例的更多信息，请参阅 [Amazon RDS 用户指南](#)。

[pci.redshift.1] Amazon Redshift 集群应禁止公共访问

合规性严重性 重大

资源类型 AWS::Redshift::Cluster

Amazon Config 规则：[redshift-cluster-public-access-check](#)

类型：Schedule 触发变更了

参数：None (无)

此控件通过评估 Amazon Redshift 集群来检查是否可以公开访问publiclyAccessible群集配置项目中的字段。

Note

亚太地区 (大阪) 不支持此控件。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您使用 Amazon Redshift 集群存储持卡人数据，则该集群不应公开访问。允许这样做可能违反只允许必要的流量进出 CDE 的要求。

PCI DSS 1.3.1 实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果您使用 Amazon Redshift 集群存储持卡人数据，则该集群不应公开访问。允许这样做可能会违反将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件的要求。

PCI DS 1.3.2：将入站互联网流量限制为 DMZ 内的 IP 地址。

如果您使用 Amazon Redshift 集群存储持卡人数据，则不应公开访问该集群，因为这可能违反将入站互联网流量限制在 DMZ 内 IP 地址的要求。

PIC DS 1.3.4：不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果您使用 Amazon Redshift 集群存储持卡人数据，则该集群不应公开访问。允许这样做可能违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DS 1.3.6：将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

如果您使用 Amazon Redshift 集群存储持卡人数据，则该集群不应公开访问。允许这样做可能违反将存储持卡人数据的系统组件放置在内部网络区域中的要求，该区域与 DMZ 和其他不可信网络隔离。

修复

禁用 Amazon Redshift 集群的公共访问

1. 打开位于 <https://console.aws.amazon.com/redshift/> 的 Amazon Redshift 控制台。

2. 在导航窗格中，选择集群然后选择您的公用 Amazon Redshift 集群。
3. 来自的Cluster下拉菜单中，选择修改集群。
4. 中公开访问，选择否。
5. 选择 Modify (修改)。

有关在 VPC 中创建集群的更多信息，请参阅。[Amazon Redshift 管理指南](#)。

[PCI.S3.1] S3 存储桶应禁止公开写入访问

合规性严重性 重大

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-public-write-prohibited](#)

Schchule 结构：定期触发，变更触发

参数：None (无)

该控制评估“阻止公开访问”设置、存储桶策略和存储桶访问控制列表 (ACL)，以检查 S3 存储桶是否允许公开写入访问。

它不会检查内部委托人 (例如 IAM 角色) 是否具有对存储桶的写入权限。您应该确保限制仅授权的委托人可以访问存储桶。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DS 1.2.1：将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您使用 S3 存储桶存储持卡人数据，存储桶应禁止公开写入访问。允许公开写入访问可能会违反以下要求：仅允许与 CDE 之间的所需流量。

PCI DS 1.3.1：实施 DMZ，将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果您使用 S3 存储桶存储持卡人数据，存储桶应禁止公开写入访问。允许公开写入访问可能会违反以下要求：将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。

除非您明确要求 Internet 上的每个人能够写入到 S3 存储桶，否则，应确保 S3 存储桶不能公开写入。

PCI DS 1.3.2：将入站互联网流量限制为 DMZ 内的 IP 地址。

如果您使用 S3 存储桶存储持卡人数据，存储桶应禁止公开写入访问。允许公共写入访问可能违反将入站互联网流量限制在 DMZ 内 IP 地址的要求。

PIC DS 1.3.4：不要允许来自持卡人数据环境的未经授权的出站流量进入互联网。

如果您使用 S3 存储桶存储持卡人数据，存储桶应禁止公开写入访问。允许公共写入访问可能违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DS 1.3.6：将存储持卡人数据的系统组件 (例如数据库) 放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

如果您使用 S3 存储桶存储持卡人数据，存储桶应禁止公开写入访问。允许公开写入访问可能会违反以下要求：将存储持卡人数据的系统组件放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。

PCI DS 7.2.1：为系统组件建立访问控制系统，根据用户的知情需要限制访问，除非特别允许，否则设置为“全部拒绝”。此访问控制系统必须包括以下参数：覆盖所有系统组件。

如果您使用 S3 存储桶存储持卡人数据，存储桶应禁止公开写入访问。允许公开写入访问可能会违反以下要求：确保将对系统组件的访问限制为所需的最小权限或用户需要了解的内容。

修复

删除 S3 存储桶的公开访问权限

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台 : <https://console.aws.amazon.com/s3/>。
2. 选择在结果中指定的存储桶的名称。
3. 选择 Permissions (权限), 然后选择 Public access settings (公有访问权限) 设置。
4. 选择 Edit (编辑), 选择所有四个选项, 然后选择 Save (保存)。
5. 如果出现提示, 输入 **confirm**, 然后选择 Confirm (确认)。

[PCI.S3.2] S3 存储桶应禁止公开读取访问

合规性严重性 重大

资源类型 : AWS::S3::Bucket

Amazon Config 规则 : [s3-bucket-public-read-prohibited](#)

Schchule 结构 : 定期触发, 变更触发

参数 : None (无)

该控制评估“阻止公开访问”设置、存储桶策略和存储桶访问控制列表 (ACL), 以检查 S3 存储桶是否允许公开读取访问。

除非您明确要求 Internet 上的每个人能够写入到 S3 存储桶, 否则, 应确保 S3 存储桶不能公开写入。

它不会检查内部委托人 (例如 IAM 角色) 是否具有对存储桶的读取权限。您应该确保限制仅授权的委托人可以访问存储桶。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关 :

PCI DS 1.2.1 : 将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量, 并特别拒绝所有其他流量。

如果您使用 S3 存储桶存储持卡人数据, 存储桶应禁止公开读取访问。公开读取访问可能会违反以下要求 : 仅允许与 CDE 之间的所需流量。

PCI DS 1.3.1 : 实施 DMZ, 将入站流量限制为仅限提供经授权的可公开访问服务、协议和端口的系统组件。

如果您使用 S3 存储桶存储持卡人数据, 存储桶应禁止公开读取访问。公开读取访问可能会违反以下要求 : 将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。

PCI DS 1.3.2 : 将入站互联网流量限制为 DMZ 内的 IP 地址。

如果您使用 S3 存储桶存储持卡人数据, 存储桶应禁止公开读取访问。公共读取权限可能违反将入站互联网流量限制在 DMZ 内 IP 地址的要求。

PCI DS 1.3.6 : 将存储持卡人数据的系统组件 (例如数据库) 放置在与 DMZ 和其他不可信网络隔离的内部网络区域中。

如果您使用 S3 存储桶存储持卡人数据, 存储桶应禁止公开读取访问。公开读取访问可能会违反以下要求 : 将存储持卡人数据的系统组件放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。

PCI DS 7.2.1 : 为系统组件建立访问控制系统, 根据用户的知情需要限制访问, 除非特别允许, 否则设置为“全部拒绝”。此访问控制系统必须包括以下参数 : 覆盖所有系统组件。

如果您使用 S3 存储桶存储持卡人数据, 存储桶应禁止公开读取访问。公开读取访问可能会违反以下要求 : 确保将对系统组件的访问限制为所需的最小权限或用户需要了解的内容。

修复

删除 S3 存储桶的公开访问权限

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台 : <https://console.aws.amazon.com/s3/>。
2. 选择在结果中指定的存储桶的名称。
3. 选择 Permissions (权限), 然后选择 Public access settings (公有访问权限) 设置。
4. 选择 Edit (编辑), 选择所有四个选项, 然后选择 Save (保存)。
5. 如果出现提示, 输入 **confirm**, 然后选择 Confirm (确认)。

[PCI.S3.3] S3 存储桶应启用跨区域复制

合规性严重性 低

资源类型 : AWS::S3::Bucket

Amazon Config 规则 : [s3-bucket-replication-enabled](#)

Schchule 结构 : 触发变更了

参数 : None (无)

该控制检查 S3 存储桶是否启用了跨区域复制。

PCI DSS 不需要使用数据复制或高可用性配置。不过, 该检查符合该控制的 Amazon 最佳实践。

除了可用性以外, 您还应该考虑其他系统强化设置。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关 :

PCI DSS 2.2 : 为所有系统组件制定配置标准。确保这些标准解决了所有已知的安全漏洞, 并与行业认可的系统强化标准保持一致。

在 S3 存储桶上启用跨区域复制可确保数据的多个版本在不同的区域可用。这样, 您就可以在甚至更远的位置中存储数据, 最小限度减少延迟, 提高运行效率以及防范 DDoS 和数据损坏事件。

这是一种用于实施系统强化配置的方法。

修复

启用 S3 存储桶复制

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台 : <https://console.aws.amazon.com/s3/>。
2. 选择未启用跨区域复制的 S3 存储桶。
3. 选择管理, 然后选择复制。
4. 选择 Add rule。如果尚未启用版本控制, 则会提示您启用该功能。
5. 选择您的源存储桶-整个桶。
6. 选择目标存储桶。如果尚未在您的账户的目标存储桶上启用版本控制, 则会提示您启用该功能。
7. 选择一个 IAM 角色。有关设置复制权限的更多信息, 请参阅 [Amazon Service 用户指南](#)。
8. 输入规则名称, 选择 Enabled 对于状态, 然后选择下一页。
9. 选择 Save (保存)。

有关复制的更多信息，请参阅[Amazon Service 用户指南](#)。

[PCI.S3.4] S3 存储桶应启用服务器端加密

合规性严重性 中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-server-side-encryption-enabled](#)

Schchule 结构：触发变更了

参数：None (无)

此控制会检查您的 Amazon S3 存储桶是否启用了 Amazon S3 默认加密，或者 S3 存储桶策略是否明确拒绝了未经服务器端加密的放置对象请求。

如果在存储桶上设置默认加密，存储桶中存储的所有新对象将在存储时进行加密，包括明文 PAN 数据。

也可以使用存储桶策略强制对存储桶中存储的所有对象进行服务器端加密。有关服务器端加密的更多信息，请参阅[Amazon Service 用户指南](#)。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 3.4：无论存储在何处（包括便携式数字媒体、备份媒体和日志），主账号 (PAN) 都无法读取。

如果您使用 S3 存储桶存储信用卡主账号 (PAN)，要使 PAN 不可读，应启用存储桶默认加密以及/或者 S3 存储桶策略应明确拒绝没有服务器端加密的放置对象请求。

修复

对 S3 存储桶启用默认加密

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 从列表中选择存储桶。
3. 选择 Properties (属性)。
4. 在 Default encryption (默认加密) 下，请选择 Edit (编辑)。
5. 通过选择以启用服务器端加密启用。然后，选择其中一个SSE-3要么SE-KMS。
 - 要使用由 Amazon S3 托管的密钥进行默认加密，请选择SSE-3。有关使用 Amazon S3 服务器端加密对数据进行加密的更多信息，请参阅[Amazon Service 用户指南](#)。
 - 使用由管理的密钥Amazon KMS对于默认加密，选择SE-KMS。然后从已创建的 Amazon KMS 主密钥列表选择一个主密钥。

如果您选择SE-KMS键入的Amazon 资源名称 (ARN)Amazon KMS要使用的密钥。您可以找到您的ARNAmazon KMS在 IAM 控制台下键入加密密钥。或者，您可以从下拉列表选择一个键名。

Important

如果您将 Amazon KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的 RPS (每秒请求数) 限制。有关的更多信息Amazon KMS限制以及如何请求提高限制，请参阅[Amazon Key Management Service开发人员指南](#)。

有关创建Amazon KMS钥匙，看看[Amazon Key Management Service开发人员指南](#)。

有关使用的更多信息Amazon KMS有关 Amazon S3，请参阅[Amazon Service 用户指南](#)。

在启用默认加密时，您可能需要更新存储桶策略。有关从存储桶策略转为默认加密的更多信息，请参阅。[Amazon Service 用户指南](#)。

6. 选择 Save (保存)。

有关默认 S3 存储桶加密的更多信息，请参阅。[Amazon Service 用户指南](#)。

[PCI.S3.5] S3 存储桶应要求请求才能使用安全套接字层

合规性严重性 中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-ssl-requests-only](#)

Schhule 结构：触发变更了

参数：None (无)

此控制检查 Amazon S3 存储桶是否有要求请求使用安全套接字层 (SSL) 的策略。

S3 存储桶应具有要求所有请求的策略 (Action: S3:*) 在 S3 资源策略中仅接受通过 HTTPS 传输数据，由条件密钥指示aws:SecureTransport。

这不检查 SSL 或 TLS 版本。根据 PCI DSS 的要求，您不应允许使用早期版本的 SSL 或 TLS (SSLv3、TLS1.0)。

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 4.1 在通过开放的公共网络传输过程中，使用强大的加密和安全协议来保护敏感的持卡人数据。

如果您使用 S3 存储桶存储持卡人数据，请确保存储桶策略要求对存储桶的请求仅接受通过 HTTPS 传输数据。例如，可以使用策略声明"aws:SecureTransport": "false"拒绝任何未通过 HTTPS 访问的请求。允许未加密传输持卡人数据可能违反在通过开放的公共网络传输过程中使用强加密和安全协议来保护敏感的持卡人数据的要求。

修复

要修复此问题，请更新 S3 存储桶的权限策略。

将 S3 存储桶配置为拒绝非安全传输

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 导航到不合规的存储桶，然后选择存储桶名称。
3. 选择 Permissions (权限)，然后选择 Bucket Policy (存储桶策略)。
4. 在下面的政策中添加类似的政策声明。Replace (替换) awsexamplebucket使用要修改的存储桶的名称。

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
```



```
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::awsexamplebucket",
      "arn:aws:s3:::awsexamplebucket/*"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    },
    "Principal": "*"
  }
]
```

5. 选择 Save (保存)。

有关更多信息，请参阅知识中心文章[要符合 S3 存储桶策略Amazon Config规则 s3-bucket-ssl-requests-only?](#)。

[PCI.S3.6] 应启用 S3 阻止公有访问设置

合规性严重性 中

资源类型：S3Amazon帐户

Amazon Config 规则：[s3-account-level-public-access-blocks-periodic](#)

Schedule 结构：定期

参数：

- ignorePublicAcls: true
- blockPublicPolicy: true
- blockPublicAcls: true
- restrictPublicBuckets: true

此控件检查是否在账户级别配置了以下公共访问屏蔽设置。

- ignorePublicAcls: true,
- blockPublicPolicy: true
- blockPublicAcls: true
- restrictPublicBuckets: true

如果所有公共访问屏蔽设置都设置为，则控制通过true。

如果将任何设置设置为，则控件将失败false，或者如果未配置任何设置。

作为Amazon最佳实践，S3 存储桶应阻止公共访问。除非您明确地要求 Internet 上的所有人都能访问您的 S3 存储桶，否则您应该确保您的 S3 存储桶不可公开访问。

Note

以下区域不支持此控制。

- 亚太地区 (大阪)
- Europe (Milan)

- Middle East (Bahrain)

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 1.2.1-将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您使用 S3 存储桶存储持卡人数据，请确保该存储桶不允许公共访问。对 S3 存储桶的公共访问可能违反了仅允许进出 CDE 的必要流量的要求。

PCI DSS 1.3.1-实施 DMZ，将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件。

如果您使用 S3 存储桶存储持卡人数据，请确保该存储桶不允许公共访问。允许公共访问您的 S3 存储桶可能违反将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件的要求。

PCI DSS 1.3.2-将入站互联网流量限制为隔离区内的 IP 地址。

如果您使用 S3 存储桶存储持卡人数据，请确保该存储桶不允许公共访问。允许公有访问您的 S3 存储桶可能违反将入站流量限制在 DMZ 内 IP 地址的要求。

PCI DSS 1.3.4 不允许未经授权的出站流量从持卡人数据环境流向互联网。

如果您使用 S3 存储桶存储持卡人数据，请确保该存储桶不允许公共访问。允许公众访问您的 S3 存储桶可能违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 1.3.6 将存储持卡人数据的系统组件（例如数据库）放置在内部网络区域中，与 DMZ 和其他不可信网络隔离。

如果您使用 S3 存储桶存储持卡人数据，请确保该存储桶不允许公共访问。允许公众访问您的 S3 存储桶可能违反将存储持卡人数据的系统组件放置在内部网络区域中的要求，与 DMZ 和其他不可信网络隔离。

修复

启用 Amazon S3 阻止公有访问

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 在导航窗格中，选择阻止公共访问（账户设置）。
3. 选择 Edit（编辑）。然后选择Block（阻止）所有公有访问权限。
4. 选择 Save changes（保存更改）。

有关更多信息，请参阅。[使用 Amazon S3 阻止公有访问](#)在Amazon Service 用户指南。

[PCI。SageMaker.1] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网

合规性严重性 高

资源类型：AWS::SageMaker::NotebookInstance

Amazon Config 规则：[sagemaker-notebook-no-direct-internet-access](#)

Schchule 结构：定期

参数：None（无）

此控件检查是否禁用了直接互联网接入 SageMaker 笔记本实例。为此，它会检查是否DirectInternetAccess该笔记本实例的字段已禁用。

如果您配置您的 SageMaker 没有 VPC 的实例，则默认情况下，您的实例上启用了直接互联网访问。您应该使用 VPC 配置您的实例，并将默认设置更改为禁用-通过 VPC 访问 Internet。

要使用笔记本电脑训练或托管模型，您需要访问互联网。要启用互联网访问，请确保您的 VPC 有 NAT 网关并且您的安全组允许出站连接。要了解有关如何将笔记本实例连接到 VPC 中的资源的更多信息，请参阅[将笔记本实例连接到 VPC 中的资源](#)在亚马逊 SageMaker 开发人员指南。

您还应确保访问您的 SageMaker 配置仅限于授权用户。限制用户的 IAM 修改权限 SageMaker 设置和资源。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 1.2.1-将入站和出站流量限制为持卡人数据环境 (CDE) 所需的流量，并特别拒绝所有其他流量。

如果您将 SageMaker 您的 CDE 中的笔记本实例，请确保笔记本实例不允许直接访问互联网。允许公共直接访问您的笔记本实例可能违反只允许必要的流量进出 CDE 的要求。

PCI DSS 1.3.1-实施 DMZ，将入站流量限制为仅提供经授权的可公开访问服务、协议和端口的系统组件。

如果您将 SageMaker 您的 CDE 中的笔记本实例，请确保笔记本实例不允许直接访问互联网。允许对笔记本实例进行直接公共访问可能违反仅允许访问提供经授权的可公开访问服务、协议和端口的系统组件的要求。

PCI DSS 1.3.2-将入站互联网流量限制为隔离区内的 IP 地址。

如果您将 SageMaker 您的 CDE 中的笔记本实例，请确保笔记本实例不允许直接访问互联网。允许对笔记本电脑实例进行直接公共访问可能违反将入站流量限制在 DMZ 内 IP 地址的要求。

PCI DSS 1.3.4 不允许未经授权的出站流量从持卡人数据环境流向互联网。

如果您将 SageMaker 您的 CDE 中的笔记本实例，请确保笔记本实例不允许直接访问互联网。允许公众直接访问您的笔记本电脑实例可能违反阻止从持卡人数据环境到互联网的未经授权的出站流量的要求。

PCI DSS 1.3.6 将存储持卡人数据的系统组件（例如数据库）放置在内部网络区域中，与 DMZ 和其他不可信网络隔离。

如果您将 SageMaker 笔记本电脑实例和笔记本电脑实例包含持卡人数据，限制直接访问互联网。允许公众直接访问您的笔记本电脑实例可能违反将存储持卡人数据的系统组件放置在内部网络区域中的要求，与 DMZ 和其他不可信网络隔离。

修复

请注意，在创建笔记本实例后，您无法更改互联网访问设置。必须停止、删除和重新创建它。

要配置 SageMaker 拒绝直接访问互联网的笔记本实例

1. 打开 SageMaker 控制台为<https://console.aws.amazon.com/sagemaker/>

2. 导航到笔记本实例。
3. 删除启用了直接互联网接入的实例。选择实例，选择操作，然后选择停止。

在实例停止后选择操作，然后选择删除。
4. 选择创建笔记本实例。提供配置详情。
5. 扩展Network部分。然后选择 VPC、子网和安全组。下面直接访问 Internet，选择禁用-通过 VPC 访问 Internet。
6. 选择创建笔记本实例。

有关更多信息，请参阅 [将笔记本实例Connect 到 VPC 中的资源](#)在亚马逊 SageMaker 开发人员指南。

[PCI.SSM.1] 安装补丁后，由 Systems Manager 管理的 Amazon EC2 实例的补丁合规状态应为“合规”

合规性严重性 中

资源类型：AWS::SSM::PatchCompliance和AWS::EC2::Instance

Amazon Config 规则：[ec2-managedinstance-patch-compliance-status-check](#)

计划：计划：触发变更了

参数：None (无)

此控件检查 Amazon EC2 Systems Manager 补丁合规性的合规性状态是否为COMPLIANT要么NON_COMPLIANT在实例上安装补丁之后。

它仅检查 Amazon Systems Manager Patch Manager 管理的实例。

它不会检查是否在 PCI DSS 要求 6.2 规定的 30 天限制内应用补丁。

它也不会验证应用的补丁是否归类为安全补丁。

您应使用适当的基准设置创建补丁组，并确保范围内的系统由 Systems Manager 中的这些补丁组管理。有关补丁组的更多信息，请参阅[Amazon Systems Manager用户指南](#)。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 6.2：通过安装供应商提供的适用安全补丁，确保所有系统组件和软件免受已知漏洞的侵害。请在发布后的一个月内存安装重要安全补丁。

供应商为 PCI DSS 范围内的系统发布的补丁应在生产环境中安装之前经过测试和验证。部署后，应验证安全设置和控制，以确保部署的补丁不会影响持卡人数据环境 (CDE) 的安全性。

如果您使用由管理的 Amazon EC2 实例Amazon Systems ManagerPatch Manager 要修补您的 CDE 中的托管实例，请确保补丁已成功应用。为此，请检查 Amazon EC2 Systems Manager 补丁合规性的合规状态是否为“合规”。Patch Manager 可以应用操作系统和应用程序的适用补丁。

这是一种用于保护系统组件和软件以免受到已知漏洞攻击的方法。

修复

修复不合规的补丁

该规则检查 Amazon EC2 Systems Manager 补丁合规性的合规状态是合规还是不合规。要了解有关补丁合规性数据的信息，请参阅[Amazon Systems Manager 用户指南](#)。

1. 访问 <https://console.aws.amazon.com/systems-manager/>，打开 Amazon Systems Manager 控制台。
2. 在导航窗格中，在节点管理，选择运行命令。
3. 选择 Run command (运行命令)。
4. 选择 AWS-RunPatchBaseline 旁边的单选按钮，然后将 Operation (操作) 更改为 Install (安装)。
5. 选择手动选择实例然后选择不合规的实例。
6. 滚动到底部，然后选择 Run (运行)。
7. 在该命令完成后，要监控修补的实例的新合规性状态，请在导航窗格中选择 Compliance (合规性)。

请参阅 Amazon Systems Manager 用户指南有关以下内容的更多信息

- [使用 Systems Manager 文档修补托管实例](#)
- [使用 Systems Manager 运行命令运行命令](#)

[PCI.SSM.2] 由 Systems Manager 管理的实例的关联合规状态应为 COMPLIANT

合规性严重性 低

资源类型：AWS::SSM::AssociationCompliance

Amazon Config 规则：[ec2-managedinstance-association-compliance-status-check](#)

Schedule 结构：触发变更了

参数：None (无)

此控件检查状态是否 Amazon Systems Manager 协会合规性是 COMPLIANT 要么 NON_COMPLIANT 在实例上运行关联之后。如果关联合规状态为，则控制通过 COMPLIANT。

状态管理器关联是分配给您的托管实例的配置。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，或必须关闭特定端口。

创建一个或多个 State Manager 关联之后，控制台、控制台、响应中将立即出现合规性状态信息 Amazon CLI 命令或相应的 Systems Manager API 操作。对于协会而言，配置合规性显示状态合规要么不合规以及分配给关联的严重性级别，例如关键要么中。要了解有关州经理协会合规性的更多信息，请参阅[关于州经理协会合规性](#)在 Amazon Systems Manager 用户指南。

您必须为 Systems Manager 关联配置范围内的 EC2 实例。您还必须为补丁供应商的安全评级配置补丁基准，并将自动批准日期设置为满足 PCI DSS 3.2.1 要求 6.2。有关如何创建关联的更多指南，请参阅[创建关联](#)在 Amazon Systems Manager 用户指南。有关在 Systems Manager 中使用补丁的更多信息，请参阅[Amazon Systems Manager 补丁管理器](#)在 Amazon Systems Manager 用户指南。

Note

以下区域不支持此控制。

- 非洲 (开普敦)

- 亚太地区 (大阪)
- 欧洲 (米兰)

相关的 PCI DSS 要求

此控制与以下 PCI DSS 要求有关。

PCI DSS 2.4 维护 PCI DSS 范围内的系统组件清单。

如果您使用由 Systems Manager 管理的 EC2 实例来收集持卡人数据环境 (CDE) 的清单，请确保这些实例已成功关联。为此，请检查 Systems Manager 关联合规性的合规性状态是否为 COMPLIANT。使用 Systems Manager 可以帮助维护 PCI DSS 范围内的系统组件清单。有关如何组织库存的更多指导，请参阅[为库存配置资源数据同步](#)在 Amazon Systems Manager 用户指南。

修复

关联失败可能与不同的事物有关，包括目标和 SSM 文档名称。要修复此问题，必须首先确定并调查这种关联。然后，您可以更新关联以更正特定问题。

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，Systems Manager 会创建一个新版本。

调查和更新失败的关联

1. 访问 <https://console.aws.amazon.com/systems-manager/>，打开 Amazon Systems Manager 控制台。
2. 在导航窗格中，在节点管理，选择 Fleet Manager。
3. 选择具有实例 ID 协会状态的已失败。
4. 请选择 View details (查看详细信息)。
5. 选择 Associations。
6. 记下具有以下条件的关联的名称协会状态的已失败。这是您需要调查的关联。在下一步骤中，您需要使用关联名称。
7. 在导航窗格中，在节点管理，选择 State Manager。搜索协会名称，然后选择该协会。

确定问题后，编辑失败的关联以更正问题。有关如何编辑关联的信息，请参阅[编辑关联](#)。

有关创建和编辑状态管理器关联的更多信息，请参见[在 Systems Manager 中使用关联](#)。在 Amazon Systems Manager 用户指南。

[PCI.SSM.3] EC2 实例应由以下人员管理 Amazon Systems Manager

合规性严重性 中

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-instance-managed-by-systems-manager](#)

Schule 结构：触发变更了

参数：None (无)

此控件会检查您账户中的 EC2 实例是否由 Systems Manager 托管。

Amazon Systems Manager 是一个 Amazon 您可以用来查看和控制您的服务 Amazon 基础设施。为了帮助您维护安全性和合规性，Systems Manager 会扫描您的托管实例。托管实例是一台已配置为与 Systems Manager 一起使用的机器。然后，Systems Manager 会报告其发现的任何违反政策的行为或采取纠正措

施。Systems Manager 还帮助您配置和维护托管实例。需要在 Systems Manager 中进行额外配置，才能将补丁部署到托管 EC2 实例。

要了解有关更多信息，请参阅 [Amazon Systems Manager 用户指南](#)。

相关的 PCI DSS 要求

该控制与以下 PCI DSS 要求相关：

PCI DSS 2.4 维护 PCI DSS 范围内的系统组件清单。

如果您使用由 Systems Manager 管理的 EC2 实例来收集持卡人数据环境 (CDE) 的清单，请确保这些实例由 Systems Manager 管理。使用 Systems Manager 可以帮助维护 PCI DSS 范围内的系统组件清单。有关如何组织库存的更多指导，请参阅 [Inventory 配置资源数据同步](#) 在 Amazon Systems Manager 用户指南。

PCI DSS 6.2 通过安装适用的供应商提供的安全补丁，确保所有系统组件和软件免受已知漏洞的侵害。请在发布后的一个月内安装重要安全补丁。

对于 PCI DSS 范围内的系统，在生产环境中安装供应商补丁之前，应先对其进行测试和验证。部署补丁后，验证安全设置和控制，以确保部署的补丁不会影响 CDE 的安全性。如果您使用由 Systems Manager 管理的 EC2 实例来修补 CDE 中的托管实例，请确保这些实例由 Systems Manager 管理。Systems Manager 部署系统补丁，这有助于保护系统组件和软件免受已知漏洞的侵害。

修复

您可以使用 Systems Manager 快速设置来设置 Systems Manager 来管理 EC2 实例。

要确定您的实例是否支持 Systems Manager 关联，请参阅 [Systems Manager](#) 在 Amazon Systems Manager 用户指南。

要确保 EC2 实例由 Systems Manager 管理

1. 访问 <https://console.aws.amazon.com/systems-manager/>，打开 Amazon Systems Manager 控制台。
2. 在导航窗格中，选择快速设置。
3. 在配置屏幕上，保留默认选项。
4. 选择 Set up Systems Manager (设置 Systems Manager)。

您可能希望禁用的 PCI DSS 控件

为了节省成本 Amazon Config，您可以禁用除一个区域以外的所有区域录制全球资源。然后禁用这些控件，这些控件处理除运行全球录制的区域之外的所有区域中的全局资源。

- [the section called "\[PCI.CW.1\] 应具有有关“根”用户使用的日志指标筛选器和警报” \(p. 320\)](#)
- [the section called "\[PCI.IAM.1\] IAM 根用户访问密钥不应存在” \(p. 333\)](#)
- [the section called "\[PCI.IAM.2\] IAM 用户不应附加 IAM 策略” \(p. 334\)](#)
- [the section called "\[PCI.IAM.3\] IAM 策略不应允许完全“*”管理权限” \(p. 335\)](#)
- [the section called "\[PCI.IAM.4\] 应该为根用户启用硬件 MFA” \(p. 335\)](#)
- [the section called "\[PCI.IAM.5\] 应该为根用户启用虚拟 MFA” \(p. 336\)](#)
- [the section called "\[PCI.IAM.6\] 应为所有 IAM 用户启用 MFA” \(p. 337\)](#)

如果您禁用这些控件并禁用特定区域中的全局资源记录，则还应禁用 [\[PCI.Config.1\] 应该启用 Amazon Config \(p. 319\)](#)。这是因为 [\[PCI.Config.1\] 应该启用 Amazon Config \(p. 319\)](#) 需要全局资源记录才能通过。

Amazon 基础安全最佳实践标准

Amazon 基础安全最佳实践标准是一组控件，用于检测部署的账户和资源偏离安全最佳实践的情况。

通过该标准，您可以持续评估所有 Amazon 账户和工作负载，以快速识别偏离最佳实践的领域。它针对如何改善和维护组织安全状况，提供了可操作的规范性指导。

这些控件包括来自多种 Amazon 服务的最佳实践。为每个控件分配一个类别以反映它应用于的安全功能。请参阅 [the section called “控件类别” \(p. 494\)](#)。

主题

- [Amazon 基础安全最佳实践控件所需的 Amazon Config 资源 \(p. 361\)](#)
- [Amazon 基础安全最佳实践控件 \(p. 362\)](#)
- [控件类别 \(p. 494\)](#)
- [您可能希望禁用的 Amazon 基础最佳实践控件 \(p. 496\)](#)

Amazon 基础安全最佳实践控件所需的 Amazon Config 资源

Amazon 基础安全最佳实践控件涉及对以下资源的查询。Amazon Security Hub 为了准确报告触发计划类型为“更改”的控件的调查结果，您必须在中启用对这些资源的记录 Amazon Config。对于具有定期计划类型的控件，您无需记录资源。

Note

在控件不可用的区域中，相应的一个或多个资源在中不可用 Amazon Config。

- AWS::ACM::Certificate
- AWS::ApiGateway::Stage
- AWS::ApiGatewayV2::Stage
- AWS::AutoScaling::AutoScalingGroup
- AWS::AutoScaling::LaunchConfiguration
- AWS::CloudFormation::Stack
- AWS::CloudFront::Distribution
- AWS::CodeBuild::Project
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NetworkAcl
- AWS::EC2::SecurityGroup
- AWS::EC2::Subnet
- AWS::EC2::TransitGateway
- AWS::EC2::Volume
- AWS::EC2::VPNConnection
- AWS::ECR::Repository
- AWS::ECS::Cluster
- AWS::ECS::Service
- AWS::ECS::TaskDefinition
- AWS::EFS::AccessPoint
- AWS::EKS::Cluster
- AWS::ElasticBeanstalk::Environment
- AWS::ElasticLoadBalancing::LoadBalancer

- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::IAM::Group
- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User
- AWS::Kinesis::Stream
- AWS::Lambda::Function
- AWS::NetworkFirewall::FirewallPolicy
- AWS::OpenSearch::Domain
- AWS::RDS::DBCluster
- AWS::RDS::DBClusterSnapshot
- AWS::RDS::DBInstance
- AWS::RDS::DBSnapshot
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::SecretsManager::Secret
- AWS::SNS::Topic
- AWS::SQS::Queue
- AWS::SSM::AssociationCompliance
- AWS::SSM::PatchCompliance
- AWS::WAFRegional::Rule
- AWS::WAFRegional::RuleGroup
- AWS::WAFRegional::WebACL
- AWS::WAF::Rule
- AWS::WAF::RuleGroup
- AWS::WAF::WebACL

Amazon 基础安全最佳实践控件

Amazon 基础安全最佳实践标准包含以下控件。对于每个控件，介绍内容包括以下信息。

- 控件适用的类别。有关类别的说明，请参阅[the section called “控件类别” \(p. 494\)](#)。
- 严重程度
- 控件评估的适用资源。我们还列出了控件的依赖资源。对于变更触发的控件，必须将资源记录在 Amazon Config 才能使控件生效。有关更多信息，请参阅[Amazon 基础安全最佳实践控件所需的 Amazon Config 资源 \(p. 361\)](#)。
- 必需的 Amazon Config 规则以及由 Amazon Security Hub 设置的任意特定参数值
- 补救步骤

请注意，控制编号中的空白表示控件尚未发布。如果将某个控件标记为“已停用”，则 Security Hub 不会生成该控件的查找结果。

按服务分类的控件

[Amazon Certificate Manager \(p. 364\)](#)

[Amazon API Gateway \(p. 365\)](#)
[Amazon EC2 Auto Scaling \(p. 368\)](#)
[Amazon CloudFormation \(p. 372\)](#)
[亚马逊 CloudFront \(p. 373\)](#)
[Amazon CloudTrail \(p. 378\)](#)
[Amazon CodeBuild \(p. 382\)](#)
[Amazon Config \(p. 385\)](#)
[Amazon Database Migration Service \(p. 386\)](#)
[Amazon DynamoDB \(p. 386\)](#)
[Amazon EC2 \(p. 388\)](#)
[Amazon ECR \(p. 403\)](#)
[Amazon ECS \(p. 404\)](#)
[AEFS zon \(p. 410\)](#)
[亚马逊 EKS \(p. 412\)](#)
[Amazon Elastic Beanstalk \(p. 413\)](#)
[Elastic Load Balancing \(p. 414\)](#)
[Amazon EMR \(p. 423\)](#)
[亚马逊 ES \(p. 423\)](#)
[亚马逊 GuardDuty \(p. 428\)](#)
[Amazon Identity and Access Management \(p. 428\)](#)
[Amazon Kinesis \(p. 435\)](#)
[Amazon Key Management Service \(p. 436\)](#)
[Amazon Lambda \(p. 439\)](#)
[Amazon Network Firewall \(p. 441\)](#)
[亚马逊 OpenSearch 服务 \(p. 444\)](#)
[Amazon Relational Database Service \(p. 448\)](#)
[Amazon Redshift \(p. 467\)](#)
[Amazon Simple Storage Service \(p. 471\)](#)
[亚马逊 SageMaker \(p. 480\)](#)
[Amazon Secrets Manager \(p. 481\)](#)
[Amazon Simple Notification Service \(p. 484\)](#)
[Amazon Simple Queue Service \(p. 486\)](#)

[Amazon EC2 Systems Manager \(p. 486\)](#)

[Amazon WAF \(p. 489\)](#)

[ACM.1] 导入的和 ACM 颁发的证书应在指定的时间段后续订

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型：AWS::ACM::Certificate

Amazon Config 规则：[acm-certificate-expiration-check](#)

时间表类型：Triger

参数：

- daysToExpiration: 30

此控制检查您账户中的 ACM 证书是否在 30 天内被标记为过期。它会检查导入的证书和 Amazon Certificate Manager 提供的证书。

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，您必须回复域名验证电子邮件。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。

有关 ACM 证书托管续订的更多信息，请参阅《Amazon Certificate Manager 用户指南》中的 [ACM 证书托管续订](#)。

Note

以下区域不支持此控制。

- 非洲 (开普敦)
- China (Beijing)
- China (Ningxia)
- 欧洲 (米兰)

修复

针对您的由 Amazon 颁发的 SSL/TLS 证书，ACM 提供了托管续订。这意味着 ACM 要么自动续订您的证书（如果您使用 DNS 验证），要么在证书过期临近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。

适用于通过电子邮件验证的域

当证书到期 45 天后，ACM 会向域名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《Amazon Certificate Manager 用户指南》中[通过电子邮件验证的域名续订](#)。

适用于通过 DNS 验证的域

ACM 会自动续订使用 DNS 验证的证书。在证书到期前 60 天，ACM 会验证证书是否可以续订。

如果无法验证域名，则 ACM 会发送一条通知，告知需要手动验证。它会在过期前 45 天、30 天、1 天和 1 天的时候发送这些通知。

有关更多信息，请参阅《Amazon Certificate Manager 用户指南》中的 [DNS 验证域的续订](#)。

[ApiGateway.1] 应该启用 API Gateway REST 和 WebSocket API 日志记录

类别：识别 > 记录

严重性：中

资源类型:AWS::ApiGateway::Stage,AWS::ApiGatewayV2::Stage

Amazon Config 规则：[api-gw-execution-logging-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查亚马逊 API Gateway REST 或 WebSocket API 的所有阶段是否都启用了日志记录。如果未为某个阶段的所有方法启用日志记录，或者ERROR既未启用也未启用日志，loggingLevel则控制将失败INFO。

API Gateway RES WebSocket T 或 API 阶段应启用相关日志。API Gateway REST 和 WebSocket API 执行日志提供向 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requestId响应和Amazon集成终端节点。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- 欧洲 (米兰)

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] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证

类别：保护 > 数据保护

严重性：中

资源类型：AWS::ApiGateway::Stage

Amazon Config 规则：[api-gw-ssl-enabled](#)

时间表类型：Triger

参数：None (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，以允许后端系统对来自 API Gateway 的请求进行身份验证。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

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 开发者指南中的[生成和配置用于后端身份验证的 SSL 证书](#)。

[ApiGateway.3] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪

类别：检测 > 检测服务

严重性：低

资源类型：AWS::ApiGateway::Stage

Amazon Config 规则：[api-gw-xray-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查您的亚马逊 API Gateway REST API 阶段是否启用了Amazon X-Ray主动跟踪。

X-Ray 主动跟踪可以更快地响应底层基础设施的性能变化。性能变化可能导致 API 的可用性不足。X-Ray 主动跟踪提供流经您的 API Gateway REST API 操作和互联服务的用户请求的实时指标。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何为 API Gateway REST API 操作启用 X-Ray 主动跟踪的详细说明，请参阅Amazon X-Ray开发者指南Amazon X-Ray中的[Amazon API Gateway 主动跟踪支持](#)。

[ApiGateway.4] API Gateway 应该与Amazon WAF Web ACL 相关联

类别：保护 > 保护服务

严重性：中

资源类型：AWS::ApiGateway::Stage

Amazon Config 规则：[api-gw-associated-with-waf](#)

时间表类型：Triger

参数：None (无)

此控件检查 API Gateway 阶段是否使用 Amazon WAF Web 访问控制列表 (ACL)。如果 Amazon WAF Web ACL 未连接到 REST API Gateway 阶段，则此控制将失败。

Amazon WAF 是一个 Web 应用程序防火墙，可帮助保护 Web 应用程序和 API 免受攻击。通过它，您可以配置 ACL，这是一组规则，基于可自定义的 Web 安全规则以及您定义的条件，允许、阻止或计数 Web 请求。确保您的 API Gateway 阶段与 Amazon WAF Web ACL 相关联，以帮助保护其免受恶意攻击。

Note

以下区域不支持此控件：

- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

有关如何使用 API Gateway 控制台将 Amazon WAF 区域 Web ACL 与现有 API Gateway 阶段相关联的信息，请参阅 API Gateway 开发人员指南中的[使用 Amazon WAF 来保护您的 API](#)。

[ApiGateway.5] API Gateway REST API 缓存数据应该在静态时加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::ApiGateway::Stage

Amazon Config 规则：api-gw-cache-encrypted（由 Security Hub 开发的自定义规则）

时间表类型：Trigger

参数：None（无）

此控件检查 API Gateway REST API 阶段中启用缓存的所有方法是否均已加密。如果 API Gateway REST API 阶段中的任何方法配置为缓存且缓存未加密，则控制将失败。

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。它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，需要有 API 权限才能解密数据，然后才能读取数据。

API Gateway REST API 缓存应进行静态加密，以增加安全层。

修复

要修复此控制，请将阶段配置为加密缓存数据。

为指定阶段配置 API 缓存

1. 通过以下网址打开 API Gateway 控制台：<https://console.aws.amazon.com/apigateway/>。
2. 选择 API。
3. 选择 Stages (阶段)。
4. 在 API 的 Stages (阶段) 列表中，选择要添加缓存的阶段。
5. 选择 Settings。
6. 选择 启用 API 缓存。
7. 更新所需的设置，然后选择“加密缓存数据”。

8. 选择 Save Changes (保存更改)。

[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

类别：识别 > 清单

严重性：低

资源类型：AWS::AutoScaling::AutoScalingGroup

Amazon Config 规则：[autoscaling-group-elb-healthcheck-required](#)

时间表类型：Triger

参数：None (无)

此控件检查与负载均衡器关联的 Auto Scaling 组是否正在使用 Elastic Load Balancing 运行状况检查。

这可确保该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 运行状况检查有助于支持使用 EC2 Auto Scaling 组的应用程序的可用性。

修复

要修复此问题，请更新 Auto Scaling 组以使用 Elastic Load Balancing 运行状况检查。

启用Elastic Load Balancing 运行状况检查

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格的 Auto Scaling 下，选择 Auto Scaling 组。
3. 选中您的 组对应的复选框。
4. 选择 Edit (编辑)。
5. 在运行Health 检查下，对于 Health 检查类型，选择 ELB。
6. 对于 Health check grace period (运行状况检查宽限期)，输入 **300**。
7. 选择页面底部的更新。

有关在 Auto Scaling 组中使用负载均衡器的更多信息，请参阅[Amazon Auto Scaling用户指南](#)。

[AutoScaling.2] Auto Scaling 组应涵盖多个可用区

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::AutoScaling::AutoScalingGroup

Amazon Config 规则：[autoscaling-multiple-az](#)

时间表类型：Triger

参数：None (无)

此控件检查 Auto Scaling 组是否跨越多个可用区。如果 Auto Scaling 组不跨越多个可用区，则控制会失败。

Amazon EC2 Auto Scaling 组可以配置为使用多个可用区。在某些用例中，例如批处理任务或需要将可用区间传输成本保持在最低水平时，首选使用具有单个可用区的 Auto Scaling 组。但是，不跨多个可用区的 Auto Scaling 组不会在另一个可用区启动实例，以补偿配置的单个可用区不可用。

修复

有关如何向现有 Auto Scaling 组添加可用区的信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的[可用区](#)。

[AutoScaling.3] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::AutoScaling::LaunchConfiguration

Amazon Config 规则：[autoscaling-launchconfig-requires-imdsv2](#)

时间表类型：Triger

参数：None (无)

此控件检查是否在 Amazon EC2 Auto Scaling 组启动的所有实例上启用了 IMDSv2。如果实例元数据服务 (IMDS) 版本未包含在启动配置中，或者如果同时启用了 IMDSv1 和 IMDSv2，则控制将失败。

IMDS 提供有关您的实例的数据，可以用来配置或管理正在运行的实例。

IMDS 版本 2 增加了在 IMDSv1 中没有的新保护措施，以进一步保护您的 EC2 实例。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

Auto Scaling 组一次与一个启动配置关联。在创建启动配置后，您无法修改启动配置。要更改 Auto Scing 组的启动配置，请将现有的启动配置作为启用 IMDSv2 的新启动配置的基础。有关更多信息，请参阅适用于 Linux 实例的 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数限制不应大于1

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::AutoScaling::LaunchConfiguration

Amazon Config 规则：[autoscaling-launch-config-hop-limit](#)

时间表类型：Triger

参数：None (无)

此控件检查元数据令牌可以传输的网络跳数。如果元数据响应跳数限制大于，则控制失败1。

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 HTTPPUT 响应限制为 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) 字段每跳减少一个。这种减少可以用来确保数据包不会在 EC2 之外传输。IMDSv2 保护可能被错误配置为开放式路由器、第 3 层防火墙、VPN、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 IMDSv2 时，包含密钥令牌的 PUT 响应无法传送到实例外部，因为默认元数据响应跳数限制设置为 1。但是，如果该值大于 1，则令牌可以离开 EC2 实例。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

有关如何修改现有启动配置的元数据响应跳数限制的详细说明，请参阅 Amazon EC2 Linux 实例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 Amazon EC2 实例不应具有公有 IP 地址

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::AutoScaling::LaunchConfiguration

Amazon Config 规则：[autoscaling-launch-config-public-ip-disabled](#)

时间表类型：Trigger

参数：None（无）

此控件检查 Auto Scaling 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，则控制将失败。

Auto Scaling 组启动配置中的 Amazon 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。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- 亚太地区（大阪）
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

Auto Scaling 组一次与一个启动配置关联。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，如以下步骤所述。

更改 Auto Scaling 组的启动配置后，将使用新的配置选项启动所有 new Scaling 组的启动配置后，将使用新的配置选项启动所有新的实例。现有实例不会受到影响。要更新现有实例，请终止这些实例，以便 Auto Scaling 组替换这些实例，或者根据您的[终止策略](#)启用自动扩展，以逐步使用较新实例替换较旧实例。

启用Elastic Load Balancing 运行状况检查

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格的 Auto Scaling 下，选择启动配置。
3. 选择启动配置并依次选择 Actions、A ctions，然后依次选择 A 这将设置与原启动配置选项相同的新启动配置，但在名称中会增加“Copy”文本。
4. 在“创建启动配置”页面上，展开“其他配置-可选”下的“高级详细信息”。
5. 在 IP 地址类型下，选择请勿向任何实例分配公有 IP 地址。
6. 完成后，选择创建启动配置。
7. 在导航窗格的 Auto Scaling 下，选择 Auto Scaling 组。
8. 选中 Auto Scaling 组旁边的复选框。
9. 将在页面底部打开一个拆分窗格，其中显示有关所选组的信息。
10. 在详细信息选项卡上，选择启动配置、编辑。
11. 对于启动配置，选择新的启动配置。
12. 更改完启动配置后，选择 Update。

[AutoScaling.6] Auto Scaling 组应在多个可用区中使用多个实例类型

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::AutoScaling::AutoScalingGroup

Amazon Config 规则：[autoscaling-multiple-instance-types](#)

时间表类型：Triger

参数：None (无)

该控件检查 Amazon EC2 Auto Scaling 组是否使用多个实例类型。如果 Auto Scaling 组仅定义了一个实例类型，则控制会失败。

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。Secury Hub 建议使用多个实例类型，这样，如果您选择的可用区中实例容量不足，Auto Scaling 组可以启动另一种实例类型。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关创建具有多个实例类型的 Auto Scaling 组的说明，请参阅 Amazon EC2 AAuto Scaling 用户指南中的具有多个实例类型和购买选项的Auto Scaling [组](#)。

[AutoScaling.9] EC2 Auto Scaling 组应使用 EC2 启动模板

类别：识别 > 资源配置

严重性：中

资源类型：AWS::AutoScaling::AutoScalingGroup

Amazon Config 规则：[autoscaling-launch-template](#)

时间表类型：Triger

参数：None (无)

此控件会检查 Amazon EC2 Auto Scaling 组是否是从 EC2 启动模板创建的。如果 Amazon EC2 Auto Scaling 组不是使用启动模板创建的，或者没有在混合实例策略中指定启动模板，则此控制将失败。

EC2 Auto Scaling 组可以从 EC2 启动模板或启动配置创建。但是，使用启动模板创建 Auto Scaling 组可确保您可以使用最新的功能和改进。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要使用 EC2 启动模板创建 AAuto Scaling 组，请参阅 Amazon EC2 AAuto Scaling 用户指南中的使用启动模板创建 AAuto Scaling [组](#)。有关如何使用启动模板替换启动配置的信息，请参阅 Amazon EC2 Windows 实例用户指南中的将启动配置替换为 [启动模板](#)。

[CloudFormation.1] CloudFormation 堆栈应与 Simple Notification Service (SNS) 集成

类别：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::CloudFormation::Stack

Amazon Config 规则：[cloudformation-stack-notification-check](#)

时间表类型：Triger

参数：

- SNSTopic1: 30
- SNSTopic2: 30
- SNSTopic3: 30
- SNSTopic4: 30
- SNSTopic5: 30

- (Optional): SNS topic ARN: 30

此控件检查亚马逊简单通知服务通知是否已集成到堆 CloudFormation 栈中。如果没有与 CloudFormation 堆栈关联的 SNS 通知，则该堆栈的控制将失败。

为您的 CloudFormation 堆栈配置 SNS 通知有助于立即将堆栈发生的任何事件或更改通知利益相关者。

Note

以下区域不支持此控件：

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- 亚太地区 (雅加达)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- 欧洲 (米兰)
- Europe (Paris)
- Europe (Stockholm)
- 中东 (巴林)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何更新 CloudFormation 堆栈的信息，请参阅 Amazon CloudFormation 用户指南中的 [Amazon CloudFormation 堆栈更新](#)。

[CloudFront.1] CloudFront 发行版应配置默认根对象

类别：保护 > 安全访问管理 > 资源不可公开访问

严重性：重大

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-default-root-object-configured](#)

时间表类型：Triger

参数：None (无)

此控件检查是否将 Amazon CloudFront 分发配置为返回作为默认根对象的特定对象。如果 CloudFront 发行版未配置默认根对象，则控制将失败。

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，指定一个默认根对象，可以帮助您避免公开 Web 分配的内容。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

有关如何为您的分配指定默认根对象的详细说明，请参阅 Amazon CloudFront 开发者指南中的 [如何指定默认根对象](#)。

[CloudFront.2] CloudFront 发行版应启用原始访问身份

类别：保护 > 安全访问管理 > 资源策略配置

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-origin-access-identity-enabled](#)

时间表类型：Triger

参数：None (无)

此控制检查具有 Amazon S3 Origin 类型的亚马逊 CloudFront 发行版是否配置了原始访问身份 (OAI)。如果未配置 OAI，则控制失败。

CloudFront OAI 阻止用户直接访问 S3 存储桶内容。当用户直接访问 S3 存储桶时，他们实际上绕过了 CloudFront 分配和应用于底层 S3 存储桶内容的任何权限。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

有关详细的补救说明，请参阅《亚马逊 CloudFront 开发者指南》中的[创建 CloudFront OAI 并将其添加到您的发行版](#)中。

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-viewer-policy-https](#)

时间表类型：Triger

参数：None (无)

此控件检查亚马逊 CloudFront 发行版是否要求查看者直接使用 HTTPS 或是否使用重定向。如果设置 ViewerProtocolPolicy 为 follow-all or defaultCacheBehavior 或 for，则控制失败 cacheBehaviors。

HTTPS (TLS) 可用于帮助防止潜在攻击者使用 person-in-the-middle 或类似攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。对传输中的数据进行加密可能会影响性能。您应该使用此功能测试您的应用程序，以了解性能概况和 TLS 的影响。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

有关详细的补救说明，请参阅查看者[之间的通信需要 HTTPS 和](#) Amazon CloudFront 开发者指南 CloudFront 中的内容。

[CloudFront.4] CloudFront 发行版应配置原始故障转移

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-origin-failover-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查 Amazon CloudFront 分发是否配置了具有两个或更多源的源组。

CloudFront 源故障转移可以提高可用性。如果主源不可用，或者返回特定的 HTTP 响应状态代码，则源故障转移自动将流量重定向到辅助源。

Note

此控件仅适用于美国东部（弗吉尼亚北部）。

修复

有关详细的补救说明，请参阅 Amazon CloudFront 开发者指南中的[创建原始组](#)。

[CloudFront.5] CloudFront 发行版应启用日志记录

类别：识别 > 记录

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-accesslogs-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查 CloudFront 发行版上是否启用了服务器访问日志。如果未为分配启用访问日志，则控制将失败。

CloudFront 访问日志提供有关 CloudFront 接收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、发出请求的查看者的 IP 地址、请求的来源以及查看器发出的请求的端口号等信息。

这些日志对于安全和访问审计以及取证调查等应用程序很有用。有关如何分析访问日志的更多指导，请参阅[Amazon Athena 用户指南中的查询亚马逊 CloudFront 日志](#)。

Note

此控件仅适用于美国东部（弗吉尼亚北部）。

修复

有关如何为 CloudFront 分配配置访问日志的信息，请参阅 Amazon CloudFront 开发者指南中的[配置和使用标准日志（访问日志）](#)。

[CloudFront.6] CloudFront 发行版应该已Amazon WAF启用

类别：保护 > 防护服务

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-associated-with-waf](#)

时间表类型：Triger

参数：None (无)

此控件检查 CloudFront 分布是否与任一 Web ACLAmazon WAF 或Amazon WAF v2 Web ACL 相关联。如果分配未与 Web ACL 关联，则控制失败。

Amazon WAF 是一个 Web 应用程序防火墙，可帮助保护 Web 应用程序和 API 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 (Web ACL)，基于可自定义的 Web 安全规则以及您定义的条件，允许、阻止或计数 Web 请求。确保您的 CloudFront 分发与Amazon WAF Web ACL 相关联，以帮助保护其免受恶意攻击。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

有关如何将 Web ACL 与 CloudFront 分配关联的信息，请参阅亚马逊 CloudFront 开发者指南中的[使用 Amazon WAF控制对内容的访问权限](#)。

[CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-custom-ssl-certificate](#)

时间表类型：Triger

参数：None (无)

此控制检查 CloudFront 发行版是否使用 CloudFront 提供的默认 SSL/TLS 证书。如果 CloudFront 发行版使用自定义 SSL/TLS 证书，则此控制通过。如果 CloudFront 分发使用默认 SSL/TLS 证书，则此控制将失败。

自定义 SSL/TLS 允许您的用户使用备用域名访问内容。您可以在Amazon Certificate Manager (推荐) 或 IAM 中存储自定义证书。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

要使用自定义 SSL/TLS 证书为您的 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 来提供 HTTPS 请求

类别：保护 > 安全网络配置

严重性：低

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-sni-enabled](#)

时间表类型：Triger

参数：None (无)

此控制检查亚马逊 CloudFront 发行版是否使用自定义 SSL/TLS 证书，并配置为使用 SNI 提供 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，则此控制将失败。

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 CloudFront 将配置为使用 SNI 处理 HTTPS 请求，则将备用域名与每个边缘站点中的 IP 地址 CloudFront 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。指向您域名的 IP 地址在 SSL/TLS 握手协商期间确定；IP 地址并非专用于您的分发。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

要将您的 CloudFront 分配配置为使用 SNI 提供 HTTPS 请求，请参阅 CloudFront 开发者指南中的[使用 SNI 提供 HTTPS 请求 \(适用于大多数客户端 \)](#)。

[CloudFront.9] CloudFront 发行版应加密流向自定义源的流量

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-traffic-to-origin-encrypted](#)

时间表类型：Triger

参数：None (无)

此控制检查亚马逊 CloudFront 发行版是否对流向自定义源的流量进行加密。对于其原始协议策略允许 “http-only” 的 CloudFront 分配，此控制会失败。如果发行版的源协议策略为 “match-viewer”，而查看者协议策略为 “allow-all”，则此控制也会失败。

HTTPS (TLS) 可用于帮助防止窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

要更新原始协议策略以要求对您的 CloudFront 连接进行加密，请参阅亚马逊 CloudFront 开发者指南中的[要求 HTTPS CloudFront 与您的自定义源之间的通信](#)。

[CloudFront.10] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::CloudFront::Distribution

Amazon Config 规则：[cloudfront-no-deprecated-ssl-protocols](#)

时间表类型：Triger

参数：None (无)

此控制检查亚马逊 CloudFront 发行版是否使用过时的 SSL 协议在 CloudFront 节点和您的自定义源之间进行 HTTPS 通信。如果 CloudFront 分布 `OriginSslProtocols` 包含 `where includes` , `CustomOriginConfig` 则此控制将失效 SSLv3。

2015 年，互联网工程任务组 (IETF) 正式宣布应弃用 SSL 3.0，因为该协议不够安全。建议您使用 TLSv1.2 或更高版本与您的自定义源进行 HTTPS 通信。

Note

此控件仅适用于美国东部 (弗吉尼亚北部)。

修复

要更新您的 CloudFront 分配的 Origin SSL 协议，请参阅亚马逊 CloudFront 开发者指南中的[要求 HTTPS CloudFront 与您的自定义源之间的通信](#)。

[CloudTrail.1] CloudTrail 应启用并配置至少一个包含读写管理事件的多区域跟踪

类别：识别 > 记录

严重性：高

资源类型：Amazon 账户

Amazon Config 规则：[multi-region-cloudtrail-enabled](#)

时间表类型：定期

参数：

- `readWriteType`: ALL

此控件检查是否存在至少一条多区域 CloudTrail 跟踪。它还会检查其中至少一条跟踪的 `ExcludeManagementEventSources` 参数是否为空。

Amazon CloudTrail 记录您账户的 Amazon API 调用并向您发送日志文件。记录的内容包括以下信息。

- 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
- Amazon 服务返回的响应元素

CloudTrail 提供账户的 Amazon API 调用历史记录，包括通过、Amazon SDK Amazon Web Services Management Console、命令行工具进行的 API 调用。历史记录还包括来自更高级别 Amazon 服务 (如 Amazon CloudFormation) 的 API 调用。

生成的 Amazon 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。全局服务事件日志记录将记录 Amazon 全局服务生成的事件。

- 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 Amazon 账户所有资源上的管理操作。

默认情况下，使用创建的 CloudTrail 跟踪 Amazon Web Services Management Console 是多区域跟踪。

修复

要修复此问题，请在中创建新的多区域跟踪 CloudTrail。

要在中创建新路线 CloudTrail

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
2. 如果您 CloudTrail 之前没有使用过，请选择“立即开始”。
3. 选择 Trails (跟踪)，然后选择 Create trail (创建跟踪)。
4. 输入跟踪的名称。
5. 在 Storage location (存储位置) 下，执行下列操作之一：
 - a. 要为 CloudTrail 日志 Create a new S3 存储桶，请选择 Create a new S3，然后输入 new S3 存储桶的名称。
 - b. 要使用现有 S3 存储桶，对于 Create a new S3 bucket (创建新 S3 存储桶)，请选择 No (否)，然后选择要使用的 S3 存储桶。
6. 在“其他设置”下，选择“高级”。在“启用日志文件验证”中，选择“启用”。
7. 选择 Create (创建)。

要在中更新现有跟踪 CloudTrail

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
2. 选择 Trails (跟踪)。
3. 在 Name (名称) 列中选择跟踪的名称。
4. 对于 Management events (管理事件)，选择 Edit (编辑)。
5. 对于读取/写入事件，请选择管理事件。
6. 在 API 活动下，选择读取和写入。

[CloudTrail.2] CloudTrail 应启用静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::CloudTrail::Trail

Amazon Config 规则：[cloud-trail-encryption-enabled](#)

时间表类型：定期

参数：None (无)

此控件检查 CloudTrail 是否配置为使用服务器端加密 (SSE) Amazon KMS key 加密。如果定义了 KmsKeyId，则检查通过。

为了给敏感 CloudTrail 日志文件增加安全层，您应该对日志文件使用[带有 Amazon KMS —managed keys \(SSE-KMS\) 的服务器端加密](#)，以便进行静态加密。CloudTrail 请注意，预设情况下，提交 CloudTrail 到您存储桶的日志文件是用 [Simple Storage Service \(Amazon S3\) 托管加密密钥 \(SSE-S3\) 通过 Amazon 服务器端加密进行加密](#) 的。

修复

要修复此问题，请更新您的跟踪以启用日志文件的 SSE-KMS 加密。

启用 CloudTrail 日志加密

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
 2. 选择 Trails (跟踪)。
 3. 选择要更新的跟踪。
 4. 在“常规详细信息”下，选择“编辑”。
 5. 对于日志文件 SSE-KMS 加密，选择启用。
 6. 对于 Create a new KMS key (创建新的 KMS 密钥)，执行以下操作之一：
 - 要创建密钥，请选择“新建”。然后在 Amazon KMS 别名中输入密钥的别名。密钥是在与 S3 存储桶相同的区域中创建的。
 - 要使用现有密钥，请选择现有密钥，然后从 Amazon KMS 别名中选择密钥。
- Amazon KMS 密钥和 S3 存储桶必须位于同一区域。
7. 选择 Save (保存)。

您可能需要修改的策略 CloudTrail 才能成功与您的 KMS 密钥交互。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 [Amazon KMS—managed 密钥 \(SSE-KMS\) 加密 CloudTrail 日志文件](#)。

[CloudTrail.4] 确保启用 CloudTrail 日志文件验证

类别：数据保护 > 数据完整性

严重性：低

资源类型：AWS::CloudTrail::Trail

Amazon Config 规则：[cloud-trail-log-file-validation-enabled](#)

时间表类型：定期

参数：None (无)

此控件检查 CloudTrail 跟踪上是否启用了日志文件完整性验证。

CloudTrail 日志文件验证会创建一个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确定日志文件是否已更改、删除或 CloudTrail 未更改。

Security Hub 建议您在所有跟踪上启用文件验证。日志文件验证提供额外的 CloudTrail 日志完整性检查。

有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的[启用验证和验证文件](#)。

修复

要修复此问题，请更新您的 CloudTrail 跟踪以启用日志文件验证。

启用 CloudTrail 日志文件验证

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
2. 选择 Trails (跟踪)。
3. 在“名称”下，选择要编辑的跟踪的名称。
4. 在“常规详细信息”下，选择“编辑”。

5. 在“其他设置”下，为“日志文件验证”选择“启用”。
6. 选择 Save changes (保存更改)。

有关更多信息，请参阅《Amazon CloudTrail用户指南》中的[验证 CloudTrail 日志文件完整性](#)。

[CloudTrail.5] 确保 CloudTrail 跟踪与亚马逊 CloudWatch 日志集成

类别：识别 > 记录

严重性：低

资源类型：AWS::CloudTrail::Trail

Amazon Config 规则：[cloud-trail-cloud-watch-logs-enabled](#)

时间表类型：定期

参数：None (无)

此控件检查 CloudTrail 跟踪是否配置为向日志发送 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Amazon API 调用。记录的信息包含：

- 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
- Amazon服务返回的响应元素

CloudTrail 使用 Amazon S3 进行日志文件存储和传输。您可以在指定的 S3 存储桶中捕获 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。

对于在账户的所有区域中启用的跟踪，CloudTrail 将来自所有这些区域的日志文件发送到 CloudWatch 日志日志组。

Security Hub 建议您将 CloudTrail 日志发送到 CloudWatch 日志。请注意，此建议旨在确保捕获、监控账户活动并对账户活动进行适当警报。您可以使用 CloudWatch 日志在您的Amazon服务中进行设置。本建议不排除使用不同的解决方案。

将 CloudTrail 日志发送到 CloudWatch 日志有助于根据用户、API、资源和 IP 地址记录实时和历史活动。您可以使用这种方法为异常或敏感账户活动建立警报和通知。

修复

您可以使用控制台启用与 CloudWatch 日志的 CloudTrail 集成。

启用与 CloudWatch 日志的 CloudTrail 集成

1. 通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
2. 选择 Trails (跟踪)。
3. 选择没有CloudWatch 日志日志组值的跟踪。
4. 在 CloudWatch Logs (日志) 下，选择 Edit (编辑)。
5. 选择 Enabled (已启用)。
6. 对于 Log 组，请执行以下操作之一：

- 要使用默认日志组，请保持名称不变。
 - 要使用现有的日志组，请选择 Existing (现有)，然后输入要使用的日志组的名称。
 - 要创建新的日志组，请选择 New (新建)，然后输入要创建的日志组的名称。
7. 对于 IAM role (IAM 角色)，执行以下操作之一：
- 要使用现有角色，请选择 Existing (现有)，然后从下拉列表中选择角色。
 - 要创建新角色，请选择新建，然后输入要创建的角色名称。将为新角色分配一个策略以授予所需的权限。
- 要查看授予角色的权限，请展开策略文档。
8. 选择 Save changes (保存更改)。

有关更多信息，请参阅 [《Amazon CloudTrail 用户指南》中的使用控制台配置 CloudWatch 日志监控](#)。

[CodeBuild.1] CodeBuild GitHub 或 Bitbucket 源存储库 URL 应使用 OAuth

类别：保护 > 安全开发

严重性：重大

资源类型：AWS::CodeBuild::Project

Amazon Config 规则：[codebuild-project-source-repo-url-check](#)

时间表类型：Triger

参数：None (无)

此控件检查 GitHub 或 Bitbucket 源存储库 URL 是否包含个人访问令牌或用户名和密码。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

身份验证凭证绝不应以明文方式存储或传输，也不应显示在存储库 URL 中。您应该使用 OAuth 来授予访问或 Bitbucket 存储库的授权，而不是个人访问令牌 GitHub 或用户名和密码。使用个人访问令牌或用户名和密码可能会导致您的凭证遭受意外的数据暴露和未经授权的访问。

修复

您可以更新您的 CodeBuild 项目以使用 OAuth。

从 CodeBuild 项目源中删除基本身份验证/(GitHub) 个人访问令牌

1. 通过 <https://console.aws.amazon.com/codebuild/> 打开 CodeBuild 控制台。
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. 选择断开与 GitHub /Bitbucket 的连接。
5. 选择“使用 OAuth Connect”，然后选择“Connect 到 GitHub/Bitbucket”。

6. 出现提示时，选择 authorize as appropriate (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 Update source (更新源)。

有关更多信息，请参阅《Amazon CodeBuild用户指南》中[基于案例的CodeBuild 使用示例](#)。

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文证书

类别：保护 > 安全开发

严重性：重大

资源类型：AWS::CodeBuild::Project

Amazon Config 规则：[codebuild-project-envvar-awscred-check](#)

时间表类型：Triger

参数：None (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。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要修复此问题，请更新您的 CodeBuild 项目以删除环境变量。

从 CodeBuild 项目中移除环境变量

1. 通过 <https://console.aws.amazon.com/codebuild/> 打开 CodeBuild 控制台。
2. 展开 Build (构建)。
3. 选择 Build project (构建项目)，然后选择包含明文凭证的构建项目。
4. 从 Edit (编辑) 中，选择 Environment (环境)。
5. 展开 Additional configuration (其他配置)。
6. 选择环境变量旁边的 Remove (删除)。
7. 选择 Update environment (更新环境)。

将敏感值存储在 Amazon EC2 Systems Manager 参数存储库中，然后从您的构建规范中检索它们

1. 通过 <https://console.aws.amazon.com/codebuild/> 打开 CodeBuild 控制台。
2. 展开 Build (构建)。
3. 选择 Build project (构建项目)，然后选择包含明文凭证的构建项目。
4. 从 Edit (编辑) 中，选择 Environment (环境)。

5. 展开 Additional configuration (其他配置), 然后滚动到 Environment variables (环境变量)。
6. 按照[本教程](#)创建包含您的敏感数据的 Systems Manager 参数。
7. 在创建参数后, 复制参数名称。
8. 回到 CodeBuild 控制台, 选择创建环境变量。
9. 输入在构建规范中显示的变量名称。
10. 对于 Value (值), 粘贴参数名称。
11. 对于 Type (类型), 选择 Parameter (参数)。
12. 要删除包含明文凭证的不合规环境变量, 请选择 Remove (删除)。
13. 选择 Update environment (更新环境)。

有关更多信息, 请参阅《Amazon CodeBuild 用户指南》中的[构建环境中的环境变量](#)。

[CodeBuild.4] CodeBuild 项目环境应该有日志配置

类别：识别 > 记录

严重性：中

资源类型：AWS::CodeBuild::Project

Amazon Config 规则：[codebuild-project-logging-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查 CodeBuild 项目环境是否至少有一个日志选项, 即 S3 或启用 CloudWatch 日志。如果 CodeBuild 项目环境没有启用至少一个日志选项, 则此控制将失败。

从安全角度来看, 日志记录是一项重要功能, 可在 future 发生任何安全事件时进行取证。将 CodeBuild 项目中的异常与威胁检测相关联可以增强人们对这些威胁检测的准确性的信心。

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

类别：保护 > 安全访问管理

严重性：高

资源类型：AWS::CodeBuild::Project

Amazon Config 规则：[codebuild-project-environment-privileged-check](#)

时间表类型：Triger

参数：None (无)

此控件检查 Amazon CodeBuild 项目环境是否启用了特权模式。当 Amazon CodeBuild 项目环境启用特权模式时, 此控制将失效。

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。设置值 privilegedMode 以 true 允许在 Docker 容器内运行 Docker 守护程序。Docker 守护程序监听 Docker API 请求并管理 Docker 对象, 例如镜像、容器、网络和卷。仅在构建项目用于构建 Docker 映像

时，此参数才应设置为 true。否则，应禁用此设置，以防止意外访问 Docker API 以及容器的底层硬件，因为意外访问privilegedMode可能会有恶意篡改或删除关键资源的风险。

修复

有关如何配置 CodeBuild 项目环境设置的更多信息，请参阅 CodeBuild 用户指南中的[创建构建项目（控制台）](#)

[Config.1] 应启用 Amazon Config

类别：识别 > 清单

严重性：中

资源类型：Amazon账户

Amazon Config规则：None（无）

时间表类型：定期

参数：None（无）

该控制检查是否已在账户中为本地区域启用了 Amazon Config，并记录所有资源。

Amazon Config 服务对您账户中支持的 Amazon 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（Amazon 资源）、配置项之间的关系以及资源之间的任何配置更改。

Security Hub 建议您在所有区域Amazon Config中启用。Amazon Config 捕获的 Amazon 配置项历史记录可用于安全分析、资源更改跟踪和合规性审计。

Note

Config.1 要求Amazon Config在您使用Security Hub 的所有区域中启用该功能。

由于 Security Hub 是一项区域服务，因此对此控制执行的检查仅检查该账户的当前区域。它不会检查所有区域。

要允许针对每个区域中的全局资源进行安全检查，您还必须记录全局资源。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。

您也可以考虑在未启用全局资源记录的区域禁用 IAM.1、IAM.2、IAM.3、IAM.5、IAM.8 和 IAM.21。由于 IAM 是一项全球服务，因此 IAM 资源将仅记录在启用全局资源记录的区域中。

要了解更多信息，请参阅Amazon Config开发者指南Amazon Config中的[入门](#)指南。

修复

启用后Amazon Config，将其配置为记录所有资源。

配置 Amazon Config 设置

1. 通过以下网址打开 Amazon Config 控制台：<https://console.aws.amazon.com/config/>。
2. 选择要在其中配置 Amazon Config 的区域。
3. 如果您Amazon Config之前没有使用过，请参阅Amazon Config开发者指南中的[入门](#)。
4. 从菜单导航到“设置”页面，然后执行以下操作：
 - 选择 Edit（编辑）。
 - 在要记录的资源类型下，选择记录该区域支持的所有资源和包括全球资源（例如Amazon IAM 资源）。
 - 在“数据保留期”下，选择Amazon Config数据的默认保留期，或指定自定义保留期。
 - 在“Amazon Config角色”下，选择“创建Amazon Config服务相关角色”或“从账户中选择一个角色”，然后选择要使用的角色。

- 在 Amazon S3 bucket (Amazon S3 存储桶) 下面，指定要使用的存储桶，或者创建存储桶并包括前缀 (可选)。
- 在 Amazon SNS 主题下，从您的账户中选择一个 Amazon SNS 主题或创建一个 Amazon SNS 主题。有关 Amazon SNS 的更多信息，请参阅 [Amazon Simple Notification Service 入门指南](#)。

5. 选择 Save (保存)。

有关使用 fromAmazon Config 的更多信息Amazon CLI，请参阅Amazon Config开发者指南Amazon Config中的[开启](#)。

您还可以使用 Amazon CloudFormation 模板自动执行这一过程。有关更多信息，请参阅Amazon CloudFormation用户指南中的[Amazon CloudFormation StackSets 示例模板](#)。

[DMS.1]Amazon Database Migration Service 复制实例不应公开

类别：保护 > 安全网络配置

严重性：重大

资源类型：AWS::DMS::ReplicationInstance

Amazon Config 规则：[dms-replication-not-public](#)

时间表类型：定期

参数：None (无)

此控件检查Amazon DMS复制实例是否为公共实例。为此，它会检查该PubliclyAccessible字段的值。

私有复制实例有一个私有 IP 地址，您无法在复制网络之外访问该地址。当源数据库和目标数据库位于同一个网络中时，复制实例应具有私有 IP 地址。网络还必须使用 VPN 或 VPC 对等连接到复制实例的 VPC。Amazon Direct Connect要了解有关公有和私有复制实例的更多信息，请参阅Amazon Database Migration Service用户指南中的[公有和私有复制实例](#)。

您还应确保仅限授权用户访问您的Amazon DMS实例配置。为此，请限制用户修改Amazon DMS设置和资源的 IAM 权限。

Note

非洲 (开普敦) 或欧洲 (开普敦) 或欧洲 (米兰) 不支持此控件。

修复

请注意，一旦创建了复制实例，就无法更改公共访问设置。必须将其删除并重新创建。

将Amazon DMS复制实例设置配置为阻止公有访问

1. 打开 Amazon Database Migration Service 控制台 (<https://console.aws.amazon.com/dms/>)。
2. 导航到复制实例，然后删除公共实例。选择实例，选择操作，然后选择删除。
3. 选择创建复制实例。提供配置详情。
4. 要禁用公共访问，请确保未选择“可公开访问”。
5. 选择 Create (创建)。

有关更多信息，请参阅Amazon Database Migration Service用户指南中有关[创建复制实例](#)的部分。

[DynamoDB.1] DynamoDB 表应根据需求自动扩展容量

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::DynamoDB::Table

Amazon Config 规则：[dynamodb-autoscaling-enabled](#)

时间表类型：定期

参数：None (无)

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。如果表使用按需容量模式或配置了 Auto Scaling 的配置模式，则此控制将通过。按需扩展容量可避免限制异常，这有助于保持应用程序的可用性。

按需容量模式下的 DynamoDB 表仅受 DynamoDB 吞吐量默认表配额限制。要提高这些配额，您可以通过提交支持请求[Amazon Web Services Support](#)。

具有自动扩展功能的预置模式下的 DynamoDB 表可根据流量模式动态调整预置的吞吐容量。有关 DynamoDB 请求限制的更多信息，请参阅 Amazon DynamoDB 开发人员指南中的[请求限制和突增容量](#)。

Note

Amazon GovCloud (美国东部) 或 Amazon GovCloud (美国西部) 不支持此控件。

修复

有关在容量模式下对现有表启用 DynamoDB 自动扩展的详细说明，请参阅 Amazon DynamoDB 开发人员指南中的对现有表启用 DynamoDB [auto 扩展](#)。

[DynamoDB.2] DynamoDB 表应启用 point-in-time 恢复功能

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：AWS::DynamoDB::Table

Amazon Config 规则：[dynamodb-pitr-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查是否为 Amazon DynamoDB 表启用了 point-in-time 恢复 (PITR)。

备份可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。DynamoDB point-in-time 恢复可自动备份 DynamoDB 表。它减少了从意外删除或写入操作中恢复的时间。启用了 PITR 的 DynamoDB 表可以还原到最近 35 天中的任何时间点。

修复

要修复此问题，请向您的 DynamoDB 表添加 point-in-time 恢复功能。

如欲为现有表启用 DynamoDB point-in-time 恢复

1. 从 <https://console.aws.amazon.com/dynamodb/> 打开 DynamoDB 控制台。
2. 选择要处理的表，然后选择 Backups (备份)。
3. 在 “Point-in-time 恢复” 部分的 “状态” 下，选择 “启用”。
4. 再次选择 “启用” 以确认更改。

[DynamoDB.3] DynamoDB Acelerator (DAX) 集群应进行静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::DAX::Cluster

Amazon Config 规则：[dax-encryption-enabled](#)

时间表类型：定期

参数：None (无)

此控件检查 DAX 集群是否进行静态加密。

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。加密增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，需要有 API 权限才能解密数据，然后才能读取数据。

修复

集群创建后，不能启用或禁用静态加密。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[使用 Amazon DynamoDB 开发人员指南Amazon Web Services Management Console中的启用静态加密](#)。

[EC2.1] Amazon EBS 快照不应公开，这取决于任何人都可恢复的可用性

类别：保护 > 安全网络配置

严重性：重大

资源类型：Amazon 账户

Amazon Config 规则：[ebs-snapshot-public-restorable-check](#)

时间表类型：定期

参数：None (无)

此控件检查亚马逊弹性块存储快照是否未公开。如果任何人都可以恢复 Amazon EBS 快照，则控制失败。

EBS 快照用于在特定时间点将 EBS 卷上的数据备份到 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。

Note

非洲（开普敦）或欧洲（开普敦）或欧洲（米兰）不支持此控件。

修复

要修复此问题，请更新您的 EBS 快照以将其设为私有而不是公开。

将公有 EBS 快照变为私有快照

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格的 E lastic Block Store 下，选择快照菜单，然后选择您的公有快照。
3. 从 Actions (操作) 中，选择 Modify permissions (修改权限)。

4. 选择 Private (私有)。
5. (可选) 添加要与之共享快照的授权账户的账号, 然后选择添加权限。Amazon
6. 选择 Save (保存)。

[EC2.2] VPC 默认安全组不应允许入站和出站流量

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::EC2::SecurityGroup

Amazon Config 规则：[vpc-default-security-group-closed](#)

时间表类型：Triger

参数：None (无)

该控制检查 VPC 的默认安全组是否不允许入站或出站流量。

[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。

我们不建议使用默认安全组。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, 请创建新的安全组并将这些安全组分配给您的资源。为防止使用默认安全组, 请删除其入站和出站规则。

创建新的安全组并将其分配给您的资源

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中, 选择 Security Groups (安全组)。查看默认安全组详细信息以了解分配给它们的资源。
3. 为资源创建一组最小权限安全组。有关如何创建安全组的详细信息, 请参阅 Amazon VPC 用户指南中的[创建安全组](#)。
4. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
5. 在 Amazon EC2 控制台上, 将使用默认安全组的资源的安全组更改为您创建的最低权限安全组。请参阅 Amazon VPC 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, 从默认安全组中移除入站和出站规则。这样可以确保不使用默认安全组。

从默认安全组中删除规则

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中, 选择 Security Groups (安全组)。
3. 选择默认安全组并选择入站规则选项卡。选择 Edit inbound rules (编辑入站规则)。然后删除所有入站规则。选择 Save rules (保存规则)。
4. 对每个默认安全组重复上一步骤。
5. 选择默认安全组并选择出站规则选项卡。选择编辑出站规则。然后删除所有出站规则。选择 Save rules (保存规则)。
6. 对每个默认安全组重复上一步骤。

有关更多信息, 请参阅 Amazon VPC 用户指南中的使用[安全组](#)。

[EC2.3] 附加的 EBS 卷应在静态时加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::EC2::Volume

Amazon Config 规则：[encrypted-volumes](#)

时间表类型：Trigger

参数：None (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《适用于 Linux 实例的 Amazon EC2 用户指南》中的[Amazon EBS 加密](#)。

Note

非洲（开普敦）或欧洲（开普敦）或欧洲（米兰）不支持此控件。

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，您都可以覆盖用于 Amazon EBS 加密的默认密钥并选择对称的客户托管密钥。

有关更多信息，请参阅适用于 Linux 实例的[Amazon EC2 用户指南中的创建 Amazon EBS 卷和复制 Amazon EBS 快照](#)。

[EC2.4] 应在指定时间段后删除已停止的 EC2 实例

类别：识别 > 清单

严重性：中

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-stopped-instance](#)

时间表类型：定期

参数：

- allowedDays: 30

此控件检查任何 EC2 实例的停止时间是否超过了允许的天数。如果 EC2 实例的停止时间超过允许的最大时间段（默认为 30 天），则无法通过此项检查。

失败的发现表明 EC2 实例在很长一段时间内没有运行。这会带来安全风险，因为 EC2 实例没有得到积极维护（分析、修补、更新）。如果稍后启动，则缺乏适当的维护可能会导致您的 Amazon 环境出现意外问题。

要在一段时间内安全地将 EC2 实例保持在非运行状态，请定期启动它进行维护，然后在维护后将其停止。理想情况下，这是一个自动化过程。

Note

非洲（开普敦）或欧洲（开普敦）或欧洲（米兰）不支持此控件。

修复

您可以使用控制台或命令行终止 EC2 实例。

在终止 EC2 实例之前，请确认您不会丢失任何数据：

- 检查您的亚马逊 EBS 卷是否在终止时被删除。
- 从 EC2 实例存储卷复制所需数据到 Amazon EBS 或 Amazon S3。

终止 EC2 实例（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的 Instances 下，选择 Instances。
3. 选择实例，然后选择操作、实例状态、终止。
4. 当系统提示您确认时，选择 Yes, Terminate（是，终止）。

终止 EC2 实例（Amazon CLI 适用于 Windows 的工具 PowerShell）

使用以下命令之一。有关命令行接口的更多信息，请参阅适用于 Linux 实例的[Amazon EC2 用户指南中的访问 Amazon EC2](#)。

- 从 Amazon CLI，使用 [terminate-instances](#)
- 在适用于 Windows 的工具 PowerShell 中，使用 [Stop-EC2Instance](#)。

要了解有关终止实例的更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的[终止实例](#)。

[EC2.6] 应在所有 VPC 中启用 VPC 流量日志记录

类别：识别 > 记录

严重性：中

资源类型：AWS::EC2::VPC

Amazon Config 规则：[vpc-flow-logs-enabled](#)

时间表类型：定期

参数：

- trafficType: REJECT

此控件检查是否找到并启用了 VPC 的 Amazon VPC 流日志。流量类型设置为 Reject。

使用 VPC 流日志功能，您可以捕获有关传入和传出您的 VPC 中网络接口的 IP 地址流量的信息。创建流日志后，您可以在 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 建议您为 VPC 的数据包拒绝启用流量记录。流日志提供对通过 VPC 的网络流量的可见性，并可以在安全工作流程中检测异常流量或提供见解。

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

要修复此问题，请启用 VPC 流量记录。

启用 VPC 流日志记录

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在“虚拟私有云”下，选择您的 VPC。
3. 选择要更新的 VPC。
4. 在页面底部，选择 Flow Logs (流日志)。
5. 选择 Create flow log (创建流日志)。
6. 对于 Filter (筛选条件)，选择 Reject (拒绝)。
7. 对于目标日志组，请选择要使用的日志组。
8. 对于 IAM 角色，选择要使用的 IAM 角色。
9. 选择 Create (创建)。

[EC2.7] 应启用 EBS 默认加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：Amazon 账户

Amazon Config 规则：[ec2-ebs-encryption-by-default](#)

时间表类型：定期

参数：None (无)

此控制检查是否为 Amazon Elastic Block Store (Amazon EBS) 默认启用账户级加密。如果未启用账户级加密，则控制将失败。

为您的账户启用加密后，Amazon EBS 卷和快照副本将进行静态加密。这为您的数据增加了一层保护。有关更多信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的[默认加密](#)。

请注意，以下实例类型不支持加密：R1、C1 和 M1。

修复

您可以使用 Amazon EC2 控制台为 Amazon EBS 卷启用默认加密。

针对某个区域配置用于 Amazon EBS 加密的默认加密

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 从导航窗格中，选择 EC2 控制面板。
3. 在页面的右上角，选择账户属性，然后选择 EBS 加密。
4. 选择管理。
5. 选择 Enable (启用)。您可以将 Amazon 托管式密钥具有您自己 alias/aws/ebs 创建的别名的保留为默认加密密钥，或者选择对称的客户托管密钥。
6. 选择更新 EBS 加密。

[EC2.8] EC2 实例应使用 imdsV2

类别：保护 > 网络安全

严重性：高

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-imdsv2-check](#)

时间表类型：Trigger

参数：None (无)

此控件检查您的 EC2 实例元数据版本是否配置有实例元数据服务版本 2 (IMDSv2)。如果 IMDSv2 设置 HttpTokens 为“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配置或管理正在运行的实例。IMDS 提供对临时、经常轮换的证书的访问权限。这些证书无需手动或以编程方式对实例进行硬编码或分发敏感证书。IMDS 在本地连接到每个 EC2 实例。它在特殊的“本地链接”IP 地址 169.254.169.254 上运行。只有在实例上运行的软件才能访问此 IP 地址。

IMDS 版本 2 为以下类型的漏洞添加了新的保护措施。这些漏洞可以用来尝试访问 IMDS。

- 打开网站应用程序防火墙
- 打开反向代理
- 服务器端请求伪造 (SSRF) 漏洞
- 打开第 3 层防火墙和网络地址转换 (NAT)

Security Hub 建议您使用 IMDSv2 配置 EC2 实例。

Note

非洲 (开普敦) 或欧洲 (开普敦) 或欧洲 (米兰) 不支持此控件。

修复

要修复未配置 IMDSv2 的 EC2 实例，您可以要求使用 IMDSv2。

要要求在现有实例上使用 IMDSv2，请在请求实例元数据时修改 Amazon EC2 元数据选项。按《适用于 Linux 实例的 Amazon EC2 用户指南》中的为现有实例配置实例[元数据选项](#)中的说明操作。

要要求在新实例启动时使用 IMDSv2，请按照 Amazon EC2 Linux [实例用户指南中为新实例配置实例元数据选项](#)中的说明进行操作。

从控制台使用 IMDSv2 配置您的新 EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 选择启动实例，然后选择启动实例。
3. 在“高级详细信息”下，对于元数据版本，选择“仅限 V2”（需要令牌）。
4. 在摘要面板中，查看您的更改，然后选择启动实例。

如果您的软件使用 IMDSv1，则可以重新配置软件，以使用 IMDSv2。有关详细信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的过渡到使用实例[元数据服务版本 2](#)。

[EC2.9] EC2 实例不应有公有 IP 地址

类别：保护 > 安全网络配置 > 公有 IP 地址

严重性：高

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-instance-no-public-ip](#)

时间表类型：Trigger

参数：None (无)

此控件检查 EC2 实例是否具有公有 IP 地址。如果 EC2 实例配置项目中存在该 publicIp 字段，则控制失败。此控制仅适用于 IPv4 地址。

公有 IPv4 地址是指可通过 Internet 访问的 IP 地址。如果您使用公有 IP 地址启动您的实例，则可从 Internet 访问您的 EC2 实例。私有 IPv4 地址是指无法通过 Internet 访问的 IP 地址。您可以使用私有 IPv4 地址，在同一 VPC 中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 用户指南中的您的 VPC 中的 [IP 寻址](#)。

如果您有合法的用例来维护具有公有 IP 地址的 EC2 实例，则可以隐藏此控制中的发现。有关前端架构选项的更多信息，请参阅[Amazon 构博客](#)或 [This Is My Architecture](#) 系列。

修复

使用非默认 VPC，这样默认情况下不会为实例分配公有 IP 地址。

在默认 VPC 中启动 EC2 实例时，系统会为它分配公有 IP 地址。当您在非默认 VPC 中启动 EC2 实例时，子网配置决定它是否接收公有 IP 地址。子网有一个用于确定子网中的新 EC2 实例是否从公有 IPv4 地址池接收公有 IP 地址的公有 IP 地址的属性。

您不能从 EC2 实例手动关联公有 IP 地址。要控制您的 EC2 实例是否接收公有 IP 地址，请执行以下操作之一：

- 修改子网的公有 IP 寻址属性。有关更多信息，请参阅 Amazon VPC 用户指南 中的 [修改子网的公有 IPv4 寻址属性](#)。
- 在启动时启用或禁用公有 IP 寻址功能。以覆盖子网的公有 IP 寻址属性。有关更多信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的 [在实例启动期间分配公有 IPv4 地址](#)。

有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南 中的 [公有 IPv4 地址和外部 DNS 主机名](#)。

如果您的 EC2 实例与弹性 IP 地址，则可从 Internet 访问您的 EC2 实例。您可以随时取消弹性 IP 地址与实例或网络接口的关联。

撤销弹性 IP 地址的关联

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要取消关联的弹性 IP 地址。
4. 在操作中，选择取消关联弹性 IP 地址。
5. 选择取消关联。

[EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 终端节点

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

Amazon Config 规则：[service-vpc-endpoint-enabled](#)

时间表类型：定期

参数：

- serviceName: ec2

此控件检查是否为每个 VPC 创建了 Amazon EC2 的服务终端节点。如果 VPC 没有为 Amazon EC2 服务创建 VPC 终端节点，则控制会失败。

此控件评估单个账户中的资源。它无法描述账户之外的资源。由于 Amazon Config 和 Security Hub 不进行跨账户检查，因此您将看到在账户间共享的 VPC 的 FAILED 调查结果。Security Hub 建议你隐瞒这些 FAILED 发现。

为了改善 VPC 的安保状况，您可以将 Amazon EC2 配置为使用接口 VPC 终端节点以使用 Amazon EC2 接口。接口终端节点由提供支持 Amazon PrivateLink，您可以使用该技术私密访问 Amazon EC2 API 操作。它将 VPC 和 Amazon EC2 之间的所有网络流量限制在 Amazon 网络以内。由于仅在同一区域内支持终端节点，因此无法在 VPC 和其他区域内的服务之间创建终端节点。这样可以防止意外调用其他区域的 Amazon EC2 API。

要了解有关为 Amazon EC2 创建 VPC 终端节点的更多信息，请参阅适用于 Linux 实例的 Amazon EC2 [和接口 VPC 终端节点](#)。

修复

要修复此问题，您可以创建与 Amazon EC2 的接口 VPC 终端节点连接。

从 Amazon VPC 控制台创建通往 Amazon EC2 的接口终端节点

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints（端点）。
3. 选择 Create Endpoint（创建终端节点）。
4. 对于服务类别，选择 Amazon 服务。
5. 对于服务名称，选择 com.amazonaws.<region>.ec2。
6. 对于类型，选择接口。
7. 完成以下信息：
 - a. 对于 VPC，选择要在其中创建端点的 VPC。
 - b. 对于 Subnets（子网），选择要在其中创建端点网络接口的子网（可用区）。并非所有可用区都支持所有 Amazon 服务。
 - c. 要为接口终端节点启用私有 DNS，请选中启用 DNS 名称对应的复选框。默认情况下，此选项处于启用状态。

要使用私有 DNS 选项，您的 VPC 的以下属性必须设置为 true：

- enableDnsHostnames
- enableDnsSupport

有关更多信息，请参阅 Amazon VPC 用户指南中的[查看和更新 VPC 的 DNS 支持](#)。

- d. 对于 Security group（安全组），选择要与端点网络接口关联的安全组。
- e. （可选）添加或删除标签。要添加标签，请选择添加标签并执行以下操作：
 - 对于 Key（键），输入标签名称。

- 对于 Value (值) , 输入键值。
 - f. 要删除标签, 请选择标签 Key and Value 右侧的删除按钮 (x)。
8. 选择 Create endpoint (创建端点) 。

为创建接口 VPC 终端节点策略

您可以向 VPC 终端节点附加策略来控制对 Amazon EC2 API 的访问。此策略指定以下内容：

- 可执行操作的委托人
- 可执行的操作
- 可对其执行操作的资源

有关创建 VPC 终端节点策略的更多详细信息, 请参阅 [Amazon EC2 Linux 实例用户指南中的 Amazon EC2 和接口 VPC 终端节点](#)。

[EC2.15] EC2 子网不应自动分配公有 IP 地址

类别：保护 > 网络安全

严重性：中

资源类型：AWS::EC2::Subnet

Amazon Config 规则：[subnet-auto-assign-public-ip-disabled](#)

时间表类型：Triger

参数：None (无)

此控件检查Amazon Virtual Private Cloud (Amazon VPC) 子网中的公有 IP 的分配是否已MapPublicIpOnLaunch设置为FALSE。如果将标志设置为，则控件通过FALSE。

所有子网都有一个用于确定在子网中创建的网络接口是否自动接收公有 IPv4 地址的属性。在启用了此属性的子网中启动的实例会为其主网络接口分配一个公有 IP 地址。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

您可以通过 Amazon VPC 控制台配置子网。

将子网配置为不分配公有 IP 地址

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets (子网) 。
3. 选择您的子网，然后依次选择 Subnet Actions、Modify auto-as s
4. 清除 Enabled Apply (启用自动分配公有 IPv4 地址) 复选框，然后选择保存

[EC2.16] 应删除未使用的网络访问控制列表

类别：预防 > 网络安全

严重性：低

资源类型：AWS::EC2::NetworkAcl

Amazon Config 规则：[vpc-network-acl-unused-check](#)

时间表类型：Triger

参数：None (无)

该控制检查是否存在任何未使用的网络访问控制列表 (ACL)。

该控件检查资源的项目配置AWS::EC2::NetworkAcl并确定网络 ACL 的关系。

如果唯一的网络 ACL 是 VPC，则控制失败。

如果列出了其他关系，则控制权通过。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何删除未使用的网络 ACL 的说明，请参阅 Amazon VPC 用户指南中的[删除网络 ACL](#)。

[EC2.17] EC2 实例不应使用多个 ENI

类别：网络安全

严重性：低

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-instance-multiple-eni-check](#)

时间表类型：Triger

参数：

- Adapterids (可选) — 附加到 EC2 实例的网络接口 ID 列表

此控制检查 EC2 实例是否使用多个弹性网络接口 (ENI) 或弹性结构适配器 (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。

多个 ENI 可能导致双宿主实例，即具有多个子网的实例。这会增加网络安全的复杂性，并引入意想不到的网络路径和访问。

如果属于 Amazon EKS 集群的 Amazon EKS 集群具有多个 ENI，则此控制也会失败。如果您需要使用具有多个 ENI 的 EC2 实例作为 Amazon EKS 集群的一部分，则可以隐藏这些发现。

Note

以下区域不支持此控件：

- 亚太地区（大阪）
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要修复此问题，请分离其他 ENI。

分离网络接口

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在网络与安全下，选择网络接口。
3. 按不合规实例 ID 筛选列表以查看关联的 ENI。
4. 选择要删除的 ENI。
5. 从“操作”菜单中选择“分离”。
6. 如果你看到提示你确定要断开以下网络接口吗？，选择“分离”。

[EC2.18] 安全组应只允许授权端口不受限制的传入流量

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

Amazon Config 规则：[vpc-sg-open-only-to-authorized-ports](#)

时间表类型：Triger

参数：

- `authorizedTcpPorts`（可选）— 以逗号分隔的允许无限制访问的端口列表。例如：`'80, 443'`。对于此规则，的默认值`authorizedTcpPorts`为 80 和 443。

此控件检查正在使用的安全组是否允许不受限制的传入流量。或者，该规则检查`authorizedTcpPorts`参数中是否列出了端口号。

- 如果安全组规则端口号允许不受限制的传入流量，但在中指定了端口号`authorizedTcpPorts`，则控制通过。`authorizedTcpPorts` 的默认值为 80, 443。
- 如果安全组规则端口号允许不受限制的传入流量，但未在`authorizedTcpPorts`输入参数中指定端口号，则控制失败。
- 如果未使用该参数，则任何具有不受限制入站规则的安全组的控制都将失败。

安全组对流向的入口和出口网络流量提供状态过滤Amazon。安全组规则应遵循最低权限访问原则。不受限制的访问（带有 /0 后缀的 IP 地址）增加了黑客 denial-of-service 攻击、攻击和数据丢失等恶意活动的机会。

除非特别允许某个端口，否则该端口应拒绝不受限制的访问。

Note

此控件在亚太地区（大阪）不支持此控件。

修复

有关如何修改安全组的信息，请参阅 Amazon VPC 用户指南中的[添加、删除或更新规则](#)。

[EC2.19] 安全组不应允许不受限制地访问高风险端口

类别：保护 > 限制网络访问

严重性：重大

资源类型：AWS::EC2::SecurityGroup

Amazon Config 规则：vpc-sg-restricted-common-ports（由 Security Hub 开发的自定义规则）

时间表类型：Triger

参数：None（无）

此控制检查风险最高的指定端口是否可以访问安全组不受限制的传入流量。当安全组中的规则均不允许从 0.0.0.0/0 进入这些端口的入站流量时，此控制即告通过。

不受限制访问 (0.0.0.0) 增加了恶意活动的机会，包括黑客 denial-of-service 攻击、攻击和数据丢失。

安全组为 Amazon 资源提供传入和传出网络流量的有状态筛选。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 Web 开发框架)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python 网页开发框架)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch 控制面板)
- 8080 (代理)
- 8088 (传统 HTTP 端口)
- 8888 (备用 HTTP 端口)
- 9200 或 9300 (OpenSearch)

修复

有关如何从安全组删除规则的信息，请参阅 Amazon EC2 Linux 实例用户指南中的[从安全组删除规则](#)。

[EC2.20]Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动

类别：弹性 > 恢复 > 高可用性

严重性：中

资源类型：AWS::EC2::VPNConnection

Amazon Config 规则：[vpc-vpn-2-tunnels-up](#)

时间表类型：Triger

参数：None (无)

VPN 隧道是一种加密链接，用于在客户网络和 Amazon 站点到站点 VPN 连接 Amazon 中传输数据或在客户网络中传输数据。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 隧道都可用于 VPN 连接，这对于确认 VPAmazon C 与您的远程网络之间的安全且高度可用的连接非常重要。

此控件检查 Site-to-Site VPN 提供的两个 VPN 隧道是否处于 UP 状态。如果一条或两条隧道处于 DOWN 状态，则控制失败。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- 中东 (巴林)

修复

要修改 VPN 隧道选项，请参阅《[Site-to-Site VPN 用户指南](#)》中的[修改 Amazon Site-to-Site VPN 隧道选项](#)。

[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::EC2::NetworkACL

Amazon Config 规则：[nacl-no-unrestricted-ssh-rdp](#)

时间表类型：Triger

参数：None (无)

此控制检查网络访问控制列表 (NACL) 是否允许无限制地访问 SSH/RDP 入口流量的默认 TCP 端口。如果 NACL 入站条目允许 TCP 端口 22 或 3389 的源 CIDR 块为 '0.0.0.0/0' 或 ':::/0'，则规则失败。

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，因为这可能允许意外访问您的 VPC 中的资源。

修复

有关 NACL 的更多信息，请参阅《VPC 用户指南》中的[网络 ACL](#)。

[EC2.22] 应移除未使用的 EC2 安全组

类别：识别 > 清单

严重性：中

资源类型:AWS::EC2::SecurityGroup,AWS::EC2::NetworkInterface

Amazon Config 规则：[ec2-security-group-attached-to-eni-periodic](#)

时间表类型：定期

参数：None (无)

此 Amazon 控制检查安全组是否已连接到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 elastic network interface。如果安全组与 Amazon EC2 实例或 elastic network interface 不关联，则控制将失败。

修复

要创建、分配和删除安全组，请参阅 Amazon EC2 用户指南中的[安全组](#)。

[EC2.23] EC2 传输网关不应自动接受 VPC 连接请求

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::EC2::TransitGateway

Amazon Config 规则：[ec2-transit-gateway-auto-vpc-attach-disabled](#)

时间表类型：Triger

参数：None (无)

此控件检查 EC2 传输网关是否自动接受共享的 VPC 附件。对于自动接受共享 VPC 连接请求的 Transit Gateway，此控制会失败。

启用 TranAutoAcceptSharedAttachments sit Gateway 可将 Transit Gateway 配置为自动接受任何跨账户 VPC 连接请求，无需验证请求或附件源账户。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，以确保仅接受授权的 VPC 连接请求。

Note

以下区域不支持此控件：

- 亚太地区 (香港)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- China (Beijing)
- China (Ningxia)
- 中东 (巴林)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何修改中Transit Gateway 的信息，请参阅 Amazon VPC 开发人员指南中的[修改中转网关](#)。

[EC2.24] 不应使用半虚拟化 EC2 实例类型

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-paravirtual-instance-check](#)

时间表类型：Trigger

参数：None (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virtualizationType的设置为，则控制失败paravirtual。

Linux Amazon 系统映像 (AMI) 使用两种虚拟化类型之一：半虚拟化 (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，请参阅适用于 [Linux 实例的 Amazon EC2 用户指南中的 Linux AMI 虚拟化类型](#)。

Note

以下区域不支持此控件：

- 美国东部 (俄亥俄州)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- 亚太地区 (雅加达)
- 亚太地区 (孟买)
- Asia Pacific (Osaka)
- 亚太地区 (首尔)
- 加拿大 (中部)
- China (Beijing)
- China (Ningxia)
- 欧洲 (伦敦)
- 欧洲 (米兰)
- Europe (Paris)
- Europe (Stockholm)
- 中东 (巴林)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何将 EC2 实例更新为新实例类型的信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的[更改实例类型](#)。

[EC2.27] 运行 EC2 实例不应使用密钥对 (已停用)

此控件将停用。

[ECR.1] ECR 私有存储库应配置图像扫描

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：AWS::ECR::Repository

Amazon Config 规则：[ecr-private-image-scanning-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查私有 ECR 存储库是否配置了图像扫描。如果私有 ECR 存储库未配置图像扫描，则此控制将失败。请注意，您还必须为每个存储库配置[推送时扫描](#)，才能通过此控制。

ECR 映像扫描有助于识别容器镜像中的软件漏洞。ECR 使用[开源 Clair 项目](#)中的常见漏洞和披露 (CVE) 数据库，并提供扫描发现结果的列表。在 ECR 存储库上启用图像扫描可为所存储图像的完整性和安全性添加一层验证层。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要为 ECR 存储库配置图像扫描，请参阅亚马逊弹性容器注册表用户指南中的[图像扫描](#)。

[ECR.2] ECR 私有存储库应配置标签不可变性

类别：识别 > 清单 > 标记

严重性：中

资源类型：AWS::ECR::Repository

Amazon Config 规则：[ecr-private-tag-immutability-enabled](#)

时间表类型：Triger

参数：None (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，则此控制将失败。如果启用了标签不可变性且其值为，则此规则通过IMMUTABLE。

Amazon ECR 标签不可变性使客户能够依赖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指一个唯一的图像。这提高了可靠性和可扩展性，因为使用静态标签将始终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。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

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镜像标签可变性设置，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

类别：识别 > 资源配置

严重性：中

资源类型：AWS::ECR::Repository

Amazon Config 规则：[ecr-private-lifecycle-policy-configured](#)

时间表类型：Triger

参数：None（无）

此控件检查 Amazon ECR 存储库是否配置了至少一个生命周期策略。如果 ECR 存储库未配置任何生命周期策略，则此控制将失败。

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，您可以根据使用期限或计数自动清理未使用镜像和镜像的过期时间。自动执行这些任务可以帮助您避免无意中使用的仓库中的过时图像。

Note

以下区域不支持此控件：

- 亚太地区（大阪）
- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

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](#)。

[ECS.1] Amazon ECS 任务定义应具有安全联网模式和用户定义

类别：保护 > 安全访问管理

严重性：高

资源类型：AWS::ECS::TaskDefinition

Amazon Config 规则：[ecs-task-definition-user-for-host-mode-check](#)

时间表类型：Triger

参数：

- SkipInactiveTaskDefinitions: true

此控件检查具有主机联网模式的活动的 Amazon ECS 任务定义是否也有privileged或user容器定义。对于具有主机网络模式和容器定义（其中privileged=false或为空或为空）的任务定义，user=root控制失败。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

如果任务定义具有提升的权限，那是因为客户已特别选择加入该配置。当任务定义启用了主机联网但客户没有选择提升权限时，此控制会检查是否存在意外的权限升级。

Note

以下区域不支持此控件：

- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

有关如何更新任务定义的信息，请参阅 Amazon Elastic 容器服务开发人员指南中的[更新任务定义](#)。

请注意，更新任务定义时，它不会更新从先前任务定义启动的正在运行的任务。要更新正在运行的任务，必须使用新的任务定义重新部署该任务。

[ECS.2] Amazon ECS 服务不应自动分配公有 IP 地址

类别：保护 > 安全网络配置 > 资源不可公开访问

严重性：高

资源类型：AWS::ECS::Service

Amazon Config 规则：ecs-service-assign-public-ip-disabled（由 Security Hub 开发的自定义规则）

时间表类型：Triger

参数：

- exemptEcsServiceArns (可选). Security Hub 不填充此参数。不受此规则约束的 Amazon ECS 服务的 ARN 列表，以逗号分隔。

COMPLIANT如果 Amazon ECS 服务已AssignPublicIP设置为ENABLED并在此参数列表中指定，则此规则为准。

NON_COMPLIANT如果 Amazon ECS 服务已AssignPublicIP设置为ENABLED且未在此参数列表中指定，则此规则为准。

此控件会检查 Amazon ECS 服务是否已配置为自动分配公有 IP 地址。如果AssignPublicIP是，则此控件将失效ENABLED。如果AssignPublicIP是，则此控件通过DISABLED。

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，则可以从互联网访问您的 Amazon ECS 实例。Amazon ECS 服务不应公开访问，因为这可能允许意外访问您的容器应用程序服务器。

Note

亚太地区（大阪）区域不支持此控件。

修复

要禁用自动公有 IP 分配，请参阅亚马逊弹性容器服务开发人员指南中的[为您的服务配置 VPC 和安全组设置](#)。

[ECS.3] ECS 任务定义不应共享主机的进程命名空间

类别：识别 > 资源配置

严重性：高

资源类型：AWS::ECS::TaskDefinition

Amazon Config规则：[ecs-task-definition-pid-模式检查](#)

时间表类型：Triger

参数：None（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。如果任务定义与在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) 命名空间提供进程之间的分离。它可以防止系统进程可见，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，它将允许容器查看宿主系统上的所有进程。这减少了主机和容器之间进程级隔离的好处。这些情况可能导致对主机本身进程的未经授权的访问，包括操纵和终止这些进程。客户不应与在其上运行的容器共享主机的进程命名空间。

修复

要在任务定义pidMode上配置，请参阅 Amazon Elastic Container Service 开发人员指南中的[任务定义参数](#)。

[ECS.4] ECS 容器应以非特权方式运行

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

Amazon Config 规则：[ecs-containers-nonprivileged](#)

时间表类型：Triger

参数：None（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的权限。当权限参数为true，将对此容器提供对主机容器实例的提升的主机容器实例权限（类似于根用户）。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要在任务定义上配置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 容器应限于对根文件系统的只读访问权限

类别：保护 > 安全访问管理

严重性：高

资源类型：AWS::ECS::TaskDefinition

Amazon Config 规则：[ecs-containers-readonly-access](#)

时间表类型：Triger

参数：None（无）

此控制检查 Amazon ECS 容器是否仅限于对已安装的根文件系统的只读访问权限。如果 Amazon ECS 任务定义的容器定义中的ReadonlyRootFilesystem参数设置为，则此控制将失败false。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

启用此选项可减少安全攻击媒介，因为容器实例的文件系统不能被篡改或写入，除非它对其文件系统文件夹和目录具有明确的读写权限。此控制还遵循最小权限原则。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

将容器定义限制为对根文件系统的只读访问权限

1. 打开 <https://console.aws.amazon.com/ecs/> 上的 Amazon ECS 控制台。
2. 在左侧导航窗格中，请选择 Task Definitions
3. 对于包含需要更新的容器定义的任务定义，请执行以下操作：

- 选择需要更新的容器定义。
- 选择“编辑容器”。对于“存储和日志”，选择“只读根文件系统”。
- 在“编辑容器”选项卡底部选择“更新”。
- 选择 Create (创建)。

[ECS.8] 密钥不应作为容器环境变量传递

类别：保护 > 安全开发 > 凭证不是硬编码的

严重性：高

资源类型：AWS::ECS::TaskDefinition

Amazon Config 规则：[ecs-no-environment-secrets](#)

时间表类型：Triger

参数：

- SecretKeys =AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY,ECS_ENGINE_AUTH_DATA

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_IDAWS_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_IDAWS_SECRET_ACCESS_KEY、或，则此控制将失败ECS_ENGINE_AUTH_DATA。此控件不涵盖从其他位置（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。

Amazon Systems Manager参数存储可以帮助您改善组织的安全状况。我们建议使用 Parameter Store 来存储密钥和证书，而不是直接将它们传递到您的容器实例或将它们硬编码到您的代码中。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要使用 SSM 创建参数，请参阅Amazon 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，请参阅亚马逊弹性容器服务开发人员指南中的[使用 Secrets Manager 指定敏感数据](#)。

[ECS.10] Fargate 服务应该在最新的 Fargate 平台版本上运行

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：AWS::ECS::Service

Amazon Config 规则：[ecs-fargate-latest-platform-version](#)

时间表类型：Triger

参数：None (无)

此控件检查亚马逊 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，则此控制将失败。

Amazon Fargate 平台版本指的是任务基础设施的特定运行时环境，即内核和容器运行时版本的组合。随着运行环境的发展，新的平台版本也随之发布。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 任务的安全更新和修补程序将自动部署。如果安全问题影响平台版本，Amazon 为平台版本提供补丁。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要更新现有服务，包括其平台版本，请参阅 Amazon Elastic Container 服务开发人员指南中的[更新](#)服务。

[ECS.12] ECS 集群应启用容器洞察

类别：识别 > 记录

严重性：中

资源类型：AWS::ECS::Cluster

Amazon Config 规则：[ecs-container-insights-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查 ECS 集群是否使用容器洞察。如果没有为集群设置容器见解，则此控制将失败。

监控是保持 Amazon ECS 集群的可靠性、可用性和性能的重要方面。使用 Container Insights 从 CloudWatch 容器化应用程序和微服务中收集、聚合和汇总指标与日志。CloudWatch 自动收集许多资源（例如 CPU、内存、磁盘和网络）的指标。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。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- 亚太地区 (大阪)
- China (Beijing)

- China (Ningxia)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要使用容器见解，请参阅亚马逊 CloudWatch 用户指南中的[更新服务](#)。

[EFS.1] 应将 Amazon EFS 配置为使用以下方法加密静态文件数据Amazon KMS

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

Amazon Config 规则：[efs-encrypted-check](#)

时间表类型：定期

参数：None (无)

此控件检查 Amazon Elastic File System 是否配置为使用加密文件数据Amazon KMS。在以下情况下，检查失败。

- Encryptedfalse在[DescribeFileSystems](#)响应中设置为。
- [DescribeFileSystems](#)响应中的KmsKeyId密钥与的KmsKeyId参数不匹配[efs-encrypted-check](#)。

请注意，此控件不使用KmsKeyId参数[efs-encrypted-check](#)。它只检查 Encrypted 的值。

要为 Amazon EFS 中的敏感数据增加安全层，您应该创建加密文件系统。Amazon EFS 支持对静态文件系统进行加密。创建 Amazon EFS 文件系统时，可以启用静态数据加密。要了解有关 Amazon EFS 加密的更多信息，请参阅《Amazon [EFS 用户指南](#)》中的[Amazon Elastic File System 中的数据加密](#)。

Note

非洲 (开普敦) 或欧洲 (开普敦) 或欧洲 (米兰) 不支持此控件。

修复

有关如何加密新 Amazon EFS 文件的详细信息，请参阅 Amazon Elastic File System 用户指南中的[加密静态数据](#)。

[EFS.2] 亚马逊 EFS 卷应包含在备份计划中

类别：恢复 > 弹性 > Backup

严重性：中

资源类型：AWS::EFS::FileSystem

Amazon Config 规则：[efs-in-backup-plan](#)

时间表类型：定期

参数：None (无)

此控制检查是否将 Amazon Elastic File System (Amazon EFS) 文件系统添加到中的备份计划中Amazon Backup。如果 Amazon EFS 文件系统未包含在备份计划中，则控制将失败。

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。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要修复此问题，请更新您的文件系统以启用自动备份。

为现有文件系统启用自动备份

1. 访问 <https://console.aws.amazon.com/efs/>，打开 Amazon Elastic File System 控制台。
2. 在文件系统页面上，选择要启用自动备份的文件系统。

将显示文件系统详细信息页面。

3. 在“常规”下，选择“编辑”。
4. 要启用自动备份，请选择启用自动备份。
5. 选择 Save changes (保存更改)。

要了解更多信息，请访问 [Amazon Elastic File System 用户指南中的使用Amazon Backup](#) Amazon EFS。

[EFS.3] EFS 接入点应强制使用根目录

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::EFS::AccessPoint

Amazon Config 规则：[efs-access-point-enforce-root-directory](#)

时间表类型：Triger

参数：None (无)

此控制检查 Amazon EFS 接入点是否配置为强制使用根目录。如果将的值设置Path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，使用访问点的 NFS 客户端使用在访问点上配置的根目录，而不是文件系统的根目录。强制为接入点设置根目录有助于通过确保接入点的用户只能访问指定子目录的文件来限制数据访问。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)

- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

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 文件系统用户指南[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

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::EFS::AccessPoint

Amazon Config 规则：[efs-access-point-enforce-user-identity](#)

时间表类型：Trigger

参数：None (无)

此控制检查 Amazon EFS 接入点是否配置为强制使用用户身份。如果在创建 EFS 接入点时未定义 POSIX 用户身份，则此控制将失败。

Amazon EFS 访问点是 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。访问点可以为通过访问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）。访问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。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要强制使用 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](#)。

[EKS.2] EKS 集群应该在支持的 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::Cluster

Amazon Config 规则：[eks-cluster-supported-version](#)

时间表类型：Trigger

参数：

- eks:oldestVersionSupported (目前支持的最旧版本是 1.19)

此控件检查 Amazon EKS 集群是否在支持的 Kubernetes 版本上运行。如果 EKS 集群在不受支持的版本上运行，则控制会失败。

如果您的应用程序不需要一个特定版本的 Kubernetes，我们建议您为您的集群使用 EKS 支持的最新可用 Kubernetes 版本。有关亚马逊 EKS 支持的 Kubernetes 版本的更多信息，请参阅[亚马逊 EKS Kubernetes 发布日历](#)和[亚马逊 EKS 版本支持以及亚马逊 EKS 用户指南中的常见问题解答](#) /para >。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要更新 EKS 集群，请在 [Amazon EKS 用户指南中更新 Amazon EKS 集群 Kubernetes 版本](#) /para >。

[ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

类别：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::ElasticBeanstalk::Environment

Amazon Config 规则：[beanstalk-enhanced-health-reporting-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查您的 Amazon 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可以更快地响应底层基础设施运行状况的变化。这些更改可能导致应用程序的可用性不足。

Elastic Beanstalk 增强型运行状况报告提供了状态描述符，用于评估已识别问题的严重性并确定可能的调查原因。支持的亚马逊系统映像 (AMI) 中包含的 Elastic Beanstalk 运行状况代理用于评估环境 EC2 实例的日志和指标。

有关更多信息，请参阅《Amazon Elastic Beanstalk 开发者指南》中的[增强型运行状况报告和监控](#)。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何启用增强型运行状况报告的说明，请参阅Amazon Elastic Beanstalk开发者指南中的[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

类别：检测 > 漏洞、补丁和版本管理

严重性：高

资源类型：AWS::ElasticBeanstalk::Environment

Amazon Config 规则：[elastic-beanstalk-managed-updates-enabled](#)

时间表类型：Triger

参数：None (无)

此控件检查是否为 Elastic Beanstalk 环境启用了托管平台更新。

启用托管平台更新可确保安装适用于环境的最新可用平台补丁、更新和功能。及时安装补丁是保护系统的重要一步。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何启用托管平台更新的说明，请参阅《Amazon Elastic Beanstalk开发者指南》中[托管平台更新下的“配置托管平台更新”](#)。

[ELB.2] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书Amazon Certificate Manager

类别：保护 > 传输中数据加密

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[elb-acm-certificate-required](#)

时间表类型：Triger

参数：None (无)

此控件检查Classic Load Balancer 是否使用Amazon Certificate Manager (ACM) 提供的 HTTPS/SSL 证书。如果使用 HTTPS/SSL 侦听器配置的Classic Load Balancer 不使用 ACM 提供的证书，则控制将失败。

要创建证书，可以使用 ACM 或支持 SSL 和 TLS 协议的工具（如 OpenSSL）。Security Hub 建议您使用 ACM 为负载均衡器创建或导入证书。

ACM 与传统负载均衡器集成，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。

Note

以下区域不支持这些控件：

- 非洲（开普敦）
- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- 欧洲（米兰）
- Amazon GovCloud（美国东部）

修复

有关如何将 ACM SSL/TLS 证书与 Classic Load Balancer 关联的信息，请参阅[Amazon 知识中心文章如何将 ACM SSL/TLS 证书与经典、应用程序或 Network Load Balancer 关联？](#)

[ELB.3] Classic Load Balancer 监听器应配置为 HTTPS 或 TLS 终止

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[elb-tls-https-listeners-only](#)

时间表类型：触发器

参数：None（无）

此控件检查经典负载均衡器监听器是用 HTTPS 或 TLS 协议配置的，用于前端（客户端到负载均衡器）连接。如果 Classic Load Balancer 有监听器，则该控件适用。如果您的 Classic Load Balancer 没有配置监听器，则该控件不会报告任何发现。

如果为前端连接配置了 TLS 或 HTTPS 的 Classic Load Balancer 监听器，则控制权通过。

如果监听器没有为前端连接配置 TLS 或 HTTPS，则控制将失败。

在开始使用负载均衡器之前，必须添加一个或多个监听器。监听器是使用配置的协议和端口检查连接请求的进程。监听器可以支持 HTTP 和 HTTPS/TLS 协议。您应始终使用 HTTPS 或 TLS 监听器，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，请更新您的监听器以使用 TLS 或 HTTPS 协议。

将所有不合规的监听器更改为 TLS/HTTPS 监听器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Load Balancers（负载均衡器）。然后，选择您的 Classic Load Balancer。
3. 选择“听众”选项卡，然后选择“编辑”。
4. 对于 Load Balancer 协议未设置为 HTTPS 或 SSL 的所有监听器，请将设置更改为 HTTPS 或 SSL。
5. 对于所有修改过的监听器，在 SSL 证书下，选择更改。
6. 对于所有修改过的监听器，选择从 ACM 选择证书。

7. 从 Celerts (证书) 下拉列表中选择证书。然后选择 Save (保存)。
8. 更新所有监听器后，选择 Save。

[ELB.4] 应将应用程序负载均衡器配置为删除 HTTP 标头

类别：保护 > 网络安全

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[alb-http-drop-invalid-header-enabled](#)

时间表类型：触发器

参数：None (无)

此控件评估 Amazon 应用程序负载均衡器，以确保将其配置为删除无效的 HTTP 标头。如果的值设置为，`routing.http.drop_invalid_header_fields.enabled` 则控制失败 `false`。

默认情况下，应用程序负载均衡器配置为删除无效的 HTTP 标头值。删除这些标头值可防止 HTTP 不同步攻击。

请注意，如果启用了 [ELB.12 \(p. 420\)](#)，则可以禁用此控件。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 欧洲 (米兰)

修复

要修复此问题，请将您的负载均衡器配置为删除无效的标头字段。

为负载均衡器配置为删除无效的标头字段

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Load Balancers (负载均衡器)。
3. 选择 Application Load Balancer。
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 Save (保存)。

[ELB.5] 应启用应用程序和传统负载均衡器日志记录

类别：日志记录

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[elb-logging-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查Application Load Balancer 传统负载均衡器是否启用了日志记录。如果access_logs.s3.enabled是，则控制失败false。

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

要修复此问题，请更新您的负载均衡器以启用日志记录。

启用访问日志

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Load Balancers (负载均衡器)。
3. 选择Application Load Balancer。
4. 在操作中，选择编辑属性。
5. 在“访问日志”下，选择“启用”。
6. 输入您的 S3 位置。这个位置可以存在，也可以为您创建。如果您未指定前缀，则访问日志存储在 S3 存储桶的根目录中。
7. 选择 Save (保存)。

[ELB.6] 应启用Application Load Balancer 删除保护

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::ElasticLoadBalancingV2::LoadBalancer

Amazon Config 规则：[elb-deletion-protection-enabled](#)

时间表类型：触发器

参数：None (无)

该控件检查Application Load Balancer 是否已启用删除保护。如果未配置删除保护，则控件将失效。

启用删除保护以保护您的Application Load Balancer 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。

从控制台启用删除保护

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 LOAD BALANCING (负载均衡) 下，选择 Load Balancers (负载均衡器)。
3. 选择负载均衡器。

4. 在 Description (说明) 选项卡上，选择 Edit attributes (编辑属性)。
5. 在编辑负载均衡器属性页面上，为删除保护选择启用，然后选择保存。
6. 选择 Save (保存)。

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[删除保护](#)。

[ELB.7] 经典负载均衡器应启用连接耗尽

类别：恢复 > 故障恢复能力

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：elb-connection-draining-enabled (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

该控件检查传统负载均衡器是否已启用连接耗尽。

在 Classic Load Balancer 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 Auto Scaling 组中的实例特别有用，可确保连接不会突然中断。

修复

要在 Classic 负载均衡器上启用连接耗尽，[请按照 Classic Load Balancer 用户指南中为传统负载均衡器配置连接耗尽](#)中的步骤操作。

[ELB.8] 带有 HTTPS/SSL 侦听器的经典负载均衡器应使用具有强配置的预定义安全策略

类别：保护 > 传输中数据加密

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[elb-predefined-security-policy-ssl-check](#)

时间表类型：触发器

参数：

- predefinedPolicyName: ELBSecurityPolicy-TLS-1-2-2017-01

此控件检查您的 Classic Load Balancer HTTPS/SSL 侦听器是否使用预定义策略 ELBSecurityPolicy-TLS-1-2-2017-01。如果 Classic Load Balancer HTTPS/SSL 侦听器不使用，则控制会失败 ELBSecurityPolicy-TLS-1-2-2017-01。

安全策略是 SSL 协议、密码和服务器顺序首选选项的组合。预定义策略控制在客户端与负载均衡器之间进行 SSL 协商期间要支持的密码、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](#)。

Note

以下区域不支持此控件：

- 非洲（开普敦）
- 亚太地区（大阪）
- 欧洲（米兰）
- Amazon GovCloud（美国东部）

修复

有关如何在 Classic Load Balancer 中使用预定义安全策略 *ELBSecurityPolicy-TLS-1-2-2017-01* 的信息，请参阅传统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

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[elb-cross-zone-load-balancing-enabled](#)

时间表类型：触发器

参数：

- predefinedPolicyName: ELBSecurityPolicy-TLS-1-2-2017-01

此控件检查是否为传统负载均衡器 (CLB) 启用了跨区域负载均衡。如果未为 CLB 启用跨区域负载均衡，则此控制将失败。

负载均衡器节点仅在其可用区中的已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。如果各可用区的注册目标数量不同，则流量将无法均匀分配，并且与另一个区域中的实例相比，一个区域中的实例最终可能会被过度利用。启用跨区域负载均衡，经典负载均衡器的每个负载均衡器节点会跨启用的所有可用区中的注册实例平均分配请求。有关详细信息，请参阅 Elastic Load Balancing [用户指南中的跨区域负载均衡](#)。

Note

非洲（开普敦）不支持此控件。

修复

要在经典负载均衡器中启用跨区域负载均衡，请参阅 Elastic Load Balancing [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

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[clb-multiple-az](#)

时间表类型：触发器

参数：None (无)

此控件检查Classic Load Balancer 是否已配置为跨越多个可用区。如果Classic Load Balancer 不跨多个可用区，则控制失败。

可以设置Classic Load Balancer，以便在单个可用区或多个可用区中的 Amazon EC2 实例间分发传入请求。如果唯一配置的可用区不可用，则不跨多个可用区的Classic Load Balancer 无法将流量重定向到另一个可用区中的目标。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何向Classic Load Balancer 添加可用区的信息，请参阅传统负载均衡器用户指南[中的添加或删除可用区](#)。

[ELB.12] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式

类别：数据保护 > 数据完整性

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[alb-desync-mode-check](#)

时间表类型：触发器

参数：

- desyncMode: 防御，最严格

此控件检查Application Load Balancer 是否配置为防御或最严格的不同步缓解模式。如果Application Load Balancer 未配置为防御性或最严格的不同步缓解模式，则控制将失败。

HTTP 不同步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不同步缓解模式的应用程序负载均衡器可保护您的应用程序免受可能由 HTTP 不同步引起的安全问题的影响。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要更新应用程序负载均衡器的不同步缓解模式，请参阅[Application Load Balancer 用户指南中的不同步缓解模式](#)。

[ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::ElasticLoadBalancingV2::LoadBalancer

Amazon Config 规则：[elbv2-multiple-az](#)

时间表类型：触发器

参数：None (无)

此控件检查Elastic Load Balancer V2 (应用程序、网络或网关Load Balancer) 是否已注册来自多个可用区的实例。如果Elastic Load Balancer V2 在少于两个可用区中注册了实例，则控制会失败。

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确保服务的可用性，因为如果一个可用区不可用，Elastic Load Balancer 将能够将流量定向到另一个可用区。配置多个可用区将有助于避免应用程序出现单点故障。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要向Application Load Balancer 添加可用区，请参阅[适用于 Application Load Balancer 的用户指南中的 Application Load Balancer 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Load Balancer 添加可用区，请参阅[网关Load Balancer 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或最严格的不同步缓解模式

类别：数据保护 > 数据完整性

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

Amazon Config 规则：[clb-desync-mode-check](#)

时间表类型：触发器

参数：

- desyncMode: 防御，最严格

此控件检查 Classic Load Balancer 是否配置为防御或最严格的不同步缓解模式。如果 Application Load Balancer 未配置为防御性或最严格的不同步缓解模式，则此控制将失败。

HTTP 不同步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据劫持或执行未经授权的命令。配置了防御性或最严格的不同步缓解模式的经典负载均衡器可保护您的应用程序免受可能由 HTTP 不同步引起的安全问题的影响。

Note

以下区域不支持此控件：

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要更新 Classic 负载均衡器的 [不同步缓解模式](#)，请参阅 [经典负载均衡器用户指南中的修改不同步缓解模式](#)。

[elbv2.1] 应将 Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型：AWS::ElasticLoadBalancingV2::LoadBalancer

Amazon Config 规则：[alb-http-to-https-redirection-check](#)

时间表类型：定期

参数：None (无)

此控件检查应用程序负载均衡器的所有 HTTP 侦听器上是否配置了 HTTP 到 HTTPS 重定向。如果应用程序负载均衡器的一个或多个 HTTP 侦听器没有配置 HTTP 到 HTTPS 重定向，则检查失败。

在开始使用 Application Load Balancer 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。可以使用 HTTPS 侦听器将加密和解密的工作交给 Application Load Balancer 完成。您应该使用 Application Load Balancer 重定向操作将客户端 HTTP 请求重定向到端口 443 上的 HTTPS 请求，以便在传输中强制加密。

要了解更多信息，请参阅《[适用于 Application Load Balancer 的用户指南](#)》中的 [应用程序负载均衡器的侦听器](#)。

Note

非洲 (开普敦) 或欧洲 (开普敦) 或欧洲 (米兰) 不支持此控件。

修复

要修复此问题，请更新您的负载均衡器以重定向 HTTP 请求。

在 Application Load Balancer 上将 HTTP 请求重定向到 HTTPS

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Load Balancers (负载均衡器)。

3. 选择 Application Load Balancer。
4. 选择 Listeners (侦听器) 选项卡。
5. 选择一个 HTTP 侦听器 (端口 80 TCP)，然后选择 Edit (编辑)。
6. 如果存在现有规则，则必须将其删除。否则，选择 Add action (添加操作)，然后选择 Redirect to... (重定向到...)
7. 选择 HTTPS，然后输入 **443**。
8. 选择圆形符号中的复选标记，然后选择 Update (更新)。

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::EMR::Cluster

Amazon Config 规则：[emr-master-no-public-ip](#)

时间表类型：定期

参数：None (无)

此控件检查 Amazon EMR 集群上的主节点是否具有公有 IP 地址。

如果主节点具有与其任何实例关联的公有 IP 地址，则控制失败。公有 IP 地址在实例的 NetworkInterfaces 配置 PublicIp 字段中指定。此控件仅检查处于 RUNNING 或 WAITING 状态的 Amazon EMR 集群。

Note

非洲 (开普敦) 或欧洲 (开普敦) 或欧洲 (米兰) 不支持此控件。

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。除非是由 Amazon EC2 启动实例向导创建的 false，否则非默认子网的 IPv4 公有寻址属性设置为。在这种情况下，向导将该属性设置为 true。

您需要在具有私有子网的 VPC 中启动集群，该子网将 IPv4 公有寻址属性设置为 false。

启动后，即无法手动将该公有 IPv4 地址与您的实例取消关联。

要修复这一发现，您需要在 VPC 私有子网中创建一个新集群。有关如何在 VPC 私有子网中启动集群的信息，请参阅 Amazon EMR 管理指南中的在 [VPC 中启动集群](#)。

[ES.1] Elasticsearch 域应启用静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：[elasticsearch-encrypted-at-rest](#)

时间表类型：定期

参数：None (无)

此控件检查 Elasticsearch 域是否启用了静态加密配置。如果未启用静态加密，检查将失败。

要为中的敏感数据增加一层安全保护 OpenSearch，您应将您的配置 OpenSearch 为静态加密。ElasticSearch 域名提供静态数据加密。该功能使用 Amazon KMS 存储和管理您的加密密钥。为执行加密，它使用具有 256 位密钥 (AES-256) 的高级加密标准算法。

要了解有关 OpenSearch 静态加密的更多信息，请参阅 [《亚马逊 OpenSearch OpenSearch 服务开发者指南》中的 Amazon Service 静态数据加密](#)。

Note

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 Service 开发 OpenSearch 人员指南中的 [支持的实例类型](#)。

修复

默认情况下，域不对数据进行静态加密，并且您无法配置现有的域以使用该功能。

要启用该功能，您必须创建另一个域并迁移数据。有关创建域的信息，请参阅 [亚马逊 OpenSearch 服务开发者指南](#)。

静态数据加密需要 OpenSearch 服务 5.1 或更高版本。有关为 OpenSearch 服务加密静态数据的更多信息，请参阅 [亚马逊 OpenSearch 服务开发者指南](#)。

[ES.2] Elasticsearch 域应该在 VPC 中

类别：保护 > 安全网络配置 > VPC 中的资源

严重性：重大

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：[elasticsearch-in-vpc-only](#)

时间表类型：定期

参数：None (无)

此控件检查 Elasticsearch 域是否在 VPC 中。它不会通过评估 VPC 子网路由配置来确定公有访问权限。您应该确保 Elasticsearch 域未连接到公有子网。请参阅亚马逊 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《亚马逊 VPC 用户指南》中的 VPC [安全最佳实践](#)。

在 VPC 中部署的 Elasticsearch 域可以通过私有 Amazon 网络与 VPC 资源通信，无需通过公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。VPC 提供多种网络控制来保护对 Elasticsearch 域的访问，包括网络 ACL 和安全组。Security Hub 建议您将公有 Elasticsearch 域迁移到 VPC，以利用这些控件。

修复

如果您创建一个具有公有终端节点的域，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终端节点。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 中启动您的亚马逊 OpenSearch 服务域](#)。

[ES.3] Elasticsearch 域应加密节点之间发送的数据

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型 : AWS::Elasticsearch::Domain

Amazon Config 规则 : [elasticsearch-node-to-node-encryption-check](#)

时间表类型 : 触发器

参数 : None (无)

此控件检查 Elasticsearch 域是否启用了 node-to-node 加密。

HTTPS (TLS) 可用于帮助防止潜在攻击者使用或类似攻击来窃听 person-in-the-middle 或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。为 Elasticsearch 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。

此配置可能会导致性能损失。在启用此选项之前，您应该注意并测试性能权衡。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- China (Beijing)
- China (Ningxia)
- 欧洲 (米兰)

修复

有关在新域和现有域上启用 node-to-node 加密的信息，请参阅 Amazon Ser OpenSearch vice 开发人员指南中的[启用 node-to-node 加密](#)。

[ES.4] 应启用 Elasticsearch 域错误记录到 CloudWatch 日志

类别 : 识别-记录

严重性 : 中

资源类型 : AWS::Elasticsearch::Domain

Amazon Config 规则 : [elasticsearch-logs-to-cloudwatch](#)

时间表类型 : 触发器

参数 :

- logtype = 'error'

此控件检查 Elasticsearch 域是否配置为向日志发送错误 CloudWatch 日志。

您应该启用 Elasticsearch 域的错误日志，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，也可以帮助诊断可用性问题。

Note

以下区域不支持此控件：

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何启用日志发布的信息，请参阅 Amazon Ser OpenSearch vice 开发人员指南中的[启用日志发布（控制台）](#)。

[ES.5] Elasticsearch 域应启用审核日志

类别：识别 > 记录

严重性：中

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：elasticsearch-audit-logging-enabled（由 Security Hub 开发的自定义规则）

时间表类型：触发器

参数：

- cloudWatchLogsLogGroupArnList (可选). Security Hub 不填充此参数。应为审核 CloudWatch 日志配置的以逗号分隔的日志日志组列表。

NON_COMPLIANT 如果未在此参数列表中指定 Elasticsearch 域的 CloudWatch 日志组，则使用此规则。

此控件检查 Elasticsearch 域是否启用了审核日志。如果 Elasticsearch 域未启用审计日志，则此控制将失败。

审核日志是高度可定制的。通过它们，您可以跟踪 Elasticsearch 集群上的用户活动，包括身份验证成功和失败、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 Service 开发 OpenSearch 人员指南中的[启用审计日志](#)。

[ES.6] Elasticsearch 域应至少有三个数据节点

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：elasticsearch-data-node-fault-tolerance（由 Security Hub 开发的自定义规则）

时间表类型：触发器

参数：None（无）

此控件检查 Elasticsearch 域是否配置了至少三个数据节点，并且 zoneAwarenessEnabled 是 true。

Elasticsearch 域需要至少三个数据节点才能实现高可用性和容错能力。部署具有至少三个数据节点的 Elasticsearch 域可确保节点出现故障时群集运行。

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/es/](https://console.aws.amazon.com/es/)。

2. 在“我的域名”下，选择要编辑的域名。
3. 选择 Edit domain (编辑域)。
4. 在“数据节点”下，将“节点数”设置为一个大于或等于的数字3。

对于三个可用区部署，设置为三的倍数以确保在可用区之间均匀分布。

5. 选择 Submit (提交)。

[ES.7] Elasticsearch 域应配置至少三个专用主节点

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：elasticsearch-primary-node-fault-tolerance (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查 Elasticsearch 域是否配置了至少三个专用主节点。如果域不使用专用的主节点，则此控制将失败。如果 Elasticsearch 域有五个专用主节点，则此控制权将通过。但是，可能没有必要使用三个以上的主节点来降低可用性风险，这会导致额外的成本。

Elasticsearch 域需要至少三个专用的主节点才能实现高可用性和容错能力。在数据节点蓝/绿部署期间，专用主节点资源可能会紧张，因为还有其他节点需要管理。部署具有至少三个专用主节点的 Elasticsearch 域可确保在节点出现故障时有足够的主节点资源容量和集群操作。

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/es/](https://console.aws.amazon.com/es/)。
2. 在“我的域名”下，选择要编辑的域名。
3. 选择 Edit domain (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三个或更多。
6. 选择 Submit (提交)。

[ES.8] 与 Elasticsearch 域的连接应使用 TLS 1.2 进行加密

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型：AWS::Elasticsearch::Domain

Amazon Config 规则：elasticsearch-https-required (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查使用 TLS 1.2 是否需要连接到 Elasticsearch 域。如果 Elasticsearch 域 TLS Security Policy 不是政策 min-tls-1-2-2019-07，则检查失败。

HTTPS (TLS) 可用于帮助防止潜在攻击者使用 person-in-the-middle 或类似攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。对传输中的数据进行加密可能会影响性能。您应该使用此功能测试您的应用程序，以了解性能概况和 TLS 的影响。与以前版本的 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 操作来配置，以便设置 [TLSSecurityPolicy](#)。有关 [DomainEndpointOptions](#) 的更多信息，请参阅 Amazon Ser OpenSearch vice 开发人员指南。

[GuardDuty.1] GuardDuty 应启用

类别：检测 > 检测服务

严重性：高

资源类型：Amazon 账户

Amazon Config 规则：[guardduty-enabled-centralized](#)

时间表类型：定期

参数：None (无)

此控件检查您的 GuardDuty 账户和地区 GuardDuty 是否启用了亚马逊。

强烈建议您在所有支持的 Amazon 区域 GuardDuty 中启用。这样做可以生成 GuardDuty 有关未经授权或异常活动的调查结果，即使在您未积极使用的区域也是如此。这还 GuardDuty 允许监控 IAM 等全球 Amazon 服务 CloudTrail 的事件。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- China (Beijing)
- China (Ningxia)
- Europe (Milan)
- Middle East (Bahrain)
- Amazon GovCloud (美国东部)

修复

要修复此问题，请启用 GuardDuty。

有关如何启用 (GuardDuty 包括 Amazon Organizations 如何使用管理多个账户) 的详细信息，请参阅亚马逊 GuardDuty 用户指南 GuardDuty 中的 [入门](#)。

[IAM.1] IAM 策略不应允许完整的 “*” 管理权限

类别：保护 > 安全访问管理

严重性：高

资源类型：AWS::IAM::Policy

Amazon Config 规则：[iam-policy-no-statements-with-admin-access](#)

时间表类型：触发器

参数：None (无)

此控件通过添加带"Effect": "Allow"有 over 的语句来检查默认版本的 IAM 策略 (也称为客户托管策略) 是否具有管理员访问权限"Resource": "*". "Action": "*"如果您的 IAM 策略包含此类语句, 则控制会失败。

该控制仅检查您创建的客户托管策略。它不检查内联和Amazon托管策略。

IAM 策略定义了一组授予用户、群组或角色的权限。按照标准安全建议, Amazon 建议您授予最低特权, 这意味着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, 您会将资源暴露给可能有有害的操作。

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。

您应该删除带"Effect": "Allow" 有 over 语句的 IAM 策略"Resource": "*". "Action": "*"

Note

Amazon Config应在您使用 Security Hub 的所有区域中启用。但是, 可以在单个区域中启用全局资源记录。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

要修改您的 IAM 策略, 使其不允许完整的 "*" 管理权限, 请参阅 [IAM 用户指南中的编辑 IAM 策略](#)。

[IAM.2] IAM 用户不应附加 IAM 政策

类别：保护 > 安全访问管理

严重性：低

资源类型：AWS::IAM::User

Amazon Config 规则：[iam-user-no-policies-check](#)

时间表类型：触发器

参数：None (无)

此控制可检查您的所有 IAM 用户是否都没有附加策略。相反, IAM 用户必须继承 IAM 群组或角色的权限。

默认情况下, IAM 用户、组和角色无法访问Amazon资源。IAM 策略向用户、群组或角色授予权限。我们建议您将 IAM 策略直接应用于群组和角色, 但不要应用于用户。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

由亚马逊简单电子邮件服务创建的 IAM 用户是使用内联策略自动创建的。Security Hub 会自动免除这些用户的此控制。

Amazon Config应在您使用 Security Hub 的所有区域中启用。但是, 可以在单个区域中启用全局资源记录。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

要解决此问题, [请创建 IAM 群组](#)并将策略附加到该群组。然后, [将用户添加到群组中](#)。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 用户的访问密钥应每 90 天或更短时间轮换一次

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::IAM::User

Amazon Config 规则：[access-keys-rotated](#)

时间表类型：定期

参数：

- maxAccessKeyAge：90

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 角色或使用[联合](#)。您可以使用这些方法允许用户使用其现有的公司凭证登录 Amazon Web Services Management Console 和 Amazon CLI。

每种方法都有其使用案例。对于拥有现有中央目录或计划需要超过 IAM 用户当前限制的企业，Federation 通常更好。在 Amazon 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 Amazon 资源。

但是，如果需要提供编程访问的资源在 Amazon 内部运行，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账户的更多信息，请参阅《Amazon 一般参考》中的[管理 Amazon 访问密钥的最佳实践](#)。另请参阅博客文章[在使用编程访问时保护 Amazon 账户的指南](#)。

如果您已经有访问密钥，Security Hub 建议您每 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。它们用于签署您对发出的编程请求 Amazon。Amazon 用户需要自己的访问密钥才能从 Amazon 从、适用于 Windows 的工具 Amazon CLI、Amazon SDK 进行编程调用 PowerShell，或者使用单个 Amazon 服务的 API 操作进行直接 HTTP 调用。

如果您的企业使用 Amazon IAM Identity Center (successor to Amazon Single Sign-On) (IAM Identity Center)，则用户可以登录到 Active Directory、内置 IAM Identity Center 目录或其他[连接到 IAM Identity Center](#)。然后，他们可以映射到 IAM 角色，这样他们就可以在不需要 IAM 用户访问密钥的情况下运行 Amazon CLI 命令或调用 Amazon 用 API 操作。要了解更多信息，请参阅[《Amazon Command Line Interface 用户指南》Amazon IAM Identity Center \(successor to Amazon Single Sign-On\) 中的配置 Amazon CLI 以使用](#)。

Note

非洲（开普敦）或欧洲（开普敦）或欧洲（米兰）不支持此控件。

Amazon Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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，请替换所有超过 90 天的密钥。

确保访问密钥的使用时长不超过 90 天

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。

2. 选择 Users (用户)。
3. 对于显示 Access key age (访问密钥使用期限) 超出 90 天的每个用户，选择用户名来打开该用户的设置。
4. 选择 Security credentials (安全凭证)。
5. 为用户创建新的密钥：
 - a. 选择创建访问密钥。
 - b. 要保存密钥内容，请下载秘密访问密钥，或者选择 Show (显示)，然后从页面中复制该密钥。
 - c. 将密钥存储在安全位置以提供给用户。
 - d. 选择 Close (关闭)。
6. 更新使用上一个密钥的所有应用程序以使用新密钥。
7. 对于上一个密钥，请选择 Make inactive (转为非活跃) 来使访问密钥转为非活动状态。用户现在无法使用该密钥发出请求。
8. 确认使用新密钥的所有应用程序都能按预期工作。
9. 确认所有应用程序都使用新密钥后，删除以前的密钥。访问密钥一经删除，就无法恢复。

要删除上一个密钥，请在行末尾选择 X，然后选择 Delete (删除)。

[IAM.4] IAM 根用户访问密钥不应存在

类别：保护 > 安全访问管理

严重性：重大

资源类型：Amazon 账户

Amazon Config 规则：[iam-root-access-key-check](#)

时间表类型：定期

参数：None (无)

此控件检查根用户访问密钥是否存在。

root 用户是 Amazon 账户中权限最高的用户。Amazon 访问密钥提供对给定账户的编程访问。

Security Hub 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。

Note

亚太地区 (雅加达) 或亚太地区 (大阪) 区域不支持此控件。

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](#)。

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::IAM::User

Amazon Config 规则：[mfa-enabled-for-iam-console-access](#)

时间表类型：定期

参数：None (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 Amazon 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 Amazon 网站时，系统会提示输入用户名和密码。此外，系统还会提示用户从他们 Amazon MFA 设备输入身份验证代码。

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

Amazon Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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》Amazon [中的使用多重身份验证 \(MFA\)](#)。

我们向符合条件的客户提供免费的 MFA 安全密钥。 [查看您的质量是否合格，然后订购免费密钥](#)。

[IAM.6] 应该为根用户启用硬件 MFA

类别：保护 > 安全访问管理

严重性：重大

资源类型：Amazon 账户

Amazon Config 规则：[root-account-hardware-mfa-enabled](#)

时间表类型：定期

参数：None (无)

此控件检查您的 Amazon 账户是否允许使用硬件多因素身份验证 (MFA) 设备使用根用户凭证登录。

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 [启用虚拟多重身份验证 \(MFA\) 设备 \(控制台\)](#)。

基于时间的一次性密码 (TOTP) 和通用第二要素 (U2F) 令牌均可作为硬件 MFA 选项。

Note

以下区域不支持此控件：

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)。

修复

要为根用户添加硬件 MFA 设备，请参阅 IAM 用户指南中的 [为 Amazon 账户根用户启用硬件 MFA 设备 \(控制台\)](#)。

我们向符合条件的客户提供免费的 MFA 安全密钥。 [查看您的质量是否合格，然后订购免费密钥](#)。

[IAM.7] IAM 用户的密码策略应具有强配置

类别：保护 > 安全访问管理

严重性：中

资源类型：Amazon 账户

Amazon Config 规则：[iam-password-policy](#)

时间表类型：定期

参数：

- RequireUppercaseCharacters: true
- RequireLowercaseCharacters: true
- RequireSymbols: true
- RequireNumbers: true
- MinimumPasswordLength: 8

此控件检查 IAM 用户的账户密码策略是否使用推荐的配置。

要访问 Amazon Web Services Management Console，IAM 用户需要密码。作为最佳实践，Security Hub 强烈建议您使用联合，而不是创建 IAM 用户。Federation 允许用户使用他们现有的公司凭据登录 Amazon Web Services Management Console。使用 Amazon IAM Identity Center (successor to Amazon Single Sign-On) (IAM 身份中心) 创建或联合用户，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的更多信息，请参阅 IAM 用户指南中的[身份提供商和联合](#)。要了解有关 IAM Identity Center 的更多信息，请参阅《[Amazon IAM Identity Center \(successor to Amazon Single Sign-On\) 用户指南](#)》。

如果您需要使用 IAM 用户，Security Hub 建议您强制创建强用户密码。您可以在 Amazon 账户上设置密码策略，以指定密码的复杂性要求和强制轮换期。当您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。一些设置将立即实施。

修复

要更新您的密码策略以使用推荐配置，请参阅 [IAM 用户指南中的为 IAM 用户设置账户密码策略](#)。

[IAM.8] 应删除未使用的 IAM 用户证书

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::IAM::User

Amazon Config 规则：[iam-user-unused-credentials-check](#)

时间表类型：定期

参数：

- maxCredentialUsageAge: 90

此控件检查您的 IAM 用户是否有 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 Amazon 资源。

Security Hub 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账户或已弃用账户的关联凭证的风险。

Note

Amazon Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域中启用全局资源记录。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

要获取监控账户是否有过期证书所需的一些信息，请使用 IAM 控制台。例如，当您查看账户中的用户时，会显示 Access key age（访问密钥使用期限）、Password age（密码使用期限）和 Last activity（上次活动时间）。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账户和识别 90 天或更长时间没有活动的账户。您可以从 IAM 控制台下载 .csv 格式的证书报告。有关证书报告的更多信息，请参阅 IAM 用户指南中的[获取 Amazon 账户的证书报告](#)。

确定非活动账户或未使用的凭证后，请使用以下步骤禁用它们。

禁用非活跃账户的证书

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 选择 Users（用户）。
3. 选择拥有超过 90 天凭证的用户的姓名。
4. 选择 Security credentials（安全凭证）。
5. 对于至少 90 天未使用的每个登录凭证和访问密钥，选择“设为非活动状态”。

[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

类别：检测 > 安全访问管理

严重性：低

资源类型：AWS::IAM::Policy

Amazon Config 规则：[iam-policy-no-statements-with-full-access](#)

时间表类型：触发器

参数：

- excludePermissionBoundaryPolicy: True

此控件检查您创建的基于身份的 IAM 策略是否具有使用 * 通配符授予对任何服务执行所有操作的权限的 Allow 语句。如果有任何策略声明包含 "Effect": "Allow"，则控制失败 "Action": "Service:*"。

例如，策略中的以下语句会导致查找失败。

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:*",  
    "Resource": "*"   
  }  
]
```

如果您使用 "Effect": "Allow" 和, 则控件也会失效 "NotAction": "**service**:*"。在这种情况下, NotAction 元素提供对 Amazon 服务中所有操作的访问权限, 中指定的操作除外 NotAction。

此控制仅适用于客户管理的 IAM 策略。它不适用于由管理的 IAM 策略 Amazon。

在为 Amazon 服务分配权限时, 务必在 IAM 策略中限定允许的 IAM 操作的范围。您应将 IAM 操作限制为仅限于所需的操作。这可以帮助您设置最低权限权限。如果将策略附加到可能不需要权限的 IAM 委托人, 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类似前缀的 IAM 操作 DescribeAvailabilityZones。DescribeFlowLogs 在这些授权案例中, 您可以在常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的通配符作为前缀的 IAM 操作, 则此控制即通过。例如, 策略中的以下语句会得出一个已通过的调查结果。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

当您以这种方式对相关的 IAM 操作进行分组时, 还可以避免超过 IAM 策略的大小限制。

Note

以下区域不支持此控件:

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

Amazon Config 应在您使用 Security Hub 的所有区域中启用。但是, 可以在单个区域中启用全局资源记录。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, 请更新您的 IAM 策略, 使其不允许完整的 "*" 管理权限。有关如何编辑 IAM 策略的详细信息, 请参阅 [IAM 用户指南中的编辑 IAM 策略](#)。

[Kinesis.1] Kinesis Data Streams 应该在静态时加密

类别: 保护 > 数据保护 > 静态数据加密

严重性: 中

资源类型: AWS::Kinesis::Stream

Amazon Config 规则: [kinesis-stream-encrypted](#)

时间表类型: 触发器

参数: None (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 流没有使用服务器端加密进行静态加密，则此控制将失败。

服务器端加密是 Amazon Kinesis Data Streams 中的一项功能，它使用在数据进入静态状态之前自动对数据进行加密Amazon KMS key。数据在写入 Kinesis 流存储层之前经过加密，从存储中检索后解密。因此，您的数据将在 Amazon Kinesis Data Streams 服务中进行静态加密。

Note

以下区域不支持此控件：

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关为 Kinesis 流启用服务器端加密的信息，请参阅[如何开始使用服务器端加密？](#)在 Amazon Kinesis 开发者指南中。

[KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥进行解密和重新加密操作

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::IAM::Policy

Amazon Config 规则：[iam-customer-policy-blocked-kms-actions](#)

时间表类型：触发器

参数：

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt
- excludePermissionBoundaryPolicy: True

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Amazon KMS解密操作。此控件使用自动推理引擎 [Zelkova](#) 来验证和警告您有关可能授予跨Amazon账户广泛访问您的机密权限的政策。

如果策略已开放，足以允许kms:Decrypt对任意 KMS 密钥kms:ReEncryptFrom执行操作，则此控制将失败，并将该策略标记为FAILED。

该控件会评估附加和未附加的客户托管策略。它不检查内联策略或Amazon托管策略。

借Amazon KMS助，您可以控制谁可以使用您的 KMS 密钥并获得对加密数据的访问权限。IAM 策略定义身份（用户、组或角色）可以对哪些资源执行哪些操作。按照安全最佳实践，Amazon建议您允许最低权限。换句话说，您应仅向身份授予kms:Decrypt或kms:ReEncryptFrom权限，并且仅授予执行任务所需的密钥的权限。否则，用户可能会使用不适合您的数据的密钥。

与其为所有密钥授予权限，不如确定用户访问加密数据所需的最小密钥集。然后设计仅允许用户使用这些密钥的策略。例如，请勿允许对所有 KMS 密钥的kms:Decrypt权限。相反，kms:Decrypt只允许在您的账户使用特定区域的密钥。通过采用最小权限原则，您可以降低意外泄露数据的风险。

Note

亚太地区（雅加达）或亚太地区（大阪）区域不支持此控件。

修复

要修复此问题，您可以修改 IAM 客户托管策略以限制对密钥的访问。

修改 IAM 客户托管策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 在 IAM 导航窗格中，选择策略。
3. 选择要修改的策略旁边的箭头。
4. 选择编辑策略。
5. 请选择 JSON 选项卡。
6. 将“Resource”值更改为要允许的一个或多个特定密钥。
7. 修改策略后，选择查看策略。
8. 选择 Save changes (保存更改)。

有关更多信息，请参阅Amazon Key Management Service开发人员指南Amazon KMS中的[将 IAM 策略与一起使用](#)。

[KMS.2] IAM 委托人不应有允许对所有 KMS 密钥进行解密和重新加密操作的 IAM 内联策略

类别：保护 > 安全访问管理

严重性：中

资源类型：

- AWS::IAM::Role
- AWS::IAM::User
- AWS::IAM::Group

Amazon Config 规则：[iam-inline-policy-blocked-kms-actions](#)

时间表类型：触发器

参数：

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt

检查您的 IAM 身份（角色、用户或群组）中嵌入的内联策略是否允许对所有 KMS Amazon KMS 密钥执行解密和重新加密操作。此控件使用自动推理引擎 [Zelkova](#) 来验证和警告您有关可能授予跨 Amazon 账户广泛访问您的机密权限的政策。

如果策略足够开放，允许对任意 KMS 密钥 kms:ReEncryptFrom 执行 kms:Decrypt 或操作，则此控制将失败。

借助 Amazon KMS，您可以控制谁可以使用您的 KMS 密钥并获得对加密数据的访问权限。IAM 策略定义身份（用户、组或角色）可以对哪些资源执行哪些操作。按照安全最佳实践，Amazon 建议您允许最低权限。换句话说，您应仅授予身份所需的权限，并且仅授予执行任务所需的密钥权限。否则，用户可能会使用不适合您的数据的密钥。

与其授予对所有密钥的权限，不如确定用户访问加密数据所需的最少密钥集。然后设计允许用户仅使用这些密钥的策略。例如，请勿允许对所有 KMS 密钥的 kms:Decrypt 权限。取而代之的是，只允许对账户的特定区域中的特定密钥授予权限。通过采用最小权限原则，您可以降低意外泄露数据的风险。

Note

亚太地区（雅加达）或亚太地区（大阪）区域不支持此控件。

修复

要修复此问题，您可以修改内联策略以限制对密钥的访问。

修改 IAM 内联策略

1. 通过以下网址打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
2. 在 IAM 导航窗格中，选择用户、群组或角色。
3. 选择要修改其 IAM 内联策略的用户、组或角色的名称。
4. 选择要修改的策略旁边的箭头。
5. 选择编辑策略。
6. 请选择 JSON 选项卡。
7. 将该"Resource"值更改为要允许的特定密钥。
8. 修改策略后，选择查看策略。
9. 选择 Save changes（保存更改）。

有关更多信息，请参阅Amazon Key Management Service开发人员指南Amazon KMS中的[将 IAM 策略与一起使用](#)。

[KMS.3] 不应无意中删除Amazon KMS密钥

类别：保护 > 数据保护 > 数据删除保护

严重性：重大

资源类型：AWS::KMS::Key

Amazon Config 规则：[kms-cmk-not-scheduled-for-deletion](#)

时间表类型：定期

参数：None（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 密钥一旦删除，将无法恢复。如果删除 KMS 密钥，则在 KMS 密钥下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 密钥解密数据或重新加密数据，除非您故意执行加密擦除。

计划删除 KMS 密钥时，如果计划有误，则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，但在计划删除 KMS 密钥时，等待期可以缩短至 7 天。在等待期限内，计划的删除可以取消，KMS 密钥不会被删除。

有关删除 KMS 密钥的更多信息，请参阅Amazon Key Management Service开发者指南中的[删除 KMS 密钥](#)。

Note

亚太地区（大阪）和欧洲（米兰）区域中不支持此控件。

修复

有关取消预定 KMS 密钥删除的详细补救说明，请参阅《Amazon Key Management Service开发者指南》中[计划和取消密钥删除（控制台）](#)下的“取消密钥删除”。

[Lambda.1] Lambda 函数策略应禁止公共访问

类别：保护 > 安全网络配置

严重性：重大

资源类型：AWS::Lambda::Function

Amazon Config 规则：[lambda-function-public-access-prohibited](#)

时间表类型：触发器

参数：None (无)

此控制检查 Lambda 函数基于资源的策略是否禁止在您的账户之外进行公共访问。

如果从 Amazon S3 调用 Lambda 函数且策略不包含条件，则控制也会失败AWS:SourceAccount。

Lambda 函数不应公开访问，因为这可能允许意外访问存储在该函数中的代码。

Note

中国（北京）或中国（宁夏）区域不支持此控件。

修复

如果 Lambda 函数未能通过此控制，则表示 Lambda 函数的基于资源的策略语句允许公共访问。

要修复该问题，必须更新策略以删除权限或添加AWS:SourceAccount条件。您只能从 Lambda API 更新基于资源的策略。

以下说明使用控制台查看策略Amazon Command Line Interface并使用删除权限。

查看 Lambda 函数基于资源的策略

1. 打开 Amazon Lambda 控制台，地址：<https://console.aws.amazon.com/lambda/>。
2. 在导航窗格中，选择 Functions (函数)。
3. 选择函数。
4. 请选择权限。基于资源的策略显示了在其他账户或 Amazon 服务尝试访问该函数时应用的权限。
5. 检查基于资源的策略。确定具有使策略公开的Principal字段值的政策声明。例如，允许""或{ "AWS": "*" }。

不能从控制台编辑策略。要删除函数的权限，请使用中的remove-permission命令Amazon CLI。

记下要删除的语句的语句 ID (Sid) 的值。

要使用移除 Lambda 函数的权限，请发出[remove-permission](#)命令。Amazon CLI

```
$ aws lambda remove-permission --function-name <function-name> --statement-id <statement-id>
```

<function-name>替换为 Lambda 函数的名称和要删除<statement-id>的语句的语句 ID。

验证权限是否已更新

1. 打开 Amazon Lambda 控制台，地址：<https://console.aws.amazon.com/lambda/>。
2. 在导航窗格中，选择 Functions (函数)。

3. 选择您更新的函数。
4. 请选择权限。

应更新基于资源的策略。如果策略中只有一个语句，则该策略为空。

有关更多信息，请参阅Amazon Lambda开发者指南Amazon Lambda中的[使用基于资源的策略](#)。

[Lambda.2] Lambda 函数应使用支持的运行时

类别：保护 > 安全开发

严重性：中

资源类型：AWS::Lambda::Function

Amazon Config 规则：[lambda-function-settings-check](#)

时间表类型：触发器

参数：

- runtime: nodejs16.x, nodejs14.x, nodejs12.x, python3.9, python3.8, python3.7, ruby2.7, java11, java8, java8.al2, go1.x, dotnetcore3.1, dotnet6

此控件检查运行时的 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。此控件检查以下运行时的功能设置：nodejs16.x、nodejs14.x、nodejs12.x、python3.9、python3.8、python3.7、ruby2.7、java11、java8和dotnet6。

该Amazon Config规则忽略包类型为的函数Image。

[Lambda 运行时](#)是围绕不断进行维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。虽然您无法创建使用已弃用运行时的函数，但函数仍可用于处理调用事件。确保您的 Lambda 函数是最新的，并且不使用 out-of-date 运行时环境。

要了解有关此控件检查支持的语言的支持的运行时的更多信息，请参阅Amazon Lambda开发者指南中的[Amazon Lambda运行时](#)。

Note

亚太地区（大阪）或中国（宁夏）不支持此控件。

修复

有关支持的运行时和弃用计划的更多信息，请参阅Amazon Lambda开发者指南的[运行时支持政策](#)部分。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。

[Lambda.4] Lambda 函数应配置死信队列（已停用）

此控件将停用。

[Lambda.5] VPC Lambda 函数应在多个可用区中运行

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::Lambda::Function

Amazon Config 规则：[lambda-vpc-multi-az-check](#)

时间表类型：触发器

参数：None (无)

此控件检查 Lambda 是否关联了多个可用区。如果只有一个可用区与 Lambda 关联，则规则失败。

跨多个可用区部署资源是确保架构内高可用性Amazon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。所有 Lambda 函数都应部署多可用区，以确保单个故障区域不会导致操作完全中断。

修复

要通过控制台在多个可用区部署 Lambda 函数，请执行以下操作：

1. 通过 <https://console.aws.amazon.com/lambda/> 打开Amazon Lambda控制台
2. 从 Lambda 控制台的函数页面选择一个函数。
3. 选择 Configuration (配置)，然后选择 VPC。
4. 选择 Edit (编辑)。
5. 如果该功能最初未连接到 VPC，请从下拉菜单中选择一个 VPC。如果该函数最初未连接到 VPC，请选择至少一个安全组连接到该函数

Note

函数执行角色必须拥有CreateNetworkInterface在 EC2 上调用的权限。

6. 选择 Save (保存)。

[NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

Amazon Config 规则：[netfw-policy-rule-group-associated](#)

时间表类型：触发器

参数：None (无)

此控件检查Network Firewall 策略是否有任何关联的状态或无状态规则组。如果未分配无状态或有状态的规则组，则控制将失败。

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过滤数据包和流量，并定义默认流量处理。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要向 Network Firewall 策略添加规则组，请参阅 Amazon Network Firewall 开发者指南中的 [更新防火墙策略](#)。有关创建和管理规则组的信息，请参阅 [中的规则组 Amazon Network Firewall](#)。

[NetworkFirewall.4] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

Amazon Config 规则：[netfw-policy-default-action-full-packets](#)

时间表类型：触发器

参数：

- statelessDefaultActions: aws:drop,aws:forward_to_sfe

此控件检查 Network Firewall 策略中完整数据包的默认无状态操作是丢弃还是转发。如果选择 Drop 或 Forward 则控制通过，如果选择 Pass 则失败。

防火墙策略定义了您的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的规则组来过滤数据包和流量。默认为 Pass 可以允许意外流量。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要更改防火墙策略，请执行以下操作：

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格的“Network Firewall”下，选择“防火墙策略”。
3. 选择要编辑的防火墙策略名称。此会将您转入防火墙策略的详细信息页面。
4. 在无状态默认操作中，选择编辑。然后选择“丢弃”或“转发到有状态规则组”作为完整数据包的默认操作。

[NetworkFirewall.5] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

Amazon Config 规则：[netfw-policy-default-action-fragment-packets](#)

时间表类型：触发器

参数：

- statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe

此控件检查Network Firewall 策略中分段数据包的默认无状态操作是丢弃还是转发。如果选择Drop或，Forward则控制通过，如果选择Pass则失败。

防火墙策略定义了您的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的规则组来过滤数据包和流量。默认为Pass可以允许意外流量。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要更改防火墙策略，请执行以下操作：

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格的“Network Firewall”下，选择“防火墙策略”。
3. 选择要编辑的防火墙策略名称。这会将您转入防火墙策略的详细信息页面。
4. 在无状态默认操作中，选择编辑。然后选择“丢弃”或“转发到有状态规则组”作为分段数据包的默认操作。

[NetworkFirewall.6] 无状态Network Firewall 规则组不应为空

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::RuleGroup

Amazon Config 规则：[netfw-stateless-rule-group-not-empty](#)

时间表类型：触发器

参数：None（无）

此控件检查中的无状态规则组是否Amazon Network Firewall包含规则。如果规则组没有规则，则规则将失败。

规则组包含定义您的防火墙如何处理 VPC 中流量的规则。当防火墙策略中存在空的无状态规则组时，可能会给人以该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

为 Network Firewall 规则组添加规则：

1. 登录到 Amazon 管理控制台并通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>
2. 在导航窗格的“Network Firewall”下，选择“Network Firewall 规则组”。
3. 在 Network Firewall 规则组页面上，选择要编辑的规则组的名称。此会将您转入防火墙规则组详细信息页面。
4. 对于无状态规则组，选择编辑规则将规则添加到规则组。

[OpenSearch.1] OpenSearch 域应启用静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-encrypted-at-rest](#)

时间表类型：触发器

参数：None (无)

此控件检查 OpenSearch 域是否已启用 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层，您应该将您的 OpenSearch 服务域配置为静态加密。配置静态数据加密时，会使用 Amazon KMS 存储和管理您的加密密钥。要执行加密，请 Amazon KMS 使用具有 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 OpenSearch 服务开发者指南》中的 Amazon Service OpenSearch 静态数据加密](#)。

修复

默认情况下，域不对数据进行静态加密，并且您无法配置现有的域以使用该功能。要启用该功能，您必须创建另一个域并迁移数据。

有关创建域的信息，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](#)。

静态数据加密需要 Amazon OpenSearch 1.0 或更高版本。有关为亚马逊加密静态数据的更多信息，请参阅[《亚马逊 OpenSearch 服务开发者指南》中的 Amazon Service 静态数据加密](#)。

[OpenSearch.2] OpenSearch 域应位于 VPC 中

类别：保护 > 安全网络配置 > VPC 中的资源

严重性：重大

资源类型：AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-in-vpc-only](#)

时间表类型：触发器

参数：None (无)

此控件检查 OpenSearch 域是否在 VPC 中。它不会通过评估 VPC 子网路由配置来确定公有访问权限。

您应确保 OpenSearch 域未连接到公有子网。请参阅《亚马逊 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 用户指南中的您的 VPC 的安全性最佳实践](#)。

OpenSearch 在 VPC 中部署的域可以通过私有 Amazon 网络与 VPC 资源通信，无需通过公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。VPC 提供多种网络控制来保护对 OpenSearch 域的访问，包括网络 ACL 和安全组。Security Hub 建议您将公共 OpenSearch 域迁移到 VPC 以利用这些控件。

修复

如果您创建一个具有公有终端节点的域，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终端节点。

您必须[创建另一个域](#)或禁用该控制。

请参阅 [Amazon Serv OpenSearch ice 开发人员指南中的在 VPC 内启动您的 Amazon Serv OpenSearch ice 域](#)

[OpenSearch.3] OpenSearch 域应加密节点之间发送的数据

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型：AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-node-to-node-encryption-check](#)

时间表类型：触发器

参数：None (无)

此控件检查 OpenSearch 域是否启用了 node-to-node 加密。如果在域上禁用 node-to-node 加密，则此控制将失败。

HTTPS (TLS) 可用于帮助防止潜在攻击者使用或类似攻击来窃听 person-in-the-middle 或操纵网络流量。只允许通过 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。

此配置可能会导致性能损失。在启用此选项之前，您应该注意并测试性能权衡。

修复

只能在新域上启用 Node-to-node 加密。要修复这一发现，请创建一个启用 Node-to-node 加密功能的新域，并将您的数据迁移到该存储中。按照亚马逊 OpenSearch 服务开发者指南中的说明[创建新域](#)，并确保在创建新域时选择 Node-to-node 加密选项。然后按照[使用快照迁移数据](#)将数据迁移到新域中。

[OpenSearch.4] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志

类别：识别 > 记录

严重性：中

资源类型：AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-logs-to-cloudwatch](#)

时间表类型：触发器

参数：

- logtype = 'error'

此控件检查 OpenSearch 域是否配置为向日志发送错误 CloudWatch 日志。如果没有为域启用错误日志记录 CloudWatch，则此控制将失败。

您应该启用 OpenSearch 域的错误日志，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，也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 Ser OpenSearch vice 开发人员指南中的[启用日志发布（控制台）](#)。

[OpenSearch.5] OpenSearch 域应启用审核日志

类别：识别 > 记录

严重性：中

资源类型：AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-audit-logging-enabled](#)

时间表类型：触发器

参数：

- cloudWatchLogsLogGroupArnList (可选). Security Hub 不填充此参数。应为审核 CloudWatch 日志配置的以逗号分隔的日志日志组列表。

NON_COMPLIANT 如果未在此参数列表中指定 OpenSearch 域的 CloudWatch 日志日志组，则使用此规则。

此控件检查 OpenSearch 域是否启用了审核日志。如果 OpenSearch 域未启用审核日志，则此控制将失败。

审核日志是高度可定制的。通过它们，您可以跟踪 OpenSearch 集群上的用户活动，包括身份验证成功和失败、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 Service 开发 OpenSearch 人员指南中的[启用审计日志](#)。

[OpenSearch.6] OpenSearch 域应至少有三个数据节点

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::OpenSearch::Domain

Amazon Config 规则：[opensearch-data-node-fault-tolerance](#)

时间表类型：触发器

参数：None (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。如果某个 OpenSearch 域小于 3 或 instanceCount zoneAwarenessEnabled 是，则此控制将失败 false。

一个 OpenSearch 域需要至少三个数据节点才能实现高可用性和容错能力。部署至少包含三个数据节点的 OpenSearch 域可确保节点出现故障时群集运行。

修复

修改 OpenSearch 域中数据节点的数量

1. 登录到 Amazon 控制台并打开 Amazon Ser OpenSearch vice 控制台，[网址：https://console.aws.amazon.com/es/](https://console.aws.amazon.com/es/)。
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”设置为一个大于3。如果您要部署到三个可用区，请将该数字设置为三的倍数，以确保在可用区之间均匀分布。
4. 选择 Submit (提交)。

[OpenSearch.7] OpenSearch 域应启用精细访问控制

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

Amazon Config 规则：[opensearch-access-control-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查 OpenSearch 域是否启用了精细访问控制。如果未启用精细访问控制，则控制会失败。精细访问控制需要advanced-security-options在 OpenSearch 参数update-domain-config中启用。

精细访问控制提供了用于控制对 Amazon Ser OpenSearch vice 上的数据的访问的其他方法。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- 亚太地区 (雅加达)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- 欧洲 (米兰)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要启用精细访问控制，请参阅《[亚马逊 OpenSearch OpenSearch 服务开发者指南](#)》中的 [Amazon Service 中的精细访问控制](#)。

[OpenSearch.8] 与 OpenSearch 域的连接应使用 TLS 1.2 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::OpenSearch::Domain

Amazon Config 规则：[opensearch-https-required](#)

时间表类型：触发器

参数：None (无)

此控件检查使用 TLS 1.2 是否需要连接到 OpenSearch 域。如果 OpenSearch 域不 TLSSecurityPolicy 是，则检查失败 Policy-Min-TLS-1-2-2019-07。

HTTPS (TLS) 可用于帮助防止潜在攻击者使用 person-in-the-middle 或类似攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。对传输中的数据进行加密可能会影响性能。您应该使用此功能测试您的应用程序，以了解性能概况和 TLS 的影响。与以前版本的 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](#) 以设置 TLSSecurityPolicy。有关更多信息，请参阅《Amazon Service 开发 OpenSearch 人员指南》中的 [Node-to-node 加密](#)。

[RDS.1] RDS 快照应为私有快照

类别：保护 > 安全网络配置

严重性：重大

资源类型：AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Amazon Config 规则：[rds-snapshots-public-prohibited](#)

时间表类型：触发器

参数：None (无)

此控件检查 Amazon RDS 快照是否公开。如果 RDS 快照是公共的，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，则所有 Amazon 账户均可使用此快照。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有访问，则 Amazon Config 规则可能在长达 12 小时内无法检测到更改。在 Amazon 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](#)。

Note

非洲 (开普敦) 或欧洲 (开普敦) 或欧洲 (米兰) 不支持此控件。

修复

要修复此问题，请更新您的 RDS 快照以删除公共访问权限。

删除 RDS 快照的公有访问权限

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 导航到 Snapshots (快照)，然后选择要修改的公有快照
3. 从 Actions (操作) 中，选择 Share Snapshots (共享快照)

4. 从 DB snapshot visibility (数据库快照可见性) 中，选择 Private (私有)
5. 在 DB snapshot visibility (数据库快照可见性) 下，选择 all (全部)。
6. 选择 Save (保存)。

[RDS.2] Amazon RDS 数据库实例应禁止公共访问，具体取决于 PubliclyAccessible 配置

类别：保护 > 安全网络配置

严重性：重大

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-instance-public-access-check](#)

时间表类型：触发器

参数：None (无)

此控件通过评估实例配置项目中的 PubliclyAccessible 字段来检查 Amazon RDS 实例是否可公开访问。

Neptune 数据库实例和 Amazon DocumentDB 集群没有 PubliclyAccessible 标志，无法进行评估。但是，这种控制仍然可以为这些资源生成调查结果。你可以抑制这些发现。

RDS 实例配置中的 PubliclyAccessible 值指示是否可以公开访问数据库实例。如果使用 PubliclyAccessible 配置了数据库实例，则它是一个面向 Internet 的实例并具有可公开解析的 DNS 名称，该名称解析为一个公有 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。

除非您打算让您的 RDS 实例可供公开访问，否则不应将 RDS 实例配置为 PubliclyAccessible 值。这样做可能会导致不必要的流量流向您的数据库实例。

修复

要修复此问题，请更新您的 RDS 数据库实例以删除公有访问权限。

从 RDS 数据库实例中删除公有访问权限

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 导航到 Databases (数据库)，然后选择公有数据库。
3. 选择 Modify (修改)。
4. 在“连接”下，展开“其他连接配置”。
5. 在“公共访问”下，选择“不可公开访问”。
6. 选择 Continue (继续)。
7. 在“调度修改”下，选择“立即应用”。
8. 选择修改数据库实例。

有关更多信息，请参阅 Amazon RDS 用户指南中的 [VPC 中使用数据库实例](#)。

[RDS.3] RDS 数据库实例应启用静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-storage-encrypted](#)

时间表类型：触发器

参数：None (无)

此控件检查您的 Amazon RDS 数据库实例是否已启用存储加密。

此控件适用于 RDS 数据库实例。但是，它也可以为 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群生成调查结果。如果这些发现没有用处，那么您可以抑制它们。

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基础存储、其自动化备份、只读副本和快照。

RDS 加密的数据库实例使用开放的标准 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] 应对 RDS 集群快照和数据库快照进行静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型:AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Amazon Config 规则：[rds-snapshots-encrypted](#)

时间表类型：触发器

参数：None (无)

此控件检查 RDS 数据库快照是否已加密。

此控件适用于 RDS 数据库实例。但是，它也可以为 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的快照生成调查结果。如果这些发现没有用处，那么您可以抑制它们。

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。应对 RDS 快照中的数据进行静态加密，以增加安全性。

修复

您可以使用 Amazon RDS 控制台来修复此问题。

对未加密的 RDS 快照进行加密

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择快照。
3. 在“手动”或“系统”下找到要加密的快照。
4. 选中要加密的快照旁边的复选框。

5. 选择操作，然后选择复制快照。
6. 在新数据库快照标识符下，键入新快照的名称。
7. 在“加密”下，选择“启用加密”。
8. 选择用于加密快照的 KMS 密钥。
9. 选择 Copy Snapshot (复制快照)。
10. 创建新快照后，删除原始快照。
11. 对于 Backup 保留期，请选择正非零值。例如，30 天。

[RDS.5] RDS 数据库实例应配置多个可用区

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-multi-az-support](#)

时间表类型：触发器

参数：None (无)

此控件检查您的 RDS 数据库实例是否启用了高可用性。

RDS 数据库实例应针对多个可用区 (AZ) 配置。这确保了存储的数据的可用性。如果可用区出现问题以及在 RDS 常规 RDS 维护期间，多可用区部署允许自动进行故障转移。

修复

要修复此问题，请更新数据库实例以启用多个可用区。

为一个数据库实例启用多个可用区

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)，然后选择要修改的数据库实例。
3. 选择修改。将显示 Modify DB Instance (修改数据库实例) 页面。
4. 在“实例规范”下，将多可用区部署设置为“是”。
5. 选择继续，然后查看修改摘要。
6. (可选) 选择立即应用以立即应用更改。选择此选项在某些情况下可能导致中断。有关更多信息，请参阅 Amazon RDS 用户指南中的[使用“立即应用”设置](#)。
7. 在确认页面上，检查您的更改。如果更改正确无误，请选择 Modify DB Instance (修改数据库实例) 保存更改。

[RDS.6] 应为 RDS 数据库实例和集群配置增强监控

类别：检测 > 检测服务

严重性：低

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-enhanced-monitoring-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查您的 RDS 数据库实例是否启用了增强监控。

在 Amazon RDS 中，增强监控可以更快地响应底层基础设施的性能变化。这些性能变化可能导致数据缺乏可用性。增强监控提供您的 RDS 数据库实例在其上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

有关如何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 群集应启用删除保护

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

Amazon Config 规则：[rds-cluster-deletion-protection-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查 RDS 集群是否已启用删除保护。

此控件适用于 RDS 数据库实例。但是，它也可以为 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群生成调查结果。如果这些发现没有用处，那么您可以抑制它们。

启用群集删除保护是防止未经授权的实体意外删除或删除数据库的额外保护层。

启用删除保护后，无法删除 RDS 集群。在删除请求成功之前，必须禁用删除保护。

Note

以下区域不支持此控件：

- China (Beijing)
- China (Ningxia)
- 中东 (巴林)
- 南美洲 (圣保罗)。

修复

要修复此问题，请更新您的 RDS 数据库集群以启用删除保护。

为 RDS 数据库集群启用删除保护

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)，然后选择数据库，然后选择数据库，然后选择数据库。
3. 选择 Modify (修改)。
4. 在“删除保护”下，选择“启用删除保护”。
5. 选择 Continue (继续)。
6. 在“调度修改”下，选择何时应用修改。选项为 Apply during the next scheduled window。
7. 选择 Modify Cluster。

[RDS.8] RDS 数据库实例应启用删除保护

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

Amazon Config 规则：[rds-instance-deletion-protection-enabled](#)

时间表类型：触发器

参数：

- databaseEngines:mariadb,mysql,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web

此控件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。

启用实例删除保护是防止未经授权的实体意外删除或删除数据库的额外保护层。

启用删除保护后，无法删除 RDS 数据库实例。在删除请求成功之前，必须禁用删除保护。

修复

要修复此问题，请更新您的 RDS 数据库实例以启用删除保护。

为 RDS 数据库实例启用删除保护

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)，然后选择数据库，然后选择数据库，然后选择数据库。
3. 选择 Modify (修改)。
4. 在“删除保护”下，选择“启用删除保护”。
5. 选择 Continue (继续)。
6. 在“调度修改”下，选择何时应用修改。选项为 Apply during the next scheduled window。
7. 选择修改数据库实例。

[RDS.9] 应启用数据库日志记录

类别：识别 > 记录

严重性：中

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-logging-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查以下 Amazon RDS 日志是否已启用并发送到 CloudWatch 日志：

- 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)
- SQQ (错误 , 代理)
- Aurora (审计、错误、常规 , SlowQuery)
- Aurora-MySQL : (审计、错误、常规 , SlowQuery)
- Aurora-PostgreSQL : (Postgresql , 升级)。

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。数据库日志可以帮助进行安全和访问审计,也可以帮助诊断可用性问题。

Note

以下区域不支持此控件:

- 非洲 (开普敦)
- 亚太地区 (大阪)
- 中国 (宁夏)
- 欧洲 (米兰)

修复

日志选项包含在与 RDS 数据库集群或实例关联的数据库参数组中。要在使用数据库引擎的默认参数组时启用日志记录,必须创建一个具有所需参数值的新数据库参数组。然后,您必须关联客户数据库参数组与数据库集群或实例。

要从启用 MariaDB、MySQL 或 PostgreSQL CloudWatch 日志并将其发布到日志 Amazon Web Services Management Console,请在自定义数据库参数组中设置以下参数:

数据库引擎	参数
MariaDB	<code>general_log=1</code> <code>slow_query_log=1</code> <code>log_output = FILE</code> MariaDB 还需要一个自定义选项组,如下所述。
MySQL	<code>general_log=1</code> <code>slow_query_log=1</code> <code>log_output = FILE</code>
PostgreSQL	<code>log_statement=all</code> <code>log_min_duration_statement=<i>minimum query duration (ms) to log</i></code>

创建自定义数据库参数组

1. 通过以下网址打开 Amazon RDS 控制台: <https://console.aws.amazon.com/rds/>。
2. 在导航窗格中,选择参数组。
3. 选择创建参数组。将显示创建参数组窗口。
4. 在参数组系列列表中,选择一个数据库参数组系列。

5. 在类型列表中，选择数据库参数组。
6. 在组名中，输入新数据库参数组的名称。
7. 在 Description (描述) 中，输入新数据库参数组的描述。
8. 选择 Create (创建)。

使用控制台为 MariaDB 日志记录创建新选项组

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择选项组。
3. 选择创建组。
4. 在创建选项组窗口中，执行以下操作：
 - a. 对于 Name (名称)，输入选项组的名称，在 Amazon 账户内该名称需具有唯一性。此名称只能包含字母、数字和连字符。
 - b. 对于说明，输入选项组的简要说明。此说明用于显示说明。
 - c. 对于引擎，选择需要的数据库引擎。
 - d. 对于主引擎版本，请选择所需的数据库引擎主版本。
5. 要继续，请选择创建。
6. 选择您刚创建的选项组的名称。
7. 选择添加选项。
8. MARIADB_AUDIT_PLUGIN从“选项名称”列表中选择。
9. 将 SERVER_AUDIT_EVENTS 设置为 CONNECT, QUERY, TABLE, QUERY_DDL, QUERY_DML, QUERY_DCL。
10. 选择添加选项。

要将 SQL Server 数据库、Oracle 数据库或 PostgreSQL 日志发布到 CloudWatch 日志，请从 Amazon Web Services Management Console

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)。
3. 选择要修改的数据库实例。
4. 选择修改。
5. 在“日志导出”下，选择所有日志文件以开始发布到 CloudWatch 日志。

Log exports (日志导出) 仅适用于支持发布到 CloudWatch 日志的数据库引擎版本。

6. 选择 Continue (继续)。然后在摘要页面上，选择修改数据库实例。

将新的数据库参数组或数据库选项组应用于 RDS 数据库实例

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)。
3. 选择要修改的数据库实例。
4. 选择修改。将显示 Modify DB Instance (修改数据库实例) 页面。
5. 在数据库选项下，根据需要更改数据库参数组和数据库选项组。
6. 完成更改后，选择“继续”。查看修改摘要。
7. (可选) 选择立即应用以立即应用更改。选择此选项在某些情况下可能导致中断。有关更多信息，请参阅 Amazon RDS 用户指南中的[使用“立即应用”设置](#)。
8. 选择修改数据库实例以保存更改。

[RDS.10] 应为 RDS 实例配置 IAM 身份验证

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

Amazon Config 规则：[rds-instance-iam-authentication-enabled](#)

时间表类型：触发器

参数：None (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。

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。数据库的出站和进站网络流量使用 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](#)。

Note

以下区域不支持此控件：

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)

修复

要修复此问题，请更新数据库实例以启用 IAM 身份验证。

为现有数据库实例启用 IAM 身份验证

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 选择 Databases (数据库)。
3. 选择要修改的数据库实例。
4. 选择 Modify (修改)。
5. 在数据库身份验证下，选择密码和 IAM 数据库身份验证。
6. 选择 Continue (继续)。
7. 在“调度修改”下，选择何时应用修改。选项为 Apply during the next scheduled window。
8. 对于集群，选择修改数据库实例。

[RDS.11] Amazon RDS 实例应启用自动备份

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：AWS::RDS::DBCluster

Amazon Config 规则：[db-instance-backup-enabled](#)

时间表类型：触发器

参数：

- backupRetentionMinimum: 7

此控制检查 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七天。如果未启用备份且保留期少于 7 天，则控制将失败。

备份可帮助您更快地从安全事件中恢复，并增强系统的弹性。Amazon RDS 提供了一种配置每日完整实例卷快照的简便方法。有关 Amazon RDS 自动备份的更多详细信息，请参阅 Amazon RDS 用户指南中的[使用备份](#)。

Note

此控件在亚太地区（大阪）不支持此控件。

修复

立即启用自动备份

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)，然后选择要修改的数据库实例。
3. 选择 Modify 打开“修改数据库实例”页面。
4. 在 Backup 保留期下，选择正非零值（例如 30 天），然后选择继续。
5. 选择“计划修改”部分，然后选择何时应用修改：您可以选择在下一个预定维护时段内应用或立即应用。
6. 然后，在确认页面上，选择 Modify DB Instance (修改数据库实例)，可保存更改并启用自动备份。

[RDS.12] 应为 RDS 集群配置 IAM 身份验证

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

Amazon Config 规则：[rds-cluster-iam-authentication-enabled](#)

时间表类型：触发器

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。数据库的出站和进站网络流量使用 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](#)。

Note

以下区域不支持此控件：

- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- 中东（巴林）
- 南美洲（圣保罗）
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

您可以通过 Amazon RDS 控制台为数据库集群启用 IAM 身份验证。

为现有数据库集群启用 IAM 身份验证

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 选择 Databases (数据库)。
3. 选择要修改的数据库集群。
4. 选择 Modify (修改)。
5. 在“数据库选项”下，选择“启用 IAM 数据库身份验证”。
6. 选择 Continue (继续)。
7. 在“调度修改”下，选择何时应用修改：在下一个计划的维护时段内应用或立即应用。
8. 选择修改集群。

[RDS.13] 应启用 RDS 自动次要版本升级

类别：检测 > 漏洞和补丁管理

严重性：高

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-automatic-minor-version-upgrade-enabled](#)

时间表类型：触发器

参数：None (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。

启用自动次要版本升级可确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新。这些升级可能包括安全补丁和错误修复。及时安装补丁是保护系统的重要一步。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

您可以从 Amazon RDS 控制台为数据库实例启用次要版本升级。

为现有数据库实例启用自动次要版本升级

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 选择 Databases (数据库)。
3. 选择要修改的数据库实例。
4. 选择 Modify (修改)。

5. 在“维护”下，为“自动次要版本升级”选择“是”。
6. 选择 Continue (继续)。
7. 在“调度修改”下，选择何时应用修改：在下一个计划的维护时段内应用或立即应用。
8. 选择修改数据库实例。

[RDS.14] Amazon Aurora 集群应启用回溯功能

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：AWS::RDS::DBCluster

Amazon Config 规则：[aurora-mysql-backtracking-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查 Amazon Aurora 集群是否启用了回溯功能。

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弹性。Aurora 回溯可将数据库恢复到某个时间点的时间。它不需要数据库恢复即可执行此操作。

有关在 Aurora 中回溯的更多信息，请参阅 Amazon Aurora 用户指南中的回滚 Aurora [数据库集群](#)。

Note

以下区域不支持此控件：

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- 欧洲 (米兰)
- Europe (Stockholm)
- Middle East (Bahrain)
- 南美洲 (圣保罗)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何启用 Aurora 回溯的详细说明，请参阅 Amazon Aurora 用户指南中的[配置反向跟踪](#)。

请注意，您无法在现有集群上启用回溯功能。相反，您可创建启用了反向跟踪功能的克隆。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](#)。

有关回溯定价的信息，请参阅[Aurora 定价页面](#)。

[RDS.15] 应为多个可用区配置 RDS 数据库集群

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::RDS::DBCluster

Amazon Config 规则：[rds-cluster-multi-az-enabled](#)

时间表类型：触发器

参数：None (无)

此控件检查您的 RDS 数据库集群是否启用了高可用性。

应为多个可用区配置 RDS 数据库集群，以确保存储的数据的可用性。部署到多个可用区允许在出现可用区可用性问题 and 定期 RDS 维护事件期间自动进行故障转移。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- 中东 (巴林)
- 南美洲 (圣保罗)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要修复此控制，请为多个可用区配置数据库集群。

为数据库集群启用多可用区

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择 Databases (数据库)，然后选择要修改的数据库实例。
3. 选择修改。将显示 Modify DB Instance (修改数据库实例) 页面。
4. 在“实例规范”下，将多可用区部署设置为“是”。
5. 选择继续，查看修改摘要。
6. (可选) 选择立即应用以立即应用更改。选择此选项在某些情况下可能导致中断。有关更多信息，请参阅 Amazon RDS 用户指南中的[使用“立即应用”设置](#)。

在确认页面上，检查您的更改。如果更改正确无误，请选择修改数据库实例。

Note

Aurora 全局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，请选择您的数据库集群。然后，选择“操作”和“添加读者”。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 RDS 数据库集群配置为将标签复制到快照

类别：识别 > 清单

严重性：低

资源类型：AWS::RDS::DBCluster

Amazon Config 规则：rds-cluster-copy-tags-to-snapshots-enabled (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查是否将 RDS 数据库集群配置为在创建快照时将所有标签复制到快照。

确定和清点 IT 资产是监管和安全性的一个至关重要的方面。您需要了解您所有的 RDS 数据库集群，以便评估它们的安全态势并对潜在的薄弱领域采取措施。快照的标记方式应与其父 RDS 数据库集群相同。启用此设置可确保快照继承其父数据库集群的标签。

Note

以下区域不支持此控件：

- 中国 (北京)
- 中东 (巴林)
- 南美洲 (圣保罗)

修复

为数据库集群启用自动标签复制到快照的功能

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 选择 Databases (数据库)。
3. 选择要修改的数据库集群。
4. 选择 Modify (修改)。
5. 在 “Backup” 下，选择 “将标签复制到快照”。
6. 选择 Continue (继续)。
7. 在 “调度修改” 下，选择何时应用修改。可以选择 Apply during the next scheduled window (在

[RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照

类别：识别 > 清单

严重性：低

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：rds-instance-copy-tags-to-snapshots-enabled (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查是否将 RDS 数据库实例配置为在创建快照时将所有标签复制到快照。

确定和清点 IT 资产是监管和安全性的一个至关重要的方面。您需要了解您所有的 RDS 数据库实例，以便评估它们的安全态势并对潜在的薄弱领域采取措施。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数据库实例的标签。

修复

为数据库实例启用自动标签复制到快照的功能

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 选择 Databases (数据库)。
3. 选择要修改的数据库实例。
4. 选择 Modify (修改)。
5. 在 “Backup” 下，选择 “将标签复制到快照”。
6. 选择 Continue (继续)。
7. 在 “调度修改” 下，选择何时应用修改。可以选择 Apply during the next scheduled window (在

[RDS.18] 应在 VPC 中部署 RDS 实例

类别：保护 > 安全网络配置 > VPC 中的资源

严重性：高

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：rds-deployed-in-vpc (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查是否在 EC2-VPC 上部署了 Amazon RDS 实例。

VPC 提供多种网络控制来保护对 RDS 资源的访问。这些控制包括 VPC 终端节点、网络 ACL 和安全组。要利用这些控件，我们建议您在 EC2-VPC 上创建 RDS 实例。

修复

有关如何将 RDS 实例移至 VPC 的详细说明，请参阅 Amazon RDS 用户指南中的[更新数据库实例的 VPC](#)。

[RDS.19] 应为关键集群事件配置 RDS 事件通知订阅

类别：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::RDS::EventSubscription

Amazon Config 规则：rds-cluster-event-notifications-configured (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查是否存在为以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。

```
DBCluster: ["maintenance","failure"]
```

RDS 事件通知使用 Amazon SNS 让您知道 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

订阅 RDS 集群事件通知

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择事件订阅。
3. 在“活动订阅”下，选择“创建活动订阅”。
4. 在创建事件订阅对话框中，请执行以下操作：
 - a. 对于名称，输入事件通知订阅的名称。
 - b. 在将通知发送到，为 SNS 主题选择现有的 Amazon SNS ARN。要使用新主题，请选择 Create topic（创建主题）来输入主题的名称和收件人列表。
 - c. 对于源类型，选择集群。
 - d. 在“要包含的实例”下，选择“所有集群”。
 - e. 在“要包括的事件类别”下，选择“特定事件类别”。如果您选择“所有事件类别”，则控件也会通过。
 - f. 选择维护和故障。
 - g. 选择 Create（创建）。

[RDS.20] 应为关键数据库实例事件配置 RDS 事件通知订阅

类别：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::RDS::EventSubscription

Amazon Config 规则：rds-instance-event-notifications-configured（由 Security Hub 开发的自定义规则）

时间表类型：触发器

参数：None（无）

此控件检查是否存在为以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。

```
DBInstance: ["maintenance","configuration change","failure"]
```

RDS 事件通知使用 Amazon SNS 让您知道 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

订阅 RDS 实例事件通知

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择事件订阅。
3. 在“活动订阅”下，选择“创建活动订阅”。
4. 在创建事件订阅对话框中，请执行以下操作：
 - a. 对于名称，输入事件通知订阅的名称。
 - b. 在将通知发送到，为 SNS 主题选择现有的 Amazon SNS ARN。要使用新主题，请选择 Create topic（创建主题）来输入主题的名称和收件人列表。
 - c. 对于源类型，选择实例。
 - d. 在“要包含的实例”下，选择“所有实例”。

- e. 在“要包括的事件类别”下，选择“特定事件类别”。如果您选择“所有事件类别”，则控件也会通过。
- f. 选择维护、配置更改和故障。
- g. 选择 Create (创建)。

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

类别：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::RDS::EventSubscription

Amazon Config 规则：rds-pg-event-notifications-configured (由Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查是否存在为以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。

```
DBParameterGroup: ["configuration change"]
```

RDS 事件通知使用 Amazon SNS 让您知道 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

订阅 RDS 数据库参数组事件通知

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择事件订阅。
3. 在“活动订阅”下，选择“创建活动订阅”。
4. 在创建事件订阅对话框中，请执行以下操作：
 - a. 对于名称，输入事件通知订阅的名称。
 - b. 在将通知发送到，为 SNS 主题选择现有的 Amazon SNS ARN。要使用新主题，请选择 Create topic (创建主题) 来输入主题的名称和收件人列表。
 - c. 对于源类型，选择参数组。
 - d. 在“要包含的实例”下，选择“所有参数组”。
 - e. 在“要包括的事件类别”下，选择“特定事件类别”。如果您选择“所有事件类别”，则控件也会通过。
 - f. 选择配置更改。
 - g. 选择 Create (创建)。

[RDS.22] 应为关键数据库安全组事件配置 RDS 事件通知订阅

类别：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::RDS::EventSubscription

Amazon Config 规则：rds-sg-event-notifications-configured (由Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (无)

此控件检查是否存在为以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 事件通知使用 Amazon SNS 让您知道 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

订阅 RDS 数据库安全组事件通知

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。
2. 在导航窗格中，选择事件订阅。
3. 在“活动订阅”下，选择“创建活动订阅”。
4. 在“创建事件订阅”对话框中，执行以下操作：
 - a. 对于名称，输入事件通知订阅的名称。
 - b. 在将通知发送到，为 SNS 主题选择现有的 Amazon SNS ARN。要使用新主题，请选择 Create topic (创建主题) 来输入主题的名称和收件人列表。
 - c. 对于源类型，选择安全组。
 - d. 在“要包含的实例”下，选择所有安全组。
 - e. 在“要包括的事件类别”下，选择“特定事件类别”。如果您选择“所有事件类别”，则控件也会通过。
 - f. 选择配置更改和失败。
 - g. 选择 Create (创建) 。

[RDS.23] RDS 数据库和集群不应使用数据库引擎的默认端口

类别：保护 > 安全网络配置

严重性：低

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：rds-no-default-ports (由 Security Hub 开发的自定义规则)

时间表类型：触发器

参数：None (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。

如果您使用已知端口部署 RDS 集群或实例，则攻击者可以猜测有关该集群或实例的信息。攻击者可以将此信息与其他信息结合使用来连接到 RDS 集群或实例或获取有关您的应用程序的其他信息。

更改端口时，还必须更新用于连接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，确保它包含允许在新端口上连接的入口规则。

修复

修改现有数据库实例的默认端口

1. 通过以下网址打开 Amazon RDS 控制台：<https://console.aws.amazon.com/rds/>。

2. 选择 Databases (数据库)。
3. 选择要修改的数据库实例
4. 选择 Modify (修改)。
5. 在 “数据库选项” 下，将数据库端口更改为非默认值。
6. 选择 Continue (继续)。
7. 在 “调度修改” 下，选择何时应用修改。可以选择 Apply during the next scheduled window (在
8. 对于集群，选择修改集群。对于实例，选择修改数据库实例。

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

类别：识别 > 资源配置

严重性：中

资源类型：AWS::RDS::DBCluster

Amazon Config 规则：[rds-cluster-default-admin-check](#)

时间表类型：触发器

参数：None (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更改为其他值。如果管理员用户名设置为默认值，则此规则将失效。

创建 Amazon RDS 数据库时，应将默认管理员用户名更改为唯一值。默认用户名是众所周知的，应在创建 RDS 数据库期间进行更改。更改默认用户名可降低意外访问的风险。

修复

要更改与 Amazon RDS 数据库集群关联的管理员用户名，[请创建新的 RDS 数据库集群](#)并在创建数据库时更改默认管理员用户名。

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

类别：识别 > 资源配置

严重性：中

资源类型：AWS::RDS::DBInstance

Amazon Config 规则：[rds-instance-default-admin-check](#)

时间表类型：触发器

参数：None (无)

此控件检查您是否已将 Amazon Relational Database Service (Amazon RDS) 数据库实例的管理用户名从默认值更改。如果将管理用户名设置为默认值，则控制将失败。

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更改为唯一值，以降低意外访问的风险。

修复

要更改与 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](#)。在创建数据库时更改默认管理用户名。

[Redshift.1] Amazon Redshift 集群应禁止公共访问

类别：保护 > 安全网络配置 > 资源不可公开访问

严重性：重大

资源类型：AWS::Redshift::Cluster

Amazon Config 规则：[redshift-cluster-public-access-check](#)

时间表类型：触发器

参数：None (无)

此控件可检查 Amazon Redshift 集群是否可公开访问。它评估集群配置项目中的PubliclyAccessible字段。

Amazon Redshift 集群配置的PubliclyAccessible属性表明该集群是否可以公开访问。将 set 配置PubliclyAccessible为true，则集群是面向 Internet 的实例，具有可解析为公有 IP 地址的可公开解析 DNS 名称。

当集群不可公开访问时，它是一个具有 DNS 名称的内部实例，可解析为私有 IP 地址。除非您打算让集群公开访问，否则不应将集群配置为PubliclyAccessible设置true。

修复

要修复此问题，请更新您的 Amazon Redshift 集群以禁用公共访问权限。

禁用 Amazon Redshift 集群的公开访问权限

1. 打开位于 <https://console.aws.amazon.com/redshift/> 的 Amazon Redshift 控制台。
2. 在导航菜单中，选择 Clusters (集群)，然后选择带有要修改的安全组的集群的名称。
3. 选择“操作”，然后选择“修改可公开访问的设置”。
4. 在“允许 VPC 外部的实例和设备通过集群终端节点连接到您的数据库”下，选择“否”。
5. 选择 Confirm (确认)。

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

类别：保护 > 数据保护 > 加密传输中的数据

严重性：中

资源类型:AWS::Redshift::Cluster,AWS::Redshift::ClusterParameterGroup

Amazon Config 规则：[redshift-require-tls-ssl](#)

时间表类型：触发器函数

参数：None (无)

此控制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 1，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。只允许通过 TLS 进行加密连接。对传输中的数据进行加密可能会影响性能。您应该使用此功能测试您的应用程序，以了解性能概况和 TLS 的影响。

Note

欧洲 (米兰) 不支持此控件。

修复

要修复此问题，请更新参数组以要求加密。

修改参数组

1. 打开位于 <https://console.aws.amazon.com/redshift/> 的 Amazon Redshift 控制台。
2. 在导航菜单中，选择 Config，然后选择工作负载管理以显示工作负载管理页面。
3. 选择要修改的参数组。
4. 选择“参数”。
5. 选择编辑参数，然后设置require_ssl为 1。
6. 输入您的更改，然后选择“保存”。

[Redshift.3] Amazon Redshift 集群应启用自动快照

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：AWS::Redshift::Cluster

Amazon Config 规则：[redshift-backup-enabled](#)

时间表类型：触发器函数

参数：

- MinRetentionPeriod = 7

此控件检查 Amazon Redshift 集群是否启用了自动快照。它还会检查快照保留期是否大于或等于七。

备份可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。该控件检查自动快照是否已启用并保留至少七天。有关 Amazon Redshift 自动快照的更多详细信息，请参阅 Amazon Redshift 管理指南中的[自动快照](#)。

Note

以下区域不支持此控件：

- 非洲（开普敦）
- 亚太地区（大阪）
- 亚太地区（悉尼）
- 中国（宁夏）
- 欧洲（米兰）

修复

要修复此问题，请将快照保留期至少更新为 7。

修改快照保留期

1. 打开位于 <https://console.aws.amazon.com/redshift/> 的 Amazon Redshift 控制台。
2. 在导航菜单中，选择 Clusters（集群），然后选择集群，然后选择要修改的集群的名称。
3. 选择 Edit（编辑）。
4. 在“Backup”下，将“快照保留期”的值设置为 7 或更大。

5. 选择 Modify Cluster。

[Redshift.4] Amazon Redshift 集群应启用审计日志

类别：识别 > 记录

严重性：中

资源类型：AWS::Redshift::Cluster

Amazon Config 规则：redshift-cluster-audit-logging-enabled (由Security Hub 开发的自定义规则)

时间表类型：触发器函数

参数：

- loggingEnabled = true

此控件检查 Amazon Redshift 集群是否启用了审计日志。

Amazon Redshift 审核日志记录提供了有关集群中的连接和用户活动的更多信息。这些数据可以在 Amazon S3 中存储和保护，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[数据库审计日志](#)。

修复

启用集群审计日志

1. 打开位于 <https://console.aws.amazon.com/redshift/> 的 Amazon Redshift 控制台。
2. 在导航菜单中，选择 Clusters (集群)，然后选择集群，然后选择要修改的集群的名称。
3. 选择维护和监控。
4. 在“审核日志”下，选择“编辑”。
5. 将“启用审核日志”设置为“是”，然后输入日志目标存储桶的详细信息。
6. 选择 Confirm (确认)。

[Redshift.6] Amazon Redshift 应该启用到主要版本的自动升级

类别：检测 > 漏洞和补丁管理

严重性：中

资源类型：AWS::Redshift::Cluster

Amazon Config 规则：[redshift-cluster-maintenancesettings-check](#)

时间表类型：触发器函数

参数：

- allowVersionUpgrade = true

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。及时安装补丁是保护系统的重要一步。

Note

中东 (巴林) 不支持此控件。

修复

要从中修复此问题Amazon CLI，请使用 Amazon Redshiftmodify-cluster 命令来设置该--allow-version-upgrade属性。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

您*clustername*的 Amazon Redshift 集群的名称在哪里。

[Redshift.7] Amazon Redshift 集群应使用增强型 VPC 路由

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

Amazon Config 规则：[redshift-enhanced-vpc-routing-enabled](#)

时间表类型：触发器函数

参数：None (无)

此控件检查是否已EnhancedVpcRouting启用 Amazon Redshift 集群。

增强型 VPC 路由强制集群COPY和数据存储库之间的所有和UNLOAD流量通过您的 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 流日志监控网络流量。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关详细的修复说明，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

类别：识别 > 资源配置

严重性：中

资源类型：AWS::Redshift::Cluster

Amazon Config 规则：[redshift-default-admin-check](#)

时间表类型：触发器函数

参数：None (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更改为其他值。如果 Redshift 集群的管理员用户名设置为，则此控制将失败awsuser。

创建 Redshift 集群时，应将默认管理员用户名更改为唯一值。默认用户名是众所周知的，应在配置时进行更改。更改默认用户名可降低意外访问的风险。

修复

创建了 Amazon Redshift 集群后，则不能再更改其管理员用户名。要创建新集群，请按照[此处](#)的说明操作。

[Redshift.9] Redshift 集群不应使用默认的数据库名称

类别：识别 > 资源配置

严重性：中

资源类型：AWS::Redshift::Cluster

Amazon Config 规则：[redshift-default-db-name-check](#)

时间表类型：触发器函数

参数：None (无)

此控件检查 Amazon Redshift 集群是否已将数据库名称从其默认值更改为其他值。如果 Redshift 集群的数据库名称设置为，则控制将失败dev。

创建 Redshift 集群时，应将默认数据库名称更改为唯一值。默认名称是众所周知的，应在配置时更改。例如，如果在 IAM 策略条件中使用知名名称，则该名称可能会导致无意访问。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

创建了 Amazon Redshift 集群后，则不能再更改该集群的数据库名称。有关创建新集群的说明，请参阅[Amazon Redshift 入门](#)指南中的 Amazon Redshift 入门。

[S3.1] 应启用 S3 阻止公有访问设置

类别：保护 > 安全网络配置

严重性：中

资源类型：Amazon 账户

Amazon Config 规则：[s3-account-level-public-access-blocks-periodic](#)

时间表类型：定期

参数：

- ignorePublicAcls: true

- `blockPublicPolicy: true`
- `blockPublicAcls: true`
- `restrictPublicBuckets: true`

此控件检查以下 Amazon S3 公有访问块设置是否在账户级别配置：

- `ignorePublicAcls: true`
- `blockPublicPolicy: true`
- `blockPublicAcls: true`
- `restrictPublicBuckets: true`

如果所有公共访问屏蔽设置都设置为，则控制通过`true`。

如果将任何设置设置为`false`，或者任何设置均未配置，则控制将失败。

Amazon S3 公共访问块旨在提供对整个Amazon账户或单个 S3 存储桶级别的控制，以确保对象永远不会获得公共访问权限。通过访问控制列表 (ACL) 和/或存储桶策略向存储桶和对象授予公有访问权限。

除非您打算公开访问您的 S3 存储桶，否则您应该配置账户级别的 Amazon S3 阻止公有访问功能。

要了解更多信息，请参阅 [Amazon Simple Storage Service 用户指南中的使用 Amazon S3 阻止公有访问](#)。

Note

以下区域不支持此控件：

- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要修复此问题，请启用 Amazon S3 阻止公有访问。

启用 Amazon S3 阻止公有访问

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 选择 Block public access (account settings) (阻止公有访问(账户设置))。
3. 选择 Edit (编辑)。
4. 选择“阻止所有公共访问”。
5. 选择 Save changes (保存更改)。

有关更多信息，请参阅《[Amazon Simple Storage Service 用户指南](#)》中的[使用 Amazon S3 阻止公有访问](#)。

[S3.2] S3 存储桶应禁止公开读取访问

类别：保护 > 安全网络配置

严重性：重大

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-public-read-prohibited](#)

时间表类型：定期触发，变更触发

参数：None (无)

该控制检查 S3 存储桶是否允许公共读取访问。它评估阻止公有访问设置、存储桶策略和存储桶访问控制列表 (ACL)。

有些使用案例要求互联网上的每个人都能够从您的 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

要修复此问题，请更新您的 S3 存储桶以删除公有访问权限。

从 S3 存储桶中删除公有访问权限

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 在左侧导航窗格中，选择存储桶。
3. 选择要更新的 S3 桶的名称。
4. 选择“权限”，然后选择“阻止公共访问”。
5. 选择 Edit (编辑) 。
6. 选择“阻止所有公共访问”。然后选择 Save (保存) 。
7. 如果出现提示，输入 **confirm**，然后选择 Confirm (确认)。

[S3.3] S3 存储桶应禁止公开写入访问

类别：保护 > 安全网络配置

严重性：重大

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-public-write-prohibited](#)

时间表类型：定期触发，变更触发

参数：None (无)

该控制检查 S3 存储桶是否允许公共写入访问。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。

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

要修复此问题，请更新您的 S3 存储桶以删除公有访问权限。

删除 S3 存储桶的公开访问权限

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 在左侧导航窗格中，选择存储桶。
3. 选择要更新的 S3 桶的名称。

4. 选择“权限”，然后选择“阻止公共访问”。
5. 选择 Edit (编辑)。
6. 选择“阻止所有公共访问”。然后选择 Save (保存)。
7. 如果出现提示，输入 **confirm**，然后选择 Confirm (确认)。

[S3.4] S3 存储桶应启用服务器端加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-server-side-encryption-enabled](#)

时间表类型：触发器函数

参数：None (无)

此控制检查您的 S3 存储桶是否已启用 Amazon S3 默认加密，或者 S3 存储桶策略是否明确拒绝未经服务器端加密的放置对象请求。

要为 S3 存储桶中的敏感数据增加一层安全保护，您应该为存储桶配置服务器端加密，以保护静态数据。Amazon S3 使用唯一的密钥来加密每个数据元。作为额外的保护，Amazon S3 会使用定期轮换的根密钥加密密钥本身。Amazon S3 服务器端加密使用可用的最强数据块密码之一、256 位高级加密标准 (AES-256) 来加密您的数据。

要了解更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用采用 Amazon S3 托管加密密钥的服务器端加密 (SSE-S3) 保护数据。

修复

要修复此问题，请更新您的 S3 存储桶以启用默认加密。

对 S3 存储桶启用默认加密

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 在左侧导航窗格中，选择存储桶。
3. 从列表中选择 S3 存储桶。
4. 请选择属性。
5. 选择 Default encryption。
6. 要进行加密，请选择 AES-256 或 Amazon-KMS。
 - 选择 AES-256 以使用由 Amazon S3 托管的密钥进行默认加密。有关使用 Amazon S3 服务器端加密对数据进行加密的更多信息，请参阅 [Amazon Simple Storage Service 用户指南](#)。
 - 选择 Amazon-KMS 使用由管理的密钥 Amazon KMS 进行默认加密。然后从您创建的根密钥列表选择一个 Amazon KMS 根密钥。

键入要使用的 Amazon KMS 密钥的 Amazon 资源名称 (ARN)。您可以在 IAM 控制台中的加密 Amazon KMS 密钥下方找到您的密钥的 ARN。或者，您可以从下拉列表选择一个键名。

Important

如果您将 Amazon KMS 选项用于默认加密配置，则需要遵循 Amazon KMS 的 RPS (每秒请求数) 配额。有关 Amazon KMS 配额以及如何请求增加配额的更多信息，请参阅 [Amazon Key Management Service 开发人员指南](#)。

有关创建 Amazon KMS 密钥的更多信息，请参阅 [Amazon Key Management Service 开发者指南](#)。

有关使用 Amazon S3 Amazon KMS 的更多信息，请参阅 Amazon S3 [Simple Storage Service 用户指南](#)。

在启用默认加密时，您可能需要更新存储桶策略。有关从存储桶策略转换为默认加密的更多信息，请参阅 [Amazon Simple Storage Service 用户指南](#)。

7. 选择 Save (保存)。

有关默认 S3 存储桶加密的更多信息，请参阅 [Amazon Simple Storage Service 用户指南](#)。

[S3.5] S3 存储桶应要求请求才能使用安全套接字层

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-ssl-requests-only](#)

时间表类型：触发器函数

参数：None (无)

此控制检查 S3 存储桶是否有要求请求使用安全套接字层 (SSL) 的策略。

在 S3 资源策略中，S3 存储桶应具有要求所有请求 (Action: S3:*) 仅接受通过 HTTPS 传输数据的策略，由条件密钥指示 `aws:SecureTransport`。

修复

要修复此问题，请更新 S3 存储桶的权限策略。

将 S3 存储桶配置为拒绝非安全传输

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 导航到不合规存储桶，然后选择存储桶名称。
3. 选择 Permissions，然后选择 Bucket Policy。
4. 在以下政策中添加与之相似的政策声明。awsexamplebucket 替换为要修改的存储桶的名称。

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::awsexamplebucket",
        "arn:aws:s3:::awsexamplebucket/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

```
    },  
    "Principal": "*"    
  }  
]  
}
```

5. 选择 Save (保存)。

有关更多信息，请参阅知识中心文章[要符合Amazon Config规则 s3，我要使用什么 S3 存储桶策略bucket-ssl-requests-only？](#)。

[S3.6] 应限制在存储桶策略中授予其他Amazon账户的 Amazon S3 权限

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

Amazon Config 规则：[s3-bucket-blacklisted-actions-prohibited](#)

时间表类型：触发器函数

参数：

- blacklistedactionpatterns: s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl

此控制检查 S3 存储桶策略是否阻止其他Amazon账户的委托人对 S3 存储桶中的资源执行被拒绝的操作。如果 S3 存储桶策略允许另一个Amazon账户中的委托人执行以下任何操作，则控制失败：

- s3:DeleteBucketPolicy
- s3:PutBucketAcl
- s3:PutBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutObjectAcl

实施最低权限访问对于减小安全风险和错误意意意意意意意意意意意意意意意意意意 如果 S3 存储桶策略允许来自外部账户的访问，则可能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。参数向外部账户授予对未包含在blacklistedactionpatterns列表中的操作模式的访问权限。

修复

要修复此问题，请编辑 S3 存储桶策略以删除权限。

编辑 S3 存储桶策略

1. 通过以下网址打开 Simple Storage Service (Amazon S3) 控制台：<https://console.aws.amazon.com/s3/>。
2. 在 Buckets nam e (存储桶名称) 列表中，选择要为其编辑策略的 S3 存储桶的名称。
3. 选择 Permissions，然后选择 Bucket Policy。
4. 在存储桶策略编辑器文本框中，执行以下操作之一：

- 删除向其他Amazon账户授予被拒绝操作访问权限的声明
 - 从语句中删除允许的被拒绝的操作
5. 选择 Save (保存)。

[S3.8] 应在存储区级别启用 S3 阻止公有访问设置

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

Amazon Config 规则：[s3-bucket-level-public-access-prohibited](#)

时间表类型：触发器函数

参数：

- excludedPublicBuckets (可选) -以逗号分隔的已知允许公有 S3 存储桶名称列表。

此控件检查 S3 存储桶是否应用了存储分区级别的公共访问阻止。如果将以下任一设置设置为，则此控制会失败false：

- ignorePublicAcls
- blockPublicPolicy
- blockPublicAcls
- restrictPublicBuckets

在 S3 存储桶级别阻止公有访问可提供控制，以确保对象永远不会获得公共访问权限。通过访问控制列表 (ACL) 和/或存储桶策略向存储桶和对象授予公有访问权限。

除非您打算公开访问您的 S3 存储桶，否则应配置存储桶级别 Amazon S3 阻止公有访问功能。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关如何在存储桶级别删除公有访问权限的信息，请参阅 [Amazon S3 用户指南中的阻止公有访问您的 Amazon S3 存储](#)。

[S3.9] 应启用 S3 存储桶服务器访问日志记录

类别：识别 > 记录

严重性：中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-bucket-logging-enabled](#)

时间表类型：触发器函数

参数：None (无)

此控件检查是否为 S3 存储桶启用了服务器访问日志。启用日志记录后，Amazon S3 会将源存储桶的访问日志传输到选定的目标存储桶。目标存储桶必须位于源存储桶所在的相同 Amazon 区域中且不得具有默认保留周期配置。如果启用了服务器访问日志，则此控制通过。目标日志存储桶不需要启用服务器访问日志记录，您应该取消对此存储桶的发现。

服务器访问日志记录详细地记录对存储桶提出的各种请求。服务器访问日志可以帮助安全和访问审计。有关更多信息，请参阅 [Amazon S3 安全性最佳实践：启用 Amazon S3 服务器访问日志记录](#)。

修复

启用 S3 存储桶访问日志记录

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：<https://console.aws.amazon.com/s3/>。
2. 从列表中选择存储桶。
3. 请选择属性。
4. 在 Server access logging (服务器访问日志记录) 下，请选择 Edit (编辑)。
5. 在“服务器访问日志”下，选择“启用”。然后，选择“保存更改”。

[S3.10] 启用版本控制的 S3 存储桶应配置生命周期策略

类别：识别 > 记录

严重性：中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-version-lifecycle-policy-check](#)

时间表类型：触发器函数

参数：None (无)

此控制检查启用了 Amazon Simple Storage Service (Amazon S3) 版本的存储桶是否配置了生命周期策略。如果未启用 Amazon S3 生命周期策略，则此规则将失败。

建议在 Amazon S3 存储桶上配置生命周期规则，因为这些规则可以帮助您定义您希望 Amazon S3 在对象的生命周期内执行的操作。

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[设置存储桶的生命周期配置和管理存储生命周期](#)。

[S3.11] S3 存储桶应启用事件通知

类别：识别 > 记录

严重性：中

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-event-notifications-enabled](#)

时间表类型：触发器函数

参数：None (无)

此控件检查是否在 Amazon S3 存储桶上启用了 S3 事件通知。如果未在存储桶上启用 S3 事件通知，则此控制将失败。

通过启用事件通知，当发生特定事件时，您将在 Amazon S3 存储桶上收到警报。例如，您可以收到对象创建、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。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关检测 S3 存储桶和对象更改的信息，请参阅 [Amazon S3 用户指南中的 Amazon S3 事件通知](#)。

[S3.12] 不应使用 S3 访问控制列表 (ACL) 来管理用户对存储区的访问

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

Amazon Config 规则：[s3-bucket-acl-prohibited](#)

时间表类型：触发器函数

参数：None (无)

此控制检查 Amazon S3 存储桶是否通过 ACL 提供用户权限。如果将 ACL 配置为管理 S3 存储区上的用户访问权限，则控制会失败。

ACL 是早于 IAM 的传统访问控制机制。我们建议使用 IAM 策略或 S3 存储桶策略而不是 ACL，以便更轻松地管理对 S3 存储桶的访问。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关管理 S3 存储桶访问权限的更多信息，请参阅 Amazon S3 [用户指南中的存储桶策略和用户策略](#)。有关如何查看当前 ACL 权限的详细信息，请参阅 Amazon S3 用户指南中的[访问控制列表 \(ACL\) 概述](#)。

[S3.13] S3 存储桶应配置生命周期策略

类别：保护 > 数据保护

严重性：低

资源类型：AWS::S3::Bucket

Amazon Config 规则：[s3-lifecycle-policy-check](#)

时间表类型：触发器函数

参数：None (无)

此控件检查是否为 Amazon S3 存储桶配置了生命周期策略。如果没有为 S3 存储桶配置生命周期策略，则此控制将失败。

在 S3 存储桶上配置生命周期规则定义您希望 S3 在对象的生命周期内执行的操作。例如，您可以将对象转换为另一个存储类别，存档对象，或在指定时间段后删除它们。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

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 Amazon S3 用户指南中的[设置存储桶生命周期配置和管理](#)存储生命周期。

[SageMaker.1] SageMaker 笔记本电脑实例不应直接访问互联网

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::SageMaker::NotebookInstance

Amazon Config 规则：[sagemaker-notebook-no-direct-internet-access](#)

时间表类型：定期

参数：None (无)

此控件检查 SageMaker 笔记本实例是否禁用了直接互联网访问。为此，它会检查 notebook 实例是否禁用了该DirectInternetAccess字段。

如果您配置的 SageMaker 实例没有 VPC，则默认情况下，您的实例上会启用直接互联网访问。您应该使用 VPC 配置您的实例，并将默认设置更改为“禁用-通过 VPC 访问互联网”。

要使用笔记本电脑训练或托管模型，您需要访问互联网。要启用互联网访问，请确保您的 VPC 有 NAT 网关，并且您的安全组允许出站连接。要了解有关如何将笔记本实例 Connect 到 VPC 中的资源的更多信息，请参阅 Amazon SageMaker 开发者指南中的[将笔记本实例连接到 VPC 中的资源](#)。

您还应确保仅限授权用户访问您的 SageMaker 配置。限制用户修改 SageMaker 设置和资源的 IAM 权限。

Note

以下区域不支持此控件：

- 非洲（开普敦）
- China (Beijing)
- China (Ningxia)
- 欧洲（米兰）
- Amazon GovCloud（美国东部）

修复

请注意，在创建笔记本实例后，您无法更改互联网访问设置。必须停止、删除和重新创建它。

将 SageMaker 笔记本电脑实例配置为拒绝直接互联网访问

1. 通过 <https://console.aws.amazon.com/sagemaker/> 打开 SageMaker 控制台
2. 导航到笔记本实例。
3. 删除启用了直接互联网接入的实例。选择实例，选择操作，然后选择停止。

实例停止后，选择操作，然后选择删除。

4. 选择创建笔记本实例。提供配置详情。
5. 展开网络部分，然后选择 VPC、子网和安全组。在“直接互联网访问”下，选择“禁用 — 通过 VPC 访问互联网”。
6. 选择创建笔记本实例。

有关更多信息，请参阅 Amazon SageMaker 开发者指南中的[将笔记本实例 Connect 到 VPC 中的资源](#)。

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

类别：保护 > 安全开发

严重性：中

资源类型：AWS::SecretsManager::Secret

Amazon Config 规则：[secretsmanager-rotation-enabled-check](#)

时间表类型：触发器函数

参数：None（无）

此控件检查存储在中的密钥 Amazon Secrets Manager 是否配置了自动轮换。

Secrets Manager 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 集中存储密钥、自动加密密钥、控制对密钥的访问以及安全、自动地轮换密钥。

Secrets Manager 可以轮换密钥。您可以使用轮换将长期机密替换为短期机密。轮换您的密钥限制了未经授权的用户可以使用已泄露的密钥的时间。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《Amazon Secrets Manager 用户指南》中的[轮换 Amazon Secrets Manager 密钥](#)。

Note

亚太地区（雅加达）或亚太地区（大阪）区域不支持此控件。

修复

要修复此问题，您可以启用密钥的自动轮换。

启用密钥自动轮换

1. 在 <https://console.aws.amazon.com/secretsmanager/> 打开 Secrets Manager 控制台
2. 要查找需要轮换的密钥，请在搜索字段中输入密钥名称。
3. 选择要轮换的密钥，这将显示密钥详细信息页面。
4. 在“旋转配置”下，选择“编辑旋转”。
5. 从编辑旋转配置中，选择启用自动旋转。
6. 在“选择旋转间隔”中，选择旋转间隔。
7. 选择一个 Lambda 函数进行轮换。有关自定义 Lambda 轮换函数的信息，请参阅 Amazon Secrets Manager 用户指南中的 [了解和自定义 Lambda 轮换函数](#)。
8. 要配置轮换的密钥，请选择 Next。

要了解有关 Secrets Manager 轮换的更多信息，请参阅 Amazon Secrets Manager 用户指南中的轮换 [Amazon Secrets Manager 密钥](#)。

[SecretsManager.2] 配置为自动轮换的 Secrets Manager 密钥应成功轮换

类别：保护 > 安全开发

严重性：中

资源类型：AWS::SecretsManager::Secret

Amazon Config 规则：[secretsmanager-scheduled-rotation-success-check](#)

时间表类型：触发器函数

参数：None（无）

此控件根据轮换时间表检查 Amazon Secrets Manager 密钥是否成功轮换。如果 `RotationOccurringAsScheduled` 是，则控制失败 `false`。该控件不评估未配置轮换的密钥。

Secrets Manager 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 集中存储密钥、自动加密密钥、控制对密钥的访问以及安全、自动地轮换密钥。

Secrets Manager 可以轮换密钥。您可以使用轮换将长期机密替换为短期机密。轮换您的密钥限制了未经授权的用户可以使用已泄露的密钥的时间。因此，您应该经常轮换机密。

除了将密钥配置为自动轮换外，您还应确保根据轮换时间表成功轮换这些密钥。

要了解有关轮换的更多信息，请参阅《Amazon Secrets Manager 用户指南》中的 [轮换 Amazon Secrets Manager 密钥](#)。

修复

如果自动轮换失败，则 Secrets Manager 可能在配置中遇到了错误。

要在 Secrets Manager 中轮换密钥，您可以使用 Lambda 函数定义如何与拥有密钥的数据库或服务交互。

有关如何诊断和修复与密钥轮换相关的常见错误的帮助，请参阅Amazon Secrets Manager用户指南中的[解决密钥Amazon Secrets Manager轮换](#)问题。

[SecretsManager.3] 移除未使用的Secrets Manager 密钥

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::SecretsManager::Secret

Amazon Config 规则：[secretsmanager-secret-unused](#)

时间表类型：定期

参数：None (无)

此控件检查您的密钥是否在指定的天数内被访问。默认值为 90 天。如果在规定的天数内未访问密钥，则此控制将失败。

删除未使用的密钥与轮换密钥同样重要。未使用的密钥可能会被其以前的用户滥用，他们不再需要访问这些密钥。此外，随着越来越多的用户获得访问密钥的权限，可能有人对其进行了错误的处理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消不再需要的用户的秘密访问权限。它还有助于降低使用Secrets Manager 的成本。因此，定期删除未使用的密钥至关重要。

Note

以下区域不支持此控件：

- 亚太地区 (大阪)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

您可以从 Secrets Manager 控制台中删除非活动密钥。

删除不活跃的秘密

1. 在 <https://console.aws.amazon.com/secretsmanager/> 打开 Secrets Manager 控制台
2. 要找到密钥，请在搜索框中输入密钥名称。
3. 选择要删除的秘密。
4. 在“密钥详细信息”下，从“操作”中选择“删除密钥”。
5. 在“计划密钥删除”下，输入删除密钥之前要等待的天数。
6. 选择计划删除。

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::SecretsManager::Secret

Amazon Config 规则：[secretsmanager-secret-periodic-rotation](#)

时间表类型：定期

参数：

- 轮换周期：默认为 90 天

此控件检查您的密钥是否在 90 天内至少轮换过一次。

轮换密钥可以帮助您降低在 Amazon 账户中未经授权使用您的密钥的风险。示例包括数据库凭证、密码、第三方 API 密钥，甚至是任意文本。如果您很长一段时间未更改密钥，密钥泄露的可能性就会增大。

随着越来越多的用户获得访问密钥的权限，更有可能有人不当处理该密钥并将其泄露给未经授权的实体。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。

您可以将您的密钥配置为自动轮换 Amazon Secrets Manager。通过自动轮换，您可以将长期机密替换为短期机密，从而显著降低泄露的风险。

Security Hub 建议你启用 Secrets Manager 的轮换。要了解有关轮换的更多信息，请参阅《Amazon Secrets Manager 用户指南》中的[轮换 Amazon Secrets Manager 密钥](#)。

Note

以下区域不支持此控件：

- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

您可以在 Secrets Manager 控制台中启用自动密钥轮换。

启用密钥轮换

1. 在 <https://console.aws.amazon.com/secretsmanager/> 打开 Secrets Manager 控制台
2. 要找到密钥，请在搜索框中输入密钥名称。
3. 选择要显示的密钥。
4. 在“旋转配置”下，选择“编辑旋转”。
5. 从编辑旋转配置中，选择启用自动旋转。
6. 从选择旋转间隔中，选择旋转间隔。
7. 选择用于轮换的 Lambda 函数。
8. 选择 Next（下一步）。
9. 将密钥配置为自动轮换后，在“轮换配置”下，选择“立即轮换密钥”。

[SNS.1] SNS 主题应使用以下方法进行静态加密 Amazon KMS

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::SNS::Topic

Amazon Config 规则：[sns-encrypted-kms](#)

时间表类型：触发器函数

参数：None (无)

此控件检查 SNS 主题是否使用静态加密 Amazon KMS。

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 Amazon。它还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，需要有 API 权限才能解密数据，然后才能读取数据。SNS 主题应进行静态加密，以增加安全层。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南 [中的静态加密](#)。

修复

要修复此问题，请更新您的 SNS 主题以启用加密。

对未加密的 SNS 主题进行加密

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 在导航窗格中，选择 Topics (主题)。
3. 选择要加密主题的名称。
4. 选择 Edit (编辑)。
5. 在“加密”下，选择“启用加密”。
6. 选择用于加密主题的 KMS 密钥。
7. 选择 Save changes (保存更改)。

[SNS.2] 应为发送到主题的通知消息启用传送状态日志功能

类别：识别 > 记录

严重性：中

资源类型：AWS::SNS::Topic

Amazon Config 规则：[sns-topic-message-delivery-notification-enabled](#)

时间表类型：触发器函数

参数：None (无)

此控件检查是否启用了发送到 Amazon SNS 主题的通知消息的传输状态的日志记录功能。如果未启用邮件的传送状态通知，则此控制将失败。

日志记录是保持服务的可靠性、可用性和性能的重要方面。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 终端节点。
- 识别从 Amazon SNS 终端节点发送到 Amazon SNS 的响应。
- 确定消息停留时间 (发布时间戳与将消息转交给 Amazon SNS 终端节点之间的时间差)。

Note

以下区域不支持此控件：

- 亚太地区 (雅加达)
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

要为主题配置传输状态日志，请参阅[亚马逊简单通知服务开发者指南中的 Amazon SNS 消息传输状态](#)。

[SQS.1] 应对 Amazon SQS 队列进行静态加密

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::SQS::Queue

Amazon Config 规则：sqs-queue-encrypted (由Security Hub 开发的自定义规则)

时间表类型：触发器函数

参数：None (无)

此控件检查 Amazon SQS 队列是否已静态加密。如果您使用 Amazon SQS 托管密钥 (SSE-SQS) 或 () 密钥 Amazon Key Management Service (SSE-KMSAmazon KMS)，则控制权将通过。

服务器端加密 (SSE) 允许您在加密队列中传输敏感数据。为了保护队列中的消息内容，SSE 使用 KMS 密钥。有关更多信息，请参阅 Amazon Simple Queue Service 开发人员指南[中的静态加密](#)。

修复

有关使用管理 SSE 的信息Amazon Web Services Management Console，请参阅 Amazon Simple Queue Service 开发人员指南[中的为队列 \(控制台 \) 配置服务器端加密](#) (SSE)。

[SSM.1] EC2 实例应由以下人员管理Amazon Systems Manager

类别：识别 > 清单

严重性：中

资源类型：AWS::EC2::Instance

Amazon Config 规则：[ec2-instance-managed-by-systems-manager](#)

时间表类型：触发器函数

参数：None (无)

此控件会检查您账户中已停止和正在运行的 EC2 实例是否由托管Amazon Systems Manager。Systems Manager 是一项Amazon服务，可以用来查看和控制您的Amazon基础设施。

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。托管实例是一个已配置为与 Systems Manager 一起使用的机器。然后，Systems Manager 会报告其发现的任何违反政策的行为或采取纠正措施。Systems Manager 还帮助您配置和维护托管实例。

要了解更多信息，请参阅[Amazon Systems Manager用户指南](#)。

修复

您可以使用 Systems Manager 控制台修复此问题。

为确保 EC2 实例由 Systems Manager 管理

1. 访问 <https://console.aws.amazon.com/systems-manager/>，打开 Amazon Systems Manager 控制台。
2. 在导航菜单中，选择快速设置。
3. 选择 Create (创建)。
4. 在“配置类型”下，选择“主机管理”，然后选择“下一步”。
5. 在配置屏幕上，您可以保留默认选项。

您可以选择进行以下更改：

- a. 如果您使用 CloudWatch 监控 EC2 实例，请选择安装并配置 CloudWatch 代理，然后每 30 天更新一次 CloudWatch 代理。
 - b. 在“目标”下，选择管理范围以确定应用此配置的账户和区域。
 - c. 在实例配置文件选项下，选择将所需的 IAM 策略添加到附加到您的实例的现有实例配置文件中。
6. 选择 Create (创建)。

要确定您的实例是否支持 Systems Manager 关联，请参阅 Amazon Systems Manager 用户指南中的 [Systems Manager 先决条件](#)。

[SSM.2] 由 Systems Manager 管理的所有 EC2 实例都应符合补丁要求

类别：检测 > 检测服务

严重性：高

资源类型：AWS::SSM::PatchCompliance

Amazon Config 规则：[ec2-managedinstance-patch-compliance-status-check](#)

时间表类型：触发器函数

参数：None (无)

此控件检查 Amazon EC2 Systems Manager 补丁合规性的合规性状态是在实例上安装补丁 NON_COMPLIANT 之后 COMPLIANT 还是处于合规状态。它仅检查由系统管理器补丁管理器管理的实例。

根据您的组织要求对 EC2 实例进行完全修补，可减少 Amazon 账户面临的攻击面。

Note

以下区域不支持此控件：

- 非洲 (开普敦)
- Europe (Milan)
- Middle East (Bahrain)

修复

要修复此问题，请在不合规的实例上安装所需的补丁。

修复不合规的补丁

1. 访问 <https://console.aws.amazon.com/systems-manager/>，打开 Amazon Systems Manager 控制台。

2. 在“节点管理”下，选择“运行命令”，然后选择“运行命令”。
3. 选择 Amazon- 旁边的按钮RunPatchBaseline。
4. 将 Operation (操作) 改为 Install (安装)。
5. 选择 Choose instances manually (手动选择实例)，然后选择不合规的实例。
6. 在页面底部选择 Run (运行)。
7. 在该命令完成后，要监控修补的实例的新合规性状态，请在导航窗格中选择 Compliance (合规性)。

有关使用 Systems Manager 文档为托管实例打补丁的更多信息，请参阅Amazon Systems Manager用户指南中的[关于修补实例的 SSM 文档](#)和[使用 Systems Manager 运行命令运行命令](#)。

[SSM.3] 由 Systems Manager 管理的实例的关联合规状态应为COMPLIANT

类别：检测 > 检测服务

严重性：低

资源类型：AWS::SSM::AssociationCompliance

Amazon Config 规则：[ec2-managedinstance-association-compliance-status-check](#)

时间表类型：触发器函数

参数：None (无)

此控件检查Amazon Systems Manager关联合规性的状态是处于COMPLIANT还是关联在实例上运行NON_COMPLIANT之后。如果关联合规状态为，则控制通过COMPLIANT。

状态管理器关联是分配给您的托管实例的配置。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，或者必须关闭特定端口。

创建一个或多个 State Manager 关联后，您可以立即获得合规性状态信息。您可以在控制台中查看合规性状态，也可以在响应Amazon 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或非-compliant)。它还显示分配给关联的严重性级别，例如Critical或Medium。

要了解有关州经理关联合规性的更多信息，请参阅Amazon Systems Manager用户指南中的[关于州经理关联合规性](#)。

Note

非洲（开普敦）或欧洲（开普敦）或欧洲（米兰）不支持此控件。

修复

关联失败可能与不同的事物有关，包括目标和 SSM 文档名称。要修复此问题，必须首先确定并调查这种关联。然后，您可以更新关联以更正特定问题。

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，Amazon Systems Manager 将创建新版本。

调查和更新失败的关联

1. 访问 <https://console.aws.amazon.com/systems-manager/>，打开 Amazon Systems Manager 控制台。
2. 在导航窗格的“节点管理”下，选择“队列管理器”。
3. 选择关联状态为“失败”的实例 ID。
4. 请选择 View details (查看详细信息)。
5. 选择“关联”。

6. 记下关联状态为“失败”的关联的名称。这是您需要调查的关联。在下一步骤中，您需要使用关联名称。
7. 在导航窗格的“节点管理”下，选择“状态管理器”。搜索协会名称，然后选择该协会。
8. 确定问题后，编辑失败的关联以更正问题。有关如何编辑关联的信息，请参阅[编辑关联](#)。

有关创建和编辑状态管理器关联的更多信息，请参阅《Amazon Systems Manager用户指南》中的 Systems Manager 中使用[关联](#)。

[SSM.4] SSM 文档不应公开

类别：保护 > 安全网络配置 > 资源不可公开访问

严重性：重大

资源类型：AWS::SSM::Document

Amazon Config 规则：[ssm-document-not-public](#)

时间表类型：定期

参数：None (无)

此控件检查账户拥有的Amazon Systems Manager文件是否公开。如果所有者的 SSM 文档Self是公开的，则此控制将失效。

公开的 SSM 文档可能允许意外访问您的文档。公开 SSM 文档可以公开有关您的账户、资源和内部流程的宝贵信息。

除非您的使用案例需要启用公开共享，否则 Secury Hub 建议您为拥有的 SSystems Manager 文档启用阻止公开共享设置Self。

Note

以下区域不支持此控件：

- Amazon GovCloud (美国东部)
- Amazon GovCloud (美国西部)

修复

有关禁用 SSM 文档的公共访问[权限的更多信息](#)，请参阅Amazon Systems Manager用户指南中的[修改共享 SSM 文档的权限和共享 SSM 文档的最佳实践](#)。

[WAF.1] 应启用Amazon WAF经典的全球 Web ACL 日志记录

类别：识别 > 记录

严重性：中

资源类型：AWS::WAF::WebACL

Amazon Config 规则：[waf-classic-logging-enabled](#)

时间表类型：定期

参数：None (无)

此控件检查是否为Amazon WAF全局 Web ACL 启用了日志记录。如果未启用 Web ACL 的日志记录，则此控制将失败。

日志记录是保持Amazon WAF全球的可靠性、可用性和性能的重要方面。这是许多组织的业务和合规性要求，允许您对应用程序行为进行故障排除。它还提供有关流量的详细信息，这些信息由所连接的 Web ACL 进行分析Amazon WAF。

Note

以下区域不支持此控件：

- 美国东部（俄亥俄州）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈）
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太区域（东京）
- 加拿大（中部）
- China (Beijing)
- China (Ningxia)
- 欧洲（法兰克福）
- 欧洲（爱尔兰）
- 欧洲（伦敦）
- 欧洲（米兰）
- Europe (Paris)
- Europe (Stockholm)
- Middle East (Bahrain)
- 南美洲（圣保罗）
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

您可以从 Kinesis Data Firehose 控制台启用 Web ACL 的日志记录。

为 Web ACL 启用日志记录

1. 打开 Kinesis Data Firehose 控制台，[网址为 https://console.aws.amazon.com/firehose/](https://console.aws.amazon.com/firehose/)。
2. 创建 Kinesis Data Firehose 传输流。

名称必须以前缀aws-waf-logs-开头。例如，aws-waf-logs-us-east-2-analytics。

在您运营的区域内创建 Kinesis DPUT ata Firehose 传输流。如果您为 Amazon 捕获日志 CloudFront，请在美国东部（弗吉尼亚北部）创建传输流。有关更多信息，请参阅 [Amazon Kinesis Data Firehose 开发人员指南中的创建 Amazon Kinesis Data Firehose 传输流](#)。

3. 从“服务”中选择 WAF & Shield。然后选择“切换到Amazon WAF经典”。
4. 在筛选器中，选择全局 (CloudFront)。
5. 选择要为其启用日志记录的 Web ACL。

6. 在“记录”下，选择“启用日志记录”。
7. 选择您之前创建的 Kinesis Data Firehose 传输流。您必须选择名称以aws-waf-logs-开头的传输流。
8. 选择启用日志记录。

[WAF.2] WAF 区域规则应至少具有一个条件

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAFRegional::Rule

Amazon Config 规则：[waf-regional-rule-not-empty](#)

时间表类型：触发器函数

参数：None (无)

此控件检查Amazon 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。规则的条件允许流量检查并采取定义的操作（允许、阻止或计数）。没有任何条件，交通未经检查即通过。WAF Regional 规则没有条件，但其名称或标签提示允许、封禁或计数，可能会导致错误地假设其中一项操作正在发生。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要向空规则添加条件，请参阅Amazon WAF开发者指南中的[在规则中添加和删除条件](#)。

[WAF.3] WAF 区域规则组应至少有一条规则

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAFRegional::RuleGroup

Amazon Config 规则：[waf-regional-rulegroup-not-empty](#)

时间表类型：触发器函数

参数：None (无)

此控件检查Amazon 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。规则的条件允许流量检查并采取定义的操作（允许、阻止或计数）。没有任何规则，交通未经检查即通过。WAF Regional 规则组没有规则，但其名称或标签提示允许、封禁或计数，可能会导致错误地假设其中一项操作正在发生。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- 亚太地区（大阪）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

要向空规则组添加规则和规则条件，请参阅Amazon WAF开发者指南[中的在Amazon WAF经典规则组中添加和删除规则和在规则中添加和删除条件](#)。

[WAF.4] WAF Classic Regional Web ACL 应至少包含一个规则或规则组

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAFRegional::WebACL

Amazon Config 规则：[waf-regional-webacl-not-empty](#)

时间表类型：触发器函数

参数：None（无）

此控件检查Amazon 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，则此控制将失败。

WAF 区域 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的集合。如果 Web ACL 为空，则网络流量可以在不被 WAF 检测或处理的情况下通过，具体取决于默认操作。

Note

以下区域不支持此控件：

- 亚太地区（雅加达）
- China (Beijing)
- China (Ningxia)
- Amazon GovCloud（美国东部）
- Amazon GovCloud（美国西部）

修复

向空的 Web ACL 添加规则或规则组

1. 通过 <https://console.aws.amazon.com/wafv2/> 打开Amazon WAF控制台。
2. 在导航窗格中，选择 ScheduledAmazon WAF s scheduled，然后选择 Web ACL。
3. 在筛选器中，选择空 Web ACL 所在的区域。
4. 选择空 Web ACL 的名称。
5. 选择规则，然后选择编辑 Web ACL。

6. 在“规则”中，选择规则或规则组，然后选择“将规则添加到 Web ACL”。
7. 此时，如果您要向 Web ACL 添加多个规则或规则组，则可以修改 Web ACL 中的规则顺序。
8. 选择 Update (更新)。

[WAF.6] WAF 全局规则应至少具有一个条件

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAF::Rule

Amazon Config 规则：[waf-global-rule-not-empty](#)

时间表类型：触发器函数

参数：None (无)

此控件检查 Amazon 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。

WAF 全局规则可以包含多个条件。规则的条件允许流量检查并采取定义的操作（允许、阻止或计数）。没有任何条件，交通未经检查即通过。WAF 全局规则没有条件，但其名称或标签提示允许、封禁或计数，可能会导致错误地假设其中一项操作正在发生。

Note

此控件仅适用于美国东部（弗吉尼亚北部）。

修复

有关创建规则和添加条件的说明，请参阅 Amazon WAF 开发者指南中的[创建规则和添加条件](#)。

[WAF.7] WAF 全局规则组应至少有一条规则

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAF::RuleGroup

Amazon Config 规则：[waf-global-rulegroup-not-empty](#)

时间表类型：触发器函数

参数：None (无)

此控件检查 Amazon 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。规则的条件允许流量检查并采取定义的操作（允许、阻止或计数）。没有任何规则，交通未经检查即通过。WAF 全局规则组没有规则，但其名称或标签提示允许、封禁或计数，可能会导致错误地假设其中一项操作正在发生。

Note

此控件仅适用于美国东部（弗吉尼亚北部）。

修复

有关向规则组添加规则的说明，请参阅 Amazon WAF 开发者指南中的[创建 Amazon WAF 经典规则组](#)。

[WAF.8] WAF 全球 Web ACL 应至少包含一个规则或规则组

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::WAF::WebACL

Amazon Config 规则：[waf-global-webacl-not-empty](#)

时间表类型：触发器函数

参数：None (无)

此控件检查Amazon 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 全球 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的集合。如果 Web ACL 为空，则网络流量可以在不被 WAF 检测或处理的情况下通过，具体取决于默认操作。

Note

此控件仅适用于美国东部（弗吉尼亚北部）。

修复

向空的 Web ACL 添加规则或规则组

1. 通过 <https://console.aws.amazon.com/wafv2/> 打开Amazon WAF控制台。
2. 在导航窗格中，选择 ScheduledAmazon WAF s scheduled，然后选择 Web ACL。
3. 在“筛选器”中，选择“全局”(CloudFront)。
4. 选择空 Web ACL 的名称。
5. 选择规则，然后选择编辑 Web ACL。
6. 在“规则”中，选择规则或规则组，然后选择“将规则添加到 Web ACL”。
7. 此时，如果您要向 Web ACL 添加多个规则或规则组，则可以修改 Web ACL 中的规则顺序。
8. 选择 Update (更新)。

控件类别

中的每个控件Amazon Security Hub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、类别中的子类别以及子类别中的分类器（可选）。例如：

- 检测 > 检测服务 > 应用程序监控
- 识别 > 清单
- 保护 > 数据保护 > 加密传输中的数据

以下是适用于当前可用的 Security Hub 控件的类别、子类别和分类器的描述。

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

是否有正确的检测服务，覆盖范围适中？

Amazon检测服务的示例包括亚马逊 CloudWatch 警报、亚马逊Detective、亚马逊 GuardDuty、Amazon InspectorAmazon IoT Device DefenderAmazon Security Hub、和Amazon Trusted Advisor。

- 应用程序监控-是否监控应用程序运行状况以保持可用性？

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。

清单

正在使用哪些资源，它们是否已批准用于此项服务的资源？

- 标记-是否为服务（包括资源所有者）实施了正确的资源标记策略？

日志记录

您是否已安全启用该服务的所有相关日志记录？日志文件示例包括：

- Amaon VPC 流日志
- Elastic Load Balancing 访问日志
- 亚马逊 CloudFront 日志
- 亚马逊 CloudWatch 日志
- Amazon Relational Database Service al D
- 亚马逊 OpenSearch 服务慢速索引日志
- X-Ray 跟踪
- Amazon Directory Service 日志
- Amazon Config物品

资源配置

您是否了解如何配置资源以减少攻击面？

漏洞、补丁和版本管理

您是否有需要修补的资源或存在不可接受漏洞的资源？您是否在使用最新版本的软件？

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

该服务是否有严格的身份验证和授权策略？

- 访问控制 — 该服务的 IAM 或资源策略是否符合最低权限实践？
- 无密码身份验证 — 是否使用联合身份或 SSO 来对用户进行身份验证，而不是 ID、密码和访问密钥？Kerberos 是否用于消除通过网络传输密码的需要？
- root 用户访问限制 — 是否避免使用 root 用户？
- 敏感 API 操作受限-服务的敏感 API 操作是否受到适当限制，尤其是那些导致权限升级或资源共享的操作？这可能适用于 IAM 或基于资源的策略。

安全网络配置

该服务是否避免了公共和不安全的远程网络访问？

- API 私有访问-是否已启用 VPC 终端节点以私有访问Amazon API？
- 资源不可公开访问-资源是否已正确分段和隔离？
- VPC 中的资源 — 是否可以正确使用 VPC，例如要求在 VPC 中运行作业？

- 安全组配置-安全组配置是否安全？

数据保护

您是否有机制来保护您的服务消费、发送或存储的数据？

- 静态@@ 数据加密-该服务是否对静态数据进行加密？
- 加密传输中的数据-该服务是否对传输中的数据进行加密？
- 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？

API 保护

该服务是否Amazon 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。中的保护服务示例Amazon包括Amazon Control Tower、、、、Amazon WAFAmazon Shield AdvancedAmazon Network FirewallAmazon Secrets Manager、AAmazon Identity and Access Management ccess Analyzer 和Amazon Resource Access Manager。

安全开发

您是否使用了安全编码实践？

- 凭证不是硬编码的-你的代码中是否有硬编码的证书？

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。

故障恢复能力

您的工作负载能否从安全事件中快速恢复？

- 启用备份 — 您是否建立并测试了备份？
- 高可用性-服务的配置是否允许流畅的故障转移、弹性扩展和高可用性？

您可能希望禁用的 Amazon 基础最佳实践控件

要节省 Amazon Config 的成本，您可以禁用所有区域（有一个区域除外）中的全局资源的记录，然后禁用处理所有区域（运行全局记录的区域除外）中的全局资源的这些控件。

- [\[IAM.1\] IAM 策略不应允许完整的 “*” 管理权限 \(p. 428\)](#)
- [\[IAM.2\] IAM 用户不应附加 IAM 政策 \(p. 429\)](#)
- [\[IAM.3\] IAM 用户的访问密钥应每 90 天或更短时间轮换一次 \(p. 430\)](#)
- [\[IAM.4\] IAM 根用户访问密钥不应存在 \(p. 431\)](#)
- [\[IAM.5\] 应为拥有控制台密码的所有 IAM 用户启用 MFA \(p. 431\)](#)
- [\[IAM.6\] 应为根用户启用硬件 MFA \(p. 432\)](#)
- [\[IAM.7\] IAM 用户的密码策略应具有强配置 \(p. 433\)](#)
- [\[IAM.8\] 应删除未使用的 IAM 用户证书 \(p. 433\)](#)
- [\[IAM.21\] 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 \(p. 434\)](#)
- [\[KMS.1\] IAM 客户托管策略不应允许对所有 KMS 密钥进行解密和重新加密操作 \(p. 436\)](#)
- [\[KMS.2\] IAM 委托人不应有允许对所有 KMS 密钥进行解密和重新加密操作的 IAM 内联策略 \(p. 437\)](#)

如果您禁用这些控件并禁用特定区域中的全局资源记录，则还应禁用 [\[Config.1\] 应该启用 Amazon Config \(p. 385\)](#)。这是因为 [\[Config.1\] 应该启用 Amazon Config \(p. 385\)](#) 需要全局资源记录才能通过。

日志系统Amazon使用 Security Hub API 调用Amazon CloudTrail

Amazon Security Hub 与 Amazon CloudTrail，提供用户、角色或用户所采取操作的记录的服务 Amazon 服务在 Security Hub 中。CloudTrail 将 Security Hub 的 API 调用捕获为事件。捕获的调用包含来自 Security Hub 控制台的调用，并且包含 Security Hub API 操作的代码调用。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Security Hub 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定向 Security Hub 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息（包括如何对其进行配置和启用），请参阅 [Amazon CloudTrail 用户指南](#)。

CloudTrail 中的 Security Hub 信息

在您创建 Amazon 账户时，将在该账户上启用 CloudTrail。当 Security Hub 中发生受支持的事件活动时，该活动将记录在 CloudTrail 事件中。Amazon 中的服务事件事件记录。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 CloudTrail 事件历史记录查看事件](#)。

要持续记录账户中的事件（包括 Security Hub 的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送到 Simple Storage Service（Amazon S3）存储桶。在控制台创建跟踪时，跟踪默认应用于所有 Amazon 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送到您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您可以配置其他 Amazon 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- [创建跟踪概览](#)
- [CloudTrail 支持的服务和集成](#)
- [为 CloudTrail 配置 Amazon SNS 通知](#)
- [从多个区域接收 CloudTrail 日志文件](#) 和 [从多个账户接收 CloudTrail 日志文件](#)

Security Hub 支持将所有 Security Hub API 操作记录为 CloudTrail 日志中的事件。要查看 Security Hub 操作的列表，请参阅 [Security Hub API 参考](#)。

当 CloudTrail 将以下操作的活动记录到 CloudTrail 时，`responseElements` 设置为 `null`。这可确保 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。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 Amazon Identity and Access Management (IAM) 用户凭证发出的
- 请求是使用角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其它 Amazon 服务发出

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

例如：Security Hub 日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Simple Storage Service (Amazon S3) 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 CreateInsight 操作。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 [中的见解AmazonSecurity Hub \(p. 195\)](#)。

```
{
  "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": "c0fffcdd-f04d-11e8-93fc-ddcd14710066",
  "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```

自动响应和补救

与 Amazon 一起 EventBridge，您可以自动执行 Amazon 自动响应系统事件，例如应用程序可用性 issue 或资源更改。来自的事件 Amazon 服务被交付到 EventBridge 在近乎实时的基础上，有保证地进行传输。您可以编写简单规则来指示所关注的事件，并指示要在事件匹配规则时执行的自动化操作。可自动触发的操作包括：

- 调用 Amazon Lambda 函数
- 调用 Amazon EC2 运行命令
- 将事件中继到 Amazon Kinesis Data Streams
- 激活 Amazon 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 会自动将所有新发现和现有调查结果的所有更新发送到 EventBridge 如同 EventBridge 事件。您还可以创建自定义操作，以便将选定的调查结果和洞察结果发送到 EventBridge。

然后你配置 EventBridge 规则来响应每种类型的事件。

有关使用的更多信息 EventBridge，请参阅[亚马逊 EventBridge 用户指南](#)。

Note

作为最佳实践，请确保向您的用户授予的访问权限 EventBridge 使用仅授予所需权限的最低权限 IAM 策略。

有关更多信息，请参阅 [亚马逊中的 Identity and Access Management EventBridge](#)。

还有一组用于跨账户自动响应和补救的模板 Amazon 解决方案。模板利用 EventBridge 事件规则和 Lambda 函数。您使用部署解决方案 Amazon CloudFormation 和 Amazon Systems Manager。该解决方案可以创建完全自动的响应和补救措施。它还可以使用 Security Hub 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[Amazon Security Hub 自动响应和修复解决方案的解决方案页面](#)。

主题

- [Security Hub 集成的类型 EventBridge \(p. 500\)](#)
- [EventBridge Security Hub 的事件格式 \(p. 501\)](#)
- [配置 EventBridge 自动发送调查结果的规则 \(p. 503\)](#)
- [使用自定义操作将检查结果和见解结果发送到 EventBridge \(p. 506\)](#)

Security Hub 集成的类型 EventBridge

Security Hub 使用以下内容 EventBridge 支持以下类型的与的集成 EventBridge。

在存储库的 EventBridge Security Hub 的控制面板所有事件包含所有这些事件类型。

所有结果 (Security Hub Findings - Imported)

Security Hub 会自动将所有新发现和现有调查结果的所有更新发送到 EventBridge 如同 Security Hub Findings - Imported 事件。各个 Security Hub Findings - Imported 事件包含一个发现。

所有 [BatchImportFindings](#) 和 [BatchUpdateFindings](#) 请求触发器 aSecurity Hub Findings - Imported event。

对于管理员帐户，中的活动源 EventBridge 包括来自他们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结果的事件。跨区域的调查结果几乎实时地包含在活动源中。有关如何配置查找聚合的信息，请参阅 [跨区域聚合 \(p. 50\)](#)。

您可以在 EventBridge 自动将结果路由到 Amazon S3 存储桶、修复工作流程或第三方工具。规则可以包括仅在查找结果具有特定属性值时才应用规则的筛选器。

您可以使用此方法自动将所有结果或具有特定特征的所有结果发送到响应或修复 workflow。

请参阅 [the section called “为自动发送的结果配置规则” \(p. 503\)](#)。

自定义操作的结果 (Security Hub Findings - Custom Action)

Security Hub 还会将与自定义操作关联的结果发送给 EventBridge 如同 Security Hub Findings - Custom Action 事件。

这对于使用 Security Hub 控制台的分析师非常有用，他们需要特定结果或一小部分结果发送到响应或修复 workflow。您可以每次为最多 20 个结果选择自定义操作。每个发现都被发送到 EventBridge 作为一个单独的 EventBridge event。

创建自定义操作时，您可以为其分配自定义操作 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 关联的查找结果后执行指定操作。

请参阅 [the section called “配置和使用自定义操作” \(p. 506\)](#)。

例如，您可以在 Security Hub 中创建一个名为自定义操作 `send_to_ticketing`。然后在 EventBridge，您创建一个规则，将在以下情况下触发 EventBridge 收到一份包含 `send_to_ticketing` 自定义操作 ID。该规则包括将结果发送到票证系统的逻辑。之后，您可以在 Security Hub 中选择结果，并使用 Security Hub 中的自定义操作手动将结果发送到票证系统。

有关如何将 Security Hub 结果发送到的示例 EventBridge 有关进一步处理，请参阅 [如何集成 Amazon Security Hub 自定义操作 PagerDuty](#) 和 [如何在 Amazon 合作伙伴网络 \(APN\) 中启用自定义操作 Amazon Security Hub](#) 在 Amazon 合作伙伴网络 (APN) 博客。

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见解结果发送到 EventBridge 如同 Security Hub Insight Results 事件。见解结果是见解匹配的资源。请注意，将见解结果发送到 EventBridge，您不会将检查结果发送到 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，您先在 Security Hub 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” \(p. 506\)](#)。

例如，假设您看到想与同事分享的特定洞察结果。在这种情况下，您可以使用自定义操作通过聊天或票证系统将见解结果发送给同事。

EventBridge Security Hub 的事件格式

这些区域有：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 将事件发送到时使用的格式 EventBridge。

Security Hub Findings - Imported

Security Hub Findings - Imported从 Security Hub 发送到的事件 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/maciekarn:aws:maciekus-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
  ],
  "detail": {
    "findings": [
      {
        "finding content"
      }
    ]
  }
}
```

*<finding content>*是事件发送的调查结果的内容（JSON 格式）。每个事件都发送一个发现结果。

有关查找属性的完整列表，请参阅[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。

有关如何配置的信息 EventBridge 由这些事件触发的规则，请参阅[the section called “为自动发送的结果配置规则” \(p. 503\)](#)。

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action从 Security Hub 发送到的事件 EventBridge 使用以下格式。每个结果将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>*是事件发送的调查结果的内容（JSON 格式）。每个事件都发送一个发现结果。

有关查找属性的完整列表，请参阅[Amazon Security Finding 格式 \(ASFF\) \(p. 68\)](#)。

有关如何配置的信息 EventBridge 由这些事件触发的规则，请参阅[the section called “配置和使用自定义操作” \(p. 506\)](#)。

Security Hub Insight Results

Security Hub Insight Results从 Security Hub 发送到的事件 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/maciek: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 EventBridge 由这些事件触发的规则，请参阅[the section called “配置和使用自定义操作” \(p. 506\)](#)。

配置 EventBridge 自动发送调查结果的规则

您可以在中创建规则 EventBridge 定义了 Security Hub Findings - Imported 已收到事件。Security Hub Findings - Imported 事件由两者的更新触发。[BatchImportFindings](#) 和 [BatchUpdateFindings](#)。

每个规则都包含一个事件模式，用于标识触发该规则的事件。事件模式始终包含事件源 (aws.securityhub) 和事件类型 (Security Hub 调查结果-导入)。事件模式还可以指定筛选器来标识规则应用到的结果。

然后，规则标识规则目标。目标是在时要采取的行动 EventBridge 收到 Security Hub 调查结果-导入事件和查找结果与过滤器匹配。

此处提供的说明使用 EventBridge 控制台。当您使用控制台时，EventBridge 自动创建所需的基于资源的策略，以启用 EventBridge 写入 CloudWatch 日志。

您也可以使用 [PutRule](#) 的 API 操作 EventBridge API。但是，如果您使用 EventBridge 然后，您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 [CloudWatch 记录权限](#) 中的亚马逊 EventBridge 用户指南。

事件模式的格式

的事件模式的格式 Security Hub 调查结果-导入事件如下：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "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，并提供事件模式的过滤器值。如果事件模式不包含detail字段中，则所有发现都触发该规则。

您可以根据任何查找属性过滤调查结果。对于每个属性，您可以提供一个逗号分隔的数组，其中包含一个或多个值。

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

如果您为某个属性提供了多个值，则这些值将通过连接OR。如果查找结果具有列出的任何值，则查找结果与单个属性的筛选器匹配。例如，如果你同时提供两者INFORMATIONAL和LOW作为的值Severity.Label，那么查找结果如果严重性标签为INFORMATIONAL要么LOW。

这些属性是由AND。如果结果符合所有提供属性的筛选条件，则会匹配结果。

当您提供属性值时，它必须反映该属性在AmazonSecurity Fin 格式 (ASFF) 结构。

在以下示例中，事件模式为ProductArn和Severity.Label，因此如果查找结果是由 Amazon Inspector 生成的，并且其严重性标签为INFORMATIONAL要么LOW。

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

创建事件规则

您可以使用预定义的事件模式或自定义事件模式在 EventBridge。如果选择预定义的模式，EventBridge 自动填写source和detail-type。EventBridge 还提供了用于为以下查找属性指定筛选器值的字段：

- AwsAccountId
- Compliance.Status
- Criticality
- ProductArn
- RecordState
- ResourceId
- ResourceType
- Severity.Label
- Types
- Workflow.Status

创建 EventBridge 规则

1. 打开 Amazon EventBridge 控制台<https://console.aws.amazon.com/events/>.
2. 使用以下值创建 EventBridge 监控查找事件的规则：
 - 对于 Rule type (规则类型)，选择 Rule with an event pattern (具有事件模式的规则)。
 - 选择如何构建事件模式。

用... 构建事件模式	请执行此操作...	
一个模板	在事件模式选择以下选项： • 适用于事件源，选择Amazon 服务. • 适用于Amazon服务，选 择Security Hub. • 适用于Event type，选 择Security Hub 调查结果-导入. • (可选) 要使规则更具体， 请添加筛选器值。例如，要 将规则限制在具有活动记录 状态的查找结果中，特定记 录状态，选择处于活动状态.	
自定义事件模式 (如果要根据未显示在 EventBridge 控制台。)	• 在事件模式部分，选择自定义模式 (JSON 编辑器) 然后，在文本区域中粘贴以下事件模式： <pre>{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribute name>": ["<value1>", "<value2>"] } } }</pre>	

用... 构建事件模式	请执行此操作...	
	<pre> } } </pre> 更新事件模式以包括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，使用以下模式示例： <pre> { "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } } </pre>	

- 适用于目标类型，选择Amazon服务，以及选择一个目标中，选择一个目标，例如 Amazon SNS 主题或Amazon Lambdafunction. 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。

有关创建规则的细节，请参阅。[创建 Amazon EventBridge 对事件做出反应的规则](#)中的亚马逊 EventBridge 用户指南。

使用自定义操作将检查结果和见解结果发送到 EventBridge

使用 Security Hub 自定义操作将调查结果或见解结果发送到 EventBridge，您先在 Security Hub 中创建自定义操作。然后在中定义规则 EventBridge。

您最多可以创建 50 个自定义操作。

如果您启用了跨区域聚合并管理聚合区域的调查结果，则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 ARN。

创建自定义操作（控制台）

创建自定义操作时，可以指定名称、说明和唯一标识符。

在 Security Hub（控制台）中创建自定义操作

1. 打开Amazon在 Security Hub 控制台<https://console.aws.amazon.com/securityhub/>.

2. 在导航窗格中，选择 Settings (设置)，然后选择 Custom actions (自定义操作)。
3. 选择 Create custom action (创建自定义操作)。
4. 为操作提供 Name (名称)、Description (描述) 和 Custom action ID (自定义操作 ID)。

Name (名称) 的长度必须少于 20 个字符。

这些区域有：自定义操作 ID 每个人必须是唯一的 Amazon account。

5. 选择 Create custom action (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。

创建自定义操作 (Security Hub API , Amazon CLI)

要创建自定义操作，您可以使用 API 调用或 Amazon Command Line Interface。

要创建自定义操作 (Security Hub API) Amazon CLI)

- Security Hub API— 使用 [CreateActionTarget](#) operation. 创建自定义操作时，请提供名称、说明和自定义操作标识符。
- Amazon CLI— 在命令行处，运行 [create-action-target](#) 命令。

```
create-action-target --name <customActionName> --description <customActionDescription> --id <customActionIdentifier>
```

示例

```
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

要处理自定义操作，您必须在中创建对应的规则。EventBridge. 规则定义包含自定义操作的 ARN。

的事件模式 Security Hub 发现-自定义操作事件采用以下格式：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

的事件模式 Security Hub 洞察结果事件采用以下格式：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

```
} }
```

在这两种模式中，`<custom action ARN>`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。

此处提供的说明是针对 EventBridge 控制台。当您使用控制台时，EventBridge 自动创建所需的基于资源的策略，以启用 EventBridge 写入 CloudWatch 日志。

您也可以使用 [PutRule](#) 的 API 操作 EventBridge API。但是，如果您使用 EventBridge 然后，您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 [CloudWatch 记录权限](#) 中的亚马逊 EventBridge 用户指南。

在 中定义规则 EventBridge

1. 打开 Amazon EventBridge 控制台 <https://console.aws.amazon.com/events/>。
2. 在导航窗格中，选择 Rules (规则)。
3. 选择 Create rule (创建规则)。
4. 为规则输入名称和描述。
5. 对于 Event bus (事件总线)，请选择要与此规则关联的事件总线。如果您希望此规则与来自您的账户的事件匹配，请选择默认。当您账户中的某个 Amazon 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 Rule type (规则类型)，选择 Rule with an event pattern (具有事件模式的规则)。
7. 选择 Next (下一步)。
8. 适用于事件源，选择 Amazon 事件。
9. 适用于事件模式，选择事件模式表。
10. 适用于事件源，选择 Amazon 服务。
11. 适用于 Amazon 服务，选择 Security Hub。
12. 对于 Event type (事件类型)，执行以下操作之一：
 - 要创建在向自定义操作发送查找结果时应用的规则，请选择 Security Hub 发现-自定义操作。
 - 要创建规则并在将见解结果发送到自定义操作时应用到，请选择 Security Hub 洞察结果。
13. 选择特定的自定义操作 ARN，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 Add 以添加更多自定义操作 ARN。

14. 选择 Next (下一步)。
15. 根据选择目标中，选择并配置要在匹配该规则时调用的目标。
16. 选择 Next (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 标签](#) 中的亚马逊 EventBridge 用户指南。
18. 选择 Next (下一步)。
19. 查看规则详细信息并选择 Create rule (创建规则)。

在您对账户中的结果或见解结果执行自定义操作时，会在中生成事件。EventBridge。

为调查结果和洞察结果选择自定义操作

在创建 Security Hub 之后自定义操作和 EventBridge 规则，您可以将调查结果和洞察结果发送到 EventBridge 用于进一步的管理和处理。

活动被发送到 EventBridge 只有在其中查看它们的账户中。如果您使用管理员帐户查看结果，则会将事件发送到 EventBridge 在管理员账户中。

适用于Amazon要使 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，必须将您切换到的角色部署到需要操作的每个成员。

将结果发送到 EventBridge

1. 打开Amazon在 Security Hub 控制台<https://console.aws.amazon.com/securityhub/>.
2. 显示结果列表：
 - 从结果其次，您可以查看来自所有已启用的产品集成和控制的结果。
 - 从安全标准其次，您可以导航到从所选控制生成的结果列表。请参阅 [the section called “查看控制的详细信息” \(p. 257\)](#)。
 - 从集成其次，您可以导航到启用的集成生成的结果列表。请参阅 [the section called “查看来自集成的结果” \(p. 210\)](#)。
 - 从见解，您可以导航到检查结果列表以获取见解结果。请参阅 [the section called “查看见解结果和调查结果” \(p. 195\)](#)。
3. 选择要发送到的结果 EventBridge. 您一次最多可选择 20 个结果。
4. 从操作选择与 EventBridge 要应用的规则。

Security Hub 发送一个单独的Security Hub 发现-自定义操作每个发现的事件。

将洞察结果发送到 EventBridge

1. 打开Amazon在 Security Hub 控制台<https://console.aws.amazon.com/securityhub/>.
2. 在导航窗格中，选择 Insights。
3. 在存储库的见解在页面上，选择包含要发送到的结果的见解 EventBridge.
4. 选择要发送到的见解结果 EventBridge. 您一次最多可选择 20 个结果。
5. 从操作选择与 EventBridge 要应用的规则。

使用亚马逊简单通知服务订阅 Security Hub 公告

本节提供有关通过 Amazon Simple Notification Service (Amazon SNS) 订阅 Security Hub 公告以接收有关 Security Hub 通知。

订阅后，您将收到有关以下事件的通知（请注意每个 AnnouncementType 活动的相应通知）：

- GENERAL— 有关 Security Hub 服务的一般通知。
- UPCOMING_STANDARDS_CONTROLS— 指定的 Security Hub 控件或标准将很快发布。此类公告可帮助您在发布之前准备响应和补救工作流程。
- NEW_REGIONS— 新版本中提供了对 Security Hub Support Amazon Web Services 区域。
- NEW_STANDARDS_CONTROLS— 添加了新的 Security Hub 控件或标准。
- UPDATED_STANDARDS_CONTROLS— 现有 Security Hub 控制措施或标准已更新。
- RETIRED_STANDARDS_CONTROLS— 现有的 Security Hub 控件或标准已停用。
- UPDATED_ASFF— Amazon 安全查找格式 (ASFF) 语法、字段或值已更新。
- NEW_INTEGRATION— 可以与其他 Amazon 服务或第三方产品进行新的集成。
- NEW_FEATURE— 新的 Security Hub 功能可用。
- UPDATED_FEATURE— 现有 Security Hub 功能已更新。

通知以 Amazon SNS 支持的所有格式提供。你可以在 Security Hub 的所有 [Amazon Web Services 区域可用版本中订阅 Security Hub](#) 公告。

用户账户必须拥有 `sns::subscribe` IAM 权限才能订阅 Amazon SNS 主题。

Note

Security Hub 向任何订阅的账户发送有关 Security Hub 服务更新的 Amazon SNS 公告。Amazon 要在您的 Security Hub 帐户中接收有关发现的通知，请参阅 [在中查看查找结果列表和详细信息 Amazon Security Hub \(p. 63\)](#)。

您可以订阅一个 Amazon SNS 主题的 Amazon Simple Queue Service (Amazon SQS) 队列节点，但必须使用同一区域的 Amazon SNS 主题。有关更多信息，请参阅 [教程：订阅 Amazon Simple Queue Service 开发人员指南中的 Amazon SNS 主题](#)。

您还可以在收到通知时使用 Amazon Lambda 函数调用事件。有关更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的 [使用 Amazon SNS 通知调用 Lambda 函数](#)。

每个区域的 Amazon SNS 主题 ARN 如下所示。

Amazon 区域	Amazon SNS 主题 ARN
美国东部（俄亥俄）	<code>arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements</code>
美国东部（弗吉尼亚北部）	<code>arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements</code>
美国西部（加利福尼亚北部）	<code>arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements</code>
美国西部（俄勒冈）	<code>arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements</code>

Amazon 区域	Amazon SNS 主题 ARN
Africa (Cape Town)	arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements
Asia Pacific (Hong Kong)	arn:aws:sns:ap-east-1:464812404305: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
Asia Pacific (Osaka)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
Asia Pacific (Seoul)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
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
亚太区域 (东京)	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
加拿大 (中部)	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
China (Beijing)	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements
China (Ningxia)	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
欧洲 (法兰克福)	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
欧洲 (爱尔兰)	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
欧洲 (伦敦)	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
欧洲 (米兰)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
Europe (Paris)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
Europe (Stockholm)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
Middle East (Bahrain)	arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements

Amazon 区域	Amazon SNS 主题 ARN
南美洲 (圣保罗)	arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements
Amazon GovCloud (美国东部)	arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements
Amazon GovCloud (美国西部)	arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements

一个分区内不同区域的消息通常是相同的，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。与成员帐户关联的公告不会复制到管理员帐户中。因此，每个帐户，包括管理员帐户，每份公告只有一份副本。您可以决定要使用哪个帐户订阅 Security Hub 公告。

有关订阅 Security Hub 公告的费用信息，请参阅 [Amazon SNS 定价](#)。

订阅 Security Hub 公告 (控制台)

1. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 在 Revice Hub 公告中，选择您要订阅 Security Hub 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. 对于协议，选择接收 Security Hub 公告的方式。如果您选择 Email address (电子邮件)，输入您要用于接收公告的电子邮件地址。
6. 选择 Create subscription (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 公告 (Amazon 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制措施的安全 Security Hub 公告。消息内容因事件类型而异。

示例：Security Hub 关于新控件 (电子邮件协议) 的公告

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub controls added to the Amazon Foundational Security Best Practices standard",
  "Description": "We have added 36 new controls to the Amazon Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
```

```
AutoScaling.4, AutoScaling.6), Amazon 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), Amazon 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), Amazon WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the Amazon Foundational Security Best Practices standard in an account and configured Security Hub to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. "
```

示例：Security Hub 关于新控件的公告（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 controls added to the Amazon Foundational Security Best Practices standard\",\"Description\":\"We have added 36 new controls to the Amazon Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), Amazon 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), Amazon 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), Amazon WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the Amazon Foundational Security Best Practices standard in an account and configured SSecurity Hub 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" : "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP+ElipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmHl37hjkiljhCg/t53QQiLFp7MH+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUs0G8yiJVCBEJhJlyS+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLI17gYKs1t+jsyd/k+7k0qGmOJRD7qhE7H+7vaGRLOptsQnbW8VmeYnDbahE08FV+Mp1rpV+70g==",
  "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"
}
```


Amazon Security Hub

最大配额

以下是每个 Security Hub 配额Amazon每区域账户。

资源	配额	注释
Security Hub 成员 账户数量	5000	每个区域的每个管理员账户可以添加的 Security Hub 成员账户的最大数量。 这是一个硬性配额。无法请求增加允许的 Security Hub 成员账户数。
Security Hub 未完 成邀请数	1000	每个区域的每个管理员账户可以发送的未完成Security Hub 成员账户邀请的最大数量。 这是一个硬性配额。无法请求增加允许的 Security Hub 未完成邀请数。
自定义操作数	50	可创建的 Security Hub 自定义操作的最大数量。 这是一个硬性配额。无法请求增加自定义操作数。
自定义见解数	100	可创建的用户定义的自定义见解的最大数量。 这是一个硬性配额。无法请求增加 Security Hub 自定义见解数。
见解结果的数量	100	为 GetInsightsResults API 操作返回的最大聚合结果数。 这是一个硬性配额。无法请求增加见解结果数。
服务相关数 Amazon Config规则	250	服务相关的最大数量Amazon ConfigSecurity Hub 为对控件执行安全检查而创建的规则。 这是一个硬性配额。无法请求增加服务相关的Amazon ConfigRules。
Security Hub 结果 保留时间	90 天	结果将在最近更新后 90 天或创建后 90 天 (如果未发生更新) 后删除。 要将结果存储 90 天以上, 您可以在中配置规则 EventBridge 将结果路由到您的 Amazon S3 存储桶。

速率配额

以下AmazonSecurity Hub 配额是每个Amazon每区域账户。

请求类型	速率限制配额 (每秒)	突发限制配额 (每秒)
BatchEnableStandards	1	1

请求类型	速率限制配额 (每秒)	突发限制配额 (每秒)
GetFindings	3	6
BatchImportFindings	10	30
BatchUpdateFindings	10	30
UpdateStandardsControl	1	5
所有其他请求类型	10	30

如果你已经设置好了[跨区域聚合 \(p. 50\)](#)，一个电话给BatchImportFindings和BatchUpdateFindings影响关联的区域和聚合区域。这些区域有：GetFindings操作从链接的 Region 和聚合 Region 中检索查找结果。但是，BatchEnableStandards和UpdateStandardsControl操作特定于区域。

区域限制

某些 Amazon Security Hub 功能仅在部分功能中可用 Amazon Web Services 区域。以下部分指定了这些区域限制。

目录

- [跨区域聚合限制 \(p. 516\)](#)
- [并非所有区域都支持集成 \(p. 517\)](#)
 - [中国 \(北京\) 和中国 \(宁夏\) 支持的集成 \(p. 517\)](#)
 - [Amazon GovCloud \(美国东部\) 和 Amazon GovCloud \(美国西部\) 中支持的集成 \(p. 517\)](#)
- [所有区域中均不支持控件 \(p. 518\)](#)
 - [美国东部 \(俄亥俄州\) \(p. 518\)](#)
 - [美国西部 \(加利福尼亚\) \(p. 519\)](#)
 - [美国西部 \(俄勒冈州\) \(p. 519\)](#)
 - [非洲 \(开普敦\) \(p. 520\)](#)
 - [亚太地区 \(香港\) \(p. 523\)](#)
 - [亚太地区 \(雅加达\) \(p. 523\)](#)
 - [亚太地区 \(孟买\) \(p. 529\)](#)
 - [亚太地区 \(大阪\) \(p. 530\)](#)
 - [亚太地区 \(首尔\) \(p. 533\)](#)
 - [亚太地区 \(新加坡\) \(p. 534\)](#)
 - [亚太地区 \(悉尼\) \(p. 534\)](#)
 - [亚太地区 \(东京\) \(p. 535\)](#)
 - [加拿大 \(中部\) \(p. 535\)](#)
 - [中国 \(北京\) \(p. 536\)](#)
 - [中国 \(宁夏\) \(p. 540\)](#)
 - [欧洲 \(法兰克福\) \(p. 543\)](#)
 - [欧洲 \(爱尔兰\) \(p. 544\)](#)
 - [欧洲 \(伦敦\) \(p. 544\)](#)
 - [欧洲 \(米兰\) \(p. 545\)](#)
 - [欧洲 \(巴黎\) \(p. 548\)](#)
 - [欧洲 \(斯德哥尔摩\) \(p. 548\)](#)
 - [中东 \(巴林\) \(p. 549\)](#)
 - [南美洲 \(圣保罗\) \(p. 550\)](#)
 - [Amazon GovCloud \(美国东部\) \(p. 551\)](#)
 - [Amazon GovCloud \(美国西部\) \(p. 555\)](#)

跨区域聚合限制

在中 Amazon GovCloud (US), [跨区域聚合 \(p. 50\)](#) Amazon GovCloud (US) 仅适用于发现、查找更新和见解。具体而言, 您只能汇总发现、查找更新以及介于 Amazon GovCloud (美国东部) 和 Amazon GovCloud (美国西部) 之间的见解。

在中国区域, 跨区域聚合仅适用于中国地区的发现、查找更新和见解。具体而言, 您只能汇总中国 (北京) 和中国 (宁夏) 之间的发现、最新动态和见解。

您不能使用默认情况下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《Amazon一般参考》中的[启用区域](#)。

并非所有区域都支持集成

某些集成并非在所有区域都可用。如果某个集成在特定区域不可用，则当您选择该区域时，它不会在 Security Hub 控制台的集成页面上列出。

中国（北京）和中国（宁夏）支持的集成

中国（北京）和中国（宁夏）区域仅支持以下[Amazon服务集成 \(p. 211\)](#)：

- Amazon Firewall Manager
- Azon GuardDuty
- IAM Access Analyzer
- Systems Man
- Systems Manager OpsCenter
- Systems Manager

中国（北京）和中国（宁夏）区域仅支持以下[第三方集成 \(p. 221\)](#)：

- 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

Amazon GovCloud（美国东部）和Amazon GovCloud（美国西部）中支持的集成

Amazon GovCloud（美国东部）和Amazon GovCloud（美国西部）区域仅支持以下[Amazon服务集成 \(p. 211\)](#)：

- Amazon Config
- Amazon Detective
- Amazon Firewall Manager
- Azon GuardDuty
- Amazon Health
- Amazon Inspector
- IAM Access Analyzer

Amazon GovCloud (美国东部) 和Amazon GovCloud (美国西部) 区域仅支持以下[第三方集成 \(p. 221\)](#) :

- Atlassian Jira Service Manager
- 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Amazon GovCloud (美国西部) 提供)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

所有区域中均不支持控件

以下区域不支持所有Security Hub 控件。对于每个区域，此列表显示了不支持的控件。

美国东部 (俄亥俄州)

美国东部 (俄亥俄) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

美国西部 (北加利福尼亚)

美国西部 (加利福尼亚北部) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

美国西部 (俄勒冈州)

美国西部 (俄勒冈) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

非洲 (开普敦)

非洲 (开普敦) 不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.4 — 确保每隔 90 天或更短时间轮换一次访问密钥 ” \(p. 267\)](#)

[the section called “1.20 - 确保已创建支持角色来管理与 Amazon Support 相关的事件 ” \(p. 272\)](#)

[the section called “4.1 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 22 ” \(p. 308\)](#)

[the section called “4.2 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 3389 ” \(p. 308\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI。CodeBuild1\] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth” \(p. 317\)](#)

[the section called “\[PCI。CodeBuild2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 318\)](#)

[the section called “\[PCI.DMS.1\]Amazon Database Migration Service复制实例不应公开” \(p. 322\)](#)

[the section called “\[PCI.EC2.1\] 亚马逊 EBS 快照不应公开恢复” \(p. 323\)](#)

[the section called “\[PCI.EC2.4\] 应删除未使用的 EC2 EIP” \(p. 326\)](#)

[the section called “\[PCI.EC2.5\] 安全组不应允许从 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 进入端口 22” \(p. 327\)](#)

[the section called “\[PCI.ELBV2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 329\)](#)

[the section called “\[PCI.GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.IAM.1\] IAM 根用户访问密钥不应存在” \(p. 333\)](#)

[the section called “\[PCI.RDS.1\] 亚马逊 RDS 快照应禁止公共访问” \(p. 345\)](#)

[the section called “\[PCI.SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)

[the section called “\[PCI.SSM.1\] 安装补丁后，由 Systems Manager 管理的 Amazon EC2 实例的补丁合规状态应为“合规”” \(p. 357\)](#)

[the section called “\[PCI.SSM.2\] 由 Systems Manager 管理的实例的关联合规状态应为 COMPLIANT” \(p. 358\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ACM.1\] 导入的和 ACM 颁发的证书应在指定的时间段后续订” \(p. 364\)](#)

[the section called “\[ApiGateway.1\] 应该启用 API Gateway REST 和 WebSocket API 日志记录” \(p. 365\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.1\] CodeBuild GitHub 或 Bitbucket 源存储库 URL 应使用 OAuth” \(p. 382\)](#)

[the section called “\[CodeBuild.2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 383\)](#)

[the section called “\[DMS.1\]Amazon Database Migration Service 复制实例不应公开” \(p. 386\)](#)

[the section called “\[EC2.1\] Amazon EBS 快照不应公开，这取决于任何人都可恢复的可用性” \(p. 388\)](#)

[the section called “\[EC2.3\] 附加的 EBS 卷应在静态时加密” \(p. 390\)](#)

[the section called “\[EC2.4\] 应在指定时间段后删除已停止的 EC2 实例” \(p. 390\)](#)

[the section called “\[EC2.8\] EC2 实例应使用 imdsV2” \(p. 393\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EFS.1\] 应将 Amazon EFS 配置为使用以下方法加密静态文件数据Amazon KMS” \(p. 410\)](#)

[the section called “\[EFS.2\] 亚马逊 EFS 卷应包含在备份计划中” \(p. 410\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.4\] 应将应用程序负载均衡器配置为删除 HTTP 标头” \(p. 416\)](#)

[the section called “\[ELB.8\] 带有 HTTPS/SSL 侦听器的经典负载均衡器应使用具有强配置的预定义安全策略” \(p. 418\)](#)

[the section called “\[elbv2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 422\)](#)

[the section called “\[EMR.1\] Amazon EMR 集群主节点不应有公有 IP 地址” \(p. 423\)](#)

[the section called “\[ES.3\] Elasticsearch 域应加密节点之间发送的数据” \(p. 424\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[IAM.3\] IAM 用户的访问密钥应每 90 天或更短时间轮换一次” \(p. 430\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[RDS.1\] RDS 快照应为私有快照” \(p. 448\)](#)

[the section called “\[RDS.9\] 应启用数据库日志记录” \(p. 453\)](#)

[the section called “\[RDS.10\] 应为 RDS 实例配置 IAM 身份验证” \(p. 456\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[Redshift.3\] Amazon Redshift 集群应启用自动快照” \(p. 468\)](#)

[the section called “\[SageMaker.1\] SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 480\)](#)

[the section called “\[SSM.2\] 由 Systems Manager 管理的所有 EC2 实例都应符合补丁要求” \(p. 487\)](#)

[the section called “\[SSM.3\] 由 Systems Manager 管理的实例的关联合规状态应为COMPLIANT” \(p. 488\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区（香港）

亚太地区（香港）不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[RDS.10\] 应为 RDS 实例配置 IAM 身份验证” \(p. 456\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区（雅加达）

亚太地区（雅加达）不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.12 — 确保不存在根用户访问密钥” \(p. 271\)](#)

[the section called “1.20 - 确保已创建支持角色来管理与 Amazon Support 相关的事件 ” \(p. 272\)](#)

[the section called “2.9 — 确保在所有 VPC 中启用 VPC 流量记录 ” \(p. 280\)](#)

- [the section called “4.1 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 22 ” \(p. 308\)](#)
- [the section called “4.2 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 3389 ” \(p. 308\)](#)
- [the section called “4.3 — 确保每个 VPC 的默认安全组限制所有流量” \(p. 309\)](#)
- [the section called “PCI DSS” \(p. 310\)](#)
- [the section called “\[PCI。CodeBuild1\] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth” \(p. 317\)](#)
- [the section called “\[PCI。CodeBuild2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 318\)](#)
- [the section called “\[PCI.DMS.1\]Amazon Database Migration Service复制实例不应公开” \(p. 322\)](#)
- [the section called “\[PCI.EC2.1\] 亚马逊 EBS 快照不应公开恢复” \(p. 323\)](#)
- [the section called “\[PCI.EC2.2\] VPC 默认安全组应禁止入站和出站流量” \(p. 325\)](#)
- [the section called “\[PCI.EC2.5\] 安全组不应允许从 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 进入端口 22” \(p. 327\)](#)
- [the section called “\[PCI.EC2.6\] 应在所有 VPC 中启用 VPC 流量记录” \(p. 328\)](#)
- [the section called “\[PCI.ELBV2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 329\)](#)
- [the section called “\[PCI.ES.1\] Elasticsearch 域应该在 VPC 中” \(p. 330\)](#)
- [the section called “\[PCI.ES.2\] Elasticsearch 域应启用静态加密” \(p. 332\)](#)
- [the section called “\[PCI。GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)
- [the section called “\[PCI.IAM.1\] IAM 根用户访问密钥不应存在” \(p. 333\)](#)
- [the section called “\[PCI.Lambda.2\] Lambda 函数应位于 VPC 中” \(p. 342\)](#)
- [the section called “\[PCI。OpenSearch.1\] 亚马逊 OpenSearch 服务域应位于 VPC 中” \(p. 343\)](#)
- [the section called “\[PCI。OpenSearch2\] OpenSearch 域应启用静态加密” \(p. 344\)](#)
- [the section called “\[PCI.RDS.1\] 亚马逊 RDS 快照应禁止公共访问” \(p. 345\)](#)
- [the section called “\[pci.redshift.1\] Amazon Redshift 集群应禁止公共访问” \(p. 348\)](#)
- [the section called “\[PCI。SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)
- [the section called “\[PCI.SSM.1\] 安装补丁后，由 Systems Manager 管理的 Amazon EC2 实例的补丁合规状态应为 “合规”” \(p. 357\)](#)
- [the section called “\[PCI.SSM.2\] 由 Systems Manager 管理的实例的关联合规状态应为 COMPLIANT” \(p. 358\)](#)
- [the section called “\[PCI.SSM.3\] EC2 实例应由以下人员管理Amazon Systems Manager” \(p. 359\)](#)
- [the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)
- [the section called “\[ApiGateway.1\] 应该启用 API Gateway REST 和 WebSocket API 日志记录” \(p. 365\)](#)
- [the section called “\[ApiGateway.2\] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证” \(p. 365\)](#)
- [the section called “\[ApiGateway.3\] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪” \(p. 366\)](#)

[the section called “\[ApiGateway.4\] API Gateway 应该与Amazon WAF Web ACL 相关联” \(p. 366\)](#)

[the section called “\[AutoScaling.2\] Auto Scaling 组应涵盖多个可用区” \(p. 368\)](#)

[the section called “\[AutoScaling.3\] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 \(IMDSv2\)” \(p. 369\)](#)

[the section called “\[AutoScaling.4\] Auto Scaling 组启动配置的元数据响应跳数限制不应大于1” \(p. 369\)](#)

[the section called “\[AutoScaling.5\] 使用 Auto Scaling 组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址” \(p. 370\)](#)

[the section called “\[AutoScaling.6\] Auto Scaling 组应在多个可用区中使用多个实例类型” \(p. 371\)](#)

[the section called “\[AutoScaling.9\] EC2 Auto Scaling 组应使用 EC2 启动模板” \(p. 372\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.1\] CodeBuild GitHub 或 Bitbucket 源存储库 URL 应使用 OAuth” \(p. 382\)](#)

[the section called “\[CodeBuild.2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 383\)](#)

[the section called “\[CodeBuild.4\] CodeBuild 项目环境应该有日志配置” \(p. 384\)](#)

[the section called “\[CodeBuild.5\] CodeBuild 项目环境不应启用特权模式” \(p. 384\)](#)

[the section called “\[DMS.1\]Amazon Database Migration Service 复制实例不应公开” \(p. 386\)](#)

[the section called “\[DynamoDB.2\] DynamoDB 表应启用 point-in-time 恢复功能” \(p. 387\)](#)

[the section called “\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) 集群应进行静态加密” \(p. 388\)](#)

[the section called “\[EC2.1\] Amazon EBS 快照不应公开，这取决于任何人都可恢复的可用性” \(p. 388\)](#)

[the section called “\[EC2.2\] VPC 默认安全组不应允许入站和出站流量 ” \(p. 389\)](#)

[the section called “\[EC2.3\] 附加的 EBS 卷应在静态时加密” \(p. 390\)](#)

[the section called “\[EC2.4\] 应在指定时间段后删除已停止的 EC2 实例” \(p. 390\)](#)

[the section called “\[EC2.6\] 应在所有 VPC 中启用 VPC 流量日志记录 ” \(p. 391\)](#)

[the section called “\[EC2.7\] 应启用 EBS 默认加密” \(p. 392\)](#)

[the section called “\[EC2.8\] EC2 实例应使用 imdsV2” \(p. 393\)](#)

[the section called “\[EC2.9\] EC2 实例不应有公有 IP 地址” \(p. 393\)](#)

[the section called “\[EC2.10\] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 终端节点” \(p. 394\)](#)

[the section called “\[EC2.15\] EC2 子网不应自动分配公有 IP 地址” \(p. 396\)](#)

[the section called “\[EC2.16\] 应删除未使用的网络访问控制列表” \(p. 397\)](#)

[the section called “\[EC2.17\] EC2 实例不应使用多个 ENI” \(p. 397\)](#)

[the section called “\[EC2.18\] 安全组应只允许授权端口不受限制的传入流量” \(p. 398\)](#)

[the section called “\[EC2.20\] Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.21\] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389” \(p. 400\)](#)

[the section called “\[EC2.22\] 应移除未使用的 EC2 安全组” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EC2.27\] 运行 EC2 实例不应使用密钥对 \(已停用 \) ” \(p. 403\)](#)

[the section called “\[ECR.1\] ECR 私有存储库应配置图像扫描” \(p. 403\)](#)

[the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)

[the section called “\[ECR.3\] ECR 存储库应至少配置一个生命周期策略” \(p. 404\)](#)

[the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)

[the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)

[the section called “\[ECS.5\] ECS 容器应限于对根文件系统的只读访问权限” \(p. 407\)](#)

[the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)

[the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)

[the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

[the section called “\[EFS.1\] 应将 Amazon EFS 配置为使用以下方法加密静态文件数据 Amazon KMS” \(p. 410\)](#)

[the section called “\[EFS.2\] 亚马逊 EFS 卷应包含在备份计划中” \(p. 410\)](#)

[the section called “\[EFS.3\] EFS 接入点应强制使用根目录” \(p. 411\)](#)

[the section called “\[ElasticBeanstalk.1\] Elastic Beanstalk 环境应启用增强型运行状况报告” \(p. 413\)](#)

[the section called “\[ElasticBeanstalk.2\] 应启用 Elastic Beanstalk 托管平台更新” \(p. 414\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书 Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.3\] Classic Load Balancer 侦听器应配置为 HTTPS 或 TLS 终止” \(p. 415\)](#)

[the section called “\[ELB.4\] 应将应用程序负载均衡器配置为删除 HTTP 标头” \(p. 416\)](#)

[the section called “\[ELB.6\] 应启用Application Load Balancer 删除保护” \(p. 417\)](#)

[the section called “\[ELB.8\] 带有 HTTPS/SSL 侦听器的经典负载均衡器应使用具有强配置的预定义安全策略” \(p. 418\)](#)

[the section called “\[ELB.9\] 经典负载均衡器应启用跨区域负载均衡” \(p. 419\)](#)

[the section called “\[ELB.10\] 经典负载均衡器应跨越多个可用区” \(p. 419\)](#)

[the section called “\[ELB.12\] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 420\)](#)

[the section called “\[ELB.13\] 应用程序、网络和网关负载均衡器应跨越多个可用区” \(p. 421\)](#)

[the section called “\[elbv2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 422\)](#)

[the section called “\[EMR.1\] Amazon EMR 集群主节点不应有公有 IP 地址” \(p. 423\)](#)

[the section called “\[ES.1\] Elasticsearch 域应启用静态加密” \(p. 423\)](#)

[the section called “\[ES.2\] Elasticsearch 域应该在 VPC 中” \(p. 424\)](#)

[the section called “\[ES.3\] Elasticsearch 域应加密节点之间发送的数据” \(p. 424\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[IAM.4\] IAM 根用户访问密钥不应存在” \(p. 431\)](#)

[the section called “\[IAM.21\] 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” \(p. 434\)](#)

[the section called “\[KMS.1\] IAM 客户托管策略不应允许对所有 KMS 密钥进行解密和重新加密操作” \(p. 436\)](#)

[the section called “\[KMS.2\] IAM 委托人不应有允许对所有 KMS 密钥进行解密和重新加密操作的 IAM 内联策略” \(p. 437\)](#)

[the section called “\[Lambda.5\] VPC Lambda 函数应在多个可用区中运行” \(p. 440\)](#)

[the section called “\[NetworkFirewall.3\] Network Firewall 策略应至少关联一个规则组” \(p. 441\)](#)

[the section called “\[NetworkFirewall.4\] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[NetworkFirewall.5\] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.1\] RDS 快照应为私有快照” \(p. 448\)](#)

[the section called “\[RDS.4\] 应对 RDS 集群快照和数据库快照进行静态加密” \(p. 450\)](#)

[the section called “\[RDS.6\] 应为 RDS 数据库实例和集群配置增强监控” \(p. 451\)](#)

[the section called “\[RDS.7\] RDS 群集应启用删除保护” \(p. 452\)](#)

[the section called “\[RDS.8\] RDS 数据库实例应启用删除保护” \(p. 453\)](#)

[the section called “\[RDS.9\] 应启用数据库日志记录” \(p. 453\)](#)

[the section called “\[RDS.10\] 应为 RDS 实例配置 IAM 身份验证” \(p. 456\)](#)

[the section called “\[RDS.11\] Amazon RDS 实例应启用自动备份” \(p. 456\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.13\] 应启用 RDS 自动次要版本升级” \(p. 458\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.16\] 应将 RDS 数据库集群配置为将标签复制到快照” \(p. 460\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[RDS.25\] RDS 数据库实例应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[Redshift.1\] Amazon Redshift 集群应禁止公共访问” \(p. 467\)](#)

[the section called “\[Redshift.2\] 与 Amazon Redshift 集群的连接应在传输过程中进行加密” \(p. 467\)](#)

[the section called “\[Redshift.3\] Amazon Redshift 集群应启用自动快照” \(p. 468\)](#)

[the section called “\[Redshift.7\] Amazon Redshift 集群应使用增强型 VPC 路由” \(p. 470\)](#)

[the section called “\[Redshift.8\] Amazon Redshift 集群不应使用默认的管理员用户名” \(p. 470\)](#)

[the section called “\[Redshift.9\] Redshift 集群不应使用默认的数据库名称” \(p. 471\)](#)

[the section called “\[S3.8\] 应在存储区级别启用 S3 阻止公有访问设置” \(p. 477\)](#)

[the section called “\[S3.10\] 启用版本控制的 S3 存储桶应配置生命周期策略” \(p. 478\)](#)

[the section called “\[S3.11\] S3 存储桶应启用事件通知” \(p. 478\)](#)

[the section called “\[S3.12\] 不应使用 S3 访问控制列表 \(ACL\) 来管理用户对存储区的访问” \(p. 479\)](#)

[the section called “\[S3.13\] S3 存储桶应配置生命周期策略” \(p. 480\)](#)

[the section called “\[SageMaker.1\] SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 480\)](#)

[the section called “\[SecretsManager.1\] Secrets Manager 密钥应启用自动轮换” \(p. 481\)](#)

[the section called “\[SecretsManager.2\] 配置为自动轮换的 Secrets Manager 密钥应成功轮换” \(p. 482\)](#)

[the section called “\[SecretsManager.3\] 移除未使用的 Secrets Manager 密钥” \(p. 483\)](#)

[the section called “\[SNS.1\] SNS 主题应使用以下方法进行静态加密 Amazon KMS” \(p. 484\)](#)

[the section called “\[SNS.2\] 应为发送到主题的通知消息启用传送状态日志功能” \(p. 485\)](#)

[the section called “\[SQS.1\] 应对 Amazon SQS 队列进行静态加密” \(p. 486\)](#)

[the section called “\[SSM.1\] EC2 实例应由以下人员管理Amazon Systems Manager” \(p. 486\)](#)

[the section called “\[SSM.2\] 由 Systems Manager 管理的所有 EC2 实例都应符合补丁要求” \(p. 487\)](#)

[the section called “\[SSM.3\] 由 Systems Manager 管理的实例的关联合规状态应为COMPLIANT” \(p. 488\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.2\] WAF 区域规则应至少具有一个条件” \(p. 491\)](#)

[the section called “\[WAF.3\] WAF 区域规则组应至少有一条规则” \(p. 491\)](#)

[the section called “\[WAF.4\] WAF Classic Regional Web ACL 应至少包含一个规则或规则组” \(p. 492\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区 (孟买)

亚太地区 (孟买) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区（大阪）

亚太地区（大阪）不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.12 — 确保不存在根用户访问密钥” \(p. 271\)](#)

[the section called “1.20 - 确保已创建支持角色来管理与 Amazon Support 相关的事件 ” \(p. 272\)](#)

[the section called “4.1 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 22 ” \(p. 308\)](#)

[the section called “4.2 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 3389 ” \(p. 308\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI。CodeBuild1\] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth” \(p. 317\)](#)

[the section called “\[PCI。CodeBuild2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 318\)](#)

[the section called “\[PCI.DMS.1\]Amazon Database Migration Service复制实例不应公开” \(p. 322\)](#)

[the section called “\[PCI.EC2.1\] 亚马逊 EBS 快照不应公开恢复” \(p. 323\)](#)

[the section called “\[PCI.EC2.5\] 安全组不应允许从 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 进入端口 22” \(p. 327\)](#)

[the section called “\[PCI.ELBV2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 329\)](#)

[the section called “\[PCI.ES.1\] Elasticsearch 域应该在 VPC 中” \(p. 330\)](#)

[the section called “\[PCI.ES.2\] Elasticsearch 域应启用静态加密” \(p. 332\)](#)

[the section called “\[PCI。GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.IAM.1\] IAM 根用户访问密钥不应存在” \(p. 333\)](#)

[the section called “\[PCI.Lambda.1\] Lambda 函数应禁止公共访问” \(p. 340\)](#)

[the section called “\[PCI.Lambda.2\] Lambda 函数应位于 VPC 中” \(p. 342\)](#)

[the section called “\[PCI.RDS.1\] 亚马逊 RDS 快照应禁止公共访问” \(p. 345\)](#)

[the section called “\[pci.redshift.1\] Amazon Redshift 集群应禁止公共访问” \(p. 348\)](#)

[the section called “\[PCI.S3.6\] 应启用 S3 阻止公有访问设置” \(p. 354\)](#)

[the section called “\[PCI。SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)

[the section called “\[PCI.SSM.1\] 安装补丁后，由 Systems Manager 管理的 Amazon EC2 实例的补丁合规状态应为 “合规”” \(p. 357\)](#)

[the section called “\[PCI.SSM.2\] 由 Systems Manager 管理的实例的关联合规状态应为 COMPLIANT” \(p. 358\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ApiGateway.2\] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证” \(p. 365\)](#)

[the section called “\[ApiGateway.3\] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪” \(p. 366\)](#)

[the section called “\[ApiGateway.4\] API Gateway 应该与Amazon WAF Web ACL 相关联” \(p. 366\)](#)

[the section called “\[AutoScaling.5\] 使用 Auto Scaling 组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址” \(p. 370\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.4\] CodeBuild 项目环境应该有日志配置” \(p. 384\)](#)

[the section called “\[CodeBuild.5\] CodeBuild 项目环境不应启用特权模式” \(p. 384\)](#)

[the section called “\[EC2.15\] EC2 子网不应自动分配公有 IP 地址” \(p. 396\)](#)

[the section called “\[EC2.16\] 应删除未使用的网络访问控制列表” \(p. 397\)](#)

[the section called “\[EC2.17\] EC2 实例不应使用多个 ENI” \(p. 397\)](#)

[the section called “\[EC2.18\] 安全组应只允许授权端口不受限制的传入流量” \(p. 398\)](#)

[the section called “\[EC2.20\]Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.22\] 应移除未使用的 EC2 安全组” \(p. 401\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)

[the section called “\[ECS.1\] Amazon ECS 任务定义应具有安全联网模式和用户定义” \(p. 404\)](#)

[the section called “\[ECS.2\] Amazon ECS 服务不应自动分配公有 IP 地址” \(p. 405\)](#)

[the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)

[the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)

[the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)

[the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)

[the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

[the section called “\[EFS.4\] EFS 接入点应强制使用用户身份” \(p. 412\)](#)

[the section called “\[EKS.2\] EKS 集群应该在支持的 Kubernetes 版本上运行” \(p. 412\)](#)

[the section called “\[ElasticBeanstalk.1\] Elastic Beanstalk 环境应启用增强型运行状况报告” \(p. 413\)](#)

[the section called “\[ElasticBeanstalk.2\] 应启用 Elastic Beanstalk 托管平台更新” \(p. 414\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书 Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.4\] 应将应用程序负载均衡器配置为删除 HTTP 标头” \(p. 416\)](#)

[the section called “\[ELB.8\] 带有 HTTPS/SSL 侦听器的经典负载均衡器应使用具有强配置的预定义安全策略” \(p. 418\)](#)

[the section called “\[ELB.9\] 经典负载均衡器应启用跨区域负载均衡” \(p. 419\)](#)

[the section called “\[IAM.4\] IAM 根用户访问密钥不应存在” \(p. 431\)](#)

[the section called “\[IAM.21\] 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” \(p. 434\)](#)

[the section called “\[KMS.1\] IAM 客户托管策略不应允许对所有 KMS 密钥进行解密和重新加密操作” \(p. 436\)](#)

[the section called “\[KMS.2\] IAM 委托人不应有允许对所有 KMS 密钥进行解密和重新加密操作的 IAM 内联策略” \(p. 437\)](#)

[the section called “\[KMS.3\] 不应无意中删除 Amazon KMS 密钥” \(p. 438\)](#)

[the section called “\[Lambda.2\] Lambda 函数应使用支持的运行时” \(p. 440\)](#)

[the section called “\[Lambda.5\] VPC Lambda 函数应在多个可用区中运行” \(p. 440\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.9\] 应启用数据库日志记录” \(p. 453\)](#)

[the section called “\[RDS.10\] 应为 RDS 实例配置 IAM 身份验证” \(p. 456\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.13\] 应启用 RDS 自动次要版本升级” \(p. 458\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[Redshift.3\] Amazon Redshift 集群应启用自动快照” \(p. 468\)](#)

[the section called “\[Redshift.7\] Amazon Redshift 集群应使用增强型 VPC 路由” \(p. 470\)](#)

[the section called “\[S3.8\] 应在存储区级别启用 S3 阻止公有访问设置” \(p. 477\)](#)

[the section called “\[SecretsManager.1\] Secrets Manager 密钥应启用自动轮换” \(p. 481\)](#)

[the section called “\[SecretsManager.3\] 移除未使用的 Secrets Manager 密钥” \(p. 483\)](#)

[the section called “\[SecretsManager.4\] Secrets Manager 密钥应在指定的天数内轮换” \(p. 483\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.3\] WAF 区域规则组应至少有一条规则” \(p. 491\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区 (首尔)

亚太地区 (首尔) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区（新加坡）

亚太地区（新加坡）不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区（悉尼）

亚太地区（悉尼）不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[Redshift.3\] Amazon Redshift 集群应启用自动快照” \(p. 468\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

亚太地区 (东京)

亚太地区 (东京) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

加拿大 (中部)

加拿大 (中部) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全局 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

中国 (北京)

中国 (北京) 不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.13 — 确保为根用户启用 MFA ” \(p. 271\)](#)

[the section called “1.14 — 确保为根用户启用硬件 MFA ” \(p. 271\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI。GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.IAM.4\] 应该为根用户启用硬件 MFA” \(p. 335\)](#)

[the section called “\[PCI.IAM.5\] 应该为根用户启用虚拟 MFA” \(p. 336\)](#)

[the section called “\[PCI.Lambda.1\] Lambda 函数应禁止公共访问” \(p. 340\)](#)

[the section called “\[PCI.Lambda.2\] Lambda 函数应位于 VPC 中” \(p. 342\)](#)

[the section called “\[PCI。SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ACM.1\] 导入的和 ACM 颁发的证书应在指定的时间段后续订” \(p. 364\)](#)

[the section called “\[ApiGateway.2\] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证” \(p. 365\)](#)

[the section called “\[ApiGateway.3\] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪” \(p. 366\)](#)

[the section called “\[ApiGateway.4\] API Gateway 应该与Amazon WAF Web ACL 相关联” \(p. 366\)](#)

[the section called “\[AutoScaling.2\] Auto Scaling 组应涵盖多个可用区” \(p. 368\)](#)

[the section called “\[AutoScaling.3\] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 \(IMDSv2\)” \(p. 369\)](#)

[the section called “\[AutoScaling.4\] Auto Scaling 组启动配置的元数据响应跳数限制不应大于1” \(p. 369\)](#)

[the section called “\[AutoScaling.6\] Auto Scaling 组应在多个可用区中使用多个实例类型” \(p. 371\)](#)

[the section called “\[AutoScaling.9\] EC2 Auto Scaling 组应使用 EC2 启动模板” \(p. 372\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.4\] CodeBuild 项目环境应该有日志配置” \(p. 384\)](#)

[the section called “\[CodeBuild.5\] CodeBuild 项目环境不应启用特权模式” \(p. 384\)](#)

[the section called “\[EC2.15\] EC2 子网不应自动分配公有 IP 地址” \(p. 396\)](#)

[the section called “\[EC2.16\] 应删除未使用的网络访问控制列表” \(p. 397\)](#)

[the section called “\[EC2.20\]Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.21\] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389” \(p. 400\)](#)

[the section called “\[EC2.22\] 应移除未使用的 EC2 安全组” \(p. 401\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EC2.27\] 运行 EC2 实例不应使用密钥对 \(已停用 \) ” \(p. 403\)](#)

[the section called “\[ECR.1\] ECR 私有存储库应配置图像扫描” \(p. 403\)](#)

[the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)

[the section called “\[ECR.3\] ECR 存储库应至少配置一个生命周期策略” \(p. 404\)](#)

[the section called “\[ECS.1\] Amazon ECS 任务定义应具有安全联网模式 and 用户定义” \(p. 404\)](#)

[the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)

[the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)

[the section called “\[ECS.5\] ECS 容器应限于对根文件系统的只读访问权限” \(p. 407\)](#)

[the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)

[the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)

[the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

[the section called “\[EFS.3\] EFS 接入点应强制使用根目录” \(p. 411\)](#)

[the section called “\[EFS.4\] EFS 接入点应强制使用用户身份” \(p. 412\)](#)

[the section called “\[EKS.2\] EKS 集群应该在支持的 Kubernetes 版本上运行” \(p. 412\)](#)

[the section called “\[ElasticBeanstalk.1\] Elastic Beanstalk 环境应启用增强型运行状况报告” \(p. 413\)](#)

[the section called “\[ElasticBeanstalk.2\] 应启用 Elastic Beanstalk 托管平台更新” \(p. 414\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书 Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.10\] 经典负载均衡器应跨越多个可用区” \(p. 419\)](#)

[the section called “\[ELB.12\] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 420\)](#)

[the section called “\[ELB.13\] 应用程序、网络和网关负载均衡器应跨越多个可用区” \(p. 421\)](#)

[the section called “\[ELB.14\] 经典负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 421\)](#)

[the section called “\[ES.3\] Elasticsearch 域应加密节点之间发送的数据” \(p. 424\)](#)

[the section called “\[ES.4\] 应启用 Elasticsearch 域错误记录到 CloudWatch 日志” \(p. 425\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[IAM.6\] 应该为根用户启用硬件 MFA” \(p. 432\)](#)

[the section called “\[IAM.21\] 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” \(p. 434\)](#)

[the section called “\[Kinesis.1\] Kinesis Data Streams 应该在静态时加密” \(p. 435\)](#)

[the section called “\[Lambda.1\] Lambda 函数策略应禁止公共访问” \(p. 439\)](#)

[the section called “\[Lambda.2\] Lambda 函数应使用支持的运行时” \(p. 440\)](#)

[the section called “\[Lambda.5\] VPC Lambda 函数应在多个可用区中运行” \(p. 440\)](#)

[the section called “\[NetworkFirewall.3\] Network Firewall 策略应至少关联一个规则组” \(p. 441\)](#)

[the section called “\[NetworkFirewall.4\] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[NetworkFirewall.5\] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.7\] RDS 群集应启用删除保护” \(p. 452\)](#)

[the section called “\[RDS.10\] 应为 RDS 实例配置 IAM 身份验证” \(p. 456\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.13\] 应启用 RDS 自动次要版本升级” \(p. 458\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.16\] 应将 RDS 数据库集群配置为将标签复制到快照” \(p. 460\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[RDS.25\] RDS 数据库实例应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[Redshift.7\] Amazon Redshift 集群应使用增强型 VPC 路由” \(p. 470\)](#)

[the section called “\[Redshift.8\] Amazon Redshift 集群不应使用默认的管理员用户名” \(p. 470\)](#)

[the section called “\[Redshift.9\] Redshift 集群不应使用默认的数据库名称” \(p. 471\)](#)

[the section called “\[S3.1\] 应启用 S3 阻止公有访问设置” \(p. 471\)](#)

[the section called “\[S3.8\] 应在存储区级别启用 S3 阻止公有访问设置” \(p. 477\)](#)

[the section called “\[S3.11\] S3 存储桶应启用事件通知” \(p. 478\)](#)

[the section called “\[S3.12\] 不应使用 S3 访问控制列表 \(ACL\) 来管理用户对存储区的访问” \(p. 479\)](#)

[the section called “\[S3.13\] S3 存储桶应配置生命周期策略” \(p. 480\)](#)

[the section called “\[SageMaker.1\] SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 480\)](#)

[the section called “\[SecretsManager.3\] 移除未使用的 Secrets Manager 密钥” \(p. 483\)](#)

[the section called “\[SecretsManager.4\] Secrets Manager 密钥应在指定的天数内轮换” \(p. 483\)](#)

[the section called “\[SNS.2\] 应为发送到主题的通知消息启用传送状态日志功能” \(p. 485\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.2\] WAF 区域规则应至少具有一个条件” \(p. 491\)](#)

[the section called “\[WAF.3\] WAF 区域规则组应至少有一条规则” \(p. 491\)](#)

[the section called “\[WAF.4\] WAF Classic Regional Web ACL 应至少包含一个规则或规则组” \(p. 492\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

中国 (宁夏)

中国 (宁夏) 不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.13 — 确保为根用户启用 MFA ” \(p. 271\)](#)

[the section called “1.14 — 确保为根用户启用硬件 MFA ” \(p. 271\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI. GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.IAM.4\] 应该为根用户启用硬件 MFA” \(p. 335\)](#)

[the section called “\[PCI.IAM.5\] 应该为根用户启用虚拟 MFA” \(p. 336\)](#)

[the section called “\[PCI.Lambda.1\] Lambda 函数应禁止公共访问” \(p. 340\)](#)

[the section called “\[PCI.Lambda.2\] Lambda 函数应位于 VPC 中” \(p. 342\)](#)

[the section called “\[PCI. SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ACM.1\] 导入的和 ACM 颁发的证书应在指定的时间段后续订” \(p. 364\)](#)

[the section called “\[ApiGateway.2\] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证” \(p. 365\)](#)

[the section called “\[ApiGateway.3\] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪” \(p. 366\)](#)

[the section called “\[ApiGateway.4\] API Gateway 应该与Amazon WAF Web ACL 相关联” \(p. 366\)](#)

[the section called “\[AutoScaling.2\] Auto Scaling 组应涵盖多个可用区” \(p. 368\)](#)

[the section called “\[AutoScaling.3\] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 \(IMDSv2\)” \(p. 369\)](#)

[the section called “\[AutoScaling.4\] Auto Scaling 组启动配置的元数据响应跳数限制不应大于1” \(p. 369\)](#)

[the section called “\[AutoScaling.6\] Auto Scaling 组应在多个可用区中使用多个实例类型” \(p. 371\)](#)

[the section called “\[AutoScaling.9\] EC2 Auto Scaling 组应使用 EC2 启动模板” \(p. 372\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.4\] CodeBuild 项目环境应该有日志配置” \(p. 384\)](#)

[the section called “\[CodeBuild.5\] CodeBuild 项目环境不应启用特权模式” \(p. 384\)](#)

[the section called “\[EC2.15\] EC2 子网不应自动分配公有 IP 地址” \(p. 396\)](#)

[the section called “\[EC2.16\] 应删除未使用的网络访问控制列表” \(p. 397\)](#)

[the section called “\[EC2.20\]Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.21\] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389” \(p. 400\)](#)

[the section called “\[EC2.22\] 应移除未使用的 EC2 安全组” \(p. 401\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EC2.27\] 运行 EC2 实例不应使用密钥对 \(已停用 \) ” \(p. 403\)](#)

[the section called “\[ECR.1\] ECR 私有存储库应配置图像扫描” \(p. 403\)](#)

[the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)

[the section called “\[ECR.3\] ECR 存储库应至少配置一个生命周期策略” \(p. 404\)](#)

[the section called “\[ECS.1\] Amazon ECS 任务定义应具有安全联网模式 and 用户定义” \(p. 404\)](#)

[the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)

[the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)

[the section called “\[ECS.5\] ECS 容器应限于对根文件系统的只读访问权限” \(p. 407\)](#)

[the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)

[the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)

[the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

[the section called “\[EFS.3\] EFS 接入点应强制使用根目录” \(p. 411\)](#)

[the section called “\[EFS.4\] EFS 接入点应强制使用用户身份” \(p. 412\)](#)

[the section called “\[EKS.2\] EKS 集群应该在支持的 Kubernetes 版本上运行” \(p. 412\)](#)

[the section called “\[ElasticBeanstalk.1\] Elastic Beanstalk 环境应启用增强型运行状况报告” \(p. 413\)](#)

[the section called “\[ElasticBeanstalk.2\] 应启用 Elastic Beanstalk 托管平台更新” \(p. 414\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.10\] 经典负载均衡器应跨越多个可用区” \(p. 419\)](#)

[the section called “\[ELB.12\] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 420\)](#)

[the section called “\[ELB.13\] 应用程序、网络和网关负载均衡器应跨越多个可用区” \(p. 421\)](#)

[the section called “\[ELB.14\] 经典负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 421\)](#)

[the section called “\[ES.3\] Elasticsearch 域应加密节点之间发送的数据” \(p. 424\)](#)

[the section called “\[ES.4\] 应启用 Elasticsearch 域错误记录到 CloudWatch 日志” \(p. 425\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[IAM.6\] 应该为根用户启用硬件 MFA” \(p. 432\)](#)

[the section called “\[IAM.21\] 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” \(p. 434\)](#)

[the section called “\[Kinesis.1\] Kinesis Data Streams 应该在静态时加密” \(p. 435\)](#)

[the section called “\[Lambda.1\] Lambda 函数策略应禁止公共访问” \(p. 439\)](#)

[the section called “\[Lambda.2\] Lambda 函数应使用支持的运行时” \(p. 440\)](#)

[the section called “\[Lambda.5\] VPC Lambda 函数应在多个可用区中运行” \(p. 440\)](#)

[the section called “\[NetworkFirewall.3\] Network Firewall 策略应至少关联一个规则组” \(p. 441\)](#)

[the section called “\[NetworkFirewall.4\] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[NetworkFirewall.5\] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.7\] RDS 群集应启用删除保护” \(p. 452\)](#)

[the section called “\[RDS.9\] 应启用数据库日志记录” \(p. 453\)](#)

[the section called “\[RDS.10\] 应为 RDS 实例配置 IAM 身份验证” \(p. 456\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.13\] 应启用 RDS 自动次要版本升级” \(p. 458\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[RDS.25\] RDS 数据库实例应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[Redshift.3\] Amazon Redshift 集群应启用自动快照” \(p. 468\)](#)

[the section called “\[Redshift.7\] Amazon Redshift 集群应使用增强型 VPC 路由” \(p. 470\)](#)

[the section called “\[Redshift.8\] Amazon Redshift 集群不应使用默认的管理员用户名” \(p. 470\)](#)

[the section called “\[Redshift.9\] Redshift 集群不应使用默认的数据库名称” \(p. 471\)](#)

[the section called “\[S3.1\] 应启用 S3 阻止公有访问设置” \(p. 471\)](#)

[the section called “\[S3.8\] 应在存储区级别启用 S3 阻止公有访问设置” \(p. 477\)](#)

[the section called “\[S3.11\] S3 存储桶应启用事件通知” \(p. 478\)](#)

[the section called “\[S3.12\] 不应使用 S3 访问控制列表 \(ACL\) 来管理用户对存储区的访问” \(p. 479\)](#)

[the section called “\[S3.13\] S3 存储桶应配置生命周期策略” \(p. 480\)](#)

[the section called “\[SageMaker.1\] SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 480\)](#)

[the section called “\[SecretsManager.3\] 移除未使用的 Secrets Manager 密钥” \(p. 483\)](#)

[the section called “\[SecretsManager.4\] Secrets Manager 密钥应在指定的天数内轮换” \(p. 483\)](#)

[the section called “\[SNS.2\] 应为发送到主题的通知消息启用传送状态日志功能” \(p. 485\)](#)

[the section called “\[WAF.1\] 应启用 Amazon WAF 经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.2\] WAF 区域规则应至少具有一个条件” \(p. 491\)](#)

[the section called “\[WAF.3\] WAF 区域规则组应至少有一条规则” \(p. 491\)](#)

[the section called “\[WAF.4\] WAF Classic Regional Web ACL 应至少包含一个规则或规则组” \(p. 492\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

欧洲 (法兰克福)

欧洲 (法兰克福) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

欧洲 (爱尔兰)

欧洲 (爱尔兰) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

欧洲 (伦敦)

欧洲 (伦敦) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

欧洲 (米兰)

欧洲 (米兰) 不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.4 — 确保每隔 90 天或更短时间轮换一次访问密钥 ” \(p. 267\)](#)

[the section called “1.20 - 确保已创建支持角色来管理与 Amazon Support 相关的事件 ” \(p. 272\)](#)

[the section called “4.1 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 22 ” \(p. 308\)](#)

[the section called “4.2 — 确保没有安全组允许从 0.0.0.0.0.0.0.0 进入端口 3389 ” \(p. 308\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI。CodeBuild1\] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth” \(p. 317\)](#)

[the section called “\[PCI。CodeBuild2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 318\)](#)

[the section called “\[PCI.DMS.1\]Amazon Database Migration Service复制实例不应公开” \(p. 322\)](#)

[the section called “\[PCI.EC2.1\] 亚马逊 EBS 快照不应公开恢复” \(p. 323\)](#)

[the section called “\[PCI.EC2.4\] 应删除未使用的 EC2 EIP” \(p. 326\)](#)

[the section called “\[PCI.EC2.5\] 安全组不应允许从 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 进入端口 22” \(p. 327\)](#)

[the section called “\[PCI.ELBV2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 329\)](#)

[the section called “\[PCI.GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.RDS.1\] 亚马逊 RDS 快照应禁止公共访问” \(p. 345\)](#)

[the section called “\[PCI.S3.6\] 应启用 S3 阻止公有访问设置” \(p. 354\)](#)

[the section called “\[PCI.SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)

[the section called “\[PCI.SSM.1\] 安装补丁后，由 Systems Manager 管理的 Amazon EC2 实例的补丁合规状态应为“合规”” \(p. 357\)](#)

[the section called “\[PCI.SSM.2\] 由 Systems Manager 管理的实例的关联合规状态应为 COMPLIANT” \(p. 358\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ACM.1\] 导入的和 ACM 颁发的证书应在指定的时间段后续订” \(p. 364\)](#)

[the section called “\[ApiGateway.1\] 应该启用 API Gateway REST 和 WebSocket API 日志记录” \(p. 365\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.1\] CodeBuild GitHub 或 Bitbucket 源存储库 URL 应使用 OAuth” \(p. 382\)](#)

[the section called “\[CodeBuild.2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 383\)](#)

[the section called “\[DMS.1\]Amazon Database Migration Service 复制实例不应公开” \(p. 386\)](#)

[the section called “\[EC2.1\] Amazon EBS 快照不应公开，这取决于任何人都可恢复的可用性” \(p. 388\)](#)

[the section called “\[EC2.3\] 附加的 EBS 卷应在静态时加密” \(p. 390\)](#)

[the section called “\[EC2.4\] 应在指定时间段后删除已停止的 EC2 实例” \(p. 390\)](#)

[the section called “\[EC2.8\] EC2 实例应使用 imdsV2” \(p. 393\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EFS.1\] 应将 Amazon EFS 配置为使用以下方法加密静态文件数据Amazon KMS” \(p. 410\)](#)

[the section called “\[EFS.2\] 亚马逊 EFS 卷应包含在备份计划中” \(p. 410\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.4\] 应将应用程序负载均衡器配置为删除 HTTP 标头” \(p. 416\)](#)

[the section called “\[ELB.8\] 带有 HTTPS/SSL 侦听器的经典负载均衡器应使用具有强配置的预定义安全策略” \(p. 418\)](#)

[the section called “\[elbv2.1\] 应将Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS” \(p. 422\)](#)

[the section called “\[EMR.1\] Amazon EMR 集群主节点不应有公有 IP 地址” \(p. 423\)](#)

[the section called “\[ES.3\] Elasticsearch 域应加密节点之间发送的数据” \(p. 424\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[IAM.3\] IAM 用户的访问密钥应每 90 天或更短时间轮换一次” \(p. 430\)](#)

[the section called “\[KMS.3\] 不应无意中删除Amazon KMS密钥” \(p. 438\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.1\] RDS 快照应为私有快照” \(p. 448\)](#)

[the section called “\[RDS.9\] 应启用数据库日志记录” \(p. 453\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[Redshift.2\] 与 Amazon Redshift 集群的连接应在传输过程中进行加密” \(p. 467\)](#)

[the section called “\[Redshift.3\] Amazon Redshift 集群应启用自动快照” \(p. 468\)](#)

[the section called “\[SageMaker.1\] SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 480\)](#)

[the section called “\[SSM.2\] 由 Systems Manager 管理的所有 EC2 实例都应符合补丁要求” \(p. 487\)](#)

[the section called “\[SSM.3\] 由 Systems Manager 管理的实例的关联合规状态应为COMPLIANT” \(p. 488\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

欧洲 (巴黎)

欧洲 (巴黎) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

欧洲 (斯德哥尔摩)

欧洲 (斯德哥尔摩) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

中东 (巴林)

中东 (巴林) 不支持以下控件。

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI。GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.S3.6\] 应启用 S3 阻止公有访问设置” \(p. 354\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[EC2.20\]Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[RDS.7\] RDS 群集应启用删除保护” \(p. 452\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.16\] 应将 RDS 数据库集群配置为将标签复制到快照” \(p. 460\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[Redshift.6\] Amazon Redshift 应该启用到主要版本的自动升级” \(p. 469\)](#)

[the section called “\[SSM.2\] 由 Systems Manager 管理的所有 EC2 实例都应符合补丁要求” \(p. 487\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

南美洲 (圣保罗)

南美洲 (圣保罗) 不支持以下控件。

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[RDS.7\] RDS 群集应启用删除保护” \(p. 452\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.16\] 应将 RDS 数据库集群配置为将标签复制到快照” \(p. 460\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

Amazon GovCloud (美国东部)

Amazon GovCloud (美国东部) 中不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.13 — 确保为根用户启用 MFA ” \(p. 271\)](#)

[the section called “1.14 — 确保为根用户启用硬件 MFA ” \(p. 271\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI. CodeBuild1\] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth” \(p. 317\)](#)

[the section called “\[PCI. CodeBuild2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 318\)](#)

[the section called “\[PCI. GuardDuty1\] GuardDuty 应启用” \(p. 332\)](#)

[the section called “\[PCI.IAM.4\] 应该为根用户启用硬件 MFA” \(p. 335\)](#)

[the section called “\[PCI.IAM.5\] 应该为根用户启用虚拟 MFA” \(p. 336\)](#)

[the section called “\[PCI. SageMaker.1\] 亚马逊 SageMaker 笔记本电脑实例不应直接访问互联网” \(p. 355\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ApiGateway.2\] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证” \(p. 365\)](#)

[the section called “\[ApiGateway.3\] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪” \(p. 366\)](#)

[the section called “\[ApiGateway.4\] API Gateway 应该与Amazon WAF Web ACL 相关联” \(p. 366\)](#)

[the section called “\[AutoScaling.2\] Auto Scaling 组应涵盖多个可用区” \(p. 368\)](#)

[the section called “\[AutoScaling.3\] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 \(IMDSv2\)” \(p. 369\)](#)

[the section called “\[AutoScaling.4\] Auto Scaling 组启动配置的元数据响应跳数限制不应大于1” \(p. 369\)](#)

[the section called “\[AutoScaling.5\] 使用 Auto Scaling 组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址” \(p. 370\)](#)

[the section called “\[AutoScaling.6\] Auto Scaling 组应在多个可用区中使用多个实例类型” \(p. 371\)](#)

[the section called “\[AutoScaling.9\] EC2 Auto Scaling 组应使用 EC2 启动模板” \(p. 372\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与 Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已 Amazon WAF 启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.1\] CodeBuild GitHub 或 Bitbucket 源存储库 URL 应使用 OAuth” \(p. 382\)](#)

[the section called “\[CodeBuild.2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 383\)](#)

[the section called “\[CodeBuild.4\] CodeBuild 项目环境应该有日志配置” \(p. 384\)](#)

[the section called “\[CodeBuild.5\] CodeBuild 项目环境不应启用特权模式” \(p. 384\)](#)

[the section called “\[DynamoDB.1\] DynamoDB 表应根据需求自动扩展容量” \(p. 386\)](#)

[the section called “\[EC2.15\] EC2 子网不应自动分配公有 IP 地址” \(p. 396\)](#)

[the section called “\[EC2.16\] 应删除未使用的网络访问控制列表” \(p. 397\)](#)

[the section called “\[EC2.17\] EC2 实例不应使用多个 ENI” \(p. 397\)](#)

[the section called “\[EC2.20\] Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.21\] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389” \(p. 400\)](#)

[the section called “\[EC2.22\] 应移除未使用的 EC2 安全组” \(p. 401\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EC2.27\] 运行 EC2 实例不应使用密钥对 \(已停用 \) ” \(p. 403\)](#)

[the section called “\[ECR.1\] ECR 私有存储库应配置图像扫描” \(p. 403\)](#)

[the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)

[the section called “\[ECR.3\] ECR 存储库应至少配置一个生命周期策略” \(p. 404\)](#)

[the section called “\[ECS.1\] Amazon ECS 任务定义应具有安全联网模式 and 用户定义” \(p. 404\)](#)

[the section called “\[ECS.2\] Amazon ECS 服务不应自动分配公有 IP 地址” \(p. 405\)](#)

[the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)

[the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)

[the section called “\[ECS.5\] ECS 容器应限于对根文件系统的只读访问权限” \(p. 407\)](#)

[the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)

[the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)

[the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

[the section called “\[EFS.2\] 亚马逊 EFS 卷应包含在备份计划中” \(p. 410\)](#)

[the section called “\[EFS.3\] EFS 接入点应强制使用根目录” \(p. 411\)](#)

[the section called “\[EFS.4\] EFS 接入点应强制使用用户身份” \(p. 412\)](#)

[the section called “\[EKS.2\] EKS 集群应该在支持的 Kubernetes 版本上运行” \(p. 412\)](#)

[the section called “\[ElasticBeanstalk.1\] Elastic Beanstalk 环境应启用增强型运行状况报告” \(p. 413\)](#)

[the section called “\[ElasticBeanstalk.2\] 应启用 Elastic Beanstalk 托管平台更新” \(p. 414\)](#)

[the section called “\[ELB.2\] 具有 HTTPS/SSL 侦听器的经典负载均衡器应使用提供的证书 Amazon Certificate Manager” \(p. 414\)](#)

[the section called “\[ELB.8\] 带有 HTTPS/SSL 侦听器的经典负载均衡器应使用具有强配置的预定义安全策略” \(p. 418\)](#)

[the section called “\[ELB.10\] 经典负载均衡器应跨越多个可用区” \(p. 419\)](#)

[the section called “\[ELB.12\] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 420\)](#)

[the section called “\[ELB.13\] 应用程序、网络 and 网关负载均衡器应跨越多个可用区” \(p. 421\)](#)

[the section called “\[ELB.14\] 经典负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 421\)](#)

[the section called “\[ES.4\] 应启用 Elasticsearch 域错误记录到 CloudWatch 日志” \(p. 425\)](#)

[the section called “\[GuardDuty.1\] GuardDuty 应启用” \(p. 428\)](#)

[the section called “\[IAM.6\] 应该为根用户启用硬件 MFA” \(p. 432\)](#)

[the section called “\[IAM.21\] 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” \(p. 434\)](#)

[the section called “\[Kinesis.1\] Kinesis Data Streams 应该在静态时加密” \(p. 435\)](#)

[the section called “\[Lambda.5\] VPC Lambda 函数应在多个可用区中运行” \(p. 440\)](#)

[the section called “\[NetworkFirewall.3\] Network Firewall 策略应至少关联一个规则组” \(p. 441\)](#)

[the section called “\[NetworkFirewall.4\] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[NetworkFirewall.5\] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.13\] 应启用 RDS 自动次要版本升级” \(p. 458\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[RDS.25\] RDS 数据库实例应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[Redshift.7\] Amazon Redshift 集群应使用增强型 VPC 路由” \(p. 470\)](#)

[the section called “\[Redshift.8\] Amazon Redshift 集群不应使用默认的管理员用户名” \(p. 470\)](#)

[the section called “\[Redshift.9\] Redshift 集群不应使用默认的数据库名称” \(p. 471\)](#)

[the section called “\[S3.1\] 应启用 S3 阻止公有访问设置” \(p. 471\)](#)

[the section called “\[S3.8\] 应在存储区级启用 S3 阻止公有访问设置” \(p. 477\)](#)

[the section called “\[S3.11\] S3 存储桶应启用事件通知” \(p. 478\)](#)

[the section called “\[S3.12\] 不应使用 S3 访问控制列表 \(ACL\) 来管理用户对存储区的访问” \(p. 479\)](#)

[the section called “\[S3.13\] S3 存储桶应配置生命周期策略” \(p. 480\)](#)

[the section called “\[SecretsManager.3\] 移除未使用的 Secrets Manager 密钥” \(p. 483\)](#)

[the section called “\[SecretsManager.4\] Secrets Manager 密钥应在指定的天数内轮换” \(p. 483\)](#)

[the section called “\[SNS.2\] 应为发送到主题的通知消息启用传送状态日志功能” \(p. 485\)](#)

[the section called “\[SSM.4\] SSM 文档不应公开” \(p. 489\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.2\] WAF 区域规则应至少具有一个条件” \(p. 491\)](#)

[the section called “\[WAF.3\] WAF 区域规则组应至少有一条规则” \(p. 491\)](#)

[the section called “\[WAF.4\] WAF Classic Regional Web ACL 应至少包含一个规则或规则组” \(p. 492\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

Amazon GovCloud (美国西部)

Amazon GovCloud (美国西部) 中不支持以下控件。

[the section called “CIS Amazon 基金会基准” \(p. 263\)](#)

[the section called “1.13 — 确保为根用户启用 MFA ” \(p. 271\)](#)

[the section called “1.14 — 确保为根用户启用硬件 MFA ” \(p. 271\)](#)

[the section called “PCI DSS” \(p. 310\)](#)

[the section called “\[PCI。CodeBuild1\] CodeBuild GitHub 或者 Bitbucket 源存储库 URL 应该使用 OAuth” \(p. 317\)](#)

[the section called “\[PCI。CodeBuild2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 318\)](#)

[the section called “\[PCI.IAM.4\] 应该为根用户启用硬件 MFA” \(p. 335\)](#)

[the section called “\[PCI.IAM.5\] 应该为根用户启用虚拟 MFA” \(p. 336\)](#)

[the section called “Amazon 基础安全最佳实践标准” \(p. 361\)](#)

[the section called “\[ApiGateway.2\] API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证” \(p. 365\)](#)

[the section called “\[ApiGateway.3\] API Gateway REST API 阶段应该启用Amazon X-Ray跟踪” \(p. 366\)](#)

[the section called “\[ApiGateway.4\] API Gateway 应该与Amazon WAF Web ACL 相关联” \(p. 366\)](#)

[the section called “\[AutoScaling.2\] Auto Scaling 组应涵盖多个可用区” \(p. 368\)](#)

[the section called “\[AutoScaling.3\] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 \(IMDSv2\)” \(p. 369\)](#)

[the section called “\[AutoScaling.4\] Auto Scaling 组启动配置的元数据响应跳数限制不应大于1” \(p. 369\)](#)

[the section called “\[AutoScaling.5\] 使用 Auto Scaling 组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址” \(p. 370\)](#)

[the section called “\[AutoScaling.6\] Auto Scaling 组应在多个可用区中使用多个实例类型” \(p. 371\)](#)

[the section called “\[AutoScaling.9\] EC2 Auto Scaling 组应使用 EC2 启动模板” \(p. 372\)](#)

[the section called “\[CloudFormation.1\] CloudFormation 堆栈应与Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)

[the section called “\[CloudFront.1\] CloudFront 发行版应配置默认根对象” \(p. 373\)](#)

[the section called “\[CloudFront.2\] CloudFront 发行版应启用原始访问身份” \(p. 374\)](#)

[the section called “\[CloudFront.3\] CloudFront 发行版在传输过程中应要求加密” \(p. 374\)](#)

[the section called “\[CloudFront.4\] CloudFront 发行版应配置原始故障转移” \(p. 374\)](#)

[the section called “\[CloudFront.5\] CloudFront 发行版应启用日志记录” \(p. 375\)](#)

[the section called “\[CloudFront.6\] CloudFront 发行版应该已Amazon WAF启用” \(p. 375\)](#)

[the section called “\[CloudFront.7\] CloudFront 发行版应使用自定义 SSL/TLS 证书” \(p. 376\)](#)

[the section called “\[CloudFront.8\] CloudFront 发行版应使用 SNI 来提供 HTTPS 请求” \(p. 376\)](#)

[the section called “\[CloudFront.9\] CloudFront 发行版应加密流向自定义源的流量” \(p. 377\)](#)

[the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)

[the section called “\[CodeBuild.1\] CodeBuild GitHub 或 Bitbucket 源存储库 URL 应使用 OAuth” \(p. 382\)](#)

[the section called “\[CodeBuild.2\] CodeBuild 项目环境变量不应包含明文证书” \(p. 383\)](#)

[the section called “\[CodeBuild.4\] CodeBuild 项目环境应该有日志配置” \(p. 384\)](#)

[the section called “\[CodeBuild.5\] CodeBuild 项目环境不应启用特权模式” \(p. 384\)](#)

[the section called “\[DynamoDB.1\] DynamoDB 表应根据需求自动扩展容量” \(p. 386\)](#)

[the section called “\[EC2.15\] EC2 子网不应自动分配公有 IP 地址” \(p. 396\)](#)

[the section called “\[EC2.16\] 应删除未使用的网络访问控制列表” \(p. 397\)](#)

[the section called “\[EC2.17\] EC2 实例不应使用多个 ENI” \(p. 397\)](#)

[the section called “\[EC2.20\] Amazon 站点到站点 VPN 连接的两个 VPN 隧道都应已启动” \(p. 400\)](#)

[the section called “\[EC2.21\] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389” \(p. 400\)](#)

[the section called “\[EC2.22\] 应移除未使用的 EC2 安全组” \(p. 401\)](#)

[the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)

[the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)

[the section called “\[EC2.27\] 运行 EC2 实例不应使用密钥对 \(已停用 \) ” \(p. 403\)](#)

[the section called “\[ECR.1\] ECR 私有存储库应配置图像扫描” \(p. 403\)](#)

[the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)

[the section called “\[ECR.3\] ECR 存储库应至少配置一个生命周期策略” \(p. 404\)](#)

[the section called “\[ECS.1\] Amazon ECS 任务定义应具有安全联网模式 and 用户定义” \(p. 404\)](#)

[the section called “\[ECS.2\] Amazon ECS 服务不应自动分配公有 IP 地址” \(p. 405\)](#)

[the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)

[the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)

[the section called “\[ECS.5\] ECS 容器应限于对根文件系统的只读访问权限” \(p. 407\)](#)

[the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)

[the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)

[the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

[the section called “\[EFS.2\] 亚马逊 EFS 卷应包含在备份计划中” \(p. 410\)](#)

[the section called “\[EFS.3\] EFS 接入点应强制使用根目录” \(p. 411\)](#)

[the section called “\[EFS.4\] EFS 接入点应强制使用用户身份” \(p. 412\)](#)

[the section called “\[EKS.2\] EKS 集群应该在支持的 Kubernetes 版本上运行” \(p. 412\)](#)

[the section called “\[ElasticBeanstalk.1\] Elastic Beanstalk 环境应启用增强型运行状况报告” \(p. 413\)](#)

[the section called “\[ElasticBeanstalk.2\] 应启用 Elastic Beanstalk 托管平台更新” \(p. 414\)](#)

[the section called “\[ELB.10\] 经典负载均衡器应跨越多个可用区” \(p. 419\)](#)

[the section called “\[ELB.12\] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 420\)](#)

[the section called “\[ELB.13\] 应用程序、网络和网关负载均衡器应跨越多个可用区” \(p. 421\)](#)

[the section called “\[ELB.14\] 经典负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 421\)](#)

[the section called “\[ES.4\] 应启用 Elasticsearch 域错误记录到 CloudWatch 日志” \(p. 425\)](#)

[the section called “\[IAM.6\] 应该为根用户启用硬件 MFA” \(p. 432\)](#)

[the section called “\[IAM.21\] 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” \(p. 434\)](#)

[the section called “\[Kinesis.1\] Kinesis Data Streams 应该在静态时加密” \(p. 435\)](#)

[the section called “\[Lambda.5\] VPC Lambda 函数应在多个可用区中运行” \(p. 440\)](#)

[the section called “\[NetworkFirewall.3\] Network Firewall 策略应至少关联一个规则组” \(p. 441\)](#)

[the section called “\[NetworkFirewall.4\] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[NetworkFirewall.5\] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)

[the section called “\[OpenSearch.1\] OpenSearch 域应启用静态加密” \(p. 444\)](#)

[the section called “\[OpenSearch.2\] OpenSearch 域应位于 VPC 中” \(p. 444\)](#)

[the section called “\[OpenSearch.3\] OpenSearch 域应加密节点之间发送的数据” \(p. 445\)](#)

[the section called “\[OpenSearch.4\] 应启用将 OpenSearch 域错误记录到 CloudWatch 日志” \(p. 445\)](#)

[the section called “\[OpenSearch.5\] OpenSearch 域应启用审核日志” \(p. 446\)](#)

[the section called “\[OpenSearch.6\] OpenSearch 域应至少有三个数据节点” \(p. 446\)](#)

[the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)

[the section called “\[OpenSearch.8\] 与 OpenSearch 域的连接应使用 TLS 1.2 进行加密” \(p. 447\)](#)

[the section called “\[RDS.12\] 应为 RDS 集群配置 IAM 身份验证” \(p. 457\)](#)

[the section called “\[RDS.13\] 应启用 RDS 自动次要版本升级” \(p. 458\)](#)

[the section called “\[RDS.14\] Amazon Aurora 集群应启用回溯功能” \(p. 459\)](#)

[the section called “\[RDS.15\] 应为多个可用区配置 RDS 数据库集群” \(p. 459\)](#)

[the section called “\[RDS.24\] RDS 数据库集群应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[RDS.25\] RDS 数据库实例应使用自定义管理员用户名” \(p. 466\)](#)

[the section called “\[Redshift.7\] Amazon Redshift 集群应使用增强型 VPC 路由” \(p. 470\)](#)

[the section called “\[Redshift.8\] Amazon Redshift 集群不应使用默认的管理员用户名” \(p. 470\)](#)

[the section called “\[Redshift.9\] Redshift 集群不应使用默认的数据库名称” \(p. 471\)](#)

[the section called “\[S3.1\] 应启用 S3 阻止公有访问设置” \(p. 471\)](#)

[the section called “\[S3.8\] 应在存储区级别启用 S3 阻止公有访问设置” \(p. 477\)](#)

[the section called “\[S3.11\] S3 存储桶应启用事件通知” \(p. 478\)](#)

[the section called “\[S3.12\] 不应使用 S3 访问控制列表 \(ACL\) 来管理用户对存储区的访问” \(p. 479\)](#)

[the section called “\[S3.13\] S3 存储桶应配置生命周期策略” \(p. 480\)](#)

[the section called “\[SecretsManager.3\] 移除未使用的 Secrets Manager 密钥” \(p. 483\)](#)

[the section called “\[SecretsManager.4\] Secrets Manager 密钥应在指定的天数内轮换” \(p. 483\)](#)

[the section called “\[SNS.2\] 应为发送到主题的通知消息启用传送状态日志功能” \(p. 485\)](#)

[the section called “\[SSM.4\] SSM 文档不应公开” \(p. 489\)](#)

[the section called “\[WAF.1\] 应启用Amazon WAF经典的全球 Web ACL 日志记录” \(p. 489\)](#)

[the section called “\[WAF.2\] WAF 区域规则应至少具有一个条件” \(p. 491\)](#)

[the section called “\[WAF.3\] WAF 区域规则组应至少有一条规则” \(p. 491\)](#)

[the section called “\[WAF.4\] WAF Classic Regional Web ACL 应至少包含一个规则或规则组” \(p. 492\)](#)

[the section called “\[WAF.6\] WAF 全局规则应至少具有一个条件” \(p. 493\)](#)

[the section called “\[WAF.7\] WAF 全局规则组应至少有一条规则” \(p. 493\)](#)

[the section called “\[WAF.8\] WAF 全球 Web ACL 应至少包含一个规则或规则组” \(p. 494\)](#)

禁用 SSecurity Hub

禁用 Amazon Security Hub，您可以使用 Security Hub 控制台或 Security Hub API

在以下情况下，您无法禁用 Security Hub：

- 您的帐户是组织的 Security Hub 指定管理员帐户。
- 您的帐户是受邀的 Security Hub 管理员帐户，并且您的成员帐户已启用。禁用 Security Hub 之前，必须取消关联所有成员帐户。请参阅 [the section called “取消成员帐户的关联” \(p. 45\)](#)。
- 您的帐户是成员帐户。在禁用 Security Hub 之前，必须先取消您的帐户与管理员帐户的关联。

对于组织帐户，只有管理员帐户可以取消关联成员帐户。请参阅 [the section called “取消成员帐户的关联” \(p. 41\)](#)。

对于手动邀请的帐户，管理员帐户或成员帐户均可取消关联成员帐户。请参阅 [the section called “取消成员帐户的关联” \(p. 45\)](#) 或 [the section called “取消与管理员帐户的关联” \(p. 47\)](#)。

当您为某个帐户禁用 Security Hub 时，它仅在当前区域被禁用。将不再为该区域的该帐户处理任何新的结果。

还会出现以下情况。

- 90 天后，您的现有发现和见解以及任何 Security Hub 配置设置都将被删除且无法恢复。

如果要保存现有发现，则必须先将其导出，然后才能禁用 Security Hub。有关更多信息，请参阅 [the section called “帐户操作对 Security Hub 数据的影响” \(p. 47\)](#)。

- 任何已启用的标准将被禁用。

禁用 Security Hub (控制台)

您可以从中禁用 Security Hub Amazon 管理控制台。

禁用 Security Hub (控制台)

1. 打开 Amazon Security Hub 控制台 <https://console.aws.amazon.com/securityhub/>。
2. 在导航窗格中，选择 Settings (设置)。
3. 在设置页面，选择普通的。
4. 下面禁用 Amazon Security Hub，选择禁用 Amazon Security Hub。然后选择禁用 Amazon Security Hub 再次。

禁用 Security Hub (Security Hub API) Amazon CLI)

要禁用 Security Hub，您可以使用 API 调用或 Amazon Command Line Interface。

要禁用 Security Hub (Security Hub API)，Amazon CLI)

- SSecurity Hub— 使用 [DisableSecurityHub](#) 操作。

- Amazon CLI— 在命令行处，运行[disable-security-hub](#)命令。

```
aws securityhub disable-security-hub
```


Amazon Security Hub 用户指南的文档历史记录

下表介绍对 Security Hub 文档的 Amazon 更新。

变更	说明	日期
Support Security Hub 公告 Amazon GovCloud (US)	现在，您可以通过 (美国东部) 和 Amazon GovCloud (美国西部) 的 Simple Notification Service (Amazon SNS) 订阅 Security Hub 公告，以接收有关 Security Hub 通知。Amazon GovCloud	2022 年 10 月 3 日
Amazon Security Hub 添加了新的安全控件	已启用 FSBP 标准的客户可以使用新的 Security Hub 控件 AutoScaling.9 。控件可能有 区域限制 。	2022 年 9 月 1 日
订阅 Security Hub 公告	现在，您可以使用 Amazon Service (Amazon SNS) 订阅 Security Hub 公告，以接收有关 Security Hub 通知。	2022 年 8 月 29 日
用于跨区域聚合的区域扩展	跨区域聚合现在可用于发现结果、查找更新和洞察 Amazon GovCloud (US)。	2022 年 8 月 2 日
新的第三方产品集成	Fortinet-ForticNP 是接收 Security Hub 调查结果的第三方集成，而 jFrog 是将发现结果发送到 Security Hub 的第三方集成。	2022 年 7 月 26 日
EC2.27 已退役	Security Hub 已停用 EC2.27-运行 EC2 实例不应使用密钥对，这是 Amazon 基础安全最佳实践 (FSBP) 标准中以前的控制措施。	2022 年 7 月 20 日
Lambda.2 不再支持 python3.6	Security Hub 不再支持 python3.6 作为 Lambda.2 的参数，Lambda.2 是 Amazon 基础安全最佳实践 (FSBP) 标准中的控件。	2022 年 7 月 19 日
Amazon Security Hub 增加了新的安全控件	启用 FSBP 标准的客户可以使用以下 36 个新的 Security Hub 控件。一些控件有 区域限制。 the section called “[AutoScaling.3] Auto Scaling 组应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)” (p. 369)	2022 年 6 月 22 日

- [the section called “\[AutoScaling.4\] Auto Scaling 组启动配置的元数据响应跳数限制不应大于1” \(p. 369\)](#)
- [the section called “\[AutoScaling.6\] Auto Scaling 组应在多个可用区中使用多个实例类型” \(p. 371\)](#)
- [the section called “\[CloudFormation.1\] CloudFormation 堆栈应与 Simple Notification Service \(SNS\) 集成” \(p. 372\)](#)
- [the section called “\[CloudFront.10\] CloudFront 发行版不应在边缘站点和自定义源之间使用过时的 SSL 协议” \(p. 377\)](#)
- [the section called “\[EC2.23\] EC2 传输网关不应自动接受 VPC 连接请求” \(p. 401\)](#)
- [the section called “\[EC2.24\] 不应使用半虚拟化 EC2 实例类型” \(p. 402\)](#)
- [the section called “\[EC2.27\] 运行 EC2 实例不应使用密钥对 \(已停用\)” \(p. 403\)](#)
- [the section called “\[ECR.1\] ECR 私有存储库应配置图像扫描” \(p. 403\)](#)
- [the section called “\[ECR.2\] ECR 私有存储库应配置标签不可变性” \(p. 403\)](#)
- [the section called “\[ECS.3\] ECS 任务定义不应共享主机的进程命名空间” \(p. 406\)](#)
- [the section called “\[ECS.4\] ECS 容器应以非特权方式运行” \(p. 406\)](#)
- [the section called “\[ECS.5\] ECS 容器应限于对根文件系统的只读访问权限” \(p. 407\)](#)
- [the section called “\[ECS.8\] 密钥不应作为容器环境变量传递” \(p. 408\)](#)
- [the section called “\[ECS.10\] Fargate 服务应该在最新的 Fargate 平台版本上运行” \(p. 408\)](#)
- [the section called “\[ECS.12\] ECS 集群应启用容器洞察” \(p. 409\)](#)

- [the section called “\[EFS.3\] EFS 接入点应强制使用根目录” \(p. 411\)](#)
- [the section called “\[EFS.4\] EFS 接入点应强制使用用户身份” \(p. 412\)](#)
- [the section called “\[EKS.2\] EKS 集群应该在支持的 Kubernetes 版本上运行” \(p. 412\)](#)
- [the section called “\[ELB.12\] 应用程序负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 420\)](#)
- [the section called “\[ELB.13\] 应用程序、网络和网关负载均衡器应跨越多个可用区” \(p. 421\)](#)
- [the section called “\[ELB.14\] 经典负载均衡器应配置为防御或最严格的不同步缓解模式” \(p. 421\)](#)
- [the section called “\[Kinesis.1\] Kinesis Data Streams 应该在静态时加密” \(p. 435\)](#)
- [the section called “\[NetworkFirewall.3\] Network Firewall 策略应至少关联一个规则组” \(p. 441\)](#)
- [the section called “\[NetworkFirewall.4\] 对于完整的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)
- [the section called “\[NetworkFirewall.5\] 对于分段数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发” \(p. 442\)](#)
- [the section called “\[OpenSearch.7\] OpenSearch 域应启用精细访问控制” \(p. 447\)](#)
- [the section called “\[Redshift.9\] Redshift 集群不应使用默认的数据库名称” \(p. 471\)](#)
- [the section called “\[S3.13\] S3 存储桶应配置生命周期策略” \(p. 480\)](#)
- [the section called “\[SNS.2\] 应为发送到主题的通知消息启用传送状态日志功能” \(p. 485\)](#)
- [the section called “\[WAF.2\] WAF 区域规则应至少具有一个条件” \(p. 491\)](#)

	• the section called "[WAF.3] WAF 区域规则组应至少有一条规则" (p. 491) • the section called "[WAF.4] WAF Classic Regional Web ACL 应至少包含一个规则或规则组" (p. 492) • the section called "[WAF.6] WAF 全局规则应至少具有一个条件" (p. 493) • the section called "[WAF.7] WAF 全局规则组应至少有一条规则" (p. 493) • the section called "[WAF.8] WAF 全球 Web ACL 应至少包含一个规则或规则组" (p. 494)	
AmazonSecurity Hub 支持新区域	Security Hub 现已在亚太地区（雅加达）推出。某些控件在此区域中不可用。	2022 年 6 月 7 日
改善了Security Hub 和Amazon安全中心之间的集成Amazon Config	Security Hub 用户可以将Amazon Config规则评估的结果视为 Security Hub 中的调查结果。	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Amazon Organizations，此功能允许您登录 Security Hub 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 并且现在 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相关的公司和产品名称	2022 年 4 月 1 日
在“Amazon基础安全最佳实践”标准中添加了新的控件	在“Amazon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
向 ASFF 添加了新的资源详细信息对象	向 ASFF 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	向AwsAutoScalingScalingGroup和添加了其他详细信息AwsCodeBuildProject。	2022 年 3 月 25 日
在“Amazon基础安全最佳实践”标准中添加了新的控件	在“Amazon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Amazon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、Amazon RDS、Amazon EC2、Elastic Load Balancing 和 CloudFront Amazon基础安全最佳实践标准添加了新的控件。还向 PCI DSS 添加了两个新的 OpenSearch 服务控件。	2022 年 2 月 15 日

向 ASFF 添加了新字段	添加了新字段：样本。	2022 年 1 月 26 日
添加了与的集成Amazon Health	Amazon Health使用 service-to-service 事件消息将结果发送到 Security Hub。	2022 年 1 月 19 日
添加了与的集成Amazon Trusted Advisor	Trusted Advisor将其检查结果作为 Security Hub 发现结果发送到 Security Hub。Security Hub 将其 Amazon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AvailabilityZones将MixedInstancesProfile添加到AwsAutoScalingAutoScalingGroup。已将 MetadataOptions 添加到 AwsAutoScalingLaunchConfiguration。已将 BucketVersioningConfiguration 添加到 AwsS3Bucket。	2022 年 1 月 12 日
更新了 ASFF 文档的输出	ASFF 属性的描述以前位于单个主题中。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
向 ASFF 添加了新的资源详细信息对象Amazon Network Firewall	对于Amazon Network Firewall，添加了以下资源详细信息对象：AwsNetworkFirewallFirewallAwsNetworkFireFirewallPolicy、和AwsNetworkFirewallRuleGroup。	2021 年 12 月 20 日
增加了对新版本的Amazon Inspector 的支持	Security Hub 与新版本的亚马逊 Inspector 以及亚马逊 InspectAmazon Inspector Classic 集成在一起。Amazon Inspector 与 Security Hub。	2021 年 11 月 29 日
更改了 EC2.19 的严重性	EC2.19 (安全组不应允许不受限制地访问高风险端口) 的严重性从“高”更改为“严重”。	2021 年 11 月 17 日
与的新集成Sonrai Dig	Security Hub 现在提供与的集成 Sonrai Dig。Sonrai Dig监控云环境以识别安全风险。Sonrai Dig将结果发送到 Security Hub。	2021 年 11 月 12 日
更新了 CIS 2.1 和 CloudTrail .1 控件的检查 (p. 561)	除了检查是否存在至少一条多区域 CloudTrail 跟踪外，CIS 2. CloudTrail 1 和 .1 现在还会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
增加了对 VPC 终端节点的支持	Security Hub 现已与 VPC 终端节点集成Amazon PrivateLink并支持 VPC 终端节点。	2021 年 11 月 3 日

在“Amazon基础安全最佳实践”标准中添加了控件	为Elastic Load Balancing (ELB.2 和 ELB.8) 和Amazon 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、Node.js 和 Ruby Web 开发框架)、5000 (Python Web 开发框架)、8088 (传统 HTTP 端口) 和 8888 (备用 HTTP 端口)	2021 年 10 月 27 日
添加了与 Logz.io Cloud 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、分析和响应安全威胁。Logz.io 接收来自 Security Hub 的调查结果。	2021 年 10 月 25 日
增加了对跨区域汇总结果的支持	跨区域聚合使您无需更改区域即可查看所有发现。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结果从关联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	已将查看者证书详细信息添加到AwsCloudFrontDistribution。向中添加了其他详细信息：AwsCodeBuildProject。已将负载均衡器属性添加到AwsElbV2LoadBalancer。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：AwsEc2VpcEndpointServiceAwsEcrRepositoryAwsEksCluster、AwsO	2021 年 10 月 8 日
从 Lambda.2 控件中移除了过时的运行时	在Amazon基础安全最佳实践标准中，从 [Lambda.2] 中删除dotnetcore2.1运行时。Lambda 函数应使用支持的运行时。	2021 年 10 月 6 日
Check Point 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 未更改。	2021 年 10 月 1 日
删除了与 Alcide 的集成 (p. 561)	与 Alcide KAudit 的集成已停止。	2021 年 9 月 30 日
更改了 EC2.19 的严重性	[EC2.19] 安全组不应允许不受限制地访问高风险端口的严重性已从“中”更改为“高”。	2021 年 9 月 30 日

中国区Amazon Organizations 现已支持与集成 (p. 561)	现已在中国 (北京) 和中国 (宁夏) 支持 Security Hub 与 Organizations 集成。	2021 年 9 月 20 日
S3.1 和 PCI.S3.6 控件的新 Amazon Config 规则 (p. 561)	S3.1 和 PCI.S3.6 均验证 Amazon S3 阻止公有访问设置是否已启用。这些控件的 Amazon 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 Lambda.2 控件中移除了过时的运行时	在 Amazon 基础安全最佳实践标准中，从 [Lambda.2] 中删除 nodejs10.x 和 ruby2.5 运行时。Lambda 函数应使用支持的运行时。	2021 年 9 月 13 日
更改了 CIS 2.2 控件的严重性	在 CIS Amazon 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
更新了 Amazon 基础安全最佳实践标准中的 ECS.1、Lambda.2 和 SSM.1	在 Amazon 基础安全最佳实践标准中，ECS.1 现在有一个 <code>SkipInactiveTaskDefinitions</code> 参数设置为 <code>true</code> 。这样可以确保该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，PCI.Lambda.2 控件现已排除 Lambda (PCI DSS) 标准中。@Edge	2021 年 9 月 7 日
添加了与集成 HackerOne Vulnerability Intelligence	Security Hub 现在提供与集成 HackerOne Vulnerability Intelligence。此集成将结果发送到 Security Hub。	2021 年 9 月 7 日
更新了 ASFF 中的资源详细信息对象	对于 <code>AwsKmsKey</code> ，已添加 <code>KeyRotationStatus</code> 。对于 <code>AwsS3Bucket</code> ，添加了 <code>AccessControlListBucketLoggingConfiguration</code> 、 <code>BucketNotificationConfiguration</code> 和 <code>BucketWebsiteConfiguration</code> 。	2021 年 9 月 2 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： <code>AwsAutoScalingLaunchConfiguration</code> 、 <code>AwsEc2VpnConnection</code> 和 <code>AwsEcrContainerImage</code> 。	2021 年 9 月 2 日
在 ASFF 中为该 Vulnerabilities 对象添加了细节	在 <code>Cvss</code> 、添加 <code>Adjustments</code> 和 <code>Source</code> 。在 <code>VulnerablePackages</code> ，添加了文件路径和包管理器。	2021 年 9 月 2 日

中国地区现在支持系统管理器资源管理器和 OpsCenter 集成 (p. 561)	Security Hub 现 OpsCenter 已在中国（北京）和中国（宁夏）推出。	2021 年 8 月 31 日
停用 Lambda.4 控件 (p. 561)	Security Hub 正在停用控件 [Lambda.4] Lambda 函数应配置死信队列。当控件停用后，它将不再显示在控制台上，而且 Security Hub 不会对其进行检查。	2021 年 8 月 31 日
停用 PCI.EC2.3 控件 (p. 561)	Security Hub 正在取消控件 [PCI.EC2.3] 应删除未使用的 EC2 安全组。当控件停用后，它将不再显示在控制台上，而且 Security Hub 不会对其进行检查。	2021 年 8 月 27 日
更改为 Security Hub 将发现结果发送到自定义操作的方式	现在，当您发现结果发送到自定义操作时，Security Hub 会在单独 Security Hub Findings - Custom Action 的事件中发送每个发现。	2021 年 8 月 20 日
为自定义 Lambda 运行时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 无法对自定义 Lambda 运行时执行检查。	2021 年 8 月 20 日
Amazon Firewall Manager 中国地区现已支持集成 (p. 561)	现已在中国（北京）和中国（宁夏）支持 Security Hub 与 Firewall Manager 集成。	2021 年 8 月 19 日
与新的集成 Caveonix Cloud 和 Forcepoint Cloud Security Gateway	Security Hub 现在提供与 Caveonix Cloud 和 Forcepoint Cloud Security Gateway 的集成。这两个集成，将结果发送到 Security Hub。	2021 年 8 月 10 日
向 ASFF 添加了新的 CompanyName、ProductName、和 Region 属性	在 ASFF 的顶层添加 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 或新 BatchUpdateFindings。在控制台上，查找过滤器使用这些新字段。在 API 中，CompanyName 和 ProductName 过滤器使用下面的属性 ProductFields。	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 <code>AwsRdsEventSubscription</code> 资源类型和资源详细信息。为资源类型添加了 <code>AwsEcsService</code> 资源详细信息。 为 <code>AwsElasticsearchDomain</code> 资源详细信息对象添加了属性。	2021 年 7 月 23 日
在“Amazon 基础安全最佳实践”标准中添加了控件	为 Amazon API Gateway (ApiGateway.5)、Amazon EC2 (EC2.19)、亚马逊 ECS (ECS.2)、Elastic Load Balancing (ELB.7)、亚马逊 OpenSearch 服务 (ES.5 到 ES.8)、亚马逊 RDS (Redshift.4) 和 Amazon SQS (SQS.1) 添加了新控件。	2021 年 7 月 20 日
在服务相关角色托管策略中移动了权限	在托管策略中移动了 <code>config:PutEvaluations</code> 权限 <code>AWSecurityHubServiceRolePolicy</code> ，使其应用于所有资源。	2021 年 7 月 14 日
在“Amazon 基础安全最佳实践”标准中添加了控件	为 Amazon API Gateway (ApiGateway.4)、亚马逊 CloudFront (CloudFront.CloudFront 5 和 .6)、Amazon EC2 (EC2.17 和 EC2.18)、亚马逊 ECS (ECS.1)、亚马逊 OpenSearch 服务 (ES.4)、亚马逊 RDS Amazon Identity and Access Management (RDS.15) 和 Amazon S3 (S3.8) 添加了新的控件。	2021 年 7 月 8 日
为控制结果添加了新的合规状态原因代码	<code>INTERNAL_SERVICE_ERROR</code> 表示出现未知错误。 <code>SNS_TOPIC_CROSS_ACCOUNT</code> 表示 SNS 主题由其他账户拥有。 <code>SNS_TOPIC_INVALID</code> 表示关联的 SNS 主题无效。	2021 年 7 月 6 日
添加了与集成 Amazon Chatbot	添加了与集成 Amazon Chatbot。Security Hub 将调查结果发送至 Amazon Chatbot。	2021 年 6 月 30 日
为服务相关角色托管策略添加了新权限	为托管策略添加了新权限， <code>AWSecurityHubServiceRolePolicy</code> 允许服务相关角色向提供评估结果 Amazon Config。	2021 年 6 月 29 日
ASFF 中新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 实例对象以列出关联的网络接口。为 API Gateway V2 阶段添加了客户端证书 ID。添加了 S3 存储桶的生命周期配置。	2021 年 6 月 24 日

更新了聚合控制状态和标准安全分数的计算 (p. 561)	Security Hub 现在每 24 小时计算一次总体控制状态和标准安全分数。对于管理员帐户，分数现在反映了每个帐户的每个控件是启用还是禁用。	2021 年 6 月 23 日
更新了有关 Security Hub 处理被暂停帐户的信息	添加了有关 Security Hub 如何处理被暂停的帐户的信息Amazon。	2021 年 6 月 23 日
添加了选项卡以显示个人管理员帐户的已启用和禁用控件	对于管理员帐户，标准详细信息页面上的主选项卡包含各个帐户的汇总信息。新的“为此帐户启用”和“为此帐户禁用”选项卡列出了个人管理员帐户启用或禁用的帐户。	2021 年 6 月 23 日
已 java8.a12 添加到的参数中Lambda.2	在Amazon基础安全最佳实践标准中，java8.a12添加到Lambda.2控件支持的运行时间中。	2021 年 6 月 8 日
与 MicroFocus ArcSight NETSCOUT 网络调查员的新集成	添加了与 MicroFocus ArcSight NETSCOUT 网络调查员的集成。MicroFocus ArcSight 接收来自 Security Hub 的结果。NETSCOUT 网络调查员将结果发送到 Security Hub	2021 年 6 月 7 日
添加了以下内容的详细信息AWSecurityHubServiceRolePolicy	更新了托管策略部分，添加了现有托管策略的详细信息AWSecurityHubServiceRolePolicy，Security Hub 服务相关角色使用该策略。	2021 年 6 月 4 日
与 Jira 服务管理的新集成	Jira 的Amazon服务管理连接器将调查结果发送到 Jira 并使用它们创建 Jira 问题。更新 Jira 问题后，Security Hub 中的相应发现也会更新。	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 CISAmazon Foundations 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 Sysdig Secure 的全新云集成	添加了与 Sysdig Secure 云端的集成。此集成将结果发送到 Security Hub。	2021 年 5 月 14 日

在“Amazon基础安全最佳实践”标准中添加了控件	为亚马逊 API Gateway (ApiGateway.2 和 ApiGateway.3)、Amazon CloudTrail (.CloudTrail 4 和 .CloudTrail 5)、Amazon EC2 (EC2.15 和 EC2.16)、Amazon Elastic Beanstalk (ElasticBeanstalk ElasticBeanstalk.1 和 .2)、Amazon Lambda 亚马逊 RDS (RDS.12 — RDS.14)、Amazon Redshift (Redshift.7)、Amazon Secrets Manager (.SecretsManager 3 和 SecretsManager.4) 和 Amazon WAF (WAF.1)。	2021 年 5 月 10 日
更新 GuardDuty 和 Amazon RDS 控件 (p. 561)	已将GuardDuty.1和的严重性PCI.GuardDuty.1从中更改为高。向。添加了一个databaseEngines参数RDS.8。	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 Amazon 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，为亚马逊 EventBridge 规则提供筛选值 (p. 561)	Security Hub EventBridge 规则的新预定义筛选模式提供了控制台字段，您可以使用这些字段来指定筛选器值。	2021 年 4 月 30 日
添加了与Amazon Systems Manager Explorer 的集成和 OpsCenter	Security Hub 现在支持与 Systems Manager Explorer 和 OpsCenter. 该集成接收来自安全中心的调查结果，并在Security Hub 更新这些发现。	2021 年 4 月 26 日
产品集成的新类型 (p. 561)	新的集成类型表示产品集成更新了从 Security Hub 收到的调查结果。UPDATE_FINDINGS_IN_SECURITY_HUB	2021 年 4 月 22 日
将“主账户”更改为“管理员帐户” (p. 561)	术语“主账户”已更改为“管理员帐户”。该术语也在 Security Hub 控制台和 API 中进行了更改。	2021 年 4 月 22 日
更新了 ApiGateway.1，将 HTTP 替换为 Websoc	更新了 ApiGateway.1 的标题、描述和补救措施。该控件现在检查 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 (p. 561)	现已在中国 (北京) 和中国 (宁夏) 区域推出 Security Hub 集成。 GuardDuty	2021 年 4 月 5 日

已添加nodejs14.x到 Lambda.2 控件支持的运行时中	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 在亚太地区 (大阪) 推出 (p. 561)	Security Hub 现已在亚太地区 (大阪) 区域推出。	2021 年 3 月 29 日
在查找详细信息中添加了查找提供者字段 (p. 561)	在查找结果详细信息面板上, 新的“查找提供者字段”部分包含可信度、重要性、相关调查结果、严重性和类型的查找提供者值。	2021 年 3 月 24 日
添加了从Amazon Macie 接收敏感发现的选项	现在可以将与 Macie 的集成配置为将敏感发现结果发送到 Security Hub。	2021 年 3 月 23 日
添加了有关过渡到使用Amazon Organizations进行账户管理的信息	对于拥有现有主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, 了解有关 Amazon S3 公共访问块配置的信息	在中Resources, 新的AwsS3AccountPublicAccessBlock资源类型和详细信息对象提供有关账户的 Amazon S3 公共访问块配置的信息。在AwsS3Bucket资源详细信息对象中, 该PublicAccessBlockConfiguration对象提供了 S3 存储桶的公共访问块配置。	2021 年 3 月 18 日
ASFF 中的新对象允许查找提供者更新特定字段	ASFF 中的新FindingProviderFields对象用于为Confidence、CriticalityRelatedFindingsSeverity、和提供值Types。BatchImportFindings只能使用更新原始字段BatchUpdateFindings。	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
为可用的合规状态代码增加了CONFIG_RETURNS_NOT_APPLICABLE值	对于NOT_AVAILABLE合规状态, 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
用于集成的新托管策略Amazon Organizations	新的托管策略为OrAWSSecurityHubOrganizationsAccess organizations 管理帐户和委派的 Security Hub 管理员帐户提供了所需的组织权限。	2021 年 3 月 15 日

托管策略和服务相关角色信息移至“安全”一章	有关托管策略的信息经过修订和扩展。托管策略信息和有关服务相关角色的信息均已移至“安全”一章。	2021 年 3 月 15 日
与 SecureCloud DB 的新集成	将 SecureCloud 数据库添加到第三方集成列表中。SecureCloudDB 是一种云原生数据库安全工具，可全面了解内部和外部安全态势和活动。SecureCloudDB 将结果发送到 Security Hub。	2021 年 3 月 4 日
修订了 CIS 1.1 和 CIS 3.1 — CIS 3.14 控制的严重性	CIS 1.1 和 CIS 3.1 — CIS 3.14 控制的严重性已更改为“低”。	2021 年 3 月 3 日
移除了 RDS.11 控件 (p. 561)	从“基础安全最佳实践”标准中移除了 RDS.11 控件。	2021 年 3 月 3 日
更新了 Turbot 的集成	Turbot 集成已更新，可以发送和接收结果。	2021 年 2 月 26 日
在“基础安全最佳实践”标准中添加了控件	为 Amazon API Gateway (ApiGateway.1)、Amazon EC2 (EC2.9 和 EC2.10)、Amazon Elastic File System (EFS.2)、亚马逊 OpenSearch 服务 (ES.2 和 ES.3)、Elastic Load Balancing (ELB.6Amazon KMS) 和 Amazon Key Management Service (KMS.3) 添加了新的控件。	2021 年 2 月 11 日
为 DescribeProducts API 添加了可选 ProductArn 过滤器	DescribeProducts API 操作现在包含一个可选 ProductArn 参数。该 ProductArn 参数用于标识要返回详细信息的特定产品集成。	2021 年 2 月 3 日
云存储安全与 Amazon S3 防病毒软件的新集成	与 Amazon S3 防病毒软件的集成将病毒扫描结果作为结果发送到 Security Hub。	2021 年 1 月 27 日
更新了主账户的安全分数计算流程	对于主账户，Security Hub 使用单独的流程来计算安全分数。新流程确保分数包含对成员账户启用但对主账户禁用的控件。	2021 年 1 月 21 日
ASFF 中的新字段和对象	添加了一个新 Action 对象来跟踪针对资源发生的操作。向 AwsEc2NetworkInterface 对象添加字段以跟踪 DNS 名称和 IP 地址。在资源详细信息中添加了一个新 AwsSsmPatchCompliance 对象。	2021 年 1 月 21 日

在“基础安全最佳实践”标准中添加了控件	为亚马逊 CloudFront (CloudFront.1 到 CloudFront 4)、Amazon DynamoDB (DynamoDB.1 到 DynamoDB.3)、Elastic Load Balancing (ELB.3 到 ELB.5)、亚马逊 RDS (Reds.9 到 Redshift.3 和 Redshift.6) 和 Amazon SNS (SNS.1) 添加了新控件。	2021 年 1 月 15 日
根据记录状态或合规性状态重置 workflow 状态	NEW 如果存档的调查结果处于活动状态，NOTIFIED 或者 RESOLVED 查找结果的合规性状态从、或，Security Hub 会自动 PASSED 将 workflow 状态从或重置为 NOT_AVAILABLE。FAILED WARNING 这些变化表明需要进一步调查。	2021 年 1 月 7 日
为基于控制的调查结果添加了 ProductFields 信息	对于由控件生成的调查结果，以 Amazon 安全查找格式 (ASFF) 添加了有关 ProductFields 对象内容的信息。	2020 年 12 月 29 日
托管洞察的更新	更改了洞察 5 的标题。添加了新的洞察 32，用于检查有可疑活动的 IAM 用户。	2020 年 12 月 22 日
对 IAM.7 和 Lambda.1 控件的更新	在“Amazon 基础安全最佳实践”标准中，更新了 IAM.7 的参数。更新了 Lambda.1 的标题和描述。	2020 年 12 月 22 日
扩展与 ServiceNow ITSM 的集成	ServiceNow ITSM 集成允许用户在收到 Security Hub 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 Security Hub 中的调查结果更新。	2020 年 12 月 11 日
与 Audit Manager 的新集成	Security Hub 现在提供与 Audit Manager 集成。该集成允许 Audit Manager 从 Security Hub 接收基于控制的调查结果。	2020 年 12 月 8 日
与 Aqua Security Kube-Bench	Security Hub 增加了与 Aqua Security Kube-Bench 的集成。此集成将结果发送到 Security Hub。	2020 年 11 月 24 日
云托管现已在中国区域推出	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	BatchImportFindings以前，您无法使用更新Confidence、CriticalityRelatedFindingsSeverity、和Types字段。现在，如果这些字段尚未由更新BatchUpdateFindings，则可以通过进行更新BatchImportFindings。它们一旦由更新BatchUpdateFindings，就无法通过进行更新BatchImportFindings。	2020 年 11 月 24 日
Security Hub 现已集成到Amazon Organizations	客户现在可以使用其Organizations 账户配置来管理成员账户。组织管理帐户指定Security Hub 管理员帐户，该管理员帐户决定在 Security Hub 中启用哪些组织帐户。手动邀请流程仍可用于非组织成员的账户。	2020 年 11 月 23 日
删除了大音量控件的单独查找列表格式 (p. 561)	当发现结果非常多时，控件的查找结果列表不再使用“调查结果”页面格式。	2020 年 11 月 19 日
新的和更新的第三方集成	Security Hub 现在支持与cloudtamer.io、3coreSec、Prowler和 StackRox Kubernetes Security的集成。IBM QRadar 不再发送调查结果。它只接收调查结果。	2020 年 10 月 30 日
添加了从控制详细信息页面下载发现结果列表的选项。	在控制详细信息页面上，一个新的下载选项允许您将查找结果列表下载到.csv文件中。下载的列表会考虑列表中的所有过滤器。如果您选择了特定的调查结果，则下载的列表仅包括这些发现。	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文件中。下载的列表会考虑列表中的所有过滤器。如果您选择了特定的控件，则下载的列表仅包含该控件。	2020 年 10 月 26 日
新的和更新的合作伙集成	Security Hub 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 云计算。同样来自帕洛阿尔托网络的 Demisto 现在是 Cortex XSOAR，Redlock 现在是 Prisma Cloud Enterprise。	2020 年 10 月 23 日
Security Hub 在中国（北京）和中国（宁夏）推出 (p. 561)	Security Hub 现已在中国（北京）和中国（宁夏）区域推出。	2020 年 10 月 21 日

修订了 ASFF 属性和第三方集成的格式 (p. 561)	ASFF 属性和合作伙伴集成 列表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	已启用标准的标准详细信息页面现在显示选项卡式控件列表。这些选项卡根据控制状态筛选控制列表。	2020 年 10 月 7 日
将 CloudWatch 事件替换为 EventBridge (p. 561)	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 forAmazon、Alcide Kaudit 和 Palo Alto Networks VM 系列进行了全新集成。	Security Hub 现已与 Blue Hexagon forAmazon、Alcide Kaudit 和 Palo Alto Networks VM 系列集成 Blue Hexagon forAmazon Kaud 将结果发送到 Security Hub。VM 系列接收来自 Security Hub 的调查结果。	2020 年 9 月 30 日
ASFF 中新的和更新的资源详细信息对象	为AwsApiGatewayRestApi、、 ~~2020年9月30日~~ StageAwsApiGatewayV2Ap和添加了新Resources.Details对象AwsRedshiftCluster。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参与者还是目标。	资源的ResourceRole属性表明该资源是查找活动的目标还是发现活动的实施者。有效值为 ACTOR 和 TARGET。	2020 年 9 月 30 日
在可用的Amazon服务集成中添加了Amazon Systems Manager补丁管理器	Amazon Systems Manager补丁管理器现已与Security Hub 集成。当客户队列中的实例不符合其补丁合规性标准时，Patch Manager 会将发现结果发送到 Security Hub。	2020 年 9 月 22 日
在“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控件：Amazon EC2 (EC2.7 和 EC2.8)、亚马逊 EMR (EMR.1)、IAM (IAM.8)、亚马逊 RDS (RDS.4 到 RDS.8)、Amazon S3 (S3.6) 和Amazon 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 策略的新上下文密钥	现在可以将 IAM 策略配置为在使用时限制对字段和字段值的访问BatchUpdateFindings。	2020 年 9 月 10 日
扩大了会员账户BatchUpdateFindings的访问权限	默认情况下，成员账户现在具有与主账户BatchUpdateFindings相同的访问权限。	2020 年 9 月 10 日

《基础安全最佳实践标准》Amazon 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)。新的控件检查 IAM 策略是否限制对Amazon KMS解密操作的访问。	2020 年 9 月 9 日
删除了账户级别的控制调查结果 (p. 561)	Security Hub 不再为控件生成账户级别的调查结果。仅生成资源级调查结果。	2020 年 9 月 1 日
ASFF 中的新PatchSummary对象	已将该PatchSummary对象添加到 ASFF 中。该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
重新设计的控制详细信息页面	控件的详细信息页面已重新设计。控制查找结果列表提供选项卡，允许您根据合规性状态快速筛选列表。您还可以快速查看被隐藏的发现。每个条目都提供对有关查找资源、Amazon Config规则和查找注释的其他详细信息的访问权限。	2020 年 8 月 28 日
发现结果的新筛选选项	要查找筛选器，您可以使用 is not 过滤器来查找字段值不等于筛选值的搜索结果。您可以使用 dos not bart with 来查找字段值不是以指定筛选器值开头的搜索结果。	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：AwsDynamoDbTableAwsEc2EipAwsIamPolicy、AwsIamUser、AwsRdsDb	2020 年 8 月 18 日
与 RSA Archer 的新集成	Security Hub 现已集成 RSA Archer。RSA Archer 接收来自 Security Hub	2020 年 8 月 18 日
新的“描述”字段 AwsKmsKey	在下面的AwsKmsKey对象中添加了一个Description字段Resources.Details。	2020 年 8 月 18 日
已将字段添加到 AwsRdsDbInstance	为下面的AwsRdsDbInstance对象添加了多个属性Resources.Details。	2020 年 8 月 18 日
更新了 Security Hub 如何确定控件的总体状态	对于没有发现结果的控件，状态为“无数据”而不是“未知”。控制状态包括账户级和资源级调查结果。控制状态不使用发现结果的工作流状态，除非忽略隐藏的调查结果。	2020 年 8 月 13 日
更新了 Security Hub 计算标准安全分数的方式	现在，在计算标准的安全分数时，Security Hub 会忽略状态为“无数据”的控件。安全分数是通过控件与已启用控件的比例，不包括没有数据的控件。	2020 年 8 月 13 日

在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 操作来配置此选项。	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。新对照的标识符是 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的新控件和更新的控件	在“基础安全最佳实践”标准中添加了新的控件。新对照组的标识符是 AutoScaling .1、DMS.1、EC2.4、EC2.6、S3.5 和 SSM.3。更新了 ACM.1 的标题并将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，该对象提供与调查结果相关的漏洞信息。	2020 年 7 月 1 日
ASFF 中适用于 Auto Scaling 组、EC2 卷和 EC2 VPC 的新Resource.Details对象	将AwsAutoScalingAutoScalingGroup、AwsEc2Volume、和AwsEc2Vpc对象添加到Resource.Details。	2020 年 7 月 1 日
ASFF 中的新NetworkPath对象	添加了NetworkPath对象，该对象提供与调查结果相关的网络路径的相关信息。	2020 年 7 月 1 日
在发现问题时Compliance.Status自动解决问题PASSED	对于来自控件的发现，如果Compliance.Status是PASSED，则 Security Hub 会自动设置Workflow.Status为RESOLVED。	2020 年 6 月 24 日
Amazon Command Line Interface (p. 561) 示例	为多个 Security Hub 任务添加了 Amazon CLI语法和示例。包括启用 Security Hub、管理见解、管理标准和控制、管理产品集成以及禁用 Security Hub。	2020 年 6 月 24 日
ASFF 中的新Severity.Original属性	添加了 Severity.Original 属性，该属性是来自结果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对象以获取有关控件状态的详细信息	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Amazon基础安全最佳实践标准	添加了新的Amazon基础安全最佳实践标准，这是一组控件，用于检测部署的账户和资源偏离安全最佳实践的情况。	2020 年 4 月 22 日

用于更新调查结果的工作流程状态的新控制台选项	添加了有关使用 Security Hub 控制台或 API 设置结果的工作流程状态的信息。	2020 年 4 月 16 日
用于客户更新调查结果的新BatchUpdateFindings API	添加了有关使用 BatchUpdateFindings 更新与某个结果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
对 SecuritAmazon y Finding (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结果。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
集成页面的更新	已更新以反映对 Integrations (集成) 页面的更改。对于每个集成，该页面现在显示集成类别以及每个集成是将发现结果发送到 Security Hub 还是接收来自 Security Hub 的发现。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：云托管人、FireEye Helix、Forcepoint CASB、Forcepoint DLP、Forcepoint NGFW、Rackspace Cloud Native SecurCognito y 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 (PCI DSS)	为支付卡行业数据安全标准 (PCI DSS) 添加了 Security Hub 安全标准 (PCI DSS)。启用此标准后，Security Hub 会自动检查与 PCI DSS 要求相关的控制措施。	2020 年 2 月 13 日
对 SecuritAmazon y Finding (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
禁用个人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
术语和概念更新	更新了一些描述并将新的术语添加到 术语和概念 。	2019 年 9 月 21 日
AmazonSecurity Hub 正式发布版本 (p. 561)	内容更新以反映预览期间对 Security Hub 做出的改进。	2019 年 6 月 25 日
为 CISAmazon 基础检查添加了补救措施	为 Security Hub 中Amazon支持的 安全标准 添加了补救步骤。	2019 年 4 月 15 日

[SAamazon ecurity Hub 预览版 \(p. 561\)](#)

发布了 Security Hub 用户指南的预览版。Amazon

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。