aws

用户指南

AWS Security Hub

AWS Security Hub: 用户指南

Table of Contents

什么是 AWS Security Hub？

AWS Security Hub 为您提供了 AWS 中安全状态的全面视图，可帮助您评测您的 AWS 环境是否符合安全行业标准和最佳实践。

Security Hub 可跨 AWS 账户、AWS 服务、和受支持的第三方产品收集安全数据，并可帮助您分析安全趋势，以及确定最高优先级的安全问题。

为了帮助您管理组织的安全状态，Security Hub 支持多种安全标准。其中包括由 AWS 制定的 AWS 基础安全最佳实践 (FSBP) 和外部合规性框架，如 Center for Internet Security (CIS)、支付卡行业数据安全标准 (PCI DSS) 和美国国家标准与技术研究所 (NIST)。每个标准都包含多个安全控件，每种控件都代表一种安全最佳实践。Security Hub 对安全控件进行检查并生成控件调查发现，以帮助您评测您是否符合安全最佳实践。

除了生成控制结果外，Security Hub 还会接收来自其他产品AWS 服务（例如亚马逊 GuardDuty、Amazon Inspector 和 Amazon Macie）和支持的第三方产品的调查结果。这使您可以通过单一窗格来解决各种与安全相关的问题。您还可以将 Security Hub 的调查发现发送到其他 AWS 服务 和受支持的第三方产品。

Security Hub 提供自动化功能，可帮助您对安全问题进行分类和修复。例如，当安全检查失败时，您可以使用自动化规则自动更新关键调查发现。您还可以利用与 Amazon 的集成 EventBridge 来触发对特定发现的自动响应。

主题

Security Hub 的优点

以下是 Security Hub 帮助您监控整个 AWS 环境中的合规性和安全状况的一些主要方法。

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 AWS 服务 和 AWS 合作伙伴产品中收集安全调查发现并确定其优先次序的工作。Security Hub 使用标准的调查发现格式 AWS 安全调查发现格式 (ASFF) 来处

理调查发现数据。这样就无需管理来自多种来源的多种格式的调查发现。Security Hub 还将各提供商的调查发现相关联，以帮助您确定其中最重要的几项的优先级。

根据最佳实践和标准进行自动安全检查

根据 AWS 最佳实践和行业标准，Security Hub 自动运行连续的账户级配置和安全检查。Security Hub 使用这些检查的结果来计算安全分数，并识别需要关注的特定账户和资源。

跨账户和提供商的结果的综合视图

Security Hub 将合并账户和提供商产品的安全调查发现，然后在 Security Hub 控制台上显示结果。您也可以通过 Security Hub API、AWS CLI 或软件开发工具包检索调查发现。通过全面了解您当前的安全性状态，您可以发现趋势、识别潜在问题并采取必要的补救措施。

自动调查发现更新和修复的能力

您可以创建自动化规则，根据您定义的标准修改或隐藏调查发现。Security Hub 还支持与亚马逊的集成 EventBridge。要自动修复特定调查发现，您可以定义在生成调查发现时要执行的自定义操作。例如，您可以配置自定义操作，将结果发送到票证系统或自动修复系统。

访问 Security Hub

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

在每个区域，您可以通过以下任一方式访问和使用 Security Hub：

Security Hub 控制台

AWS Management Console 是一个基于浏览器的界面，可用于创建和管理 AWS 资源。作为该控制台的一部分，Security Hub 控制台提供对您的 Security Hub 账户、数据和资源的访问权限。您可以使用 Security Hub 控制台执行 Security Hub 任务，包括查看调查发现、创建自动化规则、创建聚合区域等。

Security Hub API

Security Hub API 允许您以编程方式访问您的 Security Hub 账户、数据和资源。使用该 API，您可以直接向 Security Hub 发送 HTTPS 请求。有关使用 API 的信息，请参阅 AWS Security Hub API 参考。

AWS CLI

可以使用AWS CLI，在系统的命令行中运行命令来执行 Security Hub 任务。与使用控制台相比，在某些情况下使用命令行更快、更方便。如果要构建执行任务的脚本，命令行也会十分有用。有关安装和使用 AWS CLI 的更多信息，请参阅 AWS Command Line Interface 用户指南。

AWS SDK

AWS 提供由各种编程语言和平台（例如 Java、Go、Python、C++ 和 .NET）的库和示例代码组成的 SDK。这些软件开发工具包以您的首选语言提供对 Security Hub 和其他 AWS 服务 的便捷编程访问。它们还处理多个任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求。有关安装和使用 AWS SDK 的信息，请参阅在 AWS 上构建的工具。

> **Important**
>
> Security Hub 仅检测和整合启用 Security Hub 后生成的调查发现。它不会以追溯方式检测和合并在启用 Security Hub 前生成的安全调查发现。
> Security Hub 仅接收和处理您在账户中启用 Security Hub 的区域中的那些结果。
> 要完全符合 CIS AWS 基金会基准安全检查，您必须在所有受支持的 AWS 区域中启用 Security Hub。

相关服务

为了进一步保护您的 AWS 环境，可以考虑将其他 AWS 服务 与 Security Hub 结合使用。

有关发送或接收 Security Hub 调查发现的其他 AWS 服务 的列表，请参阅 AWS 服务 与 Sec AWS urity Hub 的集成。

Security Hub 使用 AWS Config 中与服务相关的规则对大多数控件执行安全检查。您必须启用 AWS Config 和记录 AWS Config 中的资源，Security Hub 才能生成大部分控件调查发现。有关更多信息，请参阅正在配置 AWS Config。

Security Hub 免费试用和定价

当您首次在 AWS 账户 中启用 Security Hub 时，这一账户会自动注册 30 天的 Security Hub 免费试用。

在免费试用期内使用 Security Hub 时，您需要为使用与 Security Hub 交互的其他服务（例如 AWS Config 项目）付费。对于仅通过 Security Hub 安全标准激活的 AWS Config 规则，您无需支付任何费用。

在免费试用期结束之前，您不必为使用 Security Hub 付费。

> **Note**
>
> 中国（北京）区域不支持免费试用 Security Hub。

查看使用详细信息和预计成本

Security Hub 提供使用信息，包括预计 30 天的 Security Hub 使用费用。使用详细信息包括免费试用的剩余时间。使用信息可以帮助您了解免费试用结束后 Security Hub 的费用可能是多少。免费试用结束后，还会提供使用信息。免费试用结束后，还可以查看使用信息。

显示使用信息（控制台）

1. 打开 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中的设置下，选择使用情况。

预计月度成本是将账户的 Security Hub 对于结果和安全检查的使用情况投射到 30 天的时段估算出来的。

使用信息和预估费用仅适用于当前账户和当前区域。在聚合区域中，使用信息和预估费用不包括关联区域。有关关联区域的更多信息，请参阅 the section called “如何执行跨区域聚合工作”。

定价详细信息

有关 Security Hub 如何对提取结果和安全检查收费的更多信息，请参阅 Security Hub 定价。

Security Hub 的概念

本主题介绍了 Sec AWS urity Hub 中的关键概念和术语，以帮助您开始使用该服务。

帐户

包含您的 AWS 资源的标准亚马逊 Web Services (AWS) 账户。您可以使用自己的帐户登录并启用 AWS Security Hub。

一个账户可以邀请其他账户启用 Security Hub，并在 Security Hub 中与该账户建立关联。接受成员资格邀请是可选的。如果邀请被接受，该账户成为管理员账户，而被添加的账户成为成员账户。管理员账户可以在其成员账户中查看结果。

如果您已注册 AWS Organizations，则您的组织会为该组织指定一个 Security Hub 管理员帐户。Security Hub 管理员账户能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。

管理员账户

Security Hub 中被授予查看相关成员账户结果权限的账户。

账户通过以下方式之一成为管理员账户：

- 该账户邀请其他账户在 Security Hub 中与其建立关联。当这些账户接受邀请时，它们就会成为成员账户，发送邀请的账户则成为他们的管理员账户。
- 该账户由组织管理账户指定为 Security Hub 管理员账户。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账户。账户不能既是管理员账户又是成员账户。

聚合区域

设置聚合区域允许您在单个控制面板 AWS 区域 中查看来自多个区域的安全发现。

聚合区域是您从中查看和管理调查发现的区域。结果将从关联区域汇总到聚合区域。调查发现的更新会跨区域复制。

在聚合区域中，安全标准、见解和结果页面包含来自所有关联区域的数据。

请参阅 跨区域聚合。

存档的结果

将 RecordState 设置为 ARCHIVED 的结果。将调查发现存档表明调查发现提供者认为该调查发现已不再相关。记录状态与工作流程状态是分开的，后者跟踪调查发现的调查状态。

结果提供者可以使用 Security Hub API 的 BatchImportFindings 操作来存档他们创建的调查发现。如果控件被禁用或相关资源被删除，根据以下其中一项标准，Security Hub 会自动归档控件的调查发现。

- 该调查发现在三到五天后才会更新（请注意，这是尽最大努力的结果且无法保证）。
- 关联的 AWS Config 评估结果将返回NOT_APPLICABLE。

默认情况下，存档的调查发现将从 Security Hub 控制台中的发现列表中排除。您可以更新筛选器以包括已存档的查找结果。

Security Hub API 的 GetFindings 操作会返回活动和存档的调查发现。您可以包含记录状态的筛选器。

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

AWS 安全调查结果格式 (ASFF)

Security Hub 聚合或生成的调查发现内容的标准化格式。 AWS 安全调查结果格式使您可以使用 Security Hub 来查看和分析由 AWS 安全服务、第三方解决方案或 Security Hub 本身在运行安全检查时生成的发现。有关更多信息，请参阅 AWS 安全调查结果格式 (ASFF)。

控件

为信息系统或组织规定的一种保护措施或对策，旨在保护信息的机密性、完整性和可用性并满足一组已定义的安全性要求。安全标准与控件集合相关联。

“安全控件”一词是指各类标准的具有单一控件 ID 和标题的控件。“标准控件”一词是指具有特定标准的控件 ID 和标题的控件。目前，Security Hub 仅支持 AWS GovCloud (US) Region 和中国区域的标准控件。所有其他区域均支持安全控件。

自定义操作

一种用于将选定结果发送到 Security Hub 的机制 EventBridge。先在 Security Hub 中创建一个自定义操作，然后将其链接到 EventBridge 规则。该规则定义在收到与自定义操作 ID 关联的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）”。

委派管理员账户 (Organizations)

在 Organizations 中，服务的委派管理员账户能够管理组织对服务的使用。

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

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

调查发现

安全检查或与安全相关的检测的可观察记录。完成控件的安全检查后，Security Hub 会生成调查发现。这些被称为“控件调查发现”。调查发现也可能来自第三方产品集成。

有关 Security Hub 中调查发现的更多信息，请参阅 调查发现。

> **Note**
>
> 调查结果将在最新更新后 90 天或创建日期后 90 天（如果未发生更新）被删除。要将发现的存储时间超过 90 天，您可以在中配置一条规则，将结果路由到您 EventBridge 的 Amazon S3 存储桶。

跨区域聚合

将关联区域的调查发现、见解、控件合规状态和安全评分汇总到聚合区域。然后，您可以查看聚合区域中的所有数据，并更新聚合区域的发现和见解。

请参阅 跨区域聚合。

调查发现摄取

将来自其他 AWS 服务和第三方合作伙伴提供商的调查结果导入 Security Hub。

调查发现摄取事件包括新调查发现和现有调查发现的更新。

见解

由聚合语句和可选的筛选器定义的相关结果的集合。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，以跟踪您的 AWS 环境和使用情况所特有的安全问题。有关更多信息，请参阅 洞察。

关联区域

启用跨区域聚合时，关联区域是将结果、见解、控件合规状态和安全评分汇总到聚合区域的区域。

在关联区域中，调查发现和见解页面仅包含该区域的调查发现。

请参阅 跨区域聚合。

成员账户

已授予管理员账户查看和处理其调查发现的权限的账户。

账户通过以下方式之一成为成员账户：

- 该账户接受来自其他账户的邀请。
- 对于组织账户，Security Hub 管理员账户将该账户启用为成员账户。

相关要求

与某个控件对应的一组行业或监管要求。

规则

一组自动化标准，用于评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

针对单一资源对规则 point-in-time 进行具体评估，结果为`PASSED`、`FAILED`、`WARNING`、或`NOT_AVAILABLE`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 成员资格的组织账户。

组织管理账户在每个区域指定 Security Hub 管理员账户。组织管理账户必须在所有区域选择相同的 Security Hub 管理员账户。

Security Hub 管理员账户也是组织中 Security Hub 的委派管理员账户。

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。控件可能与 Security Hub 中一个或多个支持的标准相关联。要了解更多关于 Security Hub 中的安全标准，请参阅 标准和控件。

严重性

分配给 Security Hub 控件的“严重性”确定了该控件的重要性。控件的严重性，可以为严重、高、中等、低或信息性。分配给控件调查发现的“严重性”等于控件本身的“严重性”。要了解 Security Hub 如何为控件分配“严重性”，请参阅 为控件调查发现分配严重性。

工作流状态

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。

启用 Security Hub 之前的建议

以下建议可以帮助您开始使用 AWS Security Hub。

与集成 AWS Organizations

AWS Organizations 是一项全球账户管理服务，使 AWS 管理员能够整合和集中管理多个 AWS 账户 组织单位 (OU)。它提供账户管理和整合账单功能，这些功能旨在满足预算、安全性和合规性需求。它不收取额外费用，并与多个集成 AWS 服务，包括Security Hub GuardDuty、Amazon和Amazon Macie。

为了帮助自动化和简化账户管理，我们强烈建议集成 Security Hub 和 AWS Organizations。如果您有多个组织使用 Security Hub，则可以与 Organi AWS 账户 zations 集成。

有关激活集成的说明，请参阅 将 Security Hub 与 AWS Organizations。

使用中心配置

在集成 Security Hub 和 Organization 时，您可以选择使用一项名为中心配置的功能来为组织设置和管理 Security Hub。我们强烈建议使用中心配置，因为其可让管理员为组织自定义安全范围。在适当情况下，委托管理员可以允许成员账户配置自己的安全范围设置。

中央配置允许委派管理员跨账户、OU 和配置 Security Hub AWS 区域。委托管理员通过创建配置策略来配置 Security Hub。在配置策略中，您可以指定以下设置：

- 启用还是禁用 Security Hub
- 哪些安全标准已启用和禁用
- 哪些安全控件已启用和禁用
- 是否自定义所选控件的参数

作为委托管理员，您可以为整个组织创建单一的配置策略，也可以为不同的账户和 OU 创建不同的配置策略。例如，测试账户和生产账户可以使用不同的配置策略。

使用配置策略的成员账户和 OU 是集中管理的，只能由委托管理员进行配置。委托管理员可以将特定的成员账户和 OU 指定为自行管理，从而使成员能够逐个区域配置自己的设置。

要了解有关中心配置的更多信息，请参阅中央配置的工作原理。

正在配置 AWS Config

AWS Security Hub 使用服务相关 AWS Config 规则对大多数控件执行安全检查。

要支持这些控制， AWS Config 必须在每个启用 Sec AWS 区域 urity Hub 的账户（包括管理员账户和成员账户）上启用这些控制。此外，对于每个启用的标准，都 AWS Config 必须配置为记录启用控件所需的资源。

我们建议您在启用 Security Hub 标准 AWS Config 之前开启资源记录功能。如果 Security Hub 在资源记录关闭时尝试运行安全检查，则检查会返回错误。

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

如果您启用了标准但尚未启用 AWS Config，Security Hub 会尝试按照以下计划创建 AWS Config 规则：

- 在您启用标准的当天
- 在您启用标准的第二天
- 在您启用标准的第三天
- 启用标准后 7 天（之后每隔 7 天持续启用一次）

如果您使用集中配置，则当您重新应用启用一个或多个标准的配置策略时，Security Hub 也会尝试创建 AWS Config 规则。

启用 AWS Config

如果您 AWS Config 尚未启用，则可以通过以下方式之一将其启用：

- 控制台或 AWS CLI — 您可以使用 AWS Config 控制台或手动启用 AWS Config AWS CLI。请参阅 AWS Config 开发人员指南中的 AWS Config入门。
- AWS CloudFormation 模板 — 如果要 AWS Config 在大量账户上启用，则可以使用 “启 AWS Config 用” CloudFormation 模板启用 AWS Config。要访问此模板，请参阅《AWS CloudFormation 用户指南》中的AWS CloudFormation StackSets 示例模板。
- Github 脚本 — Security Hub 提供的GitHub 脚本可为跨区域的多个账户启用安全中心。如果您尚未与 Organizations 集成，或者您拥有不属于您的组织的账户，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 AWS Config 为这些账户启用。

有关启用 AWS Config 以帮助您运行 Security Hub 安全检查的更多信息，请参阅优化 AWS ConfigAWS Security Hub 以有效管理您的云安全状况。

在中打开资源记录 AWS Config

当您 AWS Config 使用默认设置开启资源记录功能时，它会记录 AWS 区域 在其中 AWS Config 发现的所有支持的区域资源类型。您也可以配置 AWS 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局资源（如果您使用中心配置，我们建议将此区域作为您的主区域）。

如果您使用启用 CloudFormation StackSets AWS Config，我们建议您运行两个不同的版本 StackSets。运行一个 StackSet 以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球资源之外的所有资源。

您还可以使用快速设置（一项功能）在您的账户和区域 AWS Config 中快速配置资源记录。 AWS Systems Manager在快速设置过程中，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 AWS Systems Manager 用户指南中的 AWS Config 配置记录器。

如果聚合器中不记录 (IAM) 全球资源并启用了要求记录 IAM 全球资源的控制，则安全控制 Config.1 会为聚合器中的关联区域 AWS Identity and Access Management （主区域和完全不在查找聚合器中的区域）生成失败的调查结果。在关联区域中，Config.1 不检查是否记录了 IAM 全球资源。有关每个控件所需的资源列表，请参阅AWS Config 生成控制结果所需的资源。

如果您使用多账户脚本启用 Security Hub，它会自动为所有区域的所有资源（包括全球资源）启用资源记录。然后，您可以更新配置以仅在单个区域中记录全球资源。有关信息，请参阅《AWS Config 开发者指南》中的选择 AWS Config 记录哪些资源。

为了让 Security Hub 准确报告依赖于 AWS Config 规则的控件的调查结果，您必须启用相关资源的记录。有关控件及其相关 AWS Config 资源的列表，请参阅AWS Config 生成控制结果所需的资源。AWS Config 允许您在连续录制和每日记录资源状态变化之间进行选择。如果您选择每日记录，则在资源状态发生变化时， AWS Config 会在每 24 小时的周期结束时提供资源配置数据。如果没有任何更改，则不会传送任何数据。这可能会将变更触发的控件的 Security Hub 调查结果的生成延迟到 24 小时期限结束时完成。

> **Note**
>
> 要在安全检查后生成新的调查发现并避免过时的调查发现，您必须拥有足够的权限让附加到配置记录器的 IAM 角色评估底层资源。

费用注意事项

有关资源记录相关费用的详细信息，请参阅AWS Security Hub 定价和AWS Config 定价。

Security Hub 可能会通过更新 AWS Config 配置项目来影响您的`AWS::Config::ResourceCompliance`配置记录器成本。每当与 AWS Config 规则关联的 Security Hub 控件更改合规状态、启用或禁用或更新参数时，都可能发生更新。如果您仅将 AWS Config 配置记录器用于 Security Hub，并且不将此配置项目用于其他用途，我们建议您关闭 AWS Config 控制台中的录制或 AWS CLI。这可以降低您的 AWS Config 成本。您无需为安全检查记录 `AWS::Config::ResourceCompliance` 即可在 Security Hub 中工作。

启用 Security Hub

启用 AWS Security Hub 的方法有两种，分别是与 AWS Organizations 集成或手动启用。

在多账户和多区域环境中，我们强烈建议与 Organizations 集成。如果您有独立账户，则需要手动设置 Security Hub。

确认必要的权限

在注册 Amazon Web Services（AWS）之后，您必须启用 Security Hub 才能使用 Security Hub 的功能和特性。要使用 Security Hub，您必须设置权限，以便允许访问 Security Hub 控制台和 API 操作。为此，您或您的 AWS 管理员可以使用 AWS Identity and Access Management（IAM）附加名为 `AWSSecurityHubFullAccess` 的 AWS 托管策略到您的 IAM 身份。

要通过 Organizations 集成启用和管理 Security Hub，还应附加名为 `AWSSecurityHubOrganizationsAccess` 的 AWS 托管策略。

有关更多信息，请参阅AWS Sec AWS urity Hub 的托管策略。

启用 Security Hub 与 Organizations 的集成

要开始将 Security Hub 与 AWS Organizations 一起使用，组织的 AWS Organizations 管理账户将指定一个账户作为该组织的 Security Hub 委托管理员账户。Security Hub 会在指定区域中的委托管理员账户中自动启用。

选择您的首选方法，然后按照步骤指定委托管理员账户。

Security Hub console

要在引导阶段指定 Security Hub 的委托管理员

1. 打开 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 选择转到 Security Hub。系统会提示您登录到组织管理账户。
3. 在指定委托管理员页面的委托管理员账户部分，指定委托管理员账户。我们建议选择您为其他 AWS 安全与合规服务设置的相同委托管理员。
4. 选择添加委托管理员。

Security Hub API

从 Organizations 管理账户调用 `EnableOrganizationAdminAccount` API。提供 Security Hub 委派管理员账户的 AWS 账户 ID。

AWS CLI

从 Organizations 管理账户运行 `enable-organization-admin-account` 命令。提供 Security Hub 委派管理员账户的 AWS 账户 ID。

命令示例：

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

有关与 Organizations 集成的更多信息，请参阅将 Security Hub 与 AWS Organizations。

指定委托管理员后，我们建议您继续使用中心配置设置 Security Hub。控制台会提示您如何做。通过使用中心配置，您可以简化为组织启用和配置 Security Hub 的过程，并确保您的组织拥有足够的安全范围。

中心配置让委托管理员能够跨多个组织账户和区域自定义 Security Hub，而不必逐个区域配置。您可以为整个组织创建配置策略，也可以为不同的账户和 OU 创建不同的配置策略。这些策略指定了在关联账户中启用还是禁用 Security Hub，以及启用哪些安全标准和控件。

委托管理员可将账户指定为集中管理或自行管理。集中管理的账户只能由委托管理员配置。自行管理账户可以自行指定设置。

如果您不使用中心配置，则委托管理员配置 Security Hub 的能力将更为有限。有关更多信息，请参阅使用管理账户 AWS Organizations。

手动启用 Security Hub

如果您拥有独立账户或未与 AWS Organizations 集成，则必须手动启用 Security Hub。独立账户无法与 AWS Organizations 集成，必须使用手动启用。

手动启用 Security Hub 时，您可以指定一个 Security Hub 管理员账户并邀请其他账户成为成员账户。当潜在成员账户接受邀请时，管理员与成员的关系即已建立。

选择首选方法，然后按照以下步骤启用 Security Hub。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。

Security Hub console

1. 打开 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 首次打开 Security Hub 控制台时，选择前往 Security Hub。
3. 在欢迎页面上，安全标准部分列出了 Security Hub 支持的安全标准。

   选中标准的复选框即可将其启用，取消选中该复选框即可将其禁用。

   您可以随时启用或禁用标准或其各个控制。有关管理安全标准和控件的信息，请参阅 AWS Security Hub 中的安全控件和标准。
4. 选择 Enable Security Hub (启用 Security Hub)。

Security Hub API

调用 `EnableSecurityHub` API。从 API 中启用 Security Hub 时，它会自动启用以下默认安全标准：

- AWS 基础安全最佳实践
- Center for Internet Security（CIS）AWS 基金会基准 v1.2.0

如果您不想启用这些标准，请将 `EnableDefaultStandards` 设置为 `false`。

您也可以使用 `Tags` 参数为 hub 资源分配标签值。

AWS CLI

运行 `enable-security-hub`命令。要启用默认标准，请包括 `--enable-default-standards`。要不启用默认标准，请包括 `--no-enable-default-standards`。默认安全标准如下：

- AWS 基础安全最佳实践
- Center for Internet Security（CIS）AWS 基金会基准 v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

示例

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

多账户启用脚本

> **Note**
>
> 我们建议不要使用此脚本，而是使用中心配置在多个账户和区域中启用和配置 Security Hub。

GitHub 中的 Security Hub 多账户启用脚本允许您跨账户和区域启用 Security Hub。该脚本还自动执行向成员账户发送邀请并启用 AWS Config 的流程。

该脚本会自动为所有区域的所有资源（包括全球资源）启用资源记录。它不会将全球资源的记录限制在单个区域。

有一个相应的脚本可以跨账户和区域禁用 Security Hub。

启用 Security Hub 后的后续步骤

启用 Security Hub 后，我们建议启用对您的安全需求至关重要的安全标准和安全控件。启用控件后，Security Hub 开始运行安全检查并生成控件调查发现。您还可以利用 Security Hub 与其他 AWS 服务 和第三方解决方案之间的集成，在 Security Hub 中查看他们的调查发现。

中央配置的工作原理

中心配置是 Security Hub 的一项功能，可帮助您跨多个 AWS 账户 和 AWS 区域设置和管理 Security Hub。要使用集中配置，必须先集成 Security Hub 和 AWS Organizations。您可以通过创建组织并为该组织指定委托的 Security Hub 管理员账户来集成服务。

通过委托的 Security Hub 管理员账户，您可以指定如何在组织账户和跨区域的组织单元（OU）中配置 Security Hub 服务、安全标准和安全控件。只需几个步骤即可从一个主要区域（称为主区域）配置这些设置。如果您不使用中心配置，则必须在每个账户和区域中分别配置 Security Hub。

使用中心配置时，委托管理员可以选择要配置的账户和 OU。如果委托管理员将成员账户或 OU 指定为自行管理，则该成员可以在每个区域中单独配置自己的设置。如果委托管理员将成员账户或 OU 指定为集中管理，则只有委托管理员才能跨区域配置成员账户或 OU。您可以将组织中的所有账户和 OU 指定为集中管理、全部自行管理或两者兼而有之。

要配置集中管理的账户，委托管理员使用 Security Hub 配置策略。配置策略允许委托管理员指定是启用还是禁用 Security Hub，以及启用和禁用哪些标准和控件。它们还可以用来自定义某些控件的参数。

配置策略在主区域和所有关联区域生效。委托管理员在开始使用中心配置之前指定组织的主区域和关联区域。委托管理员可以为整个组织创建单个配置策略，也可以创建多个配置策略来为不同的账户和 OU 配置各种设置。

本部分提供中心配置概述。

中心配置的优势

中心配置的优势包括以下内容：

简化 Security Hub 服务和功能的配置

当您使用中心配置时，Security Hub 会引导您完成为组织配置安全最佳实践的过程。它还会将生成的配置策略自动部署到指定的账户和 OU。如果您已有 Security Hub 设置，例如自动启用新的安全控件，则可以将其用作配置策略的起点。此外，Security Hub 控制台上的配置页面会显示您的配置策略以及哪些账户和 OU 使用每种策略的实时摘要。

跨账户和区域进行配置

您可以使用中心配置跨多个账户和区域配置 Security Hub。这有助于确保组织的每个部分都保持一致的配置和足够的安全覆盖。

在不同的账户和 OU 中适配不同的配置

通过中心配置，您可以选择以不同的方式配置组织的账户和 OU。例如，您的测试账户和生产账户可能需要不同的配置。您还可以创建配置策略，以在新账户加入组织后涵盖这些新账户。

防止配置偏差

当用户对与委托管理员的选择冲突的服务或功能进行更改时，会发生配置偏差。中心配置可防止这种偏差。当您将账户或 OU 指定为集中管理时，只能由该组织的委托管理员对其进行配置。如果您希望特定账户或 OU 自行配置设置，则可以将其指定为自行管理。

谁应该使用中心配置？

对于包含多个 Security Hub 帐户的 AWS 环境，集中配置最有利。它旨在帮助您集中管理多个账户的 Security Hub。

您可以使用中心配置来配置 Security Hub 服务、安全标准和安全控件。您也可以使用它来自定义某些控件的参数。有关标准和控件的信息，请参阅Security Hub 中的 AWS 安全控制和标准。

中心配置术语和概念

了解以下关键术语和概念可以帮助您使用 Security Hub 中心配置。

中心配置

Security Hub 的一项功能，可帮助组织委托的 Security Hub 管理员账户跨多个账户和区域配置 Security Hub 服务、安全标准和安全控件。要配置这些设置，委托管理员为其组织中的集中管理账户创建并管理 Security Hub 配置策略。自行管理账户可以在每个区域单独配置自己的设置。要使用集中配置，必须集成 Security Hub 和 AWS Organizations。

主区域

委托管理员通过创建和管理配置策略 AWS 区域 从中集中配置 Security Hub。配置策略在主区域和所有关联区域生效。

主区域还充当 Security Hub 聚合区域，接收来自关联区域的发现、见解和其他数据。

在 2019 年 3 月 20 日当天或之后 AWS 推出的区域被称为选择加入区域。选择加入区域不能是主区域，但可以是关联区域。有关选择加入区域的列表，请参阅《AWS 账户管理参考指南》中的启用和禁用区域之前的注意事项。

关联区域

AWS 区域 可以从家乡区域进行配置。配置策略由主区域的委托管理员创建。这些策略在主区域和所有关联的区域生效。您必须指定至少一个关联区域才能使用中心配置。

关联区域还会将调查发现、见解和其他数据发送到主区域。

在 2019 年 3 月 20 日当天或之后 AWS 推出的区域被称为选择加入区域。必须先为账户启用这样的区域，然后才能对其应用配置策略。组织管理账户可以为成员账户启用选择加入区域。有关更多信息，请参阅《账户管理参考指南》中的指定 AWS 区域 您的AWS 账户可以使用哪个账户。

Security Hub 配置策略

一组 Security Hub 设置，委托管理员可以为集中管理的账户配置这些设置。这包括：

- 是启用还是禁用 Security Hub。
- 是否启用一个或多个安全标准。
- 在已启用的标准中启用哪些安全控件。委托管理员可以通过提供应启用的特定控件列表来实现此目的，Security Hub 会禁用所有其他控件（包括在新控件发布时直接禁用）。或者，委托管理员可以提供应禁用的特定控件列表，并且 Security Hub 会启用所有其他控件（包括在新控件发布时直接启用）。
- （可选）在已启用的标准中为选定的已启用控件自定义参数。

配置策略在与至少一个账户、组织单元（OU）或根关联后，将在主区域和所有关联区域中生效。

在 Security Hub 控制台上，委托管理员可以选择 Security Hub 推荐的配置策略或创建自定义配置策略。使用 Security Hub API 和 AWS CLI，委托的管理员只能创建自定义配置策略。委托管理员最多可以创建 20 个自定义配置策略。

在推荐的配置策略中，Security Hub、 AWS 基础安全最佳实践（FSBP）标准以及所有现有和新的 FSBP 控件均已启用。接受参数的控件使用默认值。推荐的配置策略适用于整个组织。

要对组织应用不同的设置，或者将不同的配置策略应用于不同的账户和 OU，请创建自定义配置策略。

本地配置

在集成 Security Hub 和之后，组织的默认配置类型 AWS Organizations。通过本地配置，委托管理员可以选择在当前区域的新组织账户中自动启用 Security Hub 和默认安全标准。如果委托管理员自动启用默认标准，则属于这些标准的所有控件也会自动启用，附带新组织账户的默认参数。这些设置不适用于现有账户，因此账户加入组织后可能会出现配置偏差。必须分别在每个账户和区域中禁用属于默认标准的特定控件以及配置其他标准和控件。

本地配置不支持使用配置策略。要使用配置策略，必须切换到中心配置。

手动账户管理

如果您未将 Security Hub 与 Security Hub 集成， AWS Organizations 或者您拥有独立账户，则必须在每个地区分别为每个账户指定设置。手动账户管理不支持使用配置策略。

中心配置 API

只有 Security Hub 委托的 Security Hub 管理员才能使用的 Security Hub 操作，可用于在主区域中集中管理账户的配置策略。操作包括：

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

特定于账户的 API

Security Hub 操作，可用于 account-by-account 根据需要启用或禁用 Security Hub、标准和控件。这些操作用于每个单独的区域。

自行管理账户可以使用特定于账户的操作来配置自己的设置。集中管理的账户不能在主区域和关联区域使用以下特定于账户的操作。在这些区域中，只有委托管理员才能通过中心配置操作和配置策略对集中管理的账户进行配置。

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

要查看账户状态，集中管理的账户的所有者可以使用 Security Hub API 的任何`Get`或`Describe`操作。

如果您使用本地配置或手动账户管理，而不是中心配置，则可以使用这些特定于账户的操作。

自行管理的账户也可以使用`*Invitations`和`*Members`操作。但是，我们建议自行管理的账户不要使用这些操作。如果成员账户的成员与委派的管理员属于不同的组织，则策略关联可能会失败。

组织部门（OU）

在 an AWS Organizations d Security Hub 中，一个容器可以容纳一群人 AWS 账户。组织单元（OU）还可以包含其他 OU，这使您能够创建类似于倒置树的层次结构，父 OU 位于顶部，OU 分支向下延伸，结束于作为树叶的账户。一个 OU 有且仅有一个父级，账户可能是且仅是一个 OU 的成员。

您可以在 AWS Organizations 或中管理 OU AWS Control Tower。有关更多信息，请参阅《AWS Organizations 用户指南》中的管理组织单元 或《AWS Control Tower 用户指南》中的使用 AWS Control Tower管理组织和账户。

委托管理员可以将配置策略与特定账户或 OU 关联，或者将配置策略与根关联以涵盖组织中的所有账户和 OU。

集中管理

只有委托管理员才能使用配置策略跨区域配置的账户、OU 或根。

委托管理员账户指定是否集中管理账户。委托管理员还可以将账户的状态从集中管理更改为自行管理，或者从自行管理更改为集中管理。

自行管理

管理自己的 Security Hub 设置的账户、组织单元或根。自行管理账户使用特定于账户的操作在每个区域中为自己单独配置 Security Hub。这与集中管理的账户形成鲜明对比，后者只能由委托管理员通过配置策略跨区域进行配置。

委托管理员账户指定账号是否为自行管理账户。委托管理员账户也可以将账户的状态从自行管理更改为集中管理，或者从集中管理更改为自行管理。

委托管理员可以对账户或 OU 应用自行管理行为。或者，账户或 OU 可以继承父代的自行管理行为。委托管理员账户本身可以是自行管理账户。

配置策略关联

配置策略与账户、组织单元（OU）或根之间的链接。当存在策略关联时，账户、OU 或根将使用配置策略定义的设置。在以下任一情况下都存在关联：

- 当委托管理员直接将配置策略应用于账户、OU 或根时
- 当账户或 OU 从父 OU 或根继承配置策略时

在应用或继承不同的配置之前，关联一直存在。

应用的配置策略

一种配置策略关联，在这种关联中，委托管理员将配置策略直接应用于目标账户、OU 或根。目标按照配置策略定义的方式进行配置，只有委托管理员才能更改其配置。如果应用于根，则该配置策略会影响组织中所有未使用不同配置（通过应用或来自最接近的父级的继承）的账户和 OU。

委托管理员还可以将自行管理的配置应用于特定账户、OU 或根。

继承的配置策略

一种配置策略关联，在这种关联中，账户或 OU 采用最近的父 OU 或根的配置。如果配置策略未直接应用于账户或 OU，则它会继承最近的父级的配置。策略的所有元素都是继承的。换句话说，账户或 OU 不能选择仅继承策略中自己选择的一部分内容。如果最近的父级是自行管理的，则子账户或 OU 将继承父级的自行管理行为。

继承不能覆盖已应用的配置。也就是说，如果将配置策略或自行管理配置直接应用于账户或 OU，则它将使用该配置，并且不会继承父级的配置。

根

在 AWS Organizations 和 Security Hub 中，组织中的顶级父节点。如果委托管理员将配置策略应用于根，则该策略将与组织中的所有账户和 OU 关联，除非他们通过应用或继承使用不同的策略，或者被指定为自行管理。如果管理员将根指定为自行管理，则组织中的所有账户和 OU 都是自行管理的，除非他们通过应用或继承使用配置策略。如果根是自行管理的，并且当前不存在任何配置策略，则组织中的所有新账户都将保留其当前设置。

加入组织的新账户在被分配到特定 OU 之前一直处于根之下。如果未将新账户分配给 OU，则该账户将继承根配置，除非委托管理员将其指定为自行管理账户。

开始使用中心配置

AWS Security Hub 委托管理员账户可以使用中心配置为 AWS 区域 的多个账户和组织单位（OU）配置 Security Hub、标准和控件。

本节介绍中心配置的先决条件以及如何开始使用。

中心配置的先决条件

在开始使用中心配置之前，必须将 Security Hub 与 AWS Organizations 集成，并指定主区域。如果您使用 Security Hub 控制台，则这些先决条件包含在中心配置的选择加入工作流程中。

与 Organizations 集成

您必须集成 Security Hub 和 Organizations 才能使用中心配置。

要集成这些服务，首先要在 Organizations 中创建一个组织。在组织管理账户中，指定一个 Security Hub 委托管理员账户。有关说明，请参阅 将 Security Hub 与 AWS Organizations。

确保您在预期主区域指定您的委托管理员。当您开始使用中心配置时，还会在所有关联区域中自动设置相同的委托管理员。组织管理账户不能设置为委托管理员账户。

> **Important**
>
> 在使用中心配置时，无法使用 Security Hub 控制台或 Security Hub API 来更改或删除委托管理员账户。如果组织管理账户使用 AWS Organizations API 更改或删除 Security Hub 委托管理员，则 Security Hub 会自动停止中心配置。您的配置策略也将被取消关联和删除。成员账户保留其在更改或删除委托管理员之前的配置。

指定主区域

您必须指定主区域才能使用中心配置。主区域是委托管理员从中配置组织的区域。

要使用中心配置，必须至少指定一个可从主区域配置的关联区域。

> **Note**
>
> 主区域不能是 AWS 已指定为选择加入区域的区域。默认情况下，选择加入区域处于禁用状态。有关选择加入区域的列表，请参阅《AWS 账户管理参考指南》中的启用和禁用区域之前的注意事项。

委托管理员只能从主区域创建和管理配置策略。配置策略在主区域和所有关联区域生效。您无法创建仅适用于某些区域而不适用于其他区域的配置策略。

主区域也是您的 Security Hub 聚合区域，用于接收来自关联区域的调查发现、见解和其他数据。

如果您已经为跨区域聚合设置了聚合区域，那么这就是中心配置的默认主区域。在开始使用中心配置之前，您可以通过删除当前的调查发现聚合器并在所需的主区域中创建一个新的聚合器来更改主区域。调查发现聚合器是一种 Security Hub 资源，用于指定主区域和关联区域。

要指定主区域，请按照设置聚合区域的步骤进行操作。如果您已经有主区域，则可以调用 GetFindingAggregator API 来查看有关它的详细信息，包括当前与其关联的区域。

启用中心配置

选择您的首选方法，然后按照步骤开始为您的组织使用中心配置。

Security Hub console

要集中配置您的组织

1. 通过以下网址打开 AWS Security Hub 控制台：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择设置和配置。然后，选择启用中心配置。

   如果要加入 Security Hub，请选择前往 Security Hub。
3. 在指定委托管理员页面上，选择您的委托管理员账户或输入其账户 ID。如果适用，我们建议选择您为其他 AWS 安全与合规服务设置的相同委托管理员。选择添加委托管理员。
4. 在集中组织页面的区域部分，选择您的主区域。您必须登录到主区域才能继续。如果您已经为跨区域聚合设置了聚合区域，则该聚合区域将显示为主区域。要更改主区域，请选择编辑区域设置。然后，您可以选择首选的主区域并返回到此工作流程。
5. 至少选择一个区域以链接到主区域。或者选择是否要自动将未来受支持的区域链接到主区域。您在此处选择的区域可由委托管理员从主区域进行配置。配置策略将在主区域和所有关联区域生效。
6. 选择确认并继续。
7. 现在可以使用中心配置了。继续按照控制台提示创建您的第一个配置策略。如果您尚未准备好创建配置策略，请选择我还没准备好配置。您可以稍后通过在导航窗格中选择设置和配置来创建策略。有关创建配置策略的说明，请参阅创建和关联 Security Hub 配置策略。

Security Hub API

要集中配置 Security Hub

1. 使用委托管理员账户的凭证，从主区域调用 UpdateOrganizationConfiguration API。

2. 将 AutoEnable 字段设置为 false。
3. 将 OrganizationConfiguration 对象中的 ConfigurationType 字段设置为 CENTRAL。此操作会产生以下影响：
   - 在所有关联区域中将调用账户指定为 Security Hub 的委托管理员。
   - 在所有关联区域的委托管理员账户中启用 Security Hub。
   - 为使用 Security Hub 且属于该组织的新账户和现有账户指定调用账户为 Security Hub 委托管理员。这发生在主区域和所有关联区域。仅当新组织账户与启用了 Security Hub 的配置策略关联时，调用账户才会被设置为新组织账户的委托管理员。仅当现有组织账户已启用 Security Hub 时，调用账户才会被设置为现有组织账户的委托管理员。
   - 在所有关联区域中将 AutoEnable 设置为 false，并在主区域和所有关联区域中将 AutoEnableStandards 设置为 NONE。当您使用中心配置时，这些参数与主区域和关联区域无关，但是您可以通过使用配置策略在组织账户中自动启用 Security Hub 和默认安全标准。
4. 现在可以使用中心配置了。委托管理员可以创建配置策略以在您的组织中配置 Security Hub。有关创建配置策略的说明，请参阅创建和关联 Security Hub 配置策略。

API 请求示例：

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

要集中配置 Security Hub

1. 使用委托管理员账户的凭证，从主区域运行 update-organization-configuration 命令。
2. 包含 no-auto-enable 参数。
3. 将 organization-configuration 对象中的 ConfigurationType 字段设置为 CENTRAL。此操作会产生以下影响：
   - 在所有关联区域中将调用账户指定为 Security Hub 的委托管理员。
   - 在所有关联区域的委托管理员账户中启用 Security Hub。

- 为使用 Security Hub 且属于该组织的新账户和现有账户指定调用账户为 Security Hub 委托管理员。这发生在主区域和所有关联区域。仅当新组织账户与启用了 Security Hub 的配置策略关联时，调用账户才会被设置为新组织账户的委托管理员。仅当现有组织账户已启用 Security Hub 时，调用账户才会被设置为现有组织账户的委托管理员。
- 在所有关联区域中将自动启用选项设置为 no-auto-enable，并在主区域和所有关联区域中将 auto-enable-standards 设置为 NONE。当您使用中心配置时，这些参数与主区域和关联区域无关，但是您可以通过使用配置策略在组织账户中自动启用 Security Hub 和默认安全标准。

4. 现在可以使用中心配置了。委托管理员可以创建配置策略以在您的组织中配置 Security Hub。有关创建配置策略的说明，请参阅创建和关联 Security Hub 配置策略。

命令示例：

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

选择账户和 OU 的管理类型

使用中央配置时， AWS Security Hub 委派的管理员可以将每个组织账户和组织单位 (OU) 指定为集中管理或自我管理。账户或 OU 的管理类型决定了如何指定和更改其 Security Hub 设置。

自我管理的账户或 OU 可以在每个 AWS 区域账户中单独配置自己的 Security Hub 设置。委托管理员无法为自行管理账户或 OU 配置 Security Hub 设置，配置策略也不能与之关联。相比之下，只有委托管理员才能为主区域和关联区域的集中管理账户和 OU 配置 Security Hub 设置。配置策略可与集中管理账户和 OU 关联。

委托管理员可以在自行管理和集中管理之间切换账户或 OU 的状态。默认情况下，当您通过 Security Hub API 启动中心配置时，所有账户和 OU 都是自行管理的。在控制台中，管理类型取决于您的第一个配置策略。与第一个策略关联的账户和 OU 是集中管理的。默认情况下，其他账户和 OU 是自行管理的。

如果您将配置策略与自我管理的账户相关联，则该策略将覆盖自我管理的指定。该账户将进行集中管理，并采用配置策略中反映的设置。

子账户和 OU 可以从自行管理的父级继承自行管理行为，就像子账户和 OU 可以从集中管理的父级继承配置策略一样。有关更多信息，请参阅 通过应用和继承进行策略关联。

自管理账户或 OU 不能从父节点或根节点继承配置策略。例如，如果您希望组织中的所有账户和 OU 都从根目录继承配置策略，则必须将自我管理节点的管理类型更改为集中管理。

为自行管理的账户指定设置

自行管理账户必须在每个区域单独配置自己的设置。

自行管理账户的所有者可以在每个区域调用 Security Hub API 的以下操作来配置其设置：

- `EnableSecurityHub` 和 `DisableSecurityHub`，启用或禁用 Security Hub 服务
- `BatchEnableStandards` 和 `BatchDisableStandards`，启用或禁用标准
- `BatchUpdateStandardsControlAssociations` 或 `UpdateStandardsControl`，启用或禁用控件

自行管理的账户也可以使用`*Invitations`和`*Members`操作。但是，我们建议自行管理的账户不要使用这些操作。如果成员账户的成员与委派的管理员属于不同的组织，则策略关联可能会失败。

有关 Security Hub API 操作的说明，请参阅 AWS Security Hub API 参考。

自行管理的账户也可以使用 Security Hub 控制台或 AWS CLI 在每个区域配置其设置。

自行管理账户无法调用与 Security Hub 配置策略和策略关联相关的任何 API。只有委托管理员才能调用中心配置 API 并使用配置策略来配置集中管理账户。

选择账户和 OU 的管理类型

选择首选方法，然后按照步骤将账户或 OU 指定为集中管理或自行管理。

Security Hub console

要选择账户和 OU 的管理类型

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 选择配置。
3. 在组织选项卡上，选择目标账户或 OU。选择编辑。
4. 在定义配置页面上，对于管理类型，如果您希望委托管理员配置目标账户或 OU，请选择集中管理。然后，如果要将现有配置策略与目标关联，请选择应用特定策略。如果希望目标继承最

接近父级的配置，请选择从我的组织继承。如果希望账户或 OU 配置自己的设置，请选择自行管理。

5. 选择下一步。检查更改，然后选择保存。

Security Hub API

要选择账户和 OU 的管理类型

1. 从主区域的 Security Hub 委托管理员账户调用 StartConfigurationPolicyAssociation API。
2. 对于 `ConfigurationPolicyIdentifier` 字段，如果希望账户或 OU 控制其自己的设置，请提供 `SELF_MANAGED_SECURITY_HUB`。如果希望委托管理员控制账户或 OU 的设置，请提供相关配置策略的 Amazon 资源名称（ARN）或 ID。
3. 在该`Target`字段中，提供要更改其管理类型的目标的 ID、OU ID 或根 ID。 AWS 账户 这会将自行管理行为或指定的配置策略与目标关联。目标的子账户可继承自行管理行为或配置策略。

指定自行管理账户的 API 请求示例：

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

要选择账户和 OU 的管理类型

1. 从主区域的 Security Hub 委托管理员账户运行 start-configuration-policy-association 命令。
2. 对于 `configuration-policy-identifier` 字段，如果希望账户或 OU 控制其自己的设置，请提供 `SELF_MANAGED_SECURITY_HUB`。如果希望委托管理员控制账户或 OU 的设置，请提供相关配置策略的 Amazon 资源名称（ARN）或 ID。
3. 在该`target`字段中，提供要更改其管理类型的目标的 ID、OU ID 或根 ID。 AWS 账户 这会将自行管理行为或指定的配置策略与目标关联。目标的子账户可继承自行管理行为或配置策略。

指定自行管理账户的命令示例：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
```

```
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Security Hub 配置策略的工作原理

委派的管理员帐户可以创建 AWS Security Hub 配置策略，以便在组织中配置 Security Hub、安全标准和安全控制。创建配置策略后，委托管理员可以将其与账户、组织部门（OU）或根关联。委托管理员还可以查看、编辑或删除配置策略。

策略注意事项

在 Security Hub 中创建配置策略之前，请注意以下事项。

- 必须关联配置策略才能生效 — 创建配置策略后，可以将其与一个或多个账户、组织单位（OU）或根相关联。配置策略可以通过直接应用或通过从父 OU 继承来与账户或 OU 关联。
- 一个账户或 OU 只能与一个配置策略相关联 — 为防止设置冲突，一个账户或 OU 在任何给定时间只能与一个配置策略相关联。或者，也可以对账户或 OU 进行自行管理。
- 配置策略已完成 — 配置策略提供了完整的设置规范。例如，子账户不能接受一个策略中的某些控件的设置和另一个策略中其他控件的设置。当您将策略与子账户关联时，请确保该策略指定了您希望该子账户使用的所有设置。
- 配置策略无法恢复 — 在将配置策略与账户或 OU 关联后，无法选择恢复该策略。例如，如果您将禁用 CloudWatch 控件的配置策略与特定账户关联，然后取消该策略的关联，则该账户中的 CloudWatch 控件将继续处于禁用状态。要再次启用 CloudWatch 控件，您可以将该账户与启用控件的新策略相关联。或者，您可以将帐户更改为自我管理并启用帐户中的每个 CloudWatch 控件。
- 配置策略在您的主区域和所有关联区域生效 — 配置策略会影响主区域中的所有关联账户以及所有关联区域。您无法创建仅在其中某些区域生效而不在其他区域生效的配置策略。唯一的例外是涉及全球资源的控制。

  在 2019 年 3 月 20 日当天或之后 AWS 推出的区域被称为选择加入区域。必须先为账户启用这样的区域，然后配置策略才会在该区域生效。组织管理账户可以为成员账户启用选择加入区域。有关启用可选区域的说明，请参阅《账户管理参考指南》中的指定 AWS 区域 您的AWS 账户可以使用哪个区域。

  如果您的策略配置的控件在主区域或一个或多个关联区域中不可用，Security Hub 则会跳过不可用区域中的控制配置，但会在有该控件可用的区域中应用该配置。

- 配置策略即资源 — 作为资源，配置策略有 Amazon 资源名称（ARN）和通用唯一标识符（UUID）。ARN 使用以下格式：`arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`*。自我管理的配置没有 ARN 或 UUID。自我管理配置的标识符是`SELF_MANAGED_SECURITY_HUB`。

配置策略的类型

每个配置策略指定以下设置：

- 启用或禁用 Security Hub。
- 启用一项或多项安全标准。
- 指明在已启用的标准中启用了哪些安全控件。为此，您可以提供应启用的特定控件列表，并且 Security Hub 会禁用所有其他控件，包括在新控件发布时直接禁用。此外，您可以提供应禁用的特定控件列表，并且 Security Hub 会启用所有其他控件，包括在新控件发布时直接启用。
- （可选）在已启用的标准中为选定的已启用控件自定义参数。

中央配置策略不包括 AWS Config 录制器设置。为了让 Secur AWS Config ity Hub 生成控制结果，您必须单独启用和开启所需资源的记录。有关更多信息，请参阅 正在配置 AWS Config。

如果您使用中央配置，Security Hub 会自动禁用涉及除本地区以外的所有区域的全球资源的控件。您选择通过配置策略启用的其他控件将在所有可用区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。当你使用中央配置时，你无法覆盖主区域和任何关联区域中不可用的控件。有关涉及全局资源的控件列表，请参阅处理全局资源的控件。

建议的配置策略

首次在 Security Hub 控制台中创建配置策略时，您可以选择 Security Hub 推荐的策略。

推荐的策略启用 Security Hub、 AWS 基础安全最佳实践 (FSBP) 标准以及所有现有和新的 FSBP 控件。接受参数的控件使用默认值。推荐的策略适用于根（所有账户和 OU，包括新账户和现有账户）。为您的组织创建推荐的策略后，您可以通过委托管理员账户对其进行修改。例如，您可以启用其他标准或控件或禁用特定的 FSBP 控件。有关修改配置策略的说明，请参阅更新 Security Hub 配置策略。

自定义配置策略

委托管理员最多可以创建 20 个自定义配置策略，而不是推荐的策略。您可以将单个自定义策略与整个组织相关联，也可以将不同的自定义策略与不同的账户和 OU 关联。对于自定义配置策略，您可以

指定所需的设置。例如，您可以创建自定义策略，启用 FSBP、 Center for Internet Security（CIS）AWS 基金会基准 v1.4.0 以及这些标准中除了 Amazon Redshift 控件之外的所有控件。您在自定义配置策略中使用的粒度级别取决于整个组织的预期安全覆盖范围。

> **Note**
>
> 您无法将禁用 Security Hub 的配置策略与委托管理员账户相关联。这样的策略可以与其他账户关联，但会跳过与委托管理员的关联。委托管理员账户保留其当前配置。

创建自定义配置策略后，您可以更新配置策略，切换到推荐的配置策略，从而反映推荐的配置。但是，在创建第一个策略后，您无法在 Security Hub 控制台中看到创建推荐配置策略的选项。

通过应用和继承进行策略关联

当你第一次选择使用中心配置时，你的组织没有任何关联关系，其行为方式与选择加入之前相同。然后，授权的管理员可以在配置策略或自我管理行为与账户、OU 或根之间建立关联。可以通过应用或继承来建立关联。

通过委托管理员账户，您可以直接将配置策略应用于账户、OU 或根。或者，授权管理员可以直接将自我管理的指定应用于账户、OU 或根。

在没有直接应用程序的情况下，账户或 OU 会继承具有配置策略或自我管理行为的最近的家长的设置。如果最近的父级与配置策略相关联，则子级将继承该策略，并且只能由来自主区域的委托管理员进行配置。如果最亲近的父母是自我管理的，则孩子将继承自我管理的行为，并且能够在每个行为中指定自己的设置。 AWS 区域

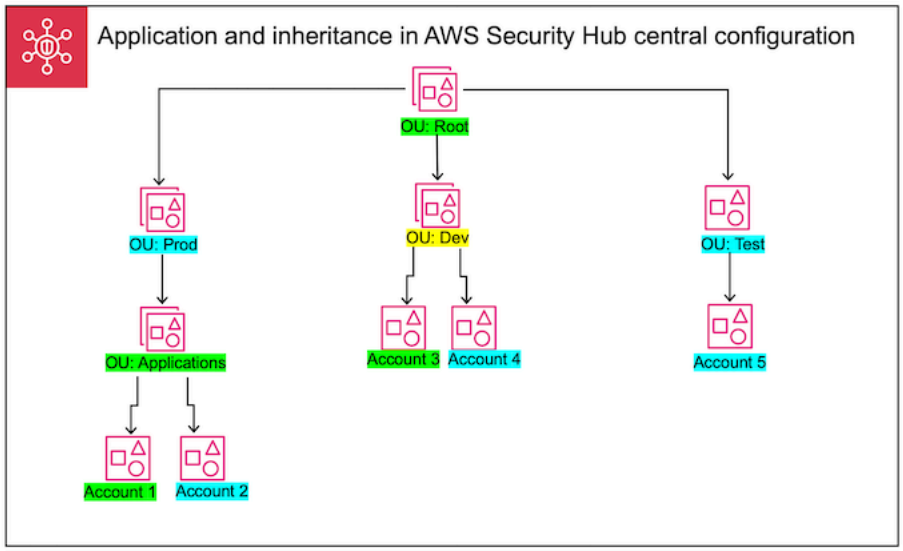
应用程序优先于继承。换句话说，继承不会覆盖委派管理员直接应用于账户或 OU 的配置策略或自我管理指定。

如果您直接将配置策略应用于自我管理的账户，则该策略将覆盖自我管理的指定。该账户将进行集中管理，并采用配置策略中反映的设置。

我们建议直接将配置策略应用于根目录。如果您对根应用策略，则加入组织的新账户将自动继承根策略，除非您将这些账户与其他策略关联或将其指定为自行管理。

在给定时间，只能通过应用或继承将配置策略与账户或 OU 关联。这旨在防止设置冲突。

下图说明了策略应用和继承在中心配置中的工作原理。



在此示例中，以绿色突出显示的节点具有已应用于该节点的配置策略。以蓝色突出显示的节点不具有已应用于该节点的配置策略。以黄色突出显示的节点已被指定为自行管理。每个账户和 OU 都使用以下配置：

- OU:Root（绿色）— 此 OU 使用已应用于它的配置策略。
- OU:Prod（蓝色）— 此 OU 继承了 OU:Root 的配置策略。
- OU:Applications（绿色）— 此 OU 使用已应用于它的配置策略。
- 账户 1（绿色）— 此账户使用已应用于它的配置策略。
- 账户 2（蓝色）-此账户继承了 OU:Applications 的配置策略。
- OU:Dev（黄色）— 此 OU 是自行管理的。
- 账户 3（绿色）— 此账户使用已应用于它的配置策略。
- 账户 4（蓝色）— 此账户继承了 OU:Dev 的自行管理行为。
- OU:Test（蓝色）— 此 OU 继承了 OU:Root 的配置策略。
- 账户 5（蓝色）— 此账户继承了 OU:Root 的配置策略，因为其直系父级 OU:Test 未与配置策略关联。

测试配置策略

要测试配置策略的效果，您可以将其与单个账户或 OU 关联，然后再将其在更大范围的整个组织内关联。

要测试配置策略

1. 创建自定义配置策略，但不要将其应用到任何账户。验证 Security Hub 的启用状况、标准和控件的指定设置是否正确。
2. 将配置策略应用于没有任何子账户或 OU 的测试帐号或 OU。
3. 验证测试账户或 OU 在您的主区域和所有关联区域中是否按预期方式使用配置策略。您还可以验证组织中的所有其他账户和 OU 是否仍是自行管理的，并且可以在每个区域中变更其自身设置。

在单个账户或 OU 中测试配置策略后，您可以将其与其他账户和 OU 关联。有关策略创建和关联的说明，请参阅创建和关联 Security Hub 配置策略。应用账户的子账户将继承该策略，除非这些子账户是自行管理的，或者应用了其他配置策略。您还可以根据需要编辑配置策略并创建其他配置策略。

创建和关联 Security Hub 配置策略

委派的管理员账户可以创建 AWS Security Hub 配置策略并将其与组织帐户、组织单位 (OU) 或根相关联。您还可以将自我管理的配置与账户、OU 或根相关联。

如果您是首次创建配置策略，我们建议您先查看 Security Hub 配置策略的工作原理。

选择您的首选访问方法，然后按照步骤创建和关联配置策略或自管理配置。使用 Security Hub 控制台时，您可以将一个配置同时与多个账户或 OU 相关联。使用 Security Hub API 或时 AWS CLI，您只能在每个请求中将配置与一个账户或 OU 关联。

> **Note**
>
> 如果您使用中央配置，Security Hub 会自动禁用涉及除本地区之外的所有区域的全球资源的控件。您选择通过配置策略启用的其他控件将在所有可用区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。当你使用中央配置时，你无法覆盖主区域和任何关联区域中不可用的控件。有关涉及全局资源的控件列表，请参阅处理全局资源的控件。

Security Hub console

要创建和关联配置策略

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。

2. 在导航窗格中，选择配置和策略选项卡。然后选择创建策略。
3. 如果这是您第一次创建配置策略，则在配置组织页面上，可以在配置类型下看到三个选项。如果您已经创建了至少一个配置策略，则只能看到自定义策略选项。

   - 选择 “在整个组织中使用 AWS 推荐的 Security Hub 配置” 以使用我们推荐的策略。推荐的策略在所有组织帐户中启用 Security Hub，启用 AWS 基础安全最佳实践 (FSBP) 标准，并启用所有新的和现有的 FSBP 控件。控件使用默认参数值。
   - 选择我还没准备好配置，以稍后创建配置策略。
   - 选择自定义策略，以创建自定义配置策略。指定是启用还是禁用 Security Hub、要启用哪些标准以及要在这些标准中启用哪些控件。（可选）为一个或多个支持自定义参数的已启用控件指定自定义参数值。
4. 在账户部分，选择要将配置策略应用于哪些目标账户、OU 或根。

   - 如果要将配置策略应用于根，请选择所有账户。这包括组织中所有未应用或继承其他策略的账户和 OU。
   - 如果要将配置策略应用于特定账户或 OU，请选择特定账户。输入账户 ID，或者从组织结构中选择账户和 OU。创建策略时，您最多可以将策略应用于 15 个目标（账户、OU 或 root）。要指定更大的数字，请在创建策略后对其进行编辑，然后将其应用于其他目标。
   - 选择仅限委托管理员，将配置策略应用于当前的委托管理员账户。
5. 选择下一步。
6. 在查看和应用页面上，查看您的配置策略详细信息。然后选择创建并应用策略。在您的主区域和关联区域中，此操作将覆盖与此配置策略关联的账户的现有配置设置。账户可以通过应用与配置策略相关联，也可以从父节点继承。已应用目标的子账户和 OU 将自动继承此配置策略，除非它们被排除在外、自行管理或使用不同的配置策略。

Security Hub API

要创建和关联配置策略

1. 从主区域的 Security Hub 委托管理员账户调用 CreateConfigurationPolicy API。
2. 对于 `Name`，输入配置策略的唯一名称。（可选）对于 `Description`，为配置策略提供描述。
3. 在 `ServiceEnabled` 字段中，指定要在此配置策略中启用还是禁用 Security Hub。
4. 在 `EnabledStandardIdentifiers` 字段中，指定要在此配置策略中启用哪些 Security Hub 标准。

5. 对于 SecurityControlsConfiguration 对象，请在此配置策略中指定要启用或禁用的控件。选择 EnabledSecurityControlIdentifiers 意味着指定的控件已启用。已启用标准中的其他控件（包括新发布的控件）将被禁用。选择 DisabledSecurityControlIdentifiers 意味着指定的控件被禁用。属于已启用标准的其他控件（包括新发布的控件）将被启用。
6. 或者，在 SecurityControlCustomParameters 字段中，指定要为其自定义参数的已启用控件。为 ValueType 字段提供 CUSTOM，为 Value 字段提供自定义参数值。该值必须是正确的数据类型，并且必须在 Security Hub 指定的有效范围内。只有精选控件支持自定义参数值。有关更多信息，请参阅 自定义控制参数。
7. 要将您的配置策略应用于账户或 OU，请从主区域的 Security Hub 委托管理员账户中调用 StartConfigurationPolicyAssociation API。
8. ConfigurationPolicyIdentifier在该字段中，提供政策的亚马逊资源名称 (ARN) 或通用唯一标识符 (UUID)。ARN 和 UUID 由 API 返回。CreateConfigurationPolicy对于自管理配置，该ConfigurationPolicyIdentifier字段等于。SELF_MANAGED_SECURITY_HUB
9. 在 Target 字段中，提供您希望此配置策略应用的 OU、账户或根 ID。您只能在每个 API 请求中提供一个目标。所选目标的子账户和 OU 将自动继承此配置策略，除非它们是自行管理的或使用不同的配置策略。

用于创建配置策略的 API 请求示例：

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
```

```
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

用于关联配置策略的 API 请求示例：

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

要创建和关联配置策略

1. 从主区域的 Security Hub 委托管理员账户运行 create-configuration-policy 命令。
2. 对于 name，输入配置策略的唯一名称。（可选）对于 description，为配置策略提供描述。
3. 在 ServiceEnabled 字段中，指定要在此配置策略中启用还是禁用 Security Hub。
4. 在 EnabledStandardIdentifiers 字段中，指定要在此配置策略中启用哪些 Security Hub 标准。
5. 在 SecurityControlsConfiguration 字段中，请在此配置策略中指定要启用或禁用的控件。选择 EnabledSecurityControlIdentifiers 意味着指定的控件已启用。已启用标准中的其他控件（包括新发布的控件）将被禁用。选择

`DisabledSecurityControlIdentifiers` 意味着指定的控件被禁用。适用于您已启用标准的其他控件（包括新发布的控件）已启用。

6. 或者，在 `SecurityControlCustomParameters` 字段中，指定要为其自定义参数的已启用控件。为 `ValueType` 字段提供 `CUSTOM`，为 `Value` 字段提供自定义参数值。该值必须是正确的数据类型，并且必须在 Security Hub 指定的有效范围内。只有精选控件支持自定义参数值。有关更多信息，请参阅 自定义控制参数。
7. 要将您的配置策略应用于账户或 OU，请从主区域的 Security Hub 委托管理员账户中运行 start-configuration-policy-association 命令。
8. 请为 `configuration-policy-identifier` 字段提供配置策略的 Amazon 资源名称（ARN）或 ID。此 ARN 和 ID 由 `create-configuration-policy` 命令返回。
9. 在 `target` 字段中，提供您希望此配置策略应用的 OU、账户或根 ID。您只能在每次运行命令时提供一个目标。所选目标的子账户将自动继承此配置策略，除非它们是自行管理的或使用不同的配置策略。

用于创建配置策略的命令示例：

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

用于关联配置策略的命令示例：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

StartConfigurationPolicyAssociation API 返回一个名为 AssociationStatus 的字段。此字段会告诉您策略关联是待处理还是处于成功或失败状态。状态从 PENDING 变为 SUCCESS 或 FAILURE 可能需要长达 24 小时的时间。有关关联状态的更多信息，请参阅配置的关联状态。

查看 Security Hub 配置策略

委托管理员账户可以查看组织的 AWS Security Hub 配置策略及其详细信息。

选择首选方法，然后按照步骤查看配置策略。

Console

要查看配置策略

1. 通过以下网址打开AWS Security Hub控制台：https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡以查看配置策略概述。
4. 选择一个配置策略，然后选择查看详细信息，查看有关该策略的其他详细信息。

API

要查看配置策略

要查看所有配置策略的摘要列表，请从主区域中的 Security Hub 委托管理员账户调用 ListConfigurationPolicies API。您可以提供可选的分页参数

API 请求示例：

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

要查看特定配置策略的摘要列表，请从主区域中的 Security Hub 委托管理员账户调用 GetConfigurationPolicy API。提供要查看其详细信息的配置策略的 Amazon 资源名称（ARN）或 ID。

API 请求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

要查看所有配置策略及其关联的摘要列表，请从主区域中的 Security Hub 委托管理员账户调用 ListConfigurationPolicyAssociations API。或者，您可以提供分页参数，或者按特定策略 ID、关联类型或关联状态筛选结果。

API 请求示例：

```
{
    "AssociationType": "APPLIED"
}
```

要查看特定账户、OU 或根的关联，请从主区域中的 Security Hub 委托管理员账户调用 GetConfigurationPolicyAssociation 或 BatchGetConfigurationPolicyAssociations API。对于 Target，请提供账户、OU ID 或根 ID。

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

要查看配置策略

要查看所有配置策略的摘要列表，请从主区域中的 Security Hub 委托管理员账户运行 list-configuration-policies 命令。

命令示例：

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

要查看特定配置策略的摘要列表，请从主区域中的 Security Hub 委托管理员账户运行 get-configuration-policy 命令。提供要查看其详细信息的配置策略的 Amazon 资源名称（ARN）或 ID。

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

要查看所有配置策略及其账户的摘要列表，请从主区域中的 Security Hub 委托管理员账户运行 list-configuration-policy-associations 命令。或者，您可以提供分页参数，或者按特定策略 ID、关联类型或关联状态筛选结果。

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

要查看特定账户的关联，请从主区域中的 Security Hub 委托管理员账户运行 get-configuration-policy-association 或 batch-get-configuration-policy-associations 命令。对于 target，请提供账户、OU ID 或根 ID。

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

配置的关联状态

以下中心配置 API 操作将返回一个名为 AssociationStatus 的字段：

- BatchGetConfigurationPolicyAssociations
- GetConfigurationPolicyAssociation
- ListConfigurationPolicyAssociations
- StartConfigurationPolicyAssociation

当基础配置为配置策略，并且是自行管理行为时，都将返回此字段。

AssociationStatus 的值会告诉您策略关联是待处理还是处于成功或失败状态。状态从 PENDING 变为 SUCCESS 或 FAILURE 可能需要长达 24 小时的时间。父 OU 或根的关联状态取决于其子级的状态。如果所有子级的关联状态均为 SUCCESS，则父级的关联状态为 SUCCESS。如果一个或多个子级的关联状态均为 FAILED，则父级的关联状态为 FAILED。

AssociationStatus 的值还取决于所有区域。如果关联在主区域和所有关联区域成功，则 AssociationStatus 的值为 SUCCESS。如果关联在一个或多个区域失败，则 AssociationStatus 的值为 FAILED。

以下行为也会影响 AssociationStatus 的值：

- 如果目标是父 OU 或根，则只有当所有子级的状态为 SUCCESS 或 FAILED 时，AssociationStatus 才具有 SUCCESS 或 FAILED 状态。在首次将父级与配置关联后，如果子账户或 OU 的关联状态变更（例如，添加或删除了关联区域时），则除非再次调用 StartConfigurationPolicyAssociation API，否则变更不会使父级的关联状态更新。
- 如果目标是账户，则只有当主区域和所有关联区域的关联结果为 SUCCESS 或 FAILED 时，AssociationStatus 才具有 SUCCESS 或 FAILED 状态。在首次将目标账户与配置关联后，如果目标账户的关联状态变更（例如，添加或删除了关联区域时），则配置的关联状态也会随之更新。但除非再次调用 StartConfigurationPolicyAssociation API，否则变更不会使父级的关联状态更新。

如果您添加新的关联区域，Security Hub 会复制新区域中处于 PENDING、SUCCESS 或 FAILED 状态的现有关联。

关联失败的常见原因

配置策略关联可能会因以下常见原因而失败：

- 组织管理账户不是成员：如果要将配置策略与组织管理账户关联，该账户必须已启用 Security Hub。这将使管理账户成为组织的成员账户。
- AWS Config 未启用或未正确配置：要在配置策略中启用标准，必须启用并配置 AWS Config 以记录相关资源。
- 必须从委托管理员账户关联：只有在登录委托管理员账户后，才能将策略与目标账户和 OU 关联。
- 必须从主区域关联：只有在登录主区域后，才能将策略与目标账户和 OU 关联。
- 未启用选择加入区域：如果关联区域是委托管理员尚未启用的选择加入区域，则该区域中的成员账户或 OU 的策略关联将会失败。您可以在从委托管理员账户启用区域后重试。
- 成员账户已暂停：如果尝试将策略与暂停的成员账户关联，则策略关联将失败。

更新 Security Hub 配置策略

委派的管理员账户可以根据需要更新 AWS Security Hub 配置策略。委托管理员可以更新策略设置和/或与策略关联的账户或 OU。更新策略设置后，与配置策略关联的账户会自动开始使用更新后的策略。

与创建配置策略时类似，您可以更新以下策略设置：

- 启用或禁用 Security Hub。
- 启用一项或多项安全标准。
- 指明在已启用的标准中启用了哪些安全控件。为此，您可以提供应启用的特定控件列表，并且 Security Hub 会禁用所有其他控件，包括在新控件发布时直接禁用。此外，您可以提供应禁用的特定控件列表，并且 Security Hub 会启用所有其他控件，包括在新控件发布时直接启用。
- （可选）在已启用的标准中为选定的已启用控件自定义参数。

选择首选方法，然后按照步骤更新配置策略。

如果您使用中央配置，Security Hub 会自动禁用涉及除本地区之外的所有区域的全球资源的控件。您选择通过配置策略启用的其他控件将在所有可用区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。当你使用中央配置时，你无法覆盖主区域和任何关联区域中不可用的控件。有关涉及全局资源的控件列表，请参阅处理全局资源的控件。

Console

要更新配置策略

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。
4. 选择要编辑的配置策略，然后选择编辑。如果需要，请编辑策略设置。如果要保持策略设置不变，请保留此部分。
5. 选择下一步。如果需要，请编辑策略关联。如果要保持策略关联不变，请保留此部分。更新策略时，您可以将策略与最多 15 个目标（账户、OU 或 root）关联或取消关联。
6. 选择下一步。

7. 检查更改，然后选择保存并应用。在您的主区域和关联区域中，此操作将覆盖与此配置策略关联的账户的现有配置设置。账户可以通过应用与配置策略相关联，也可以从父节点继承。

API

要更新配置策略

1. 要更新配置策略中的设置，请从主区域的 Security Hub 委托管理员账户调用 UpdateConfigurationPolicy API。
2. 提供要更新的配置策略的 Amazon 资源名称（ARN）或 ID。
3. 为 `ConfigurationPolicy` 下方的字段提供更新后的值。（可选）您还可以提供更新原因。
4. 要为此配置策略添加新的关联，请从主区域的 Security Hub 委托管理员账户调用 StartConfigurationPolicyAssociation API。要删除一个或多个当前关联，请从主区域的 Security Hub 委托管理员账户调用 StartConfigurationPolicyDisassociation API。
5. 对于 `ConfigurationPolicyIdentifier` 字段，提供要更新其关联的配置策略的 ARN 或 ID。
6. 对于 `Target` 字段，提供要关联或解除关联的账户、OU 或根 ID。此操作将覆盖指定 OU 或账户之前的策略关联。

> **Note**
>
> 调用 `UpdateConfigurationPolicy` API 时，Security Hub 会对 `EnabledStandardIdentifiers`、`EnabledSecurityControlIdentifiers`、`DisabledSec` 和 `SecurityControlCustomParameters` 字段执行完整列表替换。每次调用此 API 时，请提供要启用的标准的完整列表，以及要为其启用或禁用和自定义参数的控件的完整列表。

更新配置策略的 API 请求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
```

```
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
             "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

要更新配置策略

1. 要更新配置策略中的设置，请从主区域的 Security Hub 委托管理员账户运行 update-configuration-policy 命令。
2. 提供要更新的配置策略的 Amazon 资源名称（ARN）或 ID。
3. 为 `configuration-policy` 下方的字段提供更新后的值。（可选）您还可以提供更新原因。

4. 要为此配置策略添加新的关联，请从主区域的 Security Hub 委托管理员账户运行 start-configuration-policy-association 命令。要删除一个或多个当前关联，请从主区域的 Security Hub 委托管理员账户运行 start-configuration-policy-disassociation 命令。
5. 对于 `configuration-policy-identifier` 字段，提供要更新其关联的配置策略的 ARN 或 ID。
6. 对于 `target` 字段，提供要关联或解除关联的账户、OU 或根 ID。此操作将覆盖指定 OU 或账户之前的策略关联。

> **Note**
>
> 运行 `update-configuration-policy` 命令时，Security Hub 会对 `EnabledStandardIdentifiers`、`EnabledSecurityControlIdentifiers`、`DisabledSec` 和 `SecurityControlCustomParameters` 字段执行完整列表替换。每次运行此命令时，请提供要启用的标准的完整列表，以及要为其启用或禁用和自定义参数的控件的完整列表。

更新配置策略的命令示例：

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

`StartConfigurationPolicyAssociation` API 返回一个名为 `AssociationStatus` 的字段。此字段会告诉您策略关联是待处理还是处于成功或失败状态。状态从 `PENDING` 变为 `SUCCESS` 或 `FAILURE` 可能需要长达 24 小时的时间。有关关联状态的更多信息，请参阅配置的关联状态。

删除和解除 Security Hub 配置策略关联

委托管理员账户可以删除 AWS Security Hub 配置策略。或者，委托管理员账户可以保留配置策略，但解除其与特定账户或组织单位（OU）的关联。

下一节介绍了这两个选项。

删除配置策略

删除配置策略后，该策略将不再存在于组织中。目标账户、OU 和组织根无法再使用配置策略。与已删除的配置策略关联的目标将继承最接近父级的配置策略，或者如果最接近父级是自行管理的，则会变为自行管理。如果希望目标使用其他配置，可以将该目标与新的配置策略相关联。有关更多信息，请参阅创建和关联 Security Hub 配置策略。

我们建议至少创建一个配置策略，并将其与组织关联，以提供足够的安全覆盖。

在删除配置策略之前，必须解除该策略与当前应用该策略的账户、OU 或根的关联。

选择首选方法，然后按照步骤删除配置策略。

Console

要删除配置策略

1. 通过以下网址打开AWS Security Hub控制台：https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择 Policies 选项卡。选择要删除的配置策略，然后选择删除。如果配置策略仍与任何账户或 OU 关联，系统会提示您先解除策略与这些目标的关联，然后才能将其删除。
4. 查看确认消息。输入 **`confirm`**，然后选择删除。

API

要删除配置策略

从主区域的 Security Hub 委托管理员账户调用 DeleteConfigurationPolicy API。

提供要删除的配置策略的 Amazon 资源名称（ARN）或 ID。如果收到 `ConflictException` 错误，配置策略仍适用于组织中的账户或 OU。要解决此错误，请在尝试删除配置策略之前解除其与这些账户或 OU 的关联。

删除配置策略的 API 请求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

要删除配置策略

从主区域的 Security Hub 委托管理员账户运行 delete-configuration-policy 命令。

提供要删除的配置策略的 Amazon 资源名称（ARN）或 ID。如果收到 ConflictException 错误，配置策略仍适用于组织中的账户或 OU。要解决此错误，请在尝试删除配置策略之前解除其与这些账户或 OU 的关联。

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

解除配置与账户和 OU 的关联

在委托管理员账户中，您可以解除目标账户、OU 或根账户与当前适用于其的配置策略或自行管理配置的关联。您只能解除目标与已应用配置的关联，而不能解除与已继承配置的关联。要更改继承的配置，可以将配置策略或自行管理行为应用于受影响的账户或 OU。您还可以将新的配置策略（包括所需的修改）应用于最接近的父级。

解除关联不会删除配置策略。该策略保留在您的账户中，因此您可以将其与组织中的其他目标关联。解除关联完成后，受影响的目标将继承最接近的父级的配置策略或自行管理行为。如果没有可继承的配置，目标会保留解除关联之前的设置，但变为自行管理。

选择首选方法，然后按照步骤解除账户、OU 或根与其当前配置的关联。

Console

要解除账户或 OU 与其当前配置的关联

1. 通过以下网址打开AWS Security Hub控制台：https://console.aws.amazon.com/securityhub/。

使用主区域中 Security Hub 委托管理员账户的凭证登录。

2. 在导航窗格中，选择设置和配置。
3. 在组织选项卡上，选择要解除与其当前配置关联的账户、OU 或根。选择编辑。
4. 在定义配置页面上，对于管理，如果您希望委托管理员能够将策略直接应用于目标，请选择应用的策略。如果希望目标继承最接近父级的配置，请选择继承。在这两种情况下，委托管理员都将控制目标的设置。如果希望账户或 OU 控制自己的设置，请选择自行管理。
5. 查看更改后，选择下一步和应用。如果范围内的任何账户或 OU 的现有配置与当前选择冲突，此操作将覆盖这些配置。

API

要解除账户或 OU 与其当前配置的关联

1. 从主区域的 Security Hub 委托管理员账户调用 StartConfigurationPolicyDisassociation API。
2. 对于 `ConfigurationPolicyIdentifier`，提供要解除关联的配置策略的 Amazon 资源名称（ARN）或 ID。对于该字段，提供 `SELF_MANAGED_SECURITY_HUB` 以解除自行管理行为的关联。
3. 对于 `Target`，提供要与此配置策略解除关联的账户、OU 或根。

解除配置策略关联的 API 请求示例：

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

要解除账户或 OU 与其当前配置的关联

1. 从主区域的 Security Hub 委托管理员账户运行 start-configuration-policy-disassociation 命令。
2. 对于 `configuration-policy-identifier`，提供要解除关联的配置策略的 Amazon 资源名称（ARN）或 ID。对于该字段，提供 `SELF_MANAGED_SECURITY_HUB` 以解除自行管理行为的关联。

3. 对于 target，提供要与此配置策略解除关联的账户、OU 或根。

解除配置策略关联的命令示例：

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

标准或控件上下文中的中心配置

您可以在 AWS Security Hub 控制台的 “配置” 页面中使用集中配置，也可以在特定的安全标准或安全控制的环境中使用。在上下文中使用此功能时，您可以通过与现有工作流程集成，在整个组织中配置标准和控件。此外，在查看调查发现时，您还可以发现哪些标准和控件与环境最相关，同时对其进行配置。

上下文配置仅在 Security Hub 控制台上可用。以编程方式说明的话，您必须调用 UpdateConfigurationPolicy API，才能更改组织中特定标准或控件的配置方式。

在上下文中配置安全标准

按照以下步骤，通过中心配置在上下文中配置安全标准。

要在上下文中配置安全标准（仅限控制台）

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择 “安全标准”。
3. 对于要配置的标准，请选择配置。您也可以选择特定标准，然后从标准详细信息页面中选择配置。控制台列出了现有的 Security Hub 配置策略（配置策略）以及每个策略中该标准的状态。
4. 在每个配置策略中选择启用或禁用标准的选项。
5. 更改后，选择下一步。
6. 查看更改，然后选择应用。此操作会影响与配置策略关联的所有账户和 OU。您的配置将在主区域和所有关联区域生效。

在上下文中配置安全控件

按照以下步骤，通过中心配置在上下文中配置安全控件。

要在上下文中配置安全控件（仅限控制台）

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择控件。
3. 选择特定的控件，然后选择 “配置”。控制台列出了当前的配置策略以及每个策略中该控件的状态。
4. 在每个配置策略中选择启用或禁用控件的选项。您也可以选择自定义控制参数。
5. 更改后，选择下一步。
6. 查看更改，然后选择应用。此操作会影响与配置策略关联的所有账户和 OU。您的配置将在主区域和所有关联区域生效。

停止使用中心配置

当您停止在 AWS Security Hub 中使用中心配置时，委托管理员将无法跨多个 AWS 账户、组织单位（OU）和 AWS 区域 配置 Security Hub、安全标准和安全控件。相反，组织账户必须在每个区域中单独配置自己的大部分设置。

> **Important**
>
> 在停止使用中心配置之前，必须先解除账户和 OU 与其当前配置的关联，无论是配置策略还是自行管理行为。
> 在停止使用中心配置之前，还必须删除配置策略。

停止中心配置后，将发生以下变化：

- 委托管理员无法再为组织创建配置策略。
- 已应用或继承配置策略的账户将保留其当前设置，但变为自行管理。
- 组织切换到本地配置。在本地配置下，大多数 Security Hub 设置必须在每个组织账户和区域中单独配置。委托管理员可以选择自动启用 Security Hub、默认安全标准以及属于新组织账户默认标准的所有控件。默认标准是 AWS 基础安全最佳实践（FSBP）和 Center for Internet Security（CIS）AWS

基金会基准 v1.2.0。这些设置仅在当前区域生效，并且仅影响新的组织账户。委托管理员无法更改默认标准。本地配置不支持在 OU 级别使用配置策略或配置。

停止使用中心配置时，委托管理员账户的身份将保持不变。主区域和关联区域也保持不变（主区域现在称为聚合区域，可用于查找聚合）。

选择首选方法，然后按照步骤停止使用中心配置并切换到本地配置。

Security Hub console

要停止使用中心配置

1. 通过以下网址打开AWS Security Hub控制台：https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 在概述部分，选择编辑。
4. 在编辑组织配置框中，选择本地配置。如果未这样做，系统会提示您解除关联并删除当前的配置策略，然后才能停止中心配置。被指定为自行管理账户或 OU 必须与其自行管理配置解除关联。您可以在控制台中执行此操作，方法是将每个自行管理账户或 OU 的管理类型更改为集中管理和从我的组织继承。
5. （可选）为新组织账户选择本地配置默认设置。
6. 选择确认。

Security Hub API

要停止使用中心配置

1. 调用 UpdateOrganizationConfiguration API。
2. 将 `OrganizationConfiguration` 对象中的 `ConfigurationType` 字段设置为 `LOCAL`。如果您有现有的配置策略或策略关联，API 会返回错误。要解除配置策略的关联，请调用 `StartConfigurationPolicyDisassociation` API。要删除配置策略，请调用 `DeleteConfigurationPolicy` API。
3. 如果要在新组织账户中自动启用 Security Hub，请将 `AutoEnable` 字段设置为 `true`。默认情况下，此字段的值为 `false`，并且 Security Hub 不会在新组织账户中自动启用。（可选）如果要在新组织账户中自动启用默认安全标准，请将 `AutoEnableStandards` 字段

设置为 DEFAULT。这是默认值。如果不想在新组织账户中自动启用默认安全标准，请将 AutoEnableStandards 字段设置为 NONE。

API 请求示例：

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

要停止使用中心配置

1. 运行 update-organization-configuration命令。
2. 将 organization-configuration 对象中的 ConfigurationType 字段设置为 LOCAL。如果您有现有的配置策略或策略关联，命令会返回错误。要解除配置策略关联，请运行 start-configuration-policy-disassociation 命令。要删除配置策略，请运行 delete-configuration-policy 命令。
3. 如果要在新组织账户中自动启用 Security Hub，请包含 auto-enable 参数。默认情况下，此参数的值为 no-auto-enable，并且 Security Hub 不会在新组织账户中自动启用。（可选）如果要在新组织账户中自动启用默认安全标准，请将 auto-enable-standards 字段设置为 DEFAULT。这是默认值。如果不想在新组织账户中自动启用默认安全标准，请将 auto-enable-standards 字段设置为 NONE。

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

管理管理员和成员账户

如果您的 AWS 环境有多个账户，则可以将使用 AWS Security Hub 的账户视为成员账户，并将其与单个管理员账户关联。管理员可以监控您的整体安全状况，对成员账户执行允许的操作。管理员还可以大规模执行各种账户管理任务，例如监控预计使用成本和评测账户配额。

您可以通过两种方式将成员账户与管理员关联：将 Security Hub 与 AWS Organizations 集成，或者在 Security Hub 中手动发送和接受成员资格邀请。

使用 AWS Organizations 管理账户

AWS Organizations 是一项全球账户管理服务，使 AWS 管理员能够整合和管理多个 AWS 账户。它提供账户管理和整合账单功能，这些功能旨在满足预算、安全性和合规性需求。该服务不收取额外费用，可与多个 AWS 服务 集成，包括 AWS Security Hub、Amazon Macie 和 Amazon GuardDuty。有关更多信息，请参阅 AWS Organizations 用户指南。

在集成 Security Hub 和 AWS Organizations 时，组织管理账户会指定一名 Security Hub 委托管理员。Security Hub 会在指定的 AWS 区域 中的委托管理员账户中自动启用。

指定委托管理员后，我们建议使用中心配置在 Security Hub 中管理账户。这是自定义 Security Hub 并确保为组织提供足够的安全覆盖的有效方法。

中心配置让委托管理员能够跨多个组织账户和区域自定义 Security Hub，而不必逐个区域配置。您可以为整个组织创建配置策略，也可以为不同的账户和 OU 创建不同的配置策略。这些策略指定了在关联账户中启用还是禁用 Security Hub，以及启用哪些安全标准和控件。

委托管理员可将账户指定为集中管理或自行管理。集中管理的账户只能由委托管理员配置。自行管理账户可以自行指定设置。

如果您不选择使用中心配置，则委托管理员配置 Security Hub（称为本地配置）的能力将更为有限。在本地配置下，委托管理员可以在当前区域的新组织账户中自动启用 Security Hub 和默认安全标准。但现有账户不使用这些设置，因此账户加入组织后可能会出现配置偏差。

除了这些新账户设置外，本地配置是针对特定账户和特定区域的。每个组织账户必须在每个区域单独配置 Security Hub 服务、标准和控件。本地配置也不支持使用配置策略。

通过邀请手动管理账户

如果您拥有独立账户或未与 Organizations 集成，则必须在 Security Hub 中通过邀请手动管理成员账户。独立账户不能与 Organizations 集成，因此需要手动管理。如果您将来添加其他账户，我们建议与 AWS Organizations 集成，并使用中心配置。

使用手动账户管理时，要将一个账户指定为 Security Hub 管理员。管理员账户可以查看成员账户中的数据，对成员账户的调查发现执行某些操作。Security Hub 管理员邀请其他账户成为成员账户，当潜在成员账户接受邀请后，管理员与成员关系即建立。

手动账户管理不支持使用配置策略。如果没有配置策略，管理员就无法通过为不同的账户配置变量设置来集中自定义 Security Hub。相反，每个组织账户必须在每个区域中单独为自己启用和配置 Security Hub。这可能会增加确保在使用 Security Hub 的所有账户和区域中实现充分安全覆盖的难度和时间。这还可能导致配置偏差，因为成员账户可以指定自己的设置，而无需管理员输入。

要通过邀请管理账户，请参阅通过邀请管理账户。

使用管理账户 AWS Organizations

您可以 AWS Security Hub 与 AWS Organizations组织中的账户集成 Security Hub，然后对其进行管理。

要将 Security Hub 与集成 AWS Organizations，你需要在中创建一个组织 AWS Organizations。组织管理账户会将一个账户指定为该组织的 Security Hub 委托管理员。然后，委托管理员可以为组织中的其他账户启用 Security Hub，将这些账户添加为 Security Hub 成员账户，并对成员账户采取允许的操作。Security Hub 委托管理员可以为多达 1 万个成员账户启用和管理 Security Hub。

委托管理员的配置能力范围取决于您是否使用中心配置。启用中心配置后，您无需在每个成员账户和 AWS 区域中单独配置 Security Hub。委托管理员可以在各区域的指定成员账户和组织单位（OU）中强制执行特定的 Security Hub 设置。

Security Hub 委托管理员账户可以对成员账户执行以下操作：

- 如果使用中心配置，请通过创建 Security Hub 配置策略为成员账户和 OU 中心配置 Security Hub。配置策略可用于启用和禁用 Security Hub、启用和禁用标准以及启用和禁用控件。
- 在将新账户添加到组织时，自动将其视为 Security Hub 成员账户。如果您使用中心配置，则与 OU 关联的配置策略包括属于 OU 的现有账户和新账户。
- 将现有组织账户视为 Security Hub 成员账户。如果您使用中心配置，这种情况会自动出现。

- 取消关联属于该组织的成员账户。如果您使用中心配置，则只有在将成员账户指定为自行管理之后，才能取消其关联。或者，您可以将禁用 Security Hub 的配置策略与特定的集中管理成员账户相关联。

有关委托管理员可以对成员账户执行的操作的完整列表，请参阅允许对账户执行的操作。

本节中的主题说明了如何将 Security Hub 与组织中的账户集成， AWS Organizations 以及如何为组织中的账户管理 Security Hub。在相关时，每个部分都确定了中心配置用户在管理方面的好处和差异。

主题

将 Security Hub 与 AWS Organizations

要集成 AWS Security Hub 和 AWS Organizations，您可以在 Organizations 中创建组织，然后使用组织管理帐户指定委托的 Security Hub 管理员帐户。这使得 Security Hub 成为组织中值得信赖的服务。它还 AWS 区域 为委托的管理员账户启用当前的 Security Hub，并允许授权管理员为成员账户启用 Security Hub，查看成员账户中的数据，以及对成员账户执行其他允许的操作。

如果您使用中心配置，则委托管理员还可以创建 Security Hub 配置策略，指定应如何在组织账户中配置 Security Hub 服务、标准和控件。

创建企业

组织是您为整合组织而创建的实体， AWS 账户 以便您可以将其作为一个单位进行管理。

您可以使用 AWS Organizations 控制台创建组织，也可以使用来自 AWS CLI 或其中一个 SDK API 中的命令来创建组织。有关详细说明，请参阅《AWS Organizations 用户指南》中的创建组织。

您可以使用集中 AWS Organizations 查看和管理组织内的所有帐户。一个组织有一个管理账户以及零个或多个成员账户。您可以以分层树状结构来组织账户，将根放在树顶部，组织单位（OU）嵌套在根下。每个账户都可以直接放在根中，也可以放在层次结构的其中一个 OU 中。OU 是特定账户的容器。例如，您可以创建一个财务 OU，其中包括与财务操作相关的所有账户。

选择委派的 Security Hub 管理员的建议

如果您在手动邀请流程中拥有管理员帐户，并且正在过渡到使用进行账户管理 AWS Organizations，我们建议将该帐户指定为委托的 Security Hub 管理员。

尽管 Security Hub API 和控制台允许组织管理帐户成为委托的 Security Hub 管理员，但我们建议选择两个不同的帐户。这是因为有权访问组织管理账户来管理账单的用户可能与需要访问 Security Hub 进行安全管理的用户不同。

我们建议您在所有区域使用同一个委托管理员。如果您选择使用中心配置，Security Hub 会自动在您的主区域和任何关联区域中指定相同的委托管理员。

验证权限以配置委派的管理员

要指定和移除委托的 Security Hub 管理员帐户，组织管理帐户必须具有在 Security Hub 中`DisableOrganizationAdminAccount`执行`EnableOrganizationAdminAccount`和操作的权限。Organizations 管理账户还必须拥有 Organizations 的管理权限。

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

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

指定委派管理员

要指定委派的 Security Hub 管理员帐户，您可以使用 Security Hub 控制台、Security Hub API 或 AWS CLI。Security Hub AWS 区域 仅在当前区域设置委托管理员，您必须在其他区域重复该操作。如果您开始使用中心配置，则 Security Hub 会自动在主区域和关联区域中设置相同的委托管理员。

组织管理账户不必启用 Security Hub 即可指定委派的 Security Hub 管理员帐户。

我们建议组织管理账户不是委派的 Security Hub 管理员账户。但是，如果您选择组织管理帐户作为 Security Hub 的委托管理员，则该管理帐户必须启用 Security Hub。如果管理账户未启用 Security Hub，则必须手动为其启用 Security Hub。无法为组织管理账户自动启用 Security Hub。

> **Note**
>
> 您必须使用以下方法之一指定委派的 Security Hub 管理员。使用 Organizations API 指定委派的 Security Hub 管理员并不能反映在 Security Hub 中。

选择您的首选方法，然后按照步骤指定委派的 Security Hub 管理员帐户。

Security Hub console

在入职时指定委派的 Security Hub 管理员

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 选择转到 Security Hub。系统会提示你登录组织管理账户。
3. 在指定委托管理员页面的委托管理员账户部分，指定委托管理员账户。我们建议选择您为其他 AWS 安全与合规服务设置的相同委托管理员。
4. 选择添加委托管理员。系统会提示您登录委托管理员账户（如果您尚未登录），以便继续使用中心配置进行登录。如果您不想启用中心配置，请选择取消。您的委托管理员已设置完毕，但您尚未使用中心配置。

从 “设置” 页面指定委派的 Security Hub 管理员

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在 Security Hub 导航窗格中，选择设置。然后，选择常规。
3. 如果当前分配了 Security Hub 管理员账户，则必须先删除当前账户，然后才能指定新账户。

   在委派管理员下，要删除当前账户，请选择删除。
4. 输入您要指定为 Security Hub 委派管理员账户的账户 ID。

   您必须在所有区域指定同一个 Security Hub 管理员账户。如果您指定的账户与其他区域指定的账户不同，控制台会返回错误。
5. 选择 Delegate（委派）。

Security Hub API, AWS CLI

在组织管理账户中，使用 Security Hub API 的EnableOrganizationAdminAccount操作。如果您使用的是 AWS CLI，请运行该enable-organization-admin-account命令。提供委派的 Security Hub 管理员的 AWS 账户 ID。

以下示例指定委派的 Security Hub 管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

移除或更改委派的管理员

> **Warning**
>
> 在使用中心配置时，无法使用 Security Hub 控制台或 Security Hub API 来更改或删除委托管理员账户。如果组织管理账户使用 AWS Organizations 控制台或 AWS Organizations API 更改或移除委派的 Security Hub 管理员，Security Hub 会自动停止集中配置，并删除您的配置策略和策略关联。成员账户保留其在更改或删除委托管理员之前的配置。

只有组织管理帐户才能移除委派的 Security Hub 管理员帐户。

要更改委派的 Security Hub 管理员，必须先移除当前委派的管理员帐户，然后再指定一个新帐户。

如果您使用 Security Hub 控制台删除一个区域的委托管理员，该管理员将在所有区域中被自动删除。

Security Hub API 仅从发出 API 调用或命令的区域中移除委派的 Security Hub 管理员账户。您必须在其他区域重复执行此操作。

如果您使用 Organizations API 移除委托的 Security Hub 管理员账户，则该账户将在所有区域中自动删除。

移除委托管理员（Organizations API， AWS CLI）

您可以使用 Organizations 删除所有区域中委派的 Security Hub 管理员。

如果您使用中心配置来管理账户，则移除委托管理员账户会导致您的配置策略和策略关联被删除。成员账户保留其在更改或删除委托管理员之前的配置。但是，这些账户无法再由已删除的委托管理员账户进行管理。它们成为自行管理账户，必须在每个区域单独配置。

选择您的首选方法，然后按照说明删除委托的 Security Hub 管理员帐户 AWS Organizations。

Organizations API, AWS CLI

移除委派的 Security Hub 管理员

在组织管理账户中，使用 Organizations API 的DeregisterDelegatedAdministrator操作。如果您使用的是 AWS CLI，请运行该deregister-delegated-administrator命令。提供委派管理员的账户 ID 以及 Security Hub 的服务主体，即`securityhub.amazonaws.com`。

以下示例删除了委派的 Security Hub 管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

移除委派的管理员（Security Hub 控制台）

您可以使用 Security Hub 控制台移除所有区域中委派的 Security Hub 管理员。

移除委派的 Security Hub 管理员帐户后，成员账户将与已移除的委托 Security Hub 管理员账户解除关联。

成员账户仍会启用 Security Hub。它们将变为独立账户，直至新的 Security Hub 管理员将它们启用为成员账户。

如果组织管理帐户不是 Security Hub 中已启用的帐户，请使用 “欢迎使用 Security Hub” 页面上的选项。

从 “欢迎使用 Security Hub” 页面中移除委派的 Security Hub 管理员帐户

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 选择转到 Security Hub。
3. 在委托管理员下，选择删除。

如果组织管理帐户是 Sec urity Hub 中已启用的帐户，请使用 “设置” 页面的 “常规” 选项卡上的选项。

从 “设置” 页面移除委派的 Security Hub 管理员帐户

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在 Security Hub 导航窗格中，选择设置。然后，选择常规。
3. 在委托管理员下，选择删除。

移除委托的管理员（Security Hub API， AWS CLI）

您可以使用 Security Hub API 或 Security Hub 操作 AWS CLI 来移除委派的 Security Hub 管理员。当您使用其中一种方法删除委托管理员时，只有在发出 API 调用或命令的区域中的委托管理员才会被删除。Security Hub 不会更新其他区域，也不会移除中的委托管理员账户 AWS Organizations。

选择您的首选方法，然后按照以下步骤使用 Security Hub 删除委托的 Security Hub 管理员帐户。

Security Hub API, AWS CLI

移除委派的 Security Hub 管理员

在组织管理账户中，使用 Security Hub API 的DisableOrganizationAdminAccount操作。如果您使用的是 AWS CLI，请运行该disable-organization-admin-account命令。提供委派的 Security Hub 管理员的账户 ID。

以下示例删除了委派的 Security Hub 管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

禁用 Security Hub 与的集成 AWS Organizations

AWS Organizations 组织与集成后 AWS Security Hub，Organizations 管理帐户随后可以禁用该集成。作为组织管理账户的用户，您可以通过在 AWS Organizations中禁用对 Security Hub 的可信访问来实现。

当您禁用 Security Hub 的可信访问权限时，会出现以下情况：

- Security Hub 在中失去了其作为可信服务的地位 AWS Organizations。
- Security Hub 委托管理员账户将无法访问 AWS 区域中所有 Security Hub 成员账户的 Security Hub 设置、数据和资源。
- 如果您使用的是中心配置，Security Hub 会自动停止在您的组织中使用它。您的配置策略和策略关联会被删除。账户保留在您禁用可信访问之前的配置。
- 所有 Security Hub 成员账户都将成为独立账户，并保留其当前设置。如果在一个或多个区域为成员账户启用 Security Hub，则这些地区的账户将继续启用 Security Hub。启用的标准和控件也保持不变。您可以在每个账户和地区中分别更改这些设置。但是，该账户不再与任何地区的委托管理员账户关联。

有关禁用可信服务访问的结果的更多信息，请参阅《AWS Organizations 用户指南》 AWS 服务中的“AWS Organizations 与其他人一起使用”。

要禁用可信访问，您可以使用 AWS Organizations 控制台、Organizations API 或 AWS CLI。只有组织管理账户的用户，可以禁用 Security Hub 的可信服务访问权限。有关所需权限的详细信息，请参阅 AWS Organizations 用户指南中的禁用可信访问所需的权限。

在禁用可信访问权限之前，可以选择与组织的委托管理员合作，禁用成员账户的 Security Hub，并清理这些账户的 Security Hub 资源。

选择您的首选方法，然后按照以下步骤禁用 Security Hub 的受信任访问。

Organizations console

要禁用 Security Hub 的可信访问

1. AWS Management Console 使用 AWS Organizations 管理账户的凭据登录。
2. 通过以下网址打开 Organizations 控制台：https://console.aws.amazon.com/organizations/。
3. 在导航窗格中，选择服务。
4. 在集成服务下，选择 AWS Security Hub。
5. 选择 Disable trusted access（禁用信任访问权限）。
6. 确认您要禁用可信访问权限。

Organizations API

要禁用 Security Hub 的可信访问

调用 AWS Organizations API 的禁用AWSServiceAccess操作。对于 `ServicePrincipal` 参数，指定 Security Hub 服务主体（`securityhub.amazonaws.com`）。

AWS CLI

要禁用 Security Hub 的受信任访问

运行 AWS Organizations API 的disable-aws-service-access命令。对于 `service-principal` 参数，指定 Security Hub 服务主体（`securityhub.amazonaws.com`）。

示例：

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

在新组织账户中自动启用 Security Hub。

当新账户加入您的组织时，他们会被添加到 AWS Security Hub 控制台的 “帐户” 页面上的列表中。对于组织账户，类型为按组织。默认情况下，新账户在加入组织时不会成为 Security Hub 成员。他们的身份是非成员。委派的管理员账户可以自动将新账户添加为成员，并在他们加入组织时在这些账户中启用 Security Hub。

> **Note**
>
> 尽管默认情况下，您的许多区域 AWS 区域 处于活动状态 AWS 账户，但您必须手动激活某些区域。在本文档中，这些区域被称为可选区域。要在选择加入区域的新账户中自动启用 Security Hub，该账户必须先激活该区域。只有账户所有者才能激活选择加入区域。有关选择加入区域的更多信息，请参阅指定 AWS 区域 您的账户可以使用的区域。

根据您使用的是中心配置（推荐）还是本地配置，此过程会有所不同。

自动启用新组织账户（中心配置）

如果您使用集中配置，则可以通过创建启用 Security Hub 的配置策略在新的和现有组织帐户中自动启用 Security Hub。然后，您可以将该策略与组织根目录或特定组织单位 (OU) 相关联。

如果您将启用了 Security Hub 的配置策略与特定 OU 相关联，则会自动在属于该 OU 的所有账户（现有账户和新账户）中启用 Security Hub。不属于 OU 的新账户是自行管理的，并且不会自动启用 Security Hub。如果您将启用了 Security Hub 的配置策略与根相关联，则会自动在加入该组织的所有账户（现有账户和新账户）中启用 Security Hub。如果一个账户通过应用或继承使用不同的策略，或者是自行管理的，则为例外情况。

在配置策略中，您还可以定义应在 OU 中启用哪些安全标准和控件。要生成针对已启用标准的控制结果，OU 中的账户必须已 AWS Config 启用并配置为记录所需资源。有关 AWS Config 录制的更多信息，请参阅启用和配置 AWS Config。

有关创建配置策略的说明，请参阅创建和关联 Security Hub 配置策略。

自动启用新组织账户（本地配置）

当您使用本地配置并开启自动启用时，Security Hub 会将新组织账户添加为成员，并在当前区域的这些账户中启用 Security Hub。其他地区均不受影响。此外，开启自动启用不会在现有组织账户中启用 Security Hub，除非这些账户已添加为成员账户。

开启自动启用后，如果当前区域有新账户加入组织，也会自动为其启用默认安全标准。默认标准是 AWS 基础安全最佳实践 (FSBP) 和互联网安全中心 (CIS) AWS 基金会基准 v1.2.0。您不能更改默认标准。如果您想在整个组织中启用其他标准，或者为选定的账户和 OU 启用标准，我们建议使用中心配置。

要生成默认标准（和其他启用的标准）的控制结果，您组织中的账户必须已 AWS Config 启用并配置为记录所需资源。有关 AWS Config 录制的更多信息，请参阅启用和配置 AWS Config。

选择您的首选方法，然后按照步骤在新组织账户中自动启用 Security Hub。这些说明仅在您使用本地配置时适用。

Security Hub console

要将新组织账户自动启用为 Security Hub 成员

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用委托管理员账户凭证登录。
2. 在 Security Hub 导航窗格中的设置下，选择配置。
3. 在账户部分，打开自动启用账户。

Security Hub API

要将新组织账户自动启用为 Security Hub 成员

从委托管理员账户调用 `UpdateOrganizationConfiguration` API。将 `AutoEnable` 字段设置为 `true`，以便在新组织账户中自动启用 Security Hub。

AWS CLI

要将新组织账户自动启用为 Security Hub 成员

从委托管理员账户运行 `update-organization-configuration` 命令。添加 `auto-enable` 参数以在新组织账户中自动启用 Security Hub。

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

在新组织账户中手动启用 Security Hub

如果您在新组织帐户加入组织时没有自动启用 Security Hub，则可以将这些帐户添加为成员，并在他们加入组织后在其中手动启用 Security Hub。您还必须手动启用 Security Hub AWS 账户 ，因为您之前已取消与某个组织的关联。

> **Note**
>
> 如果您使用中心配置，则本节不适用于您。如果您使用中心配置，您可以创建配置策略，在特定成员账户和组织单位（OU）中启用 Security Hub。您还可以在这些账户和 OU 中启用特定的标准和控件。

如果账户已经是其他组织中的成员账户，则无法在账户中启用 Security Hub。

您也无法在当前已暂停的账户中启用 Security Hub。如果您尝试在已暂停的账户中启用服务，则账户状态会更改为账户已暂停。

- 如果该账户未启用 Security Hub，则会在该账户中启用 Security Hub。除非您关闭默认安全标准，否则账户中还会启用 AWS AWS 基础安全最佳实践 (FSBP) 标准和 CIS Foundations Benchmark v1.2.0。

  组织管理账户除外。无法在组织管理账户中自动启用 Security Hub。您必须在组织管理账户中手动启用 Security Hub，然后才能将其作为成员账户添加。
- 如果该账户已经启用了 Security Hub，则 Security Hub 不会对该账户进行任何其他更改。它仅启用成员资格。

为了让 Security Hub 生成控制结果，必须 AWS Config 启用并配置成员账户以记录所需的资源。有关更多信息，请参阅启用和配置 AWS Config。

选择您的首选方法，然后按照步骤将组织账户启用为 Security Hub 成员账户。

Security Hub console

要手动将组织账户启用为 Security Hub 成员

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用委托管理员账户凭证登录。

2. 在 Security Hub 导航窗格中的设置下，选择配置。
3. 在账户列表中，选中要启用的每个组织账户。
4. 选择操作，然后选择添加成员。

Security Hub API

要手动将组织账户启用为 Security Hub 成员

从委托管理员账户调用 CreateMembers API。对于要启用的每个账户，请提供账户 ID。

与手动邀请流程不同，当您调用 CreateMembers 启用组织账户时，无需发送邀请。

AWS CLI

要手动将组织账户启用为 Security Hub 成员

从委托管理员账户运行 create-members 命令。对于要启用的每个账户，请提供账户 ID。

与手动邀请流程不同，当您运行 create-members 启用组织账户时，无需发送邀请。

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

示例

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

取消成员账户与您组织的关联

要停止接收和查看来自 AWS Security Hub 成员账户的调查结果，您可以取消该成员账户与您的组织的关联。

> **Note**
>
> 如果您使用中心配置，则取消关联的工作原理会有所不同。您可以创建一个配置策略，在一个或多个集中管理的成员账户中禁用 Security Hub。之后，这些账户仍然是组织的一部分，但不会生成 Security Hub 的调查发现。如果您使用中心配置，但也有手动邀请的成员账户，则可以取消关联一个或多个手动邀请的账户。

使用管理的成员账户 AWS Organizations 无法取消其账户与管理员账户的关联。只有管理员账户可以取消成员账户的关联。

取消关联成员账户不会删除该账户。相反，它会从组织中删除该成员账户。已取消关联的成员账户变为独立账户 AWS 账户 ，不再由 Security Hub 与 AWS Organizations的集成管理。

选择您的首选方法，然后按照步骤取消成员账户与组织的关联。

Security Hub console

要取消成员账户与组织之间的关联

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用委托管理员账户凭证登录。
2. 在导航窗格中的设置下，选择配置。
3. 在账户部分，选中要取消关联的账户。如果您使用中心配置，则可以选择一个手动邀请的账户来取消与 `Invitation accounts` 选项卡的关联。仅当您使用中心配置时，才可以看到此选项卡。
4. 选择操作，然后选择取消账户关联。

Security Hub API

要取消成员账户与组织的关联

从委托管理员账户调用 `DisassociateMembers` API。您必须提供成员账户的 AWS 账户 ID 才能解除关联。要查看成员账户列表，请调用 `ListMembers` API。

AWS CLI

要取消成员账户与组织的关联

从委托管理员账户运行 `>disassociate-members` 命令。您必须提供成员账户的 AWS 账户 ID 才能解除关联。要查看成员账户列表，请运行 `>list-members` 命令。

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

示例

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

您也可以使用 AWS Organizations 控制台或 AWS 软件开发工具包取消成员账户与您的组织的关联。AWS CLI有关更多信息，请参阅 AWS Organizations 用户指南中的从组织中删除成员账户。

通过邀请管理账户

您可以通过两种方式集中管理多个 AWS Security Hub 帐户：将 Security Hub 与其集成， AWS Organizations 或者手动发送和接受会员邀请。如果您拥有独立账户或未与 Organizations 集成，则必须使用手动流程。在手动账户管理中，Security Hub 管理员邀请账户成为成员。当潜在成员接受邀请时，管理员与成员的关系即已建立。一个 Security Hub 管理员账户可以管理多达 1,000 个基于邀请的成员账户的 Security Hub。

> **Tip**
>
> 如果您在 Security Hub 中创建基于邀请的组织，则随后可以转换到使用 AWS Organizations。如果您有多个成员账户，我们建议您通过管理账户 AWS Organizations。

对于您通过手动邀请流程邀请的账户，可以跨区域聚合调查结果和其他数据。但是，管理员必须邀请来自聚合区域和所有关联区域的成员账户，才能使跨区域聚合发挥作用。此外，成员账户必须在聚合区域和所有关联区域中启用 Security Hub，这样管理员才能查看成员账户的调查结果。

手动邀请的成员账户不支持配置策略。相反，您必须在每个成员账户中以及使用手动邀请流程 AWS 区域 时分别配置 Security Hub 设置。

对于不属于您组织的账户，您还必须使用基于手动邀请的流程。例如，您的组织中可能不包含测试账号。或者，您可能想将来自多个组织的账户整合到一个 Security Hub 管理员账户下。Security Hub 管理员账户必须向属于其他组织的账户发送邀请。

在 Security Hub 控制台的配置页面上，通过邀请添加的账户列在邀请账户选项卡中。如果您使用 中央配置的工作原理，但同时邀请了组织外的账户，则可以在此选项卡中查看基于邀请的账户的调查发现。但是，Security Hub 管理员无法通过使用配置策略跨区域配置基于邀请的账户。

此部分介绍如何通过邀请管理成员账户。

主题

- 删除成员账户
- 取消关联您的管理员账户
- 转换到 AWS Organizations 以进行账户管理

添加和邀请成员账户

您的账户将成为接受您邀请的账户的 AWS Security Hub 管理员。

当您接受另一个账户的邀请时，您的账户成为成员账户，那个账户成为您的管理员。

如果您的账户是管理员账户，则您无法接受成为成员账户的邀请。

添加成员账户包括以下步骤：

1. 管理员账户将成员账户添加到他们的成员账户列表中。
2. 管理员账户向成员账户发送邀请。
3. 成员账户接受邀请。

添加成员账户

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

对于每个账户，您必须提供账户 ID 和一个电子邮件地址。电子邮件地址应该是就账户中的安全问题进行联系的电子邮件地址。它不用于验证账户。

选择您的首选方法，然后按照以下步骤添加成员账户。

Security Hub console

要将账户添加到您的成员账户列表中

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用管理员账户的凭证登录。
2. 在左侧窗格中，选择 Settings (设置)。
3. 在设置页面上，选择账户，然后选择添加账户。然后，您可以单独添加账户，也可以上传包含账户列表的 `.csv` 文件。

4. 要选择账户，请执行以下操作之一：

   - 要单独添加账户，在输入账户中，输入要添加的账户的账户 ID 和电子邮件地址，然后选择添加。

     为每个账户重复这一过程。
   - 要使用逗号分隔值 (.csv) 文件添加多个账户，请先创建该文件。该文件必须包含要添加的每个账户的账户 ID 和电子邮件地址。

     在 `.csv` 列表中，账户必须一行一个。`.csv` 文件的第一行必须包含标题。在标题中，第一列是 **`Account ID`**，第二列是 **`Email`**。

     后面的每一行必须包含要添加的账户的有效账户 ID 和电子邮件地址。

     以下是在文本编辑器中查看 `.csv` 文件时的示例。

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     在电子表格程序中，这些字段显示在单独的列中。基础格式仍以逗号分隔。您必须将账户 ID 的格式转化为非十进制数字。例如，账户 ID 444455556666 的格式不能为 444455556666.0。另外，请确保数字格式不会从账户 ID 中删除任何前导零。

     要选择文件，请在控制台上选择上传列表 (.csv)。然后选择浏览。

     选择该文件后，选择添加账户。
5. 添加完账户后，在要添加的账户下，选择下一步。

Security Hub API

要将账户添加到您的成员账户列表中

从管理员账户调用 `CreateMembers` API。对于要添加的每个成员账户，您都必须提供 AWS 账户 ID。

AWS CLI

要将账户添加到您的成员账户列表中

从管理员账户运行 `create-members` 命令。对于要添加的每个成员账户，您都必须提供 AWS 账户 ID。

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

示例

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

邀请成员账户

添加成员账户之后，您会向成员账户发送邀请。您也可以向已和管理员取消关联的账户重新发送邀请。

Security Hub console

要邀请潜在成员账户

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用管理员账户的凭证登录。
2. 在导航窗格中，选择设置，然后选择账户。
3. 要邀请的账户，请在状态列中选择邀请。
4. 当系统提示确认时，请选择邀请。

> **Note**
>
> 要向已取消关联的账户重新发送邀请，请在账户页面上选择每个已取消关联的账户。从操作中选择重新发送邀请。

Security Hub API

要邀请潜在成员账户

从管理员账户调用 `InviteMembers` API。对于要邀请的每个账户，您都必须提供 AWS 账户 ID。

AWS CLI

要邀请潜在成员账户

从管理员账户运行 `invite-members` 命令。对于要邀请的每个账户，您都必须提供 AWS 账户 ID。

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

示例

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

响应成员账户的邀请

您可以接受或拒绝成成员账户的邀请。

在您接受邀请后，您的账户将变为 AWS Security Hub 成员账户。发送邀请的账户将成为您的 Security Hub 管理员账户。管理员账户用户可以在 Security Hub 中查看您的成员账户的调查发现。

如果您拒绝邀请，则在管理员账户的成员账户列表中，您的账户将被标记为已放弃。

您只能接受一次成为会员账户的邀请。

在接受或拒绝邀请之前，您必须启用 Security Hub。

请记住，所有 Security Hub 账户都必须 AWS Config 启用并配置为记录所有资源。有关要求的详细信息 AWS Config，请参阅启用和配置 AWS Config。

接受邀请

选择您的首选方法，然后按照以下步骤接受邀请成为成员账户。

Security Hub console

要接受成员邀请

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择设置，然后选择账户。
3. 在管理员账户部分，开启接受，然后选择接受邀请。

Security Hub API

要接受成员邀请

调用 AcceptAdministratorInvitation API。您必须提供邀请标识符和管理员账户的 AWS 账户 ID。要检索有关邀请的详细信息，请使用 ListInvitations 操作。

AWS CLI

要接受成员邀请

运行 accept-administrator-invitation 命令。您必须提供邀请标识符和管理员账户的 AWS 账户 ID。要检索有关邀请的详细信息，运行 list-invitations 命令。

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

示例

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Security Hub 控制台继续使用 AcceptInvitation。它最终会改为使用 AcceptAdministratorInvitation。任何专门控制此功能访问权限的 IAM policy 都必须继续使用 AcceptInvitation。您还应在策略中添加 AcceptAdministratorInvitation，以确保在控制台开始使用 AcceptAdministratorInvitation 后正确的权限已到位。

拒绝邀请

您可以拒绝成为成员账户的邀请。当您在 Security Hub 控制台中拒绝邀请时，您的账户将在管理员账户的成员账户列表中会标记为已放弃。

当你拒绝邀请时，你必须登录收到邀请的成员账户。

选择您的首选方法，然后按照以下步骤拒绝邀请成为成员账户。

Security Hub console

要拒绝成员邀请

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

2. 在导航窗格中，选择设置，然后选择账户。
3. 在管理员账户部分，选择拒绝邀请。

Security Hub API

要拒绝成员邀请

调用 DeclineInvitations API。您必须提供发出邀请的管理员账户的 AWS 账户 ID。要查看有关您的邀请的信息，请使用 ListInvitations 操作。

AWS CLI

要拒绝成员邀请

运行 decline-invitations 命令。您必须提供发出邀请的管理员账户的 AWS 账户 ID。要查看有关您的邀请的信息，请运行 list-invitations 命令。

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

示例

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

取消关联成员账户

AWS Security Hub 管理员账户可以取消与成员账户的关联，以停止接收和查看来自该账户的调查结果。您必须首先取消关联成员账户，然后才能将其删除。

取消关联成员账户后，该账户仍将保留在您的成员账户列表中，其状态为已移除（已取消关联）。您的账户已从该成员账户的管理员账户信息中删除。

要恢复接收该账户的调查发现，您可以重新发送邀请。要完全移除成员账户，您可以删除该成员账户。

选择您的首选方法，然后按照步骤取消手动邀请的成员账户与管理员账户的关联。

Security Hub console

要取消手动邀请的成员账户的关联

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

使用管理员账户的凭证登录。

2. 在导航窗格中的设置下，选择配置。
3. 在账户部分，选中要取消关联的账户。
4. 选择操作，然后选择取消账户关联。

Security Hub API

要取消手动邀请的成员账户的关联

从管理员账户调用 DisassociateMembers API。您必须提供要取消关联的成员账户的 AWS 账户 ID。要查看成员账户列表，请使用 ListMembers 操作。

AWS CLI

要取消手动邀请的成员账户的关联

从管理员账户运行 disassociate-members 命令。您必须提供要取消关联的成员账户的 AWS 账户 ID。要查看成员账户列表，请运行 list-members 命令。

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

示例

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

删除成员账户

作为 AWS Security Hub 管理员帐户，您可以删除通过邀请添加的成员帐户。在您可以删除已启用的账户之前，您必须先取消其关联。

当您删除成员账户时，该账户将从列表中完全移除。要恢复该账户的成员资格，您必须将其添加并向其发送邀请，就像它是一个全新的成员账户一样。

您无法删除属于某个组织且使用与集成进行管理的帐户 AWS Organizations。

选择您的首选方法，然后按照以下步骤删除手动邀请的成员账户。

Security Hub console

要删除手动邀请的成员账户

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用管理员账户登录。
2. 在导航窗格中，选择设置，然后选择配置。
3. 选择邀请账户选项卡。然后，选择要删除的账户。
4. 选择操作，然后选择删除。此选项仅在您取消关联账户后可用。您必须先取消关联成员账户，然后才能将其删除。

Security Hub API

要删除手动邀请的成员账户

从管理员账户调用 `DeleteMembers` API。您必须提供要删除的成员账户的 AWS 账户 ID。要检索成员账户列表，请调用 `ListMembers` API。

AWS CLI

要删除手动邀请的成员账户

从管理员账户运行 `delete-members` 命令。您必须提供要删除的成员账户的 AWS 账户 ID。要检索成员账户列表，运行 `list-members` 命令。

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

示例

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

取消关联您的管理员账户

如果您的账户是通过邀请添加为 AWS Security Hub 成员账户的，则可以取消该成员账户与管理员账户的关联。取消关联成员账户后，Security Hub 不会将该账户的调查发现发送到管理员账户。

使用与的集成进行管理的成员账户 AWS Organizations 无法取消其账户与管理员账户的关联。只有 Security Hub 委托管理员才能解除与 Organizations 管理的成员账户的关联。

当您取消与管理员账户的关联后，您的账户将保留在管理员账户的成员列表中，状态为已放弃。但是，管理员账户不会收到有关您账户的任何调查发现。

在您取消与管理员账户的关联后，成为成员的邀请仍然有效。将来你可以再次接受邀请。

Security Hub console

要从管理员账户取消关联

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择设置，然后选择账户。
3. 在管理员账户部分，关闭接受，然后选择更新。

Security Hub API

要从管理员账户取消关联

调用 DisassociateFromAdministratorAccount API。

AWS CLI

要从管理员账户取消关联

运行 disassociate-from-administrator-account 命令。

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

> **Note**
>
> Security Hub 控制台继续使用 DisassociateFromMasterAccount。它最终会改为使用 DisassociateFromAdministratorAccount。任何专门控制此功能访问权限的 IAM policy 都必须继续使用 DisassociateFromMasterAccount。您还应在策略中添加 DisassociateFromAdministratorAccount，以确保在控制台开始使用 DisassociateFromAdministratorAccount 后正确的权限已到位。

转换到 AWS Organizations 以进行账户管理

在 AWS Security Hub 中手动管理账户时，必须邀请潜在的成员账户，并在每个 AWS 区域 中分别配置每个成员账户。

通过集成 Security Hub 和 AWS Organizations，您无需再发送邀请，还可以更好地控制在组织中配置和自定义 Security Hub 的方式。

可以使用组合方法，在这种方法中，您可以使用 AWS Organizations 集成，也可以手动邀请组织外部的账户。但我们建议仅使用 Organizations 集成。中心配置是一项功能，可帮助您跨多个账户和区域管理 Security Hub，仅当您与 Organizations 集成时才可用。

本节将介绍如何从基于邀请的手动账户管理转换到使用 AWS Organizations 管理账户。

将 Security Hub 与 AWS Organizations 集成

首先，您必须集成 Security Hub 和 AWS Organizations。

您可以完成以下步骤，来集成这些服务：

- 在 AWS Organizations 中创建组织。有关说明，请参阅《AWS Organizations 用户指南》中的创建组织。
- 在组织管理账户中，指定一个 Security Hub 委托管理员账户。

> **Note**
>
> 不能将组织管理账户设置为 DA 账户。

有关详细说明，请参阅 将 Security Hub 与 AWS Organizations。

完成上述步骤后，您就可以在 AWS Organizations 中授予对 Security Hub 的可信访问权限。这也会在当前 AWS 区域 中为委托管理员账户启用 Security Hub。

委托管理员可以在 Security Hub 中管理组织，主要方法是添加组织账户作为 Security Hub 成员账户。管理员还可以访问这些账户的某些 Security Hub 设置、数据和资源。

在转换到使用 Organizations 进行账户管理后，基于邀请的账户不会自动成为 Security Hub 成员。只有您添加到新组织的账户才能成为 Security Hub 成员。

中心配置与本地配置

激活集成后，您可以使用组织管理账户。有关信息，请参阅 使用管理账户 AWS Organizations。账户管理因组织的配置类型而异。

组织可能有两种配置类型：本地配置和集中配置。默认配置类型为本地配置。要查看当前配置类型，请在 Security Hub 控制台的导航窗格上选择设置，然后选择配置。您也可以调用 DescribeOrganizationConfiguration API 查看配置类型。

在本地配置下，委托管理员账户可以选择在新账户加入组织时自动启用 Security Hub 和默认安全标准。这些新账户设置在当前区域生效。其他 Security Hub 设置必须由每个区域的每个成员账户单独配置。

我们建议使用中心配置，而不是本地配置。在中心配置下，委托管理员账户可以创建跨多个区域生效的 Security Hub 配置策略，并在组织的各个账户和组织单位（OU）中指定 Security Hub 功能。您可以对整个组织应用单一的配置策略，也可以对不同的账户和 OU 应用不同的配置策略。例如，您可以在生产账户中启用一组标准和控件，在测试账户中启用另一组标准和控件。DA 可以根据需要编辑配置策略。

有关中心配置工作原理的更多信息，请参阅中央配置的工作原理。

有关从本地配置切换到中心配置的说明，请参阅开始使用中心配置。

允许对账户执行的操作

管理员和成员账户有权访问下表中记录的 AWS Security Hub 操作。表中的值具有以下含义：

- Any：该账户可为同一管理员下的任何成员账户执行操作。
- Current：该账户只能为其本身执行操作（当前登录的账户）。
- Dash：表示该账户无法执行操作。

如表中所示，允许执行的操作因是否与 AWS Organizations 集成以及组织使用的配置类型而异。有关集中配置和本地配置之间的差异的信息，请参阅使用 AWS Organizations 管理账户。

Security Hub 不会将成员账户的调查发现复制到管理员账户。在 Security Hub 中，所有的调查发现都会被摄取到特定账户的特定区域。在每个区域，管理员账户均可以查看和管理其在该区域的成员账户的调查发现。

如果设置了聚合区域，管理员账户可以查看和管理复制到聚合区域的关联区域的成员账户调查发现。有关跨区域聚合的更多信息，请参阅跨区域聚合。

此表反映了管理员和成员账户的默认权限。您可以使用自定义 IAM policy 进一步限制对 Security Hub 特性和功能的访问。有关指导和示例，请参阅博客文章《为 AWS Security Hub 根据用户角色调整 IAM policy》。

与 Organizations 集成并使用中心配置时允许执行的操作

与 Organizations 集成并使用中心配置时，管理员账户和成员账户可以按如下方式访问 Security Hub 操作。

操作	Security Hub 委托管理员账户	集中管理的成员账户	自行管理的成员账户
创建和管理 Security Hub 配置策略	对于自我管理和集中管理的账户	–	–
查看组织账户	任何	–	–
取消成员账户的关联	任何	–	–
删除成员账户	任何非组织账户	–	–
禁用 Security Hub	对于当前账户和集中管理的账户	–	Current
查看调查发现和调查发现历史	任何	Current	Current
更新调查发现	任何	Current	Current
查看见解结果	任何	Current	Current
查看控件详细信息	任何	Current	Current
开启或关闭整合控件调查发现	任何	–	–
启用和禁用标准	对于当前账户和集中管理的账户	–	Current
启用和禁用控件	对于当前账户和集中管理的账户	–	Current
启用和禁用集成	Current	Current	Current
配置跨区域聚合	任何	–	–

操作	Security Hub 委托管理员账户	集中管理的成员账户	自行管理的成员账户
选择主区域和关联区域	Any（必须停止并重新启动中心配置才能更改主区域）	–	–
配置自定义操作	Current	Current	Current
配置自动化规则	任何	–	–
配置自定义见解	Current	Current	Current

与 Organizations 集成并使用本地配置时允许执行的操作

与 Organizations 集成并使用本地配置时，管理员账户和成员账户可以按如下方式访问 Security Hub 操作。

操作	Security Hub 委托管理员账户	成员账户
创建和管理 Security Hub 配置策略	–	–
查看组织账户	任何	–
取消成员账户的关联	任何	–
删除成员账户	–	–
禁用 Security Hub	–	Current（如果账户与委托管理员解除关联）
查看调查发现和调查发现历史	任何	Current
更新调查发现	任何	Current
查看见解结果	任何	Current
查看控件详细信息	任何	Current

操作	Security Hub 委托管理员账户	成员账户
开启或关闭整合控件调查发现	任何	–
启用和禁用标准	Current	Current
在新组织账户中自动启用 Security Hub 和默认标准	对于当前账户和新组织账户	–
启用和禁用控件	Current	Current
启用和禁用集成	Current	Current
配置跨区域聚合	任何	–
配置自定义操作	Current	Current
配置自动化规则	任何	–
配置自定义见解	Current	Current

允许对基于邀请的账户执行的操作

使用基于邀请的方法手动管理账户而不是与 AWS Organizations 集成时，管理员和成员账户可以按如下方式访问 Security Hub 操作。

操作	Security Hub 管理员账户	成员账户
创建和管理 Security Hub 配置策略	–	–
查看组织账户	任何	–
取消成员账户的关联	任何	Current
删除成员账户	任何	–
禁用 Security Hub	Current（如果没有启用的成员账户）	Current（如果账户与管理员账户解除关联）

操作	Security Hub 管理员账户	成员账户
查看调查发现和调查发现历史	任何	Current
更新调查发现	任何	Current
查看见解结果	任何	Current
查看控件详细信息	任何	Current
开启或关闭整合控件调查发现	任何	–
启用和禁用标准	Current	Current
在新组织账户中自动启用 Security Hub 和默认标准	–	–
启用和禁用控件	Current	Current
启用和禁用集成	Current	Current
配置跨区域聚合	任何	–
配置自定义操作	Current	Current
配置自动化规则	任何	–
配置自定义见解	Current	Current

关于账户管理的限制和建议

以下各节总结了在 AWS Security Hub中管理成员账户时应注意的一些限制和建议。

成员账户的最大数量

如果您使用与的集成 AWS Organizations，Security Hub 在每个委托管理员账户中最多支持 10,000 个成员账户 AWS 区域。如果您手动启用和管理 Security Hub，Security Hub 在每个区域中每个管理员账户最多支持 1,000 个成员账户邀请。

账户和区域

按组织列出的成员资格

如果您将 Security Hub 与集成 AWS Organizations，则组织管理帐户可以为 Security Hub 指定委派管理员 (DA) 帐户。不能将组织管理账户设置为组织的 DA。虽然 Security Hub 允许这样做，但我们建议不要将组织管理账户设为 DA。

我们建议在所有区域选择同一个 DA 账户。如果使用中心配置，则 Security Hub 会在您为组织配置 Security Hub 的所有区域中设置相同的 DA 账户。

我们还建议您在 AWS 安全与合规服务中选择相同的 DA 帐户，以帮助您在单一管理平台中管理与安全相关的问题。

通过邀请的成员资格

对于通过邀请创建的成员账户，管理员与成员账户的关联仅在发出邀请的地区创建。管理员账户必须在要使用的每个区域中启用 Security Hub。然后，管理员账户会邀请每个账户成为该区域的成员账户。

对管理员与成员关系的限制

> **Note**
>
> 如果您将 Security Hub 集成与 AWS Organizations，并且尚未手动邀请任何成员帐户，则此部分不适用于您。

账户不能既是管理员账户又是成员账户。

一个成员账户只能与一个管理员账户关联。如果组织账户由 Security Hub 管理员账户启用，则该账户将无法接受来自其他账户的邀请。如果账户已接受邀请，Security Hub 组织管理员就无法启用该账户。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 AWS 服务的调查结果，例如亚马逊 GuardDuty、Amazon Inspector 和 Amazon Macie。Security Hub 还允许用户从调查 GuardDuty 结果转向在 Amazon Detective 中开始调查。

但是，您在这些其他服务中设置的管理员与成员关系不会自动应用于 Security Hub。Security Hub 建议所有这些服务使用与管理员账户相同的账户。此管理员账户应该是负责安全工具的账户。同一个账户也应该是 AWS Config的聚合器账户。

例如， GuardDuty 管理员账户 A 中的用户可以在 GuardDuty 控制台上查看 GuardDuty成员账户 B 和 C 的调查结果。如果账户 A 随后启用了 Security Hub，则账户 A 的用户不会自动在 Security Hub 中看到账户 B 和 C 的搜索 GuardDuty结果。这些账户还需要建立 Security Hub 管理员与成员关系。

为此，请将账户 A 设为 Security Hub 管理员账户 ，并使账户 B 和 C 成为 Security Hub 成员账户。

账户操作对 Security Hub 数据的影响

这些账户操作会对 AWS Security Hub 数据产生以下影响。

Security Hub 已启用

如果您使用中心配置，委托管理员（DA）可以创建 Security Hub 配置策略，在特定账户和组织单位（OU）中禁用 AWS Security Hub。在这种情况下，您的主区域和任何关联区域中的指定账户和 OU 将禁用 Security Hub。

如果不使用中心配置，则必须在启用了 Security Hub 的每个账户和区域中单独禁用。

如果在管理员账户中禁用了 Security Hub，则不会为管理员账户生成新的调查发现。如果在 DA 账户中禁用了 Security Hub，则也无法使用中心配置。现有结果将在 90 天后删除。

与其他 AWS 服务 的集成将被删除。

已启用的安全标准和控件将被禁用。

其他 Security Hub 数据和设置（包括自定义操作、见解和第三方产品订阅）将会保留。

会员帐号与管理员帐号解除关联

当成员账户与管理员账户解除关联时，管理员账户将失去查看成员账户中的调查发现的权限。但两个账户仍启用了 Security Hub。

如果使用中心配置，则 DA 无法为与 DA 账户解除关联的成员账户配置 Security Hub。

为管理员账户定义的自定义设置或集成不会应用于前成员账户的调查发现。例如，取消关联账户后，您可能会在管理员账户中使用自定义操作作为 Amazon EventBridge 规则中的事件模式。但是，此自定义操作不能在成员账户中使用。

在 Security Hub 管理员账户的账户列表中，已删除账户的状态为已解除关联。

成员账户从组织中移除

从组织中删除成员账户后，Security Hub 管理员账户将失去在成员账户中查看调查发现的权限。但两个账户仍启用了 Security Hub，其设置与删除之前的设置相同。

如果使用中心配置，则在将成员账户从委托管理员所属的组织中删除后，就将无法为其配置 Security Hub。但除非您手动更改，否则该账户将保留删除之前的设置。

在 Security Hub 管理员账户的账户列表中，已删除账户的状态为已删除。

账户已暂停

当账户在 AWS 中被暂停时，该账户将失去在 Security Hub 中查看其调查发现的权限。没有为该账户生成任何新的调查发现。已暂停账户的管理员账户可以查看现有账户的调查发现。

对于组织账户，成员账户状态也可以更改为账户已暂停。如果在管理员账户尝试启用账户的同时该账户被暂停，则会发生这种情况。已暂停账户的管理员账户无法查看该账户的调查发现。否则，暂停状态不会影响成员账户状态。

如果使用中心配置，则当委托管理员尝试将配置策略与已暂停的账户关联时，策略关联将会失败。

90 天后，账户将被终止或重新激活。重新激活账户后，将恢复其 Security Hub 权限。如果成员账户状态为账户已暂停，则管理员账户必须手动启用该账户。

账户已关闭

AWS 账户 关闭后，Security Hub 会按如下方式对关闭做出响应。

Security Hub 会将账户的调查发现保留自账户关闭生效之日起 90 天内。90 天期限结束后，Security Hub 会永久删除该账户的所有结果。

- 要将结果保留超过 90 天，您可以使用带有 EventBridge 规则的自定义操作，将结果存储在 Amazon S3 存储桶中。只要 Security Hub 保留调查发现，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发现。
- 如果该账户是 Security Hub 管理员账户，则会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《AWS 账单与成本管理用户指南》中的关闭账户。

Important

对于 AWS 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

通过跨区域聚合，您可以将多个区域的调查发现、调查发现更新、见解、控件合规状态和安全评分汇总到单个聚合区域。然后，您可以管理聚合区域中的所有这些数据。

> **Note**
>
> 在中 AWS GovCloud (US)，跨区域聚合仅支持对调查结果、发现更新和洞察进行跨 AWS GovCloud (US)区域聚合。具体而言，您只能汇总 AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）之间的调查结果、最新发现和见解。在中国区域，跨区域聚合仅支持对中国区域的调查发现、调查发现更新和见解进行跨区域聚合。具体而言，您只能聚合中国（北京）和中国（宁夏）之间的调查发现、调查发现更新和见解。

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

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

要查看跨区域安全评分和合规状态，请向使用 Security Hub 的 IAM 角色添加以下权限：

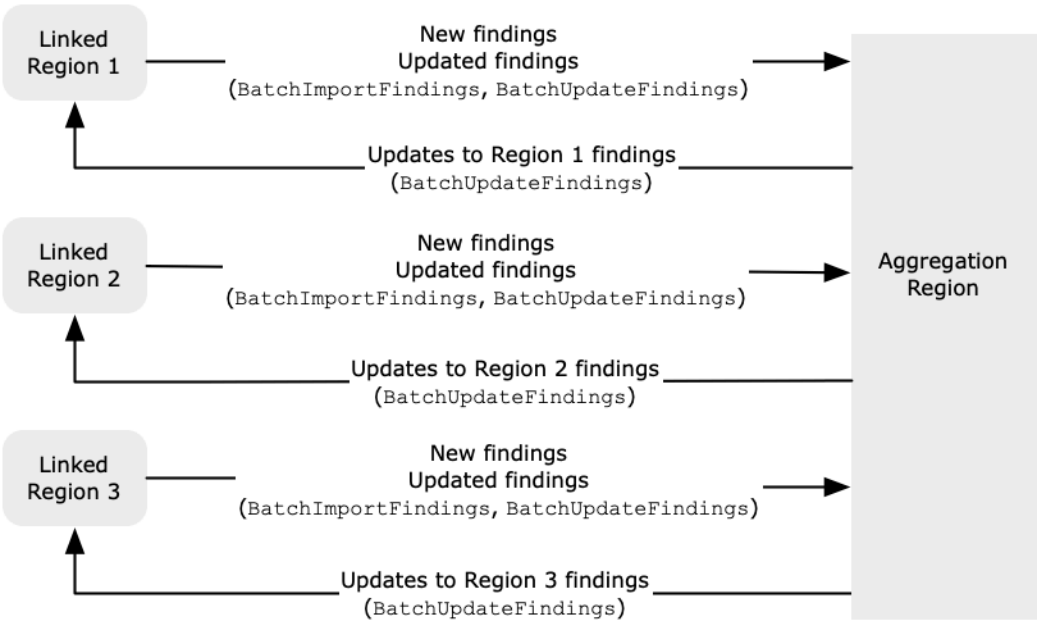
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

如何执行跨区域聚合工作

启用跨区域聚合后，Security Hub 会将以下数据从链接的区域复制到聚合区域。每个启用了跨区域聚合的账户都会发生这种情况。

- 调查发现
- 洞察
- 控制合规性状态
- 安全分数

除了先前列表中的新数据之外，Security Hub 还会在关联区域和聚合区域之间复制对这些数据的更新。关联区域中发生的更新将被复制到聚合区域。聚合区域中发生的更新将被复制到关联区域。



如果聚合区域和关联区域的更新相互冲突，则使用最新的更新。

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

在聚合区域中，摘要页面提供了您在关联区域中活动调查发现的视图。有关信息，请参阅按严重性查看跨区域调查发现摘要。其他用于分析调查发现的摘要页面面板还会显示来自关联区域的信息。

您在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的控件数量和已启用的控件数量来计算的。此外，如果在至少一个关联区域中启用了控件，则该控件将在聚合区域的安全标准详细信息页面上可见。标准详情页面上控件的合规状态反映了关联区域的调查发现。如果与控件关联的安全检查在一个或多个关联区域中失败，则该控件的合规性状态将在聚合区域的标准详细信息页面上显示为失败。安全检查的数量包括来自所有关联区域的调查发现。

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

管理员和成员账户的聚合

独立账户、成员账户和管理员账户可以配置跨区域聚合。如果由管理员配置，则管理员帐户的存在对于跨区域聚合在托管账户中发挥作用至关重要。如果管理员账户被移除或取消与成员账户的关联，则该成员账户的跨区域聚合将停止。即使账户在管理员-成员关系开始之前启用了跨区域聚合，也是如此。

当管理员帐户启用跨区域聚合时，Security Hub 会将管理员帐户在所有关联区域中生成的数据复制到聚合区域。此外，Security Hub 可以识别与该管理员关联的成员账户，并且每个成员账户都继承管理员的跨区域聚合设置。Security Hub 会将成员账户在所有关联区域生成的数据复制到聚合区域。

管理员可以访问和管理来自管理区域内所有成员账户的安全调查结果。但是，作为 Security Hub 管理员，您必须登录到聚合区域才能查看来自所有成员账户和关联区域的聚合数据。

作为 Security Hub 成员账户，您必须登录到聚合区域才能查看来自您账户的所有关联区域的汇总数据。成员账户无权查看其他成员账户的数据。

管理员账户可以手动邀请成员账户，也可以作为与之集成的组织的委托管理员 AWS Organizations。对于手动邀请的成员账户，管理员必须邀请来自聚合区域和所有关联区域的账户，才能使跨区域聚合生效。此外，成员账户必须在聚合区域和所有关联区域中启用 Security Hub，这样管理员才能查看成员账户的调查结果。如果您不将聚合区域用于其他目的，则可以在该区域禁用 Security Hub 标准和集成以防止收费。

如果您计划使用跨区域聚合，并且拥有多个管理员账户，我们建议您遵循以下最佳实践：

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

> **Note**
>
> 要了解跨区域聚合如何影响中央配置，请参阅中心配置和跨区域聚合。

中心配置和跨区域聚合

中央配置是 Security Hub 中的一项可选功能，如果您与 AWS Organizations之集成，则可以使用该功能。如果您使用中心配置，则委托管理员账户可以为组织中的账户和组织单元（OU）配置 Security Hub 服务、标准和控件。要配置账户和 OU，委托管理员需要创建 Security Hub 配置策略。配置策略可用于定义是启用还是禁用 Security Hub，以及启用哪些标准和控件。委托管理员将配置策略与特定账户、OU 或根（整个组织）关联起来。

委托管理员只能从聚合区域为组织创建和管理配置策略。此外，配置策略在聚合区域和所有关联区域中生效。您无法创建仅适用于某些关联区域而不适用于其他区域的配置策略。在中心配置中，聚合区域称为主区域。要实现中心配置，必须将同一个区域用作主区域，要实现跨区域聚合，必须将同一区域用作聚合区域。有关跨区域聚合的信息，请参阅跨区域聚合。

要使用中央配置，必须指定一个主区域和至少一个关联区域。

更改跨区域聚合设置可能会影响您的配置策略。当您添加关联区域时，您的配置策略将在该区域生效。如果该区域是选择加入的区域，则必须启用该区域才能使您的配置策略在该区域生效。相反，当您移除关联区域后，配置策略在该区域不再生效。在该区域中，账户将保留移除关联区域时的区域设置。您可以更改这些设置，但必须在分别每个账户和区域中进行更改。

如果您移除或更改主区域，则您的配置策略和策略关联将被删除。您将不能再在任何区域使用中心配置或创建配置策略。账户将保留更改或移除主区域之前的设置。您可以随时更改这些设置，但由于您不再使用中心配置，因此必须分别在每个账户和区域中修改设置。如果您指定了新的主区域，则可以使用中心配置并再次创建配置策略。

有关中心配置的更多信息，请参阅中央配置的工作原理。

启用跨区域聚合

您必须从要指定为聚合区域 AWS 区域 的中启用跨区域聚合。

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 AWS 一般参考中的启用区域。

启用跨区域聚合（控制台）

启用跨区域聚合时，您可以选择关联区域。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。

要启用跨区域聚合

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 使用 AWS 区域 选择器登录要用作聚合区域的区域。
3. 在 Security Hub 导航菜单中，选择设置，然后选择区域。
4. 对于调查发现聚合，选择配置调查发现聚合。

   默认情况下，聚合区域设置为无聚合区域。
5. 在聚合区域下，选择将当前区域指定为聚合区域的选项。
6. （可选）对于关联区域，选择要从中聚合数据的区域。
7. 要自动聚合来自分区中新区域的数据（当 Security Hub 支持这些区域并且您选择加入这些区域），请选择关联未来区域。

8. 选择保存。

启用跨区域聚合（Security Hub API，AWS CLI）

您可以使用 Security Hub API 启用跨区域聚合。

要通过 Security Hub API 启用跨区域聚合，您需要创建一个调查发现聚合器。您必须从要用作聚合区域的区域中创建调查发现聚合器。

要创建调查结果聚合器（Security Hub API，AWS CLI）

- Security Hub API：在要用作聚合区域的区域中，使用 `CreateFindingAggregator` 操作。对于 `RegionLinkingMode`，您可以从以下选项中进行选择：
  - `ALL_REGIONS`- Security Hub 汇总来自所有地区的数据。Security Hub 还会汇总来自新区域的数据（当这些区域是支持的并且您选择加入这些区域）。
  - `ALL_REGIONS_EXCEPT_SPECIFIED`- Security Hub 汇总来自所有区域的数据，但您要排除的区域除外。Security Hub 还会汇总来自新区域的数据（当这些区域是支持的并且您选择加入这些区域）。用 `Regions` 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 不会自动汇总来自新区域的数据。使用 `Regions` 用于提供要聚合的区域列表。
- AWS CLI： 在命令行处，运行 `create-finding-aggregator` 命令。用空格分隔每个区域。

```
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，为所选区域配置了跨区域聚合。聚合区域为美国东部（弗吉尼亚州北部）。关联区域是美国西部（北加利福尼亚）和美国西部（俄勒冈州）。

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

查看跨区域聚合设置

您可以从任何区域查看当前的跨区域聚合配置。配置包括聚合区域、关联区域以及是否自动关联新区域。

查看跨区域聚合配置（控制台）

设置页面的区域选项卡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的选项。请参阅 the section called “启用跨区域聚合”。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 Security Hub 支持且您选择加入的新区域的调查发现、见解、控件状态和安全评分
- 关联区域列表

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

您可以使用 Security Hub API 或 AWS CLI 查看当前的跨区域聚合配置。您可以在任何区域中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， AWS CLI）

- Security Hub API：使用 `GetFindingAggregator` API。发出请求时，必须提供调查发现聚合器 ARN。要获取调查发现聚合器 ARN，请使用 `ListFindingAggregators`。
- AWS CLI： 在命令行处，运行 `get-finding-aggregator` 命令。要获取调查发现聚合器 ARN，请使用 `list-finding-aggregators`。

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

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关联 AWS 区域 。您还可以更改是否自动汇总来自新区域的调查发现、见解、控件状态和安全评分。

只有在 AWS 账户中启用选择加入区域后，才会对该区域实施跨区域聚合的更改。在 2019 年 3 月 20 日当天或之后 AWS 推出的区域为可选区域。

当您停止汇总来自关联区域的数据时，Security Hub 不会从聚合区域中删除任何现有的汇总数据。

您不能使用更新过程来更改聚合区域。要更改聚合区域，您必须执行以下操作：

1. 停止跨区域聚合。请参阅 the section called “停止跨区域聚合”。
2. 更改为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”。

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。

除 AWS 区域 聚合区域外，“查找结果” 聚合面板会显示一条消息，提示您必须在聚合区域中编辑配置。选择此消息以显示导航至聚合区域的链接。

要更改当前聚合区域的关联区域

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 更改为当前聚合区域。
3. 在 Security Hub 导航菜单中，选择设置，然后选择区域。
4. 在调查发现聚合下，选择编辑。
5. 在关联区域下，更新所选的关联区域。
6. 如有必要，更改是否选择关联未来区域。此设置决定 Security Hub 是否自动关联新区域（当 Security Hub 支持这些区域并且您选择加入这些区域）。
7. 选择保存。

更新跨区域聚合配置（Security Hub API， AWS CLI）

您可以使用 Security Hub API 或 AWS 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。

您可以更改区域关联模式。如果关联模式为 `ALL_REGIONS_EXCEPT_SPECIFIED` 或 `SPECIFIED_REGIONS`，则可以更改已排除或已包含区域的列表。

更改排除或已包含区域的列表时，必须提供包含更新的完整列表。例如，假设您当前美国东部（俄亥俄州）的调查发现，同时还要聚合美国西部（俄勒冈州）的调查发现。调用 `UpdateFindingAggregator` 时，您需要提供一份同时包含美国东部（俄亥俄州）和美国西部（俄勒冈州）的 `Regions` 列表。

要更新跨区域聚合（Security Hub API， AWS CLI）

- Security Hub API；使用 UpdateFindingAggregator API 操作。要识别调查发现聚合器，必须提供调查发现聚合器 ARN。要获取调查发现聚合器 ARN，请使用 ListFindingAggregators。

  您提供区域关联模式以及已排除或已包含区域的更新列表。

- AWS CLI： 在命令行处，运行 update-finding-aggregator 命令。用空格分隔每个区域。

```
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，跨区域聚合配置已更改为选定区域的聚合。从当前聚合区域（即美国东部（弗吉尼亚州北部））运行命令。关联区域是美国西部（北加利福尼亚）和美国西部（俄勒冈州）。

```
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者想要更改聚合区域，请停止跨区域聚合。

停止跨区域聚合后，Security Hub 会停止聚合数据。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）

您必须从当前聚合区域停止跨区域聚合。

在聚合区域以外的区域中，调查发现聚合面板会显示一条消息，提示您必须在聚合区域中编辑配置。选择此消息可显示切换到聚合区域的链接。

要停止跨区域聚合

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 更改为当前聚合区域。
3. 在 Security Hub 导航菜单中，选择设置，然后选择区域。

4. 在调查发现聚合下，选择编辑。
5. 在聚合区域下，选择无聚合区域。
6. 选择保存。
7. 在确认对话框的确认字段中，键入 **Confirm**。
8. 选择确认。

停止跨区域聚合（Security Hub API， AWS CLI）

您可以使用 Security Hub API 来停止跨区域聚合。您必须从聚合区域停止跨区域聚合。

停止跨区域聚合（Security Hub API， AWS CLI）

- Security Hub API：使用 DeleteFindingAggregator 操作。要识别要删除的调查发现聚合器，请提供调查发现聚合器 ARN。要获取调查发现聚合器 ARN，请使用 ListFindingAggregators。
- AWS CLI： 在命令行处，运行 delete-finding-aggregator 命令。

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

Sec AWS urity Hub 中的调查结果

AWS 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 AWS 账户、资源和工作负载的安全性所需的工作量。

Security Hub 接收来自以下来源的调查发现。

- Security Hub 检查已启用的控制。请参阅 the section called “生成和更新控件调查发现”。
- 与 AWS 服务 您启用的集成。请参阅 the section called “AWS 服务 集成”。
- 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”。
- 您配置的自定义集成。请参阅 the section called “使用自定义产品集成”。

Security Hub 使用一种名为 “ AWS 安全调查结果格式” 的标准调查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”。

Security Hub 将各集成产品的调查发现进行关联，以确定最重要产品的优先级。

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 还允许您聚合各区域的调查发现，以便您可以从一个地方查看所有调查发现。请参阅 跨区域聚合。

主题

- 在 AWS Security Hub中创建和更新调查发现
- 管理和查看查找结果的详细信息和历史记录
- 对调查结果采取行动 AWS Security Hub
- AWS 安全调查结果格式 (ASFF)

在 AWS Security Hub中创建和更新调查发现

在中 AWS Security Hub，查找结果可能来自以下类型的查找提供者之一。

- Security Hub 中已启用的安全控件
- 已启用与其他集成 AWS 服务
- 支持与第三方产品的集成

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 BatchUpdateFindingsAPI 操作更新调查结果的调查状态。BatchUpdateFindings也可以由代表客户使用票务、事件管理、编排、补救或 SIEM 工具。

  通过 Security Hub 控制台，客户可以管理调查发现的工作流程状态，以及将调查发现发送到自定义操作。请参阅 the section called “根据结果采取措施。”。

Security Hub 还会自动更新和删除调查发现。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调查发现聚合到聚合区域。Security Hub 还会复制调查发现的更新。关联区域中发生的更新将被复制到聚合区域。聚合区域中发生的更新将复制到链接区域。有关跨区域聚合的更多信息，请参阅 跨区域聚合。

主题

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、SIEM、票务工具和SOAR工具用于BatchUpdateFindings更新他们对寻找提供商的调查结果的调查。请参阅 the section called “使用 BatchUpdateFindings”。

每当 AWS Security Hub 收到创建或更新调查结果的BatchImportFindings请求时，它都会自动在 Amazon 中生成一个Security Hub Findings - Imported事件 EventBridge。请参阅 the section called “自动响应和补救”。

账户要求和批处理大小

BatchImportFindings 必须由以下之一调用：

- 与调查发现关联的账户。关联账户的标识符是调查发现的 AwsAccountId 属性值。

- 被列入正式的 Security Hub 合作伙伴集成允许列表的账户。

Security Hub 只能接受已启用 Security Hub 的账户的调查发现更新。还必须启用结果提供商。如果禁用 Security Hub，或者未启用调查发现提供商集成，则会在 `FailedFindings` 列表中返回调查发现，并显示 `InvalidAccess` 错误。

`BatchImportFindings` 每批最多接受 100 个调查发现，每个调查发现最多 240 KB，每批最多 6 MB。每个区域每个账户的节流速率限制为 10 TPS（每秒事务数），突增值为 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发现，Security Hub 需要检查 `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` 与现有调查发现确实匹配，则 Security Hub 会检查 `UpdatedAt` 字段是否有更新。

- 如果更新的 `UpdatedAt` 匹配或出现在现有调查发现的 `UpdatedAt` 之前，则忽略更新。
- 如果更新的 `UpdatedAt` 出现在现有结果的 `UpdatedAt` 之后，则更新现有结果。

BatchImportFindings 的受限属性

对于现有发现，查找提供程序不能`BatchImportFindings`用于更新以下属性和对象。这些属性只能使用 `BatchUpdateFindings` 进行更新。

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

Security Hub 会忽略在`BatchImportFindings`请求这些属性和对象时提供的任何内容。客户或代表他们行事的其他提供商使用 `BatchUpdateFindings` 来更新属性和对象。

使用 FindingProviderFields

查找提供者也不应使用`BatchImportFindings`来更新以下属性。

- `Confidence`
- `Criticality`

- RelatedFindings
- Severity
- Types

相反，调查发现提供商使用 FindingProviderFields 对象为这些属性提供值。

示例

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

对于 BatchImportFindings 请求，Security Hub 按如下方式 FindingProviderFields 处理顶级属性中的值。

（首选）**BatchImportFindings**为 **FindingProviderFields** 中的属性提供值，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 FindingProviderFields 中属性的值。

仅当属性尚未由BatchUpdateFindings更新时，它才会将该值复制到顶级属性。

BatchImportFindings 为顶级属性提供值，但不为 **FindingProviderFields** 中的相应属性提供值。

例如，BatchImportFindings 提供 Confidence，但不提供 FindingProviderFields.Confidence。

Security Hub 使用该值来更新 FindingProviderFields 中的属性。它会覆盖任何现有值。

只有当顶级属性尚未由 BatchUpdateFindings 更新时，Security Hub 才会更新该属性。

BatchImportFindings 为顶级属性和 **FindingProviderFields** 中的相应属性提供了一个值。

例如，BatchImportFindings 同时提供 Confidence 和 FindingProviderFields.Confidence。

对于新调查发现，Security Hub 使用 FindingProviderFields 中的值填充顶级属性和 FindingProviderFields 中的相应属性。它不使用提供的顶级属性值。

对于现有调查发现，Security Hub 使用这两个值。但是，只有当属性尚未由 BatchUpdateFindings 更新时，它才会更新顶级属性值。

使用来自的batch-import-findings命令 AWS CLI

在中 AWS Command Line Interface，您可以使用batch-import-findings命令来创建或更新调查结果。

您需要将每个调查发现作为一个 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",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "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",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

使用 BatchUpdateFindings 更新结果

BatchUpdateFindings 操作用于更新与客户处理调查发现提供商的调查发现相关的信息。它可以由客户使用，也可以由代表客户工作的 SIEM、票务、事件管理或 SOAR 工具使用。您可以使用BatchUpdateFindings更新 AWS 安全结果格式 (ASFF) 中的特定字段。

您不能使用 BatchUpdateFindings 来创建新调查发现。您可以用它来一次更新多达 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 the section called “自动响应和补救”。

BatchUpdateFindings不会更改查找结果的UpdatedAt字段。 UpdatedAt仅反映搜索结果提供者的最新更新。

BatchUpdateFindings 可用字段

管理员账户可以使用 >BatchUpdateFindings 更新其账户或其成员账户的调查发现。成员账户可以使用 >BatchUpdateFindings 更新其账户的调查发现。

客户只能使用 >BatchUpdateFindings 来更新以下字段和对象。

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity

- Types
- UserDefinedFields
- VerificationState
- Workflow

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

例如，您可能只允许将成员账户从 Workflow.Status 设置为 RESOLVED。或者，您可能不允许成员账户更改 Severity.Label。

配置对 BatchUpdateFindings 的访问权限

您可以配置 IAM policy 来限制使用 BatchUpdateFindings 来更新字段和字段值。

在限制访问 BatchUpdateFindings 的语句中，使用以下值：

- Action 是 securityhub:BatchUpdateFindings
- Effect 是 Deny
- 对于 Condition，您可以根据以下条件拒绝 BatchUpdateFindings 请求：
  - 调查发现包括一个特定的字段。
  - 调查发现包括一个特定的字段值。

条件键

这些是限制访问 BatchUpdateFindings 的条件键。

ASFF 字段

ASFF 字段的条件键如下所示：

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

<fieldName> 替换为 ASFF 字段。配置访问 BatchUpdateFindings 权限时，请在 IAM policy 中包含一个或多个特定的 ASFF 字段，而不是父级字段。例如，要限制对 Workflow.Status 字段的访问权限，您必须在策略中包含 securityhub:ASFFSyntaxPath/Workflow.Status 而不是 Workflow 父级字段。

禁止对某个字段进行所有更新

要防止用户对特定字段进行任何更新，请使用如下条件：

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
                }
}
```

例如，以下语句表示 BatchUpdateFindings 不能用于更新工作流程状态。

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

禁用特定的字段值

要防止用户将字段设置为特定值，请使用如下条件：

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

例如，以下语句表示 BatchUpdateFindings 不能用于把 Workflow.Status 设置为 SUPPRESSED。

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

```
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

您还可以提供不允许的值的列表。

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

例如，以下语句表示BatchUpdateFindings 不能用于把 Workflow.Status 设置为 RESOLVED 或 SUPPRESSED。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

使用来自的 batch-update-findings命令 AWS CLI

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

对于每项要更新的调查发现，您都要提供生成该调查发现的产品的调查发现 ID 和 ARN。

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

在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 格式更新 Note 对象的示例：

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

以下是使用快捷方式格式的相同更新：

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

《AWS CLI 命令参考》提供了每个字段的 JSON 和快捷语法。

以下 >batch-update-findings 示例更新了两个结果，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"}'
```

这是同一示例，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"
```

管理和查看查找结果的详细信息和历史记录

在 AWS Security Hub 控制台上查看查找列表的方法有多种：

- 调查结果页面-显示所有已启用的控件和产品集成的调查结果的完整列表。默认情况下，会显示处于NEW或NOTIFIED工作流程状态的活动调查结果。
- 控件详细信息页面-显示在过去 24 小时内针对特定控件生成的结果列表。
- 见解页面-显示匹配见解的发现结果列表。洞察力是特定于集合的发现。有关更多信息，请参阅 the section called “查看见解结果和调查结果”。
- 集成页面-显示集成产品 AWS 服务 或第三方产品生成的调查结果列表。

您可以对这些列表中的发现结果进行筛选和分组，以专注于特定类型的发现。您也可以在前面的页面上选择特定的调查结果以查看有关该发现的详细信息。

要以编程方式查看发现结果列表，请使用 Security Hub API 的GetFindings操作。您可以添加过滤器来检索特定类型的调查结果。

如果您启用跨区域聚合，则可以检索跨区域的控制状态、安全评分、见解和发现。在聚合区域中，查找数据包括来自聚合区域和关联区域的数据。在其他区域，查找数据仅针对该区域。有关配置跨区域聚合的信息，请参阅跨区域聚合。

筛选和分组结果（控制台）

在 Security Hub 控制台的 “调查结果” 页面、“集成” 页面或 “见解” 页面上显示发现结果列表时，将根据记录状态和工作流程状态对列表进行预过滤。这是用于见解或集成的筛选条件的补充。

记录状态表示查找结果是处于活动状态还是已存档。默认情况下，查找结果列表仅显示有效的查找结果。查找结果提供者可以将查找结果存档。 AWS Security Hub 如果关联的资源被删除，还会自动存档控制结果。

工作流程状态表示调查结果的状态。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。您可以更新调查结果的工作流程状态。

如果您启用了查找结果聚合并登录到聚合区域，则可以在 “调查结果” 和 “见解” 页面上按区域筛选结果。

有关使用控制结果的信息，请参见the section called “对结果进行筛选和排序”。此页面上的信息适用于 “调查结果”、“见解” 和 “集成” 页面上的查找列表。

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。

筛选调查发现列表时，Security Hub 将 AND 逻辑应用于筛选条件集。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 为产品名称的筛选器和资源类型的筛选器，则匹配的结果必须符合这两个条件。`AwsS3Bucket`

不过，Security Hub 会对使用的属性相同但值不同的筛选条件应用 OR 逻辑。例如，您可以将两者 GuardDuty 和 Amazon Inspector 添加为商品名称的筛选值。在这种情况下，如果调查结果由任一用户 GuardDuty 或 Amazon Inspector 生成，则该结果与之匹配。

向结果列表添加筛选器

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 要显示调查发现列表，请执行以下操作之一：
   - 在 Security Hub 导航窗格中，选择结果。
   - 在 Security Hub 导航窗格中，选择见解。选择见解。然后在结果列表上，选择一个见解结果。
   - 在 Security Hub 导航窗格中，选择集成。选择查看集成的调查发现。
3. 在 “添加筛选器” 框中，为 “过滤器” 选择一个过滤器。

   当您按公司名称或产品名称进行筛选时，控制台将使用顶层`CompanyName`和`ProductName`字段。API 使用 `ProductFields` 中的值。
4. 选择筛选器匹配类型。

   对于字符串筛选条件，您可以从以下比较选项中进行选择：

   - 是——查找与筛选值完全匹配的值。
   - 以...开头——查找以筛选值开头的值。
   - 不是——查找与筛选值不匹配的值。
   - 不以...开头——查找不以筛选值开头的值。

   对于数值筛选条件，您可以选择是提供单个数字简单还是数值范围范围。

   对于日期或时间筛选条件，您可以选择是提供从当前日期时间开始的时间长度滚动窗口还是提供具体日期范围固定范围。

   添加多个筛选条件具有以下交互作用：

   - 是和以...开头筛选条件由“或”连接。如果一个值包含任何筛选条件值，则该值匹配。例如，如果您将“严重性”标签指定为“重大”，“严重性”标签为“高”，则结果将包括重大和高严重性结果。

- 不是，不以...开头筛选条件由“和”连接的。仅当值不包含任何这些筛选条件值时才匹配。例如，如果您将 “严重性” 标签指定为 “低”，“严重性” 标签不为 “中”，则结果不包括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 i s not 或 a 不以过滤器开头。

5. 指定筛选器值。

   对于字符串过滤器，筛选器值区分大小写。

   例如，对于来自 Security Hub 的调查发现，产品名称为 Security Hub。如果使用 EQUALS 运算符查看来自 Security Hub 的调查发现，则必须输入 **`Security Hub`** 作为筛选条件值。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 结果。如果您输入 **`sec`**，则不会显示任何 Security Hub 结果。

6. 选择 应用。

对结果进行分组

除了变更筛选条件外，您还可以根据所选属性的值对结果进行分组。

对调查发现进行分组时，调查发现列表将替换为匹配调查发现中选定属性的值列表。对于每个值，列表显示与其他筛选条件匹配的调查发现数。

例如，如果您按 AWS 账户 ID 对发现结果进行分组，则会看到账户标识符列表，其中包含每个账户的匹配结果数量。

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，将显示该值的匹配调查发现列表。

将结果分组到结果列表中

1. 在调查发现列表上，选择添加筛选条件框。
2. 对于分组，请选择分组依据。
3. 在列表中，选择要用于分组的属性。
4. 选择 应用。

更改筛选条件值或分组属性

对于现有筛选器，您可以更改筛选器值。您还可以更改分组属性。

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。

编辑筛选条件或分组属性

1. 在筛选的调查发现列表中，选择筛选或分组属性。
2. 对于分组依据，选择新属性，然后选择应用。
3. 对于筛选条件，选择新值，然后选择应用。

删除筛选条件或分组属性

要删除筛选条件或分组属性，请选择 x 图标。

列表会自动更新以反映更改。删除分组属性时，列表将从字段值列表更改回调查发现列表。

可用的查找信息

您可以在 Security Hub 控制台上或通过调用 Security Hub API 的GetFindings操作来获取各种发现的详细信息。以下是您可以获得的查找详细信息的部分列表。

- 应用程序元数据-如果您创建了应用程序，则提供调查结果中涉及的应用程序的名称和 Amazon 资源名称 (ARN)。并向其中添加了 AWS 应用程序标签。我们建议在中创建应用程序AWS Service Catalog AppRegistry。
- 查找历史记录-提供过去 90 天内的查找结果历史记录。
- 在 Detective 中查找调查（仅限控制台）— 提供一个链接，使用自动日志收集、安全分析和 AWS 服务 资源探索工具，进一步调查 Detective 中的调查结果。如果您启用 Detective，则只有从其他人那里收到的 Security Hub 调查结果 AWS 服务 才会包含此信息。
- 查找提供者字段-显示查找提供者提供的置信度、重要性、相关发现、严重性和查找结果类型的值。
- 参数-显示安全控制的当前参数值。Security Hub 在对控件进行安全检查时使用这些参数值。
- 补救-提供修复失败控制结果的说明的链接。
- 资源-提供有关查找结果中涉及的 AWS 资源的信息。
- 资源标签-为查找结果中涉及的资源提供标签键和值信息。您可以为标记 API `GetResources` 操作支持的资源 AWS Resource Groups 添加标签。如果 AWS 安全调查结果格式 (ASFF) `Resource.Id`

字段填充了资源 ARN，Security Hub 会通过服务相关角色调用此操作并检索资源 AWS 标签。无效的资源 ID 将被忽略。有关在调查结果中包含资源标签的更多信息，请参阅标签。

- 类型和相关调查结果-包含有关查找结果类型的信息。
- 漏洞详情-有关在发现结果中检测到的漏洞和受影响的软件包的信息。如果您启用 Amazon Inspector 来查看亚马逊检查器发送到 Security Hub 的调查结果，则可以获得这些详细信息。

请查看以下章节，了解如何访问这些详细信息以获得调查结果。

查看发现历史记录

调查发现历史记录是 Security Hub 的一项功能，可让您跟踪过去 90 天内对调查发现所做的更改。它适用于活跃和已存档的调查发现。调查发现历史记录提供了随着时间的推移对调查发现所做的更改的不可改变的跟踪，包括更改的内容、发生的时间以及由哪个用户所做的更改。

具体而言，您可以跟踪对 AWS 安全调查结果格式 (ASFF) 中的字段所做的更改。Security Hub 会根据自动化规则跟踪您手动进行的变更。

查找历史记录可在 Security Hub 控制台、API 和 AWS CLI。

如果您登录了 Security Hub 管理员账户，则可以获取该管理员账户和所有成员账户的调查发现历史记录。

选择您的首选方法，然后按照步骤查看查找历史记录。

Security Hub console

查看发现历史记录

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在左侧导航窗格中，选择发现。
3. 选择一个调查发现。在出现的面板中，选择历史记录选项卡。

Security Hub API

查看发现历史记录

1. 运行 GetFindings，或者如果你使用的是 AWS CLI，则运行get-findings命令。 根据需要使用适当的筛选器来识别您要查看历史记录的发现。API 响应将为您提供调查发现的 `ProductArn` 和 `Id`。在第三步中，您需要这些字段的值。

2. 运行 GetFindingHistory，或者如果你使用的是 AWS CLI，则运行get-finding-history命令。
3. 使用 ProductArn 和 Id 字段确定要获取历史记录的调查发现。有关这些字段的更多信息，请参阅AwsSecurityFindingIdentifier。每个请求只能获取一个调查发现的历史记录。
4. 为StartTime. 和提供值EndTime，将查找历史记录限制在特定的时间段内。
5. 为 MaxResults 提供一个值，将调查发现历史记录限制为特定数量的结果。如果未提供，API 响应将返回调查发现历史记录的前 100 个结果。
6. 为 NextToken 提供一个值，以查看调查发现的后续 100 个结果（如适用）。在初始 API 请求中，NextToken 的值应为 NULL。

以下 CLI 命令检索指定发现的历史记录。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

查看发现详情

选择您的首选方法，然后按照步骤在 Security Hub 中查看查找详情。

Security Hub console

查看发现详情

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 要显示查找结果列表，请执行以下操作之一：
   - 在 Security Hub 导航窗格中，选择调查发现。根据需要添加搜索过滤器以缩小查找结果列表的范围。
   - 在 Security Hub 导航窗格中，选择见解。选择见解。然后在结果列表上，选择一个见解结果。
   - 在 Security Hub 导航窗格中，选择集成。选择查看集成的调查发现。

3. 选择调查发现标题。
4. 在查找结果详细信息面板中，您可以执行其他操作，如下所示：
   - 要显示调查发现的完整 JSON，请选择调查发现 ID。从查找 JSON 中，下载查找 JSON。
   - 要查看基于 AWS Config 规则的结果，要显示适用规则的列表，请选择规则。
   - 选择 “使用 Macie 调查”，调查在 Macie 控制台的调查结果中发现的敏感数据。只有在您启用 Amazon Macie 及其自动敏感数据发现功能时，此选项才可用。
   - 选择 “资源” 以查看查找结果中涉及的资源的信息。
   - 选择 “在 Amazon Detec tive 中调查”，在 Detective 控制台中调查调查结果。只有在您启用 Amazon Detective 时，此选项才可用。
   - 选择 “历史记录” 选项卡可查看长达 90 天的查找历史记录。

> **Note**
>
> 调查发现详细信息面板的顶部包含有关该调查发现的概述信息，包括账户、严重程度、日期和状态。如果您与之集成， AWS Organizations 并且您登录的账户是组织成员账户，则详细信息面板将包含账户名称。对于手动邀请而非通过 Organizations 集成邀请的成员账户，详细信息面板仅会包含账户 ID。

Security Hub API

查看发现详情

使用 Security Hub API 的`GetFindings`操作，或者如果你使用的是 AWS CLI，则运行 get-findings 命令。

您可以为`Filters`参数提供一个或多个值，以缩小要检索的结果范围。

如果结果量太大，则可以使用`MaxResults`参数将结果限制为指定数量，使用`NextToken`参数对结果进行分页。使用`SortCriteria`参数按特定字段对结果进行排序。

如果您已启用跨区域聚合并从聚合区域调用此操作，则结果将包括来自聚合和关联区域的结果。

以下 CLI 命令检索与提供的筛选条件匹配的结果，并按字段的降序对其进行排序。`LastObservedAt`此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

查看发现详情

1. 使用 Get-SHUBFinding cmdlet。
2. 或者，填充 Filter 参数以缩小要检索的调查发现范围。

示例

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> 当您按CompanyName或筛选查找结果时ProductName，Security Hub 会使用作为 ProductFields ASFF 对象一部分的值。Security Hub 不使用顶层CompanyName和ProductName字段。

对调查结果采取行动 AWS Security Hub

AWS Security Hub 允许您跟踪调查结果的当前状态。

您也可以将结果发送到自定义操作进行处理。

主题

- 设置调查发现的工作流程状态
- 将结果发送到自定义操作

设置调查发现的工作流程状态

工作流程状态跟踪对调查发现的调查进度。工作流程状态特定于单个调查发现。它不影响新调查发现的产生。例如，将查找结果的工作流程状态设置为SUPPRESSED或RESOLVED不会 AWS Security Hub 阻止针对同一问题生成新的调查结果。

工作流程状态可以是以下值：

NEW

调查发现在被审查前的初始状态。

从集成 AWS 服务（例如）中提取的发现以 AWS Config其初始状态NEW为初始状态。

在以下情况下，Security Hub 还会将工作流程状态从 NOTIFIED 或 RESOLVED 重置为 NEW：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status 从 PASSED 变为 FAILED、WARNING 或 NOT_AVAILABLE。

这些变化表明需要进一步调查。

NOTIFIED

表示您已将安全问题告知资源拥有者。如果您不是资源拥有者，并且需要资源拥有者的干预才能解决安全问题，则可以使用此状态。

如果出现以下情况之一，则工作流程状态将自动从 NOTIFIED 更改为 NEW：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status 从 PASSED 变为 FAILED、WARNING 或 NOT_AVAILABLE。

SUPPRESSED

表示您已查看调查发现，但认为不需要采取任何操作。

如果 RecordState 从 ARCHIVED 变为 ACTIVE，则 SUPPRESSED 调查发现的工作流程状态不会改变。

RESOLVED

已对结果进行审查并采取了补救措施，现在被视为已解决。

除非出现下列情况之一，否则调查发现将保持为 RESOLVED：

- RecordState 从 ARCHIVED 变为 ACTIVE。
- Compliance.Status 从 PASSED 变为 FAILED、WARNING 或 NOT_AVAILABLE。

在这种情况下，工作流程状态会自动重置为 NEW。

对于来自控件的调查发现，如果 Compliance.Status 是 PASSED，则 Security Hub 会自动将工作流程状态设置为 RESOLVED。

设置调查发现的工作流程状态

选择首选方法，然后按照步骤设置一个或多个调查发现的工作流程状态。

要自动更新特定调查发现的工作流程状态，请参阅 自动化规则。

Security Hub console

要更新调查发现的工作流程状态

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 要显示调查发现列表，请执行以下操作之一：
   - 在 Security Hub 导航窗格中，选择结果。
   - 在 Security Hub 导航窗格中，选择见解。选择见解。然后在结果列表上，选择一个见解结果。
   - 在 Security Hub 导航窗格中，选择集成。选择查看集成的调查发现。
   - 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，选择一个控件以查看该控件的调查发现列表。
3. 在调查发现列表中，选中要更新的每个调查发现的复选框。
4. 在列表顶部，针对工作流程状态，选择状态。
5. 在 “设置工作流状态” 对话框中，提供可选注释，详细说明更新工作流程状态的原因。选择 “设置状态”。

Security Hub API

调用 BatchUpdateFindings API。提供用于生成调查发现的产品调查发现 ID 和 ARN。您可以通过调用 GetFindings API 来获取这些详细信息。

AWS CLI

运行 batch-update-findings 命令。提供用于生成调查发现的产品调查发现 ID 和 ARN。您可以通过运行 get-findings 命令来获取这些详细信息。

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

示例

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

将结果发送到自定义操作

您可以创建 AWS Security Hub 自定义操作，通过亚马逊 Security Hub 实现自动化 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 the section called “自动响应和补救”。

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（控制台）

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 要显示调查发现列表，请执行以下操作之一：
   - 在 Security Hub 导航窗格中，选择结果。
   - 在 Security Hub 导航窗格中，选择见解。选择见解。然后在结果列表上，选择一个见解结果。
   - 在 Security Hub 导航窗格中，选择集成。选择查看集成的调查发现。
   - 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. 在调查发现列表中，选中要发送到自定义操作的每个调查发现的复选框。

   您一次最多可以发送 20 个结果。
4. 对于操作，选择自定义操作。

AWS 安全调查结果格式 (ASFF)

AWS Security Hub 使用、汇总、整理来自 AWS 安全服务和第三方产品集成的结果，并对其进行优先排序。Security Hub 使用一种称为 AWS 安全调查结果格式 (ASFF) 的标准调查结果格式来处理这些发现，这样就无需进行耗时的数据转换工作。然后，它将从各个产品摄取的调查发现进行关联，以确定最重要问题的优先级。

主题

AWS 安全调查结果格式 (ASFF) 语法

本页提供了 AWS 安全调查结果格式 (ASFF) 中查找结果的 JSON 的完整概述。该格式源自 JSON 架构。选择链接对象名称以查看该对象的调查发现示例。您可以将 Security Hub 结果与此处显示的资源和示例进行比较，以帮助您解释结果。

要查看所需的 ASFF 属性的描述，请参阅 the section called “必需的顶级属性”。

要查看其他顶级 ASFF 属性的描述，请参见 the section called “可选顶级属性”。

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
```

```
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "ServiceName": "string"
      },
      "DnsRequestAction": {
       "Blocked": boolean,
       "Domain": "string",
       "Protocol": "string"
      },
      "NetworkConnectionAction": {
       "Blocked": boolean,
       "ConnectionDirection": "string",
       "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
       },
       "Protocol": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
```

```
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        }
       }]
```

```
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
       {
        "Description": "string",
        "ReasonCode": "string"
       }
      ]
     },
     "Confidence": number,
     "CreatedAt": "string",
     "Criticality": number,
     "Description": "string",
     "FindingProviderFields": {
      "Confidence": number,
      "Criticality": number,
      "RelatedFindings": [{
       "ProductArn": "string",
       "Id": "string"
      }],
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Types": ["string"]
     },
     "FirstObservedAt": "string",
```

```
    "GeneratorId": "string",
    "Id": "string",
    "LastObservedAt": "string",
    "Malware": [{
     "Name": "string",
     "Path": "string",
     "State": "string",
     "Type": "string"
    }],
    "Network": {
     "DestinationDomain": "string",
     "DestinationIpV4": "string",
     "DestinationIpV6": "string",
     "DestinationPort": number,
     "Direction": "string",
     "OpenPortRange": {
      "Begin": integer,
      "End": integer
     },
     "Protocol": "string",
     "SourceDomain": "string",
     "SourceIpV4": "string",
     "SourceIpV6": "string",
     "SourceMac": "string",
     "SourcePort": number
    },
    "NetworkPath": [{
     "ComponentId": "string",
     "ComponentType": "string",
     "Egress": {
      "Destination": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
        "End": integer
       }]
      },
      "Protocol": "string",
      "Source": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
        "End": integer
       }]
```

```
        }
       },
       "Ingress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
       }
      }],
      "Note": {
       "Text": "string",
       "UpdatedAt": "string",
       "UpdatedBy": "string"
      },
      "PatchSummary": {
       "FailedCount": number,
       "Id": "string",
       "InstalledCount": number,
       "InstalledOtherCount": number,
       "InstalledPendingReboot": number,
       "InstalledRejectedCount": number,
       "MissingCount": number,
       "Operation": "string",
       "OperationEndTime": "string",
       "OperationStartTime": "string",
       "RebootOption": "string"
      },
      "Process": {
       "LaunchedAt": "string",
       "Name": "string",
       "ParentPid": number,
       "Path": "string",
       "Pid": number,
```

```
      "TerminatedAt": "string"
     },
     "ProductArn": "string",
     "ProductFields": {
      "string": "string"
     },
     "ProductName": "string",
     "RecordState": "string",
     "Region": "string",
     "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
     }],
     "Remediation": {
      "Recommendation": {
       "Text": "string",
       "Url": "string"
      }
     },
     "Resources": [{
      "ApplicationArn": "string",
      "ApplicationName": "string",
      "DataClassification": {
       "DetailedResultsLocation": "string",
       "Result": {
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
         "Detections": [{
          "Arn": "string",
          "Count": integer,
          "Name": "string",
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
```

```
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
```

```
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
```

```
          "UseAwsOwnedKey": boolean
         },
         "EngineType": "string",
         "EngineVersion": "string",
         "HostInstanceType": "string",
         "Logs": {
          "Audit": boolean,
          "AuditLogGroup": "string",
          "General": boolean,
          "GeneralLogGroup": "string"
         },
         "MaintenanceWindowStartTime": {
          "DayOfWeek": "string",
          "TimeOfDay": "string",
          "TimeZone": "string"
         },
         "PubliclyAccessible": boolean,
         "SecurityGroups": [
          "string"
         ],
         "StorageType": "string",
         "SubnetIds": [
          "string",
          "string"
         ],
         "Users": [{
          "Username": "string"
         }]
        },
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
         "Name": "string",
         "Version": "string"
        },
        "AwsApiGatewayStage": {
         "AccessLogSettings": {
```

```
          "DestinationArn": "string",
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
         },
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DeploymentId": "string",
         "Description": "string",
         "DocumentationVersion": "string",
         "LastUpdatedDate": "string",
         "MethodSettings": [{
          "CacheDataEncrypted": boolean,
          "CachingEnabled": boolean,
          "CacheTtlInSeconds": number,
          "DataTraceEnabled": boolean,
          "HttpMethod": "string",
          "LoggingLevel": "string",
          "MetricsEnabled": boolean,
          "RequireAuthorizationForCacheControl": boolean,
          "ResourcePath": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number,
          "UnauthorizedCacheControlHeaderStrategy": "string"
         }],
         "StageName": "string",
         "TracingEnabled": boolean,
         "Variables": {
          "string": "string"
         },
         "WebAclArn": "string"
        },
        "AwsApiGatewayV2Api": {
         "ApiEndpoint": "string",
         "ApiId": "string",
```

```
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
```

```
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
         },
         {
          "AuthenticationType": "string"
         }
         ],
         "ApiId": "string",
         "Arn": "string",
         "AuthenticationType": "string",
         "Id": "string",
         "LogConfig": {
          "CloudWatchLogsRoleArn": "string",
          "ExcludeVerboseContent": boolean,
          "FieldLogLevel": "string"
         },
         "Name": "string",
         "XrayEnabled": boolean
        }
       },
       "AwsAthenaWorkGroup": {
        "Description": "string",
        "Name": "string",
        "WorkgroupConfiguration": {
         "ResultConfiguration": {
          "EncryptionConfiguration": {
           "EncryptionOption": "string",
           "KmsKey": "string"
          }
         }
        },
        "State": "string"
       },
```

```
        "AwsAutoScalingAutoScalingGroup": {
         "AvailabilityZones": [{
          "Value": "string"
         }],
         "CreatedTime": "string",
         "HealthCheckGracePeriod": integer,
         "HealthCheckType": "string",
         "LaunchConfigurationName": "string",
         "LoadBalancerNames": ["string"],
         "LaunchTemplate": {
                        "LaunchTemplateId": "string",
                        "LaunchTemplateName": "string",
                        "Version": "string"
                    },
         "MixedInstancesPolicy": {
          "InstancesDistribution": {
           "OnDemandAllocationStrategy": "string",
           "OnDemandBaseCapacity": number,
           "OnDemandPercentageAboveBaseCapacity": number,
           "SpotAllocationStrategy": "string",
           "SpotInstancePools": number,
           "SpotMaxPrice": "string"
          },
          "LaunchTemplate": {
           "LaunchTemplateSpecification": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
           },
           "CapacityRebalance": boolean,
           "Overrides": [{
            "InstanceType": "string",
            "WeightedCapacity": "string"
           }]
          }
         }
        },
        "AwsAutoScalingLaunchConfiguration": {
         "AssociatePublicIpAddress": boolean,
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteOnTermination": boolean,
           "Encrypted": boolean,
```

```
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
       "SecurityGroups": ["string"],
       "SpotPrice": "string",
       "UserData": "string"
      },
      "AwsBackupBackupPlan": {
       "BackupPlan": {
        "AdvancedBackupSettings": [{
         "BackupOptions": {
          "WindowsVSS":"string"
         },
         "ResourceType":"string"
        }],
        "BackupPlanName": "string",
        "BackupPlanRule": [{
         "CompletionWindowMinutes": integer,
```

```
          "CopyActions": [{
           "DestinationBackupVaultArn": "string",
           "Lifecycle": {
            "DeleteAfterDays": integer,
            "MoveToColdStorageAfterDays": integer
           }
          }],
          "Lifecycle": {
           "DeleteAfterDays": integer
          },
          "RuleName": "string",
          "ScheduleExpression": "string",
          "StartWindowMinutes": integer,
          "TargetBackupVault": "string"
         }]
        },
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "VersionId": "string"
      },
       "AwsBackupBackupVault": {
        "AccessPolicy": {
         "Statement": [{
          "Action": ["string"],
          "Effect": "string",
          "Principal": {
           "AWS": "string"
          },
          "Resource": "string"
         }],
         "Version": "string"
        },
        "BackupVaultArn": "string",
        "BackupVaultName": "string",
        "EncryptionKeyArn": "string",
        "Notifications": {
         "BackupVaultEvents": ["string"],
         "SNSTopicArn": "string"
        }
       },
       "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
```

```
        "CalculatedLifecycle": {
         "DeleteAt": "string",
         "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
         "DeleteAfterDays": integer,
         "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
       },
       "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
```

```
        "ExtendedKeyUsages": [{
         "Name": "string",
         "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
```

```
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
         "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
       },
       "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
         "Items": [{
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
```

```
          "StatusCodes": {
           "Items": [number],
           "Quantity": number
          }
         }
        }]
       },
       "Origins": {
        "Items": [{
         "CustomOriginConfig": {
          "HttpPort": number,
          "HttpsPort": number,
          "OriginKeepaliveTimeout": number,
          "OriginProtocolPolicy": "string",
          "OriginReadTimeout": number,
          "OriginSslProtocols": {
           "Items": ["string"],
           "Quantity": number
          }
         },
         "DomainName": "string",
         "Id": "string",
         "OriginPath": "string",
         "S3OriginConfig": {
          "OriginAccessIdentity": "string"
         }
        }]
       },
       "Status": "string",
       "ViewerCertificate": {
        "AcmCertificateArn": "string",
        "Certificate": "string",
        "CertificateSource": "string",
        "CloudFrontDefaultCertificate": boolean,
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
```

```
        "HomeRegion": "string",
        "IncludeGlobalServiceEvents": boolean,
        "IsMultiRegionTrail": boolean,
        "IsOrganizationTrail": boolean,
        "KmsKeyId": "string",
        "LogFileValidationEnabled": boolean,
        "Name": "string",
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "SnsTopicArn": "string",
        "SnsTopicName": "string",
        "TrailArn": "string"
      },
      "AwsCloudWatchAlarm": {
        "ActionsEnabled": boolean,
        "AlarmActions": ["string"],
        "AlarmArn": "string",
        "AlarmConfigurationUpdatedTimestamp": "string",
        "AlarmDescription": "string",
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
          "Name": "string",
          "Value": "string"
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
      },
      "AwsCodeBuildProject": {
        "Artifacts": [{
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
```

```
        "Location": "string",
        "Name": "string",
        "NamespaceType": "string",
        "OverrideArtifactName": boolean,
        "Packaging": "string",
        "Path": "string",
        "Type": "string"
      }],
      "SecondaryArtifacts": [{
                  "ArtifactIdentifier": "string",
                  "Type": "string",
                  "Location": "string",
                  "Name": "string",
                  "NamespaceType": "string",
                  "Packaging": "string",
                  "Path": "string",
                  "EncryptionDisabled": boolean,
                  "OverrideArtifactName": boolean
              }],
      "EncryptionKey": "string",
      "Certificate": "string",
      "Environment": {
        "Certificate": "string",
        "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
        }],
        "ImagePullCredentialsType": "string",
        "PrivilegedMode": boolean,
        "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
        },
        "Type": "string"
      },
      "LogsConfig": {
        "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
        },
        "S3Logs": {
          "EncryptionDisabled": boolean,
```

```
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
        }
       },
       "AwsDmsEndpoint": {
        "CertificateArn": "string",
        "DatabaseName": "string",
        "EndpointArn": "string",
        "EndpointIdentifier": "string",
        "EndpointType": "string",
        "EngineName": "string",
        "KmsKeyId": "string",
        "Port": integer,
        "ServerName": "string",
        "SslMode": "string",
        "Username": "string"
       },
       "AwsDmsReplicationInstance": {
        "AllocatedStorage": integer,
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
```

```
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
       },
       "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
         "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
         "string": "string"
        },
        "TargetEndpointArn": "string"
       },
       "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
         "AttributeName": "string",
         "AttributeType": "string"
        }],
        "BillingModeSummary": {
         "BillingMode": "string",
         "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
         "Backfilling": boolean,
         "IndexArn": "string",
         "IndexName": "string",
         "IndexSizeBytes": number,
         "IndexStatus": "string",
         "ItemCount": number,
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
```

```
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         },
         "ProvisionedThroughput": {
          "LastDecreaseDateTime": "string",
          "LastIncreaseDateTime": "string",
          "NumberOfDecreasesToday": number,
          "ReadCapacityUnits": number,
          "WriteCapacityUnits": number
         }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
```

```
        }],
        "KmsMasterKeyId": "string",
        "ProvisionedThroughputOverride": {
         "ReadCapacityUnits": number
        },
        "RegionName": "string",
        "ReplicaStatus": "string",
        "ReplicaStatusDescription": "string"
       }],
       "RestoreSummary": {
        "RestoreDateTime": "string",
        "RestoreInProgress": boolean,
        "SourceBackupArn": "string",
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
```

```
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
       "SessionTimeoutHours": "integer",
       "SplitTunnel": boolean,
       "TransportProtocol": "string",
       "VpcId": "string",
       "VpnPort": integer
      },
      "AwsEc2Eip": {
       "AllocationId": "string",
       "AssociationId": "string",
       "Domain": "string",
       "InstanceId": "string",
       "NetworkBorderGroup": "string",
       "NetworkInterfaceId": "string",
       "NetworkInterfaceOwnerId": "string",
       "PrivateIpAddress": "string",
       "PublicIp": "string",
       "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
       "IamInstanceProfileArn": "string",
       "ImageId": "string",
       "IpV4Addresses": ["string"],
       "IpV6Addresses": ["string"],
       "KeyName": "string",
       "LaunchedAt": "string",
       "MetadataOptions": {
        "HttpEndpoint": "string",
        "HttpProtocolIpv6": "string",
        "HttpPutResponseHopLimit": number,
        "HttpTokens": "string",
        "InstanceMetadataTags": "string"
```

```
        },
        "Monitoring": {
         "State": "string"
        },
        "NetworkInterfaces": [{
         "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
       },
       "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
         "Monitoring": {
          "Enabled": boolean
         },
         "NetworkInterfaces": [{
          "AssociatePublicIpAddress" : boolean
         }]
        },
        "LaunchTemplateName": "string",
        "LicenseSpecifications": ["string"],
        "SecurityGroupIds": ["string"],
```

```
        "SecurityGroups": ["string"],
        "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
        "Associations": [{
          "NetworkAclAssociationId": "string",
          "NetworkAclId": "string",
          "SubnetId": "string"
        }],
        "Entries": [{
          "CidrBlock": "string",
          "Egress": boolean,
          "IcmpTypeCode": {
            "Code": number,
            "Type": number
          },
          "Ipv6CidrBlock": "string",
          "PortRange": {
            "From": number,
            "To": number
          },
          "Protocol": "string",
          "RuleAction": "string",
          "RuleNumber": number
        }],
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
      },
      "AwsEc2NetworkInterface": {
        "Attachment": {
          "AttachmentId": "string",
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "DeviceIndex": number,
          "InstanceId": "string",
          "InstanceOwnerId": "string",
          "Status": "string"
        },
        "Ipv6Addresses": [{
          "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
```

```
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
         "GroupName": "string"
        }],
        "SourceDestCheck": boolean
       },
       "AwsEc2RouteTable": {
        "AssociationSet": [{
         "AssociationState": {
          "State": "string"
         },
         "Main": boolean,
         "RouteTableAssociationId": "string",
         "RouteTableId": "string"
        }],
        "PropogatingVgwSet": [],
        "RouteTableId": "string",
        "RouteSet": [
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         },
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
       "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
         "FromPort": number,
```

```
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "IpPermissionsEgress": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "OwnerId": "string",
       "VpcId": "string"
```

```
      },
      "AwsEc2Subnet": {
       "AssignIpv6AddressOnCreation": boolean,
       "AvailabilityZone": "string",
       "AvailabilityZoneId": "string",
       "AvailableIpAddressCount": number,
       "CidrBlock": "string",
       "DefaultForAz": boolean,
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "Ipv6CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "MapPublicIpOnLaunch": boolean,
       "OwnerId": "string",
       "State": "string",
       "SubnetArn": "string",
       "SubnetId": "string",
       "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
       "DefaultRouteTablePropagation": "string",
       "Description": "string",
       "DnsSupport": "string",
       "Id": "string",
       "MulticastSupport": "string",
       "PropagationDefaultRouteTableId": "string",
       "TransitGatewayCidrBlocks": ["string"],
       "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
       "Attachments": [{
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "InstanceId": "string",
        "Status": "string"
       }],
       "CreateTime": "string",
       "DeviceName": "string",
       "Encrypted": boolean,
```

```
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlockState": "string",
          "Ipv6CidrBlock": "string"
        }],
        "State": "string"
      },
      "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
          "ServiceType": "string"
        }]
      },
      "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
          "CidrBlock": "string",
          "CidrBlockSet": [{
            "CidrBlock": "string"
          }],
          "Ipv6CidrBlockSet": [{
```

```
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "Status": {
         "Code": "string",
         "Message": "string"
        },
        "VpcPeeringConnectionId": "string"
       },
       "AwsEc2VpnConnection": {
        "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": {
        "Architecture": "string",
        "ImageDigest": "string",
        "ImagePublishedAt": "string",
        "ImageTags": ["string"],
        "RegistryId": "string",
        "RepositoryName": "string"
       },
       "AwsEcrRepository": {
        "Arn": "string",
```

```
        "ImageScanningConfiguration": {
         "ScanOnPush": boolean
        },
        "ImageTagMutability": "string",
        "LifecyclePolicy": {
         "LifecyclePolicyText": "string",
         "RegistryId": "string"
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
       },
       "AwsEcsCluster": {
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
         "Name": "string",
         "Value": "string"
        }],
        "Configuration": {
         "ExecuteCommandConfiguration": {
          "KmsKeyId": "string",
          "LogConfiguration": {
           "CloudWatchEncryptionEnabled": boolean,
           "CloudWatchLogGroupName": "string",
           "S3BucketName": "string",
           "S3EncryptionEnabled": boolean,
           "S3KeyPrefix": "string"
          },
          "Logging": "string"
         }
        },
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
```

```
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
         "MaximumPercent": number,
         "MinimumHealthyPercent": number
        },
        "DeploymentController": {
         "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
```

```
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
```

```
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
          "Name": "string",
          "Value": "string"
         }],
         "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
         }],
         "Essential": boolean,
         "ExtraHosts": [{
          "Hostname": "string",
          "IpAddress": "string"
         }],
         "FirelensConfiguration": {
          "Options": {
           "string": "string"
          },
          "Type": "string"
         },
         "HealthCheck": {
          "Command": ["string"],
          "Interval": number,
          "Retries": number,
          "StartPeriod": number,
          "Timeout": number
         },
```

```
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
```

```
          "HostPort": number,
          "Protocol": "string"
         }],
         "Privileged": boolean,
         "PseudoTerminal": boolean,
         "ReadonlyRootFilesystem": boolean,
         "RepositoryCredentials": {
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
         "Secrets": [{
          "Name": "string",
          "ValueFrom": "string"
         }],
         "StartTimeout": number,
         "StopTimeout": number,
         "SystemControls": [{
          "Namespace": "string",
          "Value": "string"
         }],
         "Ulimits": [{
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
         "User": "string",
         "VolumesFrom": [{
          "ReadOnly": boolean,
          "SourceContainer": "string"
         }],
         "WorkingDirectory": "string"
        }],
        "Cpu": "string",
        "ExecutionRoleArn": "string",
        "Family": "string",
        "InferenceAccelerators": [{
         "DeviceName": "string",
         "DeviceType": "string"
        }],
        "IpcMode": "string",
        "Memory": "string",
```

```
        "NetworkMode": "string",
        "PidMode": "string",
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "ProxyConfiguration": {
         "ContainerName": "string",
         "ProxyConfigurationProperties": [{
          "Name": "string",
          "Value": "string"
         }],
         "Type": "string"
        },
        "RequiresCompatibilities": ["string"],
        "Status": "string",
        "TaskRoleArn": "string",
        "Volumes": [{
         "DockerVolumeConfiguration": {
          "Autoprovision": boolean,
          "Driver": "string",
          "DriverOpts": {
           "string": "string"
          },
          "Labels": {
           "string": "string"
          },
          "Scope": "string"
         },
         "EfsVolumeConfiguration": {
          "AuthorizationConfig": {
           "AccessPointId": "string",
           "Iam": "string"
          },
          "FilesystemId": "string",
          "RootDirectory": "string",
          "TransitEncryption": "string",
          "TransitEncryptionPort": number
         },
         "Host": {
          "SourcePath": "string"
         },
         "Name": "string"
        }]
```

```
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
```

```
        "DateUpdated": "string",
        "Description": "string",
        "EndpointUrl": "string",
        "EnvironmentArn": "string",
        "EnvironmentId": "string",
        "EnvironmentLinks": [{
         "EnvironmentName": "string",
         "LinkName": "string"
        }],
        "EnvironmentName": "string",
        "OptionSettings": [{
         "Namespace": "string",
         "OptionName": "string",
         "ResourceName": "string",
         "Value": "string"
        }],
        "PlatformArn": "string",
        "SolutionStackName": "string",
        "Status": "string",
        "Tier": {
         "Name": "string",
         "Type": "string",
         "Version": "string"
        },
        "VersionLabel": "string"
       },
       "AwsElasticSearchDomain": {
        "AccessPolicies": "string",
        "DomainStatus": {
         "DomainId": "string",
         "DomainName": "string",
         "Endpoint": "string",
         "Endpoints": {
          "string": "string"
         }
        },
        "DomainEndpointOptions": {
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
```

```
        "InstanceCount": number,
        "InstanceType": "string",
        "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
      },
      "ElasticsearchVersion": "string",
      "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
      },
      "LogPublishingOptions": {
        "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        },
        "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        },
        "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        }
      },
      "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
      },
      "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
      },
      "VPCOptions": {
        "AvailabilityZones": [
          "string"
        ],
        "SecurityGroupIds": [
          "string"
```

```
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
         "EmitInterval": number,
         "Enabled": boolean,
         "S3BucketName": "string",
         "S3BucketPrefix": "string"
        },
```

```
        "ConnectionDraining": {
         "Enabled": boolean,
         "Timeout": number
        },
        "ConnectionSettings": {
         "IdleTimeout": number
        },
        "CrossZoneLoadBalancing": {
         "Enabled": boolean
        },
        "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
         "PolicyName": "string"
        }],
        "LbCookieStickinessPolicies": [{
         "CookieExpirationPeriod": number,
         "PolicyName": "string"
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "SourceSecurityGroup": {
        "GroupName": "string",
        "OwnerAlias": "string"
       },
       "Subnets": ["string"],
       "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
       "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
       },
       "CanonicalHostedZoneId": "string",
       "CreatedTime": "string",
       "DNSName": "string",
```

```
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
         "Key": "string",
         "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
         "Code": "string",
         "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
       },
       "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
       },
       "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
```

```
            }
          }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
            "AuditLogs": {
              "Status": "string"
            }
          },
          "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
              "EbsVolumes": {
                "Status": "string"
              }
            },
            "ServiceRole": "string"
          }
        }
      },
      "AwsIamAccessKey": {
        "AccessKeyId": "string",
```

```
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
       },
       "AwsIamGroup": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
       "AwsIamPolicy": {
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
```

```
        "CreateDate": "string",
        "IsDefaultVersion": boolean,
        "VersionId": "string"
       }],
       "UpdateDate": "string"
      },
      "AwsIamRole": {
       "AssumeRolePolicyDocument": "string",
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "InstanceProfileList": [{
        "Arn": "string",
        "CreateDate": "string",
        "InstanceProfileId": "string",
        "InstanceProfileName": "string",
        "Path": "string",
        "Roles": [{
         "Arn": "string",
         "AssumeRolePolicyDocument": "string",
         "CreateDate": "string",
         "Path": "string",
         "RoleId": "string",
         "RoleName": "string"
        }]
       }],
       "MaxSessionDuration": number,
       "Path": "string",
       "PermissionsBoundary": {
        "PermissionsBoundaryArn": "string",
        "PermissionsBoundaryType": "string"
       },
       "RoleId": "string",
       "RoleName": "string",
       "RolePolicyList": [{
        "PolicyName": "string"
       }]
      },
      "AwsIamUser": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
```

```
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
```

```
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
         },
         "Error": {
          "ErrorCode": "string",
          "Message": "string"
         }
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
         "CodeSize": number
        },
        "PackageType": "string",
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
        },
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
```

```
      "AwsMskCluster": {
       "ClusterInfo": {
        "ClientAuthentication": {
         "Sasl": {
          "Scram": {
           "Enabled": boolean
          },
          "Iam": {
           "Enabled": boolean
          }
         },
         "Tls": {
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
```

```
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
       "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
       "Description": "string",
       "RuleGroup": {
        "RulesSource": {
         "RulesSourceList": {
          "GeneratedRulesType": "string",
          "Targets": ["string"],
          "TargetTypes": ["string"]
         },
         "RulesString": "string",
         "StatefulRules": [{
          "Action": "string",
```

```
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
         }],
         "StatelessRulesAndCustomActions": {
          "CustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
             }]
            }
           },
           "ActionName": "string"
          }],
          "StatelessRules": [{
           "Priority": number,
           "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
             "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Destinations": [{
              "AddressDefinition": "string"
             }],
             "Protocols": [number],
             "SourcePorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Sources": [{
              "AddressDefinition": "string"
             }],
```

```
            "TcpFlags": [{
             "Flags": ["string"],
             "Masks": ["string"]
            }]
           }
          }
         }]
        }
       },
       "RuleVariables": {
        "IpSets": {
         "Definition": ["string"]
        },
        "PortSets": {
         "Definition": ["string"]
        }
       }
      },
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "Type": "string"
     },
     "AwsOpenSearchServiceDomain": {
      "AccessPolicies": "string",
      "AdvancedSecurityOptions": {
       "Enabled": boolean,
       "InternalUserDatabaseEnabled": boolean,
       "MasterUserOptions": {
        "MasterUserArn": "string",
        "MasterUserName": "string",
        "MasterUserPassword": "string"
       }
      },
      "Arn": "string",
      "ClusterConfig": {
       "DedicatedMasterCount": number,
       "DedicatedMasterEnabled": boolean,
       "DedicatedMasterType": "string",
       "InstanceCount": number,
       "InstanceType": "string",
       "WarmCount": number,
       "WarmEnabled": boolean,
       "WarmType": "string",
```

```
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
       "DomainEndpoint": "string",
       "DomainEndpointOptions": {
        "CustomEndpoint": "string",
        "CustomEndpointCertificateArn": "string",
        "CustomEndpointEnabled": boolean,
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "DomainEndpoints": {
        "string": "string"
       },
       "DomainName": "string",
       "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
       },
       "EngineVersion": "string",
       "Id": "string",
       "LogPublishingOptions": {
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
```

```
        "Description": "string",
        "NewVersion": "string",
        "OptionalDeployment": boolean,
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VpcOptions": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       }
      },
      "AwsRdsDbCluster": {
       "ActivityStreamStatus": "string",
       "AllocatedStorage": number,
       "AssociatedRoles": [{
        "RoleArn": "string",
        "Status": "string"
       }],
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZones": ["string"],
       "BackupRetentionPeriod": integer,
       "ClusterCreateTime": "string",
       "CopyTagsToSnapshot": boolean,
       "CrossAccountClone": boolean,
       "CustomEndpoints": ["string"],
       "DatabaseName": "string",
       "DbClusterIdentifier": "string",
       "DbClusterMembers": [{
        "DbClusterParameterGroupStatus": "string",
        "DbInstanceIdentifier": "string",
        "IsClusterWriter": boolean,
        "PromotionTier": integer
       }],
       "DbClusterOptionGroupMemberships": [{
        "DbClusterOptionGroupName": "string",
        "Status": "string"
       }],
       "DbClusterParameterGroup": "string",
       "DbClusterResourceId": "string",
       "DbSubnetGroup": "string",
       "DeletionProtection": boolean,
       "DomainMemberships": [{
        "Domain": "string",
        "Fqdn": "string",
```

```
        "IamRoleName": "string",
        "Status": "string"
       }],
       "EnabledCloudwatchLogsExports": ["string"],
       "Endpoint": "string",
       "Engine": "string",
       "EngineMode": "string",
       "EngineVersion": "string",
       "HostedZoneId": "string",
       "HttpEndpointEnabled": boolean,
       "IamDatabaseAuthenticationEnabled": boolean,
       "KmsKeyId": "string",
       "MasterUsername": "string",
       "MultiAz": boolean,
       "Port": integer,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ReaderEndpoint": "string",
       "ReadReplicaIdentifiers": ["string"],
       "Status": "string",
       "StorageEncrypted": boolean,
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRdsDbClusterSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZones": ["string"],
       "ClusterCreateTime": "string",
       "DbClusterIdentifier": "string",
       "DbClusterSnapshotAttributes": [{
        "AttributeName": "string",
        "AttributeValues": ["string"]
       }],
       "DbClusterSnapshotIdentifier": "string",
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "PercentProgress": integer,
       "Port": integer,
```

```
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
```

```
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
```

```
        "EngineVersion": "string",
        "Iops": number,
        "LicenseModel": "string",
        "MasterUserPassword": "string",
        "MultiAZ": boolean,
        "PendingCloudWatchLogsExports": {
         "LogTypesToDisable": ["string"],
         "LogTypesToEnable": ["string"]
        },
        "Port": number,
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "StorageType": "string"
       },
       "PerformanceInsightsEnabled": boolean,
       "PerformanceInsightsKmsKeyId": "string",
       "PerformanceInsightsRetentionPeriod": number,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ProcessorFeatures": [{
        "Name": "string",
        "Value": "string"
       }],
       "PromotionTier": number,
       "PubliclyAccessible": boolean,
       "ReadReplicaDBClusterIdentifiers": ["string"],
       "ReadReplicaDBInstanceIdentifiers": ["string"],
       "ReadReplicaSourceDBInstanceIdentifier": "string",
       "SecondaryAvailabilityZone": "string",
       "StatusInfos": [{
        "Message": "string",
        "Normal": boolean,
        "Status": "string",
        "StatusType": "string"
       }],
       "StorageEncrypted": boolean,
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcSecurityGroups": [{
        "VpcSecurityGroupId": "string",
        "Status": "string"
       }]
```

```
      },
      "AwsRdsDbSecurityGroup": {
       "DbSecurityGroupArn": "string",
       "DbSecurityGroupDescription": "string",
       "DbSecurityGroupName": "string",
       "Ec2SecurityGroups": [{
        "Ec2SecurityGroupuId": "string",
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
       }],
       "IpRanges": [{
        "CidrIp": "string",
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "OptionGroupName": "string",
       "PercentProgress": integer,
       "Port": integer,
       "ProcessorFeatures": [],
       "SnapshotCreateTime": "string",
       "SnapshotType": "string",
       "SourceDbSnapshotIdentifier": "string",
       "SourceRegion": "string",
       "Status": "string",
       "StorageType": "string",
       "TdeCredentialArn": "string",
```

```
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
            "ParameterApplyErrorDescription": "string",
            "ParameterApplyStatus": "string",
            "ParameterName": "string"
          }],
          "ParameterApplyStatus": "string",
          "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
          "ClusterSecurityGroupName": "string",
          "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
          "DestinationRegion": "string",
```

```
         "ManualSnapshotRetentionPeriod": number,
         "RetentionPeriod": number,
         "SnapshotCopyGrantName": "string"
        },
        "ClusterStatus": "string",
        "ClusterSubnetGroupName": "string",
        "ClusterVersion": "string",
        "DBName": "string",
        "DeferredMaintenanceWindows": [{
         "DeferMaintenanceEndTime": "string",
         "DeferMaintenanceIdentifier": "string",
         "DeferMaintenanceStartTime": "string"
        }],
        "ElasticIpStatus": {
         "ElasticIp": "string",
         "Status": "string"
        },
        "ElasticResizeNumberOfNodeOptions": "string",
        "Encrypted": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number
        },
        "EnhancedVpcRouting": boolean,
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
```

```
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRoute53HostedZone": {
        "HostedZone": {
```

```
        "Id": "string",
        "Name": "string",
        "Config": {
         "Comment": "string"
        }
       },
       "NameServers": ["string"],
       "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
         "CloudWatchLogsLogGroupArn": "string",
         "Id": "string",
         "HostedZoneId": "string"
        }
       },
       "Vpcs": [
        {
         "Id": "string",
         "Region": "string"
        }
       ]
      },
      "AwsS3AccessPoint": {
       "AccessPointArn": "string",
       "Alias": "string",
       "Bucket": "string",
       "BucketAccountId": "string",
       "Name": "string",
       "NetworkOrigin": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "VpcConfiguration": {
        "VpcId": "string"
       }
      },
      "AwsS3AccountPublicAccessBlock": {
       "BlockPublicAcls": boolean,
       "BlockPublicPolicy": boolean,
       "IgnorePublicAcls": boolean,
       "RestrictPublicBuckets": boolean
      },
```

```
      "AwsS3Bucket": {
       "AccessControlList": "string",
       "BucketLifecycleConfiguration": {
        "Rules": [{
         "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": number
         },
         "ExpirationDate": "string",
         "ExpirationInDays": number,
         "ExpiredObjectDeleteMarker": boolean,
         "Filter": {
          "Predicate": {
           "Operands": [{
             "Prefix": "string",
             "Type": "string"
            },
            {
             "Tag": {
              "Key": "string",
              "Value": "string"
             },
             "Type": "string"
            }
           ],
           "Type": "string"
          }
         },
         "Id": "string",
         "NoncurrentVersionExpirationInDays": number,
         "NoncurrentVersionTransitions": [{
          "Days": number,
          "StorageClass": "string"
         }],
         "Prefix": "string",
         "Status": "string",
         "Transitions": [{
          "Date": "string",
          "Days": number,
          "StorageClass": "string"
         }]
        }]
       },
       "BucketLoggingConfiguration": {
        "DestinationBucketName": "string",
```

```
        "LogFilePrefix": "string"
       },
       "BucketName": "string",
       "BucketNotificationConfiguration": {
        "Configurations": [{
         "Destination": "string",
         "Events": ["string"],
         "Filter": {
          "S3KeyFilter": {
           "FilterRules": [{
            "Name": "string",
            "Value": "string"
           }]
          }
         },
         "Type": "string"
        }]
       },
       "BucketVersioningConfiguration": {
        "IsMfaDeleteEnabled": boolean,
        "Status": "string"
       },
       "BucketWebsiteConfiguration": {
        "ErrorDocument": "string",
        "IndexDocumentSuffix": "string",
        "RedirectAllRequestsTo": {
         "HostName": "string",
         "Protocol": "string"
        },
        "RoutingRules": [{
         "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "KeyPrefixEquals": "string"
         },
         "Redirect": {
          "HostName": "string",
          "HttpRedirectCode": "string",
          "Protocol": "string",
          "ReplaceKeyPrefixWith": "string",
          "ReplaceKeyWith": "string"
         }
        }]
       },
       "CreatedAt": "string",
```

```
        "ObjectLockConfiguration": {
         "ObjectLockEnabled": "string",
         "Rule": {
          "DefaultRetention": {
           "Days": integer,
           "Mode": "string",
           "Years": integer
          }
         }
        },
        "OwnerAccountId": "string",
        "OwnerId": "string",
        "OwnerName": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
       },
       "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
         "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
```

```
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
          "AutomaticallyAfterDays": integer
        }
      },
      "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
          "Endpoint": "string",
          "Protocol": "string"
        },
        "TopicName": "string"
      },
      "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
```

```
      },
      "AwsSsmPatchCompliance": {
       "Patch": {
        "ComplianceSummary": {
         "ComplianceType": "string",
         "CompliantCriticalCount": integer,
         "CompliantHighCount": integer,
         "CompliantInformationalCount": integer,
         "CompliantLowCount": integer,
         "CompliantMediumCount": integer,
         "CompliantUnspecifiedCount": integer,
         "ExecutionType": "string",
         "NonCompliantCriticalCount": integer,
         "NonCompliantHighCount": integer,
         "NonCompliantInformationalCount": integer,
         "NonCompliantLowCount": integer,
         "NonCompliantMediumCount": integer,
         "NonCompliantUnspecifiedCount": integer,
         "OverallSeverity": "string",
         "PatchBaselineId": "string",
         "PatchGroup": "string",
         "Status": "string"
        }
       }
      },
      "AwsStepFunctionStateMachine": {
       "StateMachineArn": "string",
       "Name": "string",
       "Status": "string",
       "RoleArn": "string",
       "Type": "string",
       "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
       },
       "TracingConfiguration": {
        "Enabled": boolean
       }
      },
      "AwsWafRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
```

```
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
      },
      "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
          "DataId": "string",
          "Negated": boolean,
          "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
      },
      "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
      },
      "AwsWafRegionalRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
          "Action": {
            "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string"
        }]
      },
      "AwsWafRegionalWebAcl": {
        "DefaultAction": "string",
```

```
        "MetricName" : "string",
        "Name": "string",
        "RulesList" : [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string",
         "ExcludedRules": [{
          "ExclusionType": "string",
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         }
        }],
        "WebAclId": "string"
       },
       "AwsWafRule": {
        "MetricName": "string",
        "Name": "string",
        "PredicateList": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "RuleId": "string"
       },
       "AwsWafRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }]
       },
       "AwsWafv2RuleGroup": {
        "Arn": "string",
```

```
        "Capacity": number,
        "Description": "string",
        "Id": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
         "Allow": {
          "CustomRequestHandling": {
           "InsertHeaders": [
            {
            "Name": "string",
            "Value": "string"
            },
            {
            "Name": "string",
            "Value": "string"
            }
           ]
          }
         }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string",
          "SampledRequestsEnabled": boolean
         }
        }],
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
```

```
        }],
        "OverrideAction": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }],
       "WebAclId": "string"
      },
      "AwsWafv2WebAcl": {
       "Arn": "string",
       "Capacity": number,
       "CaptchaConfig": {
        "ImmunityTimeProperty": {
         "ImmunityTime": number
        }
       },
       "DefaultAction": {
        "Block": {}
       },
       "Description": "string",
       "ManagedbyFirewallManager": boolean,
       "Name": "string",
       "Rules": [{
        "Action": {
         "RuleAction": {
          "Block": {}
         }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       }],
       "VisibilityConfig": {
        "SampledRequestsEnabled": boolean,
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string"
       }
      },
```

```
      "AwsXrayEncryptionConfig": {
       "KeyId": "string",
       "Status": "string",
       "Type": "string"
      },
      "Container": {
       "ContainerRuntime": "string",
       "ImageId": "string",
       "ImageName": "string",
       "LaunchedAt": "string",
       "Name": "string",
       "Privileged": boolean,
       "VolumeMounts": [{
        "Name": "string",
        "MountPath": "string"
       }]
      },
      "Other": {
       "string": "string"
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
       "FileName": "string",
       "FilePath": "string",
       "Hash": "string",
       "ResourceId": "string"
      }],
```

```
      "ItemCount": number,
      "Name": "string",
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
     "Vulnerabilities": [{
      "CodeVulnerabilities": [{
       "Cwes": [
        "string",
        "string"
       ],
       "FilePath": {
        "EndLine": integer,
        "FileName": "string",
        "FilePath": "string",
        "StartLine": integer
       },
       "SourceArn":"string"
      }],
      "Cvss": [{
       "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
       }],
       "BaseScore": number,
       "BaseVector": "string",
       "Source": "string",
       "Version": "string"
      }],
      "EpssScore": number,
```

```
      "ExploitAvailable": "string",
      "FixAvailable": "string",
      "Id": "string",
      "LastKnownExploitAt": "string",
      "ReferenceUrls": ["string"],
      "RelatedVulnerabilities": ["string"],
      "Vendor": {
       "Name": "string",
       "Url": "string",
       "VendorCreatedAt": "string",
       "VendorSeverity": "string",
       "VendorUpdatedAt": "string"
      },
      "VulnerablePackages": [{
       "Architecture": "string",
       "Epoch": "string",
       "FilePath": "string",
       "FixedInVersion": "string",
       "Name": "string",
       "PackageManager": "string",
       "Release": "string",
       "Remediation": "string",
       "SourceLayerArn": "string",
       "SourceLayerHash": "string",
       "Version": "string"
      }]
     }],
     "Workflow": {
      "Status": "string"
     },
     "WorkflowState": "string"
    }
]
```

合并对 ASFF 字段和值的影响

Security Hub 提供两种类型的整合：

- 整合的控件视图（始终开启；无法关闭）——每个控件在各类标准中都有一个标识符。Security Hub 控制台的控件页面会显示您各类标准的所有控件。
- 整合的控件调查发现（可以开启或关闭）——开启整合的控件调查发现后，即使在多个标准之间共享检查，Security Hub 也会为安全检查生成单个调查发现。这旨在减少调查发现中的噪音。如果您在

2023 年 2 月 23 日当天或之后启用 Security Hub，则默认情况下会为您启用整合控制结果。否则，它会默认关闭。但是，只有在管理员账户中启用整合的控件调查发现后，Security Hub 成员账户才会启用该功能。如果该功能在管理员账户中关闭，则在成员账户中也会关闭。有关开启此功能的说明，请参阅 开启整合的控件调查发现。

这两个功能都对 AWS 安全调查结果格式 (ASFF) 中的控件调查发现字段和值进行了更改。本部分汇总了这些更改。

整合的控件视图——ASFF 变更

合并控件视图功能引入了以下更改来控制 ASFF 中的查找字段和值。

如果工作流程不依赖这些控件调查发现字段的值，则无需执行任何操作。

如果您的工作流程依赖于这些控制查找字段的特定值，请更新您的工作流程以使用当前值。

ASFF 字段	整合的控件视图之前的样本值	整合的控件视图后的样本值，以及变更描述
合规。 SecurityControlId	不适用（新字段）	EC2.2 引入各类标准的单一控件 ID。`ProductFields.RuleId` 仍然为 CIS v1.2.0 控件提供基于标准的控件 ID。`ProductFields.ControlId` 仍然为其他标准中的控件提供基于标准的控件 ID。
合规。 AssociatedStandards	不适用（新字段）	[{” StandardsId “: “standards/ aws-foundational-security-best-practices/v/1.0.0"}]

ASFF 字段	整合的控件视图之前的样本值	整合的控件视图后的样本值，以及变更描述
		显示启用控件的标准。
ProductFields。 ArchivalReasons:0/描述	不适用（新字段）	“调查发现处于已存档状态，因为整合的控件调查发现已开启或关闭。这会导致在生成新调查发现时存档先前状态的调查发现。” 描述 Security Hub 为何对现有调查发现进行存档。
ProductFields。 ArchivalReasons:0/ReasonCode	不适用（新字段）	"CONSOLIDATED_CONTROL_FINDINGS_UPDATE" 提供了 Security Hub 存档现有调查发现的原因。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此字段不再引用标准。

ASFF 字段	整合的控件视图之前的样本值	整合的控件视图后的样本值，以及变更描述
Remediation.Recommendation.Text	“有关如何解决此问题的说明，请参阅 SecAWS urity Hub PCI DSS 文档。”	“有关如何更正此问题的说明，请参阅 SAWS ecurity Hub 控制文档。” 此字段不再引用标准。
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此字段不再引用标准。

整合的控件调查发现——ASFF 的变化

如果您启用整合的控件调查发现，则可能会受到 ASFF 中控件调查发现字段和值的以下更改的影响。这些更改是对之前描述的整合控件视图更改的补充。

如果工作流程不依赖这些控件调查发现字段的值，则无需执行任何操作。

如果您的工作流程依赖于这些控制查找字段的特定值，请更新您的工作流程以使用当前值。

> **Note**
>
> AWS v2.0.0 上的自动安全响应支持整合的控制结果。如果您使用此版本的解决方案，则可以在开启整合的控件调查发现时保持工作流程。

ASFF 字段	开启整合的控件调查发现之前的示例值	开启整合的控件调查发现后的示例值和变更描述
GeneratorId	aws-foundational-security-best-练习/v/1.0.0/config.1	security-control/Config.1 此字段不再引用标准。
Title	应该启用 pci.config.1 AWS Config	AWS Config 应该启用 此字段不再引用特定于标准的信息。
Id	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 此字段不再引用标准。
ProductFields.ControlId	PCI.EC2.2	已删除。请改而参阅 `Compliance.SecurityControlId` 。 该字段已被删除，取而代之的是单一的、与标准无关的控制 ID。
ProductFields.RuleId	1.3	已删除。请改而参阅 `Compliance.SecurityControlId` 。 该字段已被删除，取而代之的是单一的、与标准无关的控制 ID。
描述	此 PCI DSS 控制检查当前账户和地区 AWS Config 是否已启用。	此 AWS 控件检查当前账户和区域中 AWS Config 是否已启用。 此字段不再引用标准。
严重性	"Severity": { “产品”：90， “标签”：“重大”，	"Severity": { “标签”：“重大”， “标准化”：90，

ASFF 字段	开启整合的控件调查发现之前的示例值	开启整合的控件调查发现后的示例值和变更描述
	“标准化”：90， “原始”：“重大” }	“原始”：“重大” } Security Hub 不再使用 “产品” 字段来描述发现的严重性。
类型	[“软件和配置检查/行业和监管标准/PCI-DSS”]	[“软件和配置检查/行业和监管标准”] 此字段不再引用标准。
合规。 RelatedRequirements	["PCI DSS 10.5.2", “PCI DSS 11.5”， “独联体 AWS 基金会 2.5"]	["PCI DSS v3.2.1/10.5.2", "PCI DSS v3.2.1/11.5", “独联体 AWS 基金会基准测试 v1.2.0/2.5"] 此字段显示所有已启用标准中的相关要求。
CreatedAt	2022-05-05T08:18:13.138Z	2022-09-25T08:18:13.138Z 格式保持不变，但是当您打开合并控制结果时，值会重置。
FirstObservedAt	2022-05-07T08:18:13.138Z	2022-09-28T08:18:13.138Z 格式保持不变，但是当您打开合并控制结果时，值会重置。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	已删除。请改而参阅 `Remediation.Recommendation.Url` 。

ASFF 字段	开启整合的控件调查发现之前的示例值	开启整合的控件调查发现后的示例值和变更描述
ProductFields.StandardsArn	arn: aws: securityhub::: standards/-practices/v/1.0.0 aws-foundational-security-best	已删除。请改而参阅 `Compliance.AssociatedStandards` 。
ProductFields.StandardsControlArn	arn: aws: securityhub: us-east-1:123456789012: control/-practices/v/1.0.0/config.1 aws-foundational-security-best	已删除。Security Hub 生成一项调查结果，用于跨标准的安全检查。
ProductFields.StandardsGuideArn	arn: aws: securityhub::: ruleset/ / v/1.2.0 cis-aws-foundations-benchmark	已删除。请改而参阅 `Compliance.AssociatedStandards` 。
ProductFields.StandardsGuideSubscriptionArn	arn: aws: securityhub: us-east-2 :123456789012: subscription/ / v/1.2.0 cis-aws-foundations-benchmark	已删除。Security Hub 生成一项调查结果，用于跨标准的安全检查。
ProductFields.StandardsSubscriptionArn	arn: aws: securityhub: us-east-1 :123456789012: subscription/-practices/v/1.0.0 aws-foundational-security-best	已删除。Security Hub 生成一项调查结果，用于跨标准的安全检查。
ProductFields.aws/securityhub/ FindingId	arn: aws: securityhub: us-east-1 :: product/aws/securityhub/arn : aws: securityhub: us-east-1 :123456789012: 订阅/-practices/v/1.0.0/config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 aws-foundational-security-best	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 此字段不再引用标准。

启用合并控制结果后客户提供的 ASFF 字段的值

如果您启用整合的控件调查发现，Security Hub 会生成一个各类标准的调查发现并存档原始调查发现（每个标准都有单独的调查发现）。要查看已存档的调查发现，您可以访问 Security Hub 控制台的调查发现页面，并将记录状态筛选条件设置为已存档，或者使用 `GetFindings` API 操作。您在 Security Hub 控制台中或使用 BatchUpdateFindingsAPI 对原始发现所做的更新不会保留在新发现中（如果需要，您可以通过参考存档的发现来恢复这些数据）。

客户提供的 ASFF 字段	开启整合的控件调查发现后的变更描述
置信度	重置为空状态。
严重性	重置为空状态。
备注	重置为空状态。
RelatedFindings	重置为空状态。
严重性	调查发现的默认严重性（与控件的严重性相匹配）。
类型	重置为与标准无关的值。
UserDefinedFields	重置为空状态。
VerificationState	重置为空状态。
工作流	新的失败调查发现的默认值为 `NEW`。新通过的调查发现的默认值为 `RESOLVED`。

开启整合的控件调查发现之前和之后的生成器 ID

以下是开启整合的控件调查发现时控件的生成器 ID 更改列表。这些适用于自 2023 年 2 月 15 日起 Security Hub 支持的控件。

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.1 cis-aws-foundations-benchmark	安全控制/ .1 CloudWatch

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.10 cis-aws-foundations-benchmark	security-control/IAM.16
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.11 cis-aws-foundations-benchmark	security-control/IAM.17
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.12 cis-aws-foundations-benchmark	security-control/IAM.4
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.13 cis-aws-foundations-benchmark	security-control/IAM.9
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.14 cis-aws-foundations-benchmark	security-control/IAM.6
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.16 cis-aws-foundations-benchmark	security-control/IAM.2
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.2 cis-aws-foundations-benchmark	security-control/IAM.5
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.20 cis-aws-foundations-benchmark	security-control/IAM.18
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/1.22 cis-aws-foundations-benchmark	security-control/IAM.1
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.3 cis-aws-foundations-benchmark	security-control/IAM.8
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.4 cis-aws-foundations-benchmark	security-control/IAM.3
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.5 cis-aws-foundations-benchmark	security-control/IAM.11
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.6 cis-aws-foundations-benchmark	security-control/IAM.12

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.7 cis-aws-foundations-benchmark	security-control/IAM.13
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.8 cis-aws-foundations-benchmark	security-control/IAM.14
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/1.9 cis-aws-foundations-benchmark	security-control/IAM.15
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.1 cis-aws-foundations-benchmark	安全控制/ .1 CloudTrail
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.2 cis-aws-foundations-benchmark	安全控制/ .4 CloudTrail
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.3 cis-aws-foundations-benchmark	安全控制/ .6 CloudTrail
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.4 cis-aws-foundations-benchmark	安全控制/ .5 CloudTrail
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.5 cis-aws-foundations-benchmark	security-control/Config.1
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.6 cis-aws-foundations-benchmark	安全控制/ .7 CloudTrail
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.7 cis-aws-foundations-benchmark	安全控制/ .2 CloudTrail
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.8 cis-aws-foundations-benchmark	security-control/KMS.4
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/2.9 cis-aws-foundations-benchmark	security-control/EC2.6
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.1 cis-aws-foundations-benchmark	安全控制/ .2 CloudWatch

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.2 cis-aws-foundations-benchmark	安全控制/ .3 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.3 cis-aws-foundations-benchmark	安全控制/ .1 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.4 cis-aws-foundations-benchmark	安全控制/ .4 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.5 cis-aws-foundations-benchmark	安全控制/ .5 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.6 cis-aws-foundations-benchmark	安全控制/ .6 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.7 cis-aws-foundations-benchmark	安全控制/ .7 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.8 cis-aws-foundations-benchmark	安全控制/ .8 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/3.9 cis-aws-foundations-benchmark	安全控制/ .9 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/3.10 cis-aws-foundations-benchmark	安全控制/ .10 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/3.11 cis-aws-foundations-benchmark	安全控制/ .11 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/3.12 cis-aws-foundations-benchmark	安全控制/ .12 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/3.13 cis-aws-foundations-benchmark	安全控制/ .13 CloudWatch
arn: aws: securityhub:: ruleset/ /v/1.2.0/ rule/3.14 cis-aws-foundations-benchmark	安全控制/ .14 CloudWatch

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/4.1 cis-aws-foundations-benchmark	security-control/EC2.13
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/4.2 cis-aws-foundations-benchmark	security-control/EC2.14
arn: aws: securityhub:: ruleset/ /v/1.2.0/rule/4.3 cis-aws-foundations-benchmark	security-control/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	security-control/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	安全控制/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/1.8	security-control/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	security-control/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	安全控制/ .1 CloudTrail

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
cis-aws-foundations-benchmark/v/1.4.0/3.2	安全控制/ .4 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.4	安全控制/ .5 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	安全控制/ .2 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	security-control/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	安全控制/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.4	安全控制/ .4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.5	安全控制/ .5 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	安全控制/ .6 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	安全控制/ .7 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	安全控制/ .8 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	安全控制/ .9 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.10	安全控制/ .10 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	安全控制/ .11 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.12	安全控制/ .12 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	安全控制/ .13 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	安全控制/ .14 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	security-control/EC2.21

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
cis-aws-foundations-benchmark/v/1.4.0/5.3	security-control/EC2.2
aws-foundational-security-best-练习/v/1.0.0/Account.1	security-control/Account.1
aws-foundational-security-best-练习/v/1.0.0/acm.1	security-control/ACM.1
aws-foundational-security-best-practices/v/1.0.0/apiGateway.1	security-control/APIGateway.1
aws-foundational-security-best-practices/v/1.0.0/apiGateway.2	security-control/APIGateway.2
aws-foundational-security-best-practices/v/1.0.0/apiGateway.3	security-control/APIGateway.3
aws-foundational-security-best-practices/v/1.0.0/apiGateway.4	security-control/APIGateway.4
aws-foundational-security-best-practices/v/1.0.0/apiGateway.5	security-control/APIGateway.5
aws-foundational-security-best-practices/v/1.0.0/apiGateway.8	security-control/APIGateway.8
aws-foundational-security-best-practices/v/1.0.0/apiGateway.9	security-control/APIGateway.9
aws-foundational-security-best-practices/v/1.0.0/ .1 AutoScaling	安全控制/ .1 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/ .2 AutoScaling	安全控制/ .2 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/ .3 AutoScaling	安全控制/ .3 AutoScaling

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-Practices/v/1.0.0/autoscaling.5	security-control/Autoscaling.5
aws-foundational-security-best-practices/v/1.0.0/ .6 AutoScaling	安全控制/ .6 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/ .9 AutoScaling	安全控制/ .9 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/ .1 CloudFront	安全控制/ .1 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .3 CloudFront	安全控制/ .3 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .4 CloudFront	安全控制/ .4 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .5 CloudFront	安全控制/ .5 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .6 CloudFront	安全控制/ .6 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .7 CloudFront	安全控制/ .7 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .8 CloudFront	安全控制/ .8 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .9 CloudFront	安全控制/ .9 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .10 CloudFront	安全控制/ .10 CloudFront
aws-foundational-security-best-practices/v/1.0.0/ .12 CloudFront	安全控制/ .12 CloudFront

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-practices/v/1.0.0/ .1 CloudTrail	安全控制/ .1 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/ .2 CloudTrail	安全控制/ .2 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/ .4 CloudTrail	安全控制/ .4 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/ .5 CloudTrail	安全控制/ .5 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/ .1 CodeBuild	安全控制/ .1 CodeBuild
aws-foundational-security-best-practices/v/1.0.0/ .2 CodeBuild	安全控制/ .2 CodeBuild
aws-foundational-security-best-practices/v/1.0.0/ .3 CodeBuild	安全控制/ .3 CodeBuild
aws-foundational-security-best-practices/v/1.0.0/ .4 CodeBuild	安全控制/ .4 CodeBuild
aws-foundational-security-best-练习/v/1.0.0/config.1	security-control/Config.1
aws-foundational-security-best-练习/v/1.0.0/dms.1	security-control/DMS.1
aws-foundational-security-best-practices/v/1.0.0/dynamoDB.1	security-control/DynamoDB.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.2	security-control/DynamoDB.2
aws-foundational-security-best-practices/v/1.0.0/dynamodB.3	security-control/DynamoDB.3

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/ec2.1	security-control/EC2.1
aws-foundational-security-best-练习/v/1.0.0/ec2.3	security-control/EC2.3
aws-foundational-security-best-练习/v/1.0.0/ec2.4	security-control/EC2.4
aws-foundational-security-best-练习/v/1.0.0/ec2.6	security-control/EC2.6
aws-foundational-security-best-练习/v/1.0.0/ec2.7	security-control/EC2.7
aws-foundational-security-best-练习/v/1.0.0/ec2.8	security-control/EC2.8
aws-foundational-security-best-练习/v/1.0.0/ec2.9	security-control/EC2.9
aws-foundational-security-best-practices/v/1.0.0/ec2.10	security-control/EC2.10
aws-foundational-security-best-practices/v/1.0.0/ec2.15	security-control/EC2.15
aws-foundational-security-best-practices/v/1.0.0/ec2.16	security-control/EC2.16
aws-foundational-security-best-practices/v/1.0.0/ec2.17	security-control/EC2.17
aws-foundational-security-best-practices/v/1.0.0/ec2.18	security-control/EC2.18
aws-foundational-security-best-practices/v/1.0.0/ec2.19	security-control/EC2.19

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/ec2.2	security-control/EC2.2
aws-foundational-security-best-练习/v/1.0.0/ec2.20	security-control/EC2.20
aws-foundational-security-best-practices/v/1.0.0/ec2.21	security-control/EC2.21
aws-foundational-security-best-练习/v/1.0.0/ec2.23	security-control/EC2.23
aws-foundational-security-best-practices/v/1.0.0/ec2.24	security-control/EC2.24
aws-foundational-security-best-practices/v/1.0.0/ec2.25	security-control/EC2.25
aws-foundational-security-best-练习/v/1.0.0/ecr.1	security-control/ECR.1
aws-foundational-security-best-练习/v/1.0.0/ecr.2	security-control/ECR.2
aws-foundational-security-best-练习/v/1.0.0/ecr.3	security-control/ECR.3
aws-foundational-security-best-练习/v/1.0.0/ecs.1	security-control/ECS.1
aws-foundational-security-best-practices/v/1.0.0/ecs.10	security-control/ECS.10
aws-foundational-security-best-practices/v/1.0.0/ecs.12	security-control/ECS.12
aws-foundational-security-best-练习/v/1.0.0/ecs.2	security-control/ECS.2

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/ecs.3	security-control/ECS.3
aws-foundational-security-best-练习/v/1.0.0/ecs.4	security-control/ECS.4
aws-foundational-security-best-练习/v/1.0.0/ecs.5	security-control/ECS.5
aws-foundational-security-best-practices/v/1.0.0/ecs.8	security-control/ECS.8
aws-foundational-security-best-practices/v/1.0.0/efs.1	security-control/EFS.1
aws-foundational-security-best-practices/v/1.0.0/efs.2	security-control/EFS.2
aws-foundational-security-best-practices/v/1.0.0/efs.3	security-control/EFS.3
aws-foundational-security-best-practices/v/1.0.0/efs.4	security-control/EFS.4
aws-foundational-security-best-练习/v/1.0.0/eks.2	security-control/EKS.2
aws-foundational-security-best-practices/v/1.0.0/ .1 ElasticBeanstalk	安全控制/ .1 ElasticBeanstalk
aws-foundational-security-best-practices/v/1.0.0/ .2 ElasticBeanstalk	安全控制/ .2 ElasticBeanstalk
aws-foundational-security-best-练习/v/1.0.0/elbv2.1	security-control/ELB.1
aws-foundational-security-best-练习/v/1.0.0/elb.2	security-control/ELB.2

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/elb.3	security-control/ELB.3
aws-foundational-security-best-练习/v/1.0.0/elb.4	security-control/ELB.4
aws-foundational-security-best-练习/v/1.0.0/elb.5	security-control/ELB.5
aws-foundational-security-best-practices/v/1.0.0/elb.6	security-control/ELB.6
aws-foundational-security-best-练习/v/1.0.0/elb.7	security-control/ELB.7
aws-foundational-security-best-练习/v/1.0.0/elb.8	security-control/ELB.8
aws-foundational-security-best-practices/v/1.0.0/elb.9	security-control/ELB.9
aws-foundational-security-best-practices/v/1.0.0/elb.10	security-control/ELB.10
aws-foundational-security-best-practices/v/1.0.0/elb.11	security-control/ELB.11
aws-foundational-security-best-practices/v/1.0.0/elb.12	security-control/ELB.12
aws-foundational-security-best-practices/v/1.0.0/elb.13	security-control/ELB.13
aws-foundational-security-best-practices/v/1.0.0/elb.14	security-control/ELB.14
aws-foundational-security-best-practices/v/1.0.0/emr.1	security-control/EMR.1

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/es.1	security-control/ES.1
aws-foundational-security-best-练习/v/1.0.0/es.2	security-control/ES.2
aws-foundational-security-best-练习/v/1.0.0/es.3	security-control/ES.3
aws-foundational-security-best-练习/v/1.0.0/es.4	security-control/ES.4
aws-foundational-security-best-练习/v/1.0.0/es.5	security-control/ES.5
aws-foundational-security-best-练习/v/1.0.0/es.6	security-control/ES.6
aws-foundational-security-best-练习/v/1.0.0/es.7	security-control/ES.7
aws-foundational-security-best-练习/v/1.0.0/es.8	security-control/ES.8
aws-foundational-security-best-practices/v/1.0.0/ .1 GuardDuty	安全控制/ .1 GuardDuty
aws-foundational-security-best-练习/v/1.0.0/iam.1	security-control/IAM.1
aws-foundational-security-best-练习/v/1.0.0/iam.2	security-control/IAM.2
aws-foundational-security-best-practices/v/1.0.0/iam.21	security-control/IAM.21
aws-foundational-security-best-练习/v/1.0.0/iam.3	security-control/IAM.3

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-practices/v/1.0.0/iam.4	security-control/IAM.4
aws-foundational-security-best-practices/v/1.0.0/iam.5	security-control/IAM.5
aws-foundational-security-best-practices/v/1.0.0/iam.6	security-control/IAM.6
aws-foundational-security-best-practices/v/1.0.0/iam.7	security-control/IAM.7
aws-foundational-security-best-practices/v/1.0.0/iam.8	security-control/IAM.8
aws-foundational-security-best-练习/v/1.0.0/kinesis.1	security-control/Kinesis.1
aws-foundational-security-best-练习/v/1.0.0/kms.1	security-control/KMS.1
aws-foundational-security-best-练习/v/1.0.0/kms.2	security-control/KMS.2
aws-foundational-security-best-练习/v/1.0.0/kms.3	security-control/KMS.3
aws-foundational-security-best-练习/v/1.0.0/Lambda.1	security-control/Lambda.1
aws-foundational-security-best-练习/v/1.0.0/Lambda.2	security-control/Lambda.2
aws-foundational-security-best-练习/v/1.0.0/Lambda.5	security-control/Lambda.5
aws-foundational-security-best-practices/v/1.0.0/ .3 NetworkFirewall	安全控制/ .3 NetworkFirewall

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-practices/v/1.0.0/ .4 NetworkFirewall	安全控制/ .4 NetworkFirewall
aws-foundational-security-best-practices/v/1.0.0/ .5 NetworkFirewall	安全控制/ .5 NetworkFirewall
aws-foundational-security-best-practices/v/1.0.0/ .6 NetworkFirewall	安全控制/ .6 NetworkFirewall
aws-foundational-security-best-练习/v/1.0.0/openSearch.1	security-control/Opensearch.1
aws-foundational-security-best-练习/v/1.0.0/openSearch.2	security-control/Opensearch.2
aws-foundational-security-best-练习/v/1.0.0/openSearch.3	security-control/Opensearch.3
aws-foundational-security-best-practices/v/1.0.0/openSearch.4	security-control/Opensearch.4
aws-foundational-security-best-practices/v/1.0.0/openSearch.5	security-control/Opensearch.5
aws-foundational-security-best-practices/v/1.0.0/openSearch.6	security-control/Opensearch.6
aws-foundational-security-best-practices/v/1.0.0/openSearch.7	security-control/Opensearch.7
aws-foundational-security-best-practices/v/1.0.0/openSearch.8	security-control/Opensearch.8
aws-foundational-security-best-practices/v/1.0.0/rds.1	security-control/RDS.1
aws-foundational-security-best-practices/v/1.0.0/rds.10	security-control/RDS.10

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-practices/v/1.0.0/rds.11	security-control/RDS.11
aws-foundational-security-best-practices/v/1.0.0/rds.12	security-control/RDS.12
aws-foundational-security-best-practices/v/1.0.0/rds.13	security-control/RDS.13
aws-foundational-security-best-practices/v/1.0.0/rds.14	security-control/RDS.14
aws-foundational-security-best-practices/v/1.0.0/rds.15	security-control/RDS.15
aws-foundational-security-best-practices/v/1.0.0/rds.16	security-control/RDS.16
aws-foundational-security-best-practices/v/1.0.0/rds.17	security-control/RDS.17
aws-foundational-security-best-practices/v/1.0.0/rds.18	security-control/RDS.18
aws-foundational-security-best-practices/v/1.0.0/rds.19	security-control/RDS.19
aws-foundational-security-best-practices/v/1.0.0/rds.2	security-control/RDS.2
aws-foundational-security-best-practices/v/1.0.0/rds.20	security-control/RDS.20
aws-foundational-security-best-practices/v/1.0.0/rds.21	security-control/RDS.21
aws-foundational-security-best-practices/v/1.0.0/rds.22	security-control/RDS.22

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-practices/v/1.0.0/rds.23	security-control/RDS.23
aws-foundational-security-best-practices/v/1.0.0/rds.24	security-control/RDS.24
aws-foundational-security-best-practices/v/1.0.0/rds.25	security-control/RDS.25
aws-foundational-security-best-practices/v/1.0.0/rds.3	security-control/RDS.3
aws-foundational-security-best-practices/v/1.0.0/rds.4	security-control/RDS.4
aws-foundational-security-best-practices/v/1.0.0/rds.5	security-control/RDS.5
aws-foundational-security-best-practices/v/1.0.0/rds.6	security-control/RDS.6
aws-foundational-security-best-practices/v/1.0.0/rds.7	security-control/RDS.7
aws-foundational-security-best-practices/v/1.0.0/rds.8	security-control/RDS.8
aws-foundational-security-best-practices/v/1.0.0/rds.9	security-control/RDS.9
aws-foundational-security-best-practices/v/1.0.0/redshift.1	security-control/Redshift.1
aws-foundational-security-best-practices/v/1.0.0/redshift.2	security-control/Redshift.2
aws-foundational-security-best-practices/v/1.0.0/redshift.3	security-control/Redshift.3

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-practices/v/1.0.0/redshift.4	security-control/Redshift.4
aws-foundational-security-best-practices/v/1.0.0/redshift.6	security-control/Redshift.6
aws-foundational-security-best-practices/v/1.0.0/redshift.7	security-control/Redshift.7
aws-foundational-security-best-practices/v/1.0.0/redshift.8	security-control/Redshift.8
aws-foundational-security-best-practices/v/1.0.0/redshift.9	security-control/Redshift.9
aws-foundational-security-best-练习/v/1.0.0/s3.1	security-control/S3.1
aws-foundational-security-best-练习/v/1.0.0/s3.12	security-control/S3.12
aws-foundational-security-best-练习/v/1.0.0/s3.13	security-control/S3.13
aws-foundational-security-best-练习/v/1.0.0/s3.2	security-control/S3.2
aws-foundational-security-best-练习/v/1.0.0/s3.3	security-control/S3.3
aws-foundational-security-best-练习/v/1.0.0/s3.5	security-control/S3.5
aws-foundational-security-best-练习/v/1.0.0/s3.6	security-control/S3.6
aws-foundational-security-best-练习/v/1.0.0/s3.8	security-control/S3.8

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/s3.9	security-control/S3.9
aws-foundational-security-best-practices/v/1.0.0/ .1 SageMaker	安全控制/ .1 SageMaker
aws-foundational-security-best-practices/v/1.0.0/ .2 SageMaker	安全控制/ .2 SageMaker
aws-foundational-security-best-practices/v/1.0.0/ .3 SageMaker	安全控制/ .3 SageMaker
aws-foundational-security-best-practices/v/1.0.0/ .1 SecretsManager	安全控制/ .1 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/ .2 SecretsManager	安全控制/ .2 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/ .3 SecretsManager	安全控制/ .3 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/ .4 SecretsManager	安全控制/ .4 SecretsManager
aws-foundational-security-best-练习/v/1.0.0/sqs.1	security-control/SQS.1
aws-foundational-security-best-练习/v/1.0.0/ssm.1	security-control/SSM.1
aws-foundational-security-best-练习/v/1.0.0/ssm.2	security-control/SSM.2
aws-foundational-security-best-练习/v/1.0.0/ssm.3	security-control/SSM.3
aws-foundational-security-best-practices/v/1.0.0/ssm.4	security-control/SSM.4

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
aws-foundational-security-best-练习/v/1.0.0/waf.1	security-control/WAF.1
aws-foundational-security-best-练习/v/1.0.0/waf.2	security-control/WAF.2
aws-foundational-security-best-练习/v/1.0.0/waf.3	security-control/WAF.3
aws-foundational-security-best-练习/v/1.0.0/waf.4	security-control/WAF.4
aws-foundational-security-best-练习/v/1.0.0/waf.6	security-control/WAF.6
aws-foundational-security-best-练习/v/1.0.0/waf.7	security-control/WAF.7
aws-foundational-security-best-练习/v/1.0.0/waf.8	security-control/WAF.8
aws-foundational-security-best-练习/v/1.0.0/waf.10	security-control/WAF.10
pci-dss/v/3.2.1/PCI。 AutoScaling.1	安全控制/ .1 AutoScaling
pci-dss/v/3.2.1/PCI。 CloudTrail.1	安全控制/ .2 CloudTrail
pci-dss/v/3.2.1/PCI。 CloudTrail.2	安全控制/ .3 CloudTrail
pci-dss/v/3.2.1/PCI。 CloudTrail.3	安全控制/ .4 CloudTrail
pci-dss/v/3.2.1/PCI。 CloudTrail.4	安全控制/ .5 CloudTrail
pci-dss/v/3.2.1/PCI。 CodeBuild.1	安全控制/ .1 CodeBuild
pci-dss/v/3.2.1/PCI。 CodeBuild.2	安全控制/ .2 CodeBuild
pci-dss/v/3.2.1/PCI.Config.1	security-control/Config.1

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
pci-dss/v/3.2.1/PCI.CW.1	安全控制/ .1 CloudWatch
pci-dss/v/3.2.1/PCI.DMS.1	security-control/DMS.1
pci-dss/v/3.2.1/PCI.EC2.1	security-control/EC2.1
pci-dss/v/3.2.1/PCI.EC2.2	security-control/EC2.2
pci-dss/v/3.2.1/PCI.EC2.4	security-control/EC2.12
pci-dss/v/3.2.1/PCI.EC2.5	security-control/EC2.13
pci-dss/v/3.2.1/PCI.EC2.6	security-control/EC2.6
pci-dss/v/3.2.1/PCI.ELBv2.1	security-control/ELB.1
pci-dss/v/3.2.1/PCI.ES.1	security-control/ES.2
pci-dss/v/3.2.1/PCI.ES.2	security-control/ES.1
pci-dss/v/3.2.1/PCI。 GuardDuty.1	安全控制/ .1 GuardDuty
pci-dss/v/3.2.1/PCI.IAM.1	security-control/IAM.4
pci-dss/v/3.2.1/PCI.IAM.2	security-control/IAM.2
pci-dss/v/3.2.1/PCI.IAM.3	security-control/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	security-control/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	security-control/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	security-control/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	security-control/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	security-control/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	security-control/KMS.4

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
pci-dss/v/3.2.1/PCI.Lambda.1	security-control/Lambda.1
pci-dss/v/3.2.1/PCI.Lambda.2	security-control/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	security-control/Opensearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	security-control/Opensearch.1
pci-dss/v/3.2.1/PCI.RDS.1	security-control/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	security-control/RDS.2
pci-dss/v/3.2.1/PCI.Redshift.1	security-control/Redshift.1
pci-dss/v/3.2.1/PCI.S3.1	security-control/S3.3
pci-dss/v/3.2.1/PCI.S3.2	security-control/S3.2
pci-dss/v/3.2.1/PCI.S3.3	security-control/S3.7
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.5
pci-dss/v/3.2.1/PCI.S3.6	security-control/S3.1
pci-dss/v/3.2.1/PCI。 SageMaker.1	安全控制/ .1 SageMaker
pci-dss/v/3.2.1/PCI.SSM.1	security-control/SSM.2
pci-dss/v/3.2.1/PCI.SSM.2	security-control/SSM.3
pci-dss/v/3.2.1/PCI.SSM.3	security-control/SSM.1
service-managed-aws-control-Tower/v/1.0.0/acm.1	security-control/ACM.1
service-managed-aws-control-Tower/v/1.0.0/apiGateway.1	security-control/APIGateway.1
service-managed-aws-control-Tower/v/1.0.0/Apigateway.2	security-control/APIGateway.2

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/apiGateway.3	security-control/APIGateway.3
service-managed-aws-control-Tower/v/1.0.0/apigateway.4	security-control/APIGateway.4
service-managed-aws-control-Tower/v/1.0.0/apigateway.5	security-control/APIGateway.5
service-managed-aws-control-tower/v/1.0.0/ .1 AutoScaling	安全控制/ .1 AutoScaling
service-managed-aws-control-tower/v/1.0.0/ .2 AutoScaling	安全控制/ .2 AutoScaling
service-managed-aws-control-tower/v/1.0.0/ .3 AutoScaling	安全控制/ .3 AutoScaling
service-managed-aws-control-tower/v/1.0.0/ .4 AutoScaling	安全控制/ .4 AutoScaling
service-managed-aws-control-Tower/V/1.0.0/Autoscaling.5	security-control/Autoscaling.5
service-managed-aws-control-tower/v/1.0.0/ .6 AutoScaling	安全控制/ .6 AutoScaling
service-managed-aws-control-tower/v/1.0.0/ .9 AutoScaling	安全控制/ .9 AutoScaling
service-managed-aws-control-tower/v/1.0.0/ .1 CloudTrail	安全控制/ .1 CloudTrail
service-managed-aws-control-tower/v/1.0.0/ .2 CloudTrail	安全控制/ .2 CloudTrail
service-managed-aws-control-tower/v/1.0.0/ .4 CloudTrail	安全控制/ .4 CloudTrail

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-tower/v/1.0.0/ .5 CloudTrail	安全控制/ .5 CloudTrail
service-managed-aws-control-tower/v/1.0.0/ .1 CodeBuild	安全控制/ .1 CodeBuild
service-managed-aws-control-tower/v/1.0.0/ .2 CodeBuild	安全控制/ .2 CodeBuild
service-managed-aws-control-tower/v/1.0.0/ .4 CodeBuild	安全控制/ .4 CodeBuild
service-managed-aws-control-tower/v/1.0.0/ .5 CodeBuild	安全控制/ .5 CodeBuild
service-managed-aws-control-Tower/v/1.0.0/ dms.1	security-control/DMS.1
service-managed-aws-control-Tower/v/1.0.0/ dynamoDB.1	security-control/DynamoDB.1
service-managed-aws-control-Tower/v/1.0.0/ DynamoDB.2	security-control/DynamoDB.2
service-managed-aws-control-Tower/v/1.0.0/ ec2.1	security-control/EC2.1
service-managed-aws-control-Tower/v/1.0.0/ ec2.2	security-control/EC2.2
service-managed-aws-control-Tower/v/1.0.0/ ec2.3	security-control/EC2.3
service-managed-aws-control-Tower/v/1.0.0/ ec2.4	security-control/EC2.4
service-managed-aws-control-Tower/v/1.0.0/ ec2.6	security-control/EC2.6

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/ec2.7	security-control/EC2.7
service-managed-aws-control-Tower/v/1.0.0/ec2.8	security-control/EC2.8
service-managed-aws-control-Tower/v/1.0.0/ec2.9	security-control/EC2.9
service-managed-aws-control-Tower/v/1.0.0/ec2.10	security-control/EC2.10
service-managed-aws-control-Tower/v/1.0.0/ec2.15	security-control/EC2.15
service-managed-aws-control-Tower/v/1.0.0/ec2.16	security-control/EC2.16
service-managed-aws-control-Tower/v/1.0.0/ec2.17	security-control/EC2.17
service-managed-aws-control-Tower/v/1.0.0/ec2.18	security-control/EC2.18
service-managed-aws-control-Tower/v/1.0.0/ec2.19	security-control/EC2.19
service-managed-aws-control-Tower/v/1.0.0/ec2.20	security-control/EC2.20
service-managed-aws-control-Tower/v/1.0.0/ec2.21	security-control/EC2.21
service-managed-aws-control-Tower/v/1.0.0/ec2.22	security-control/EC2.22
service-managed-aws-control-Tower/v/1.0.0/ecr.1	security-control/ECR.1

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/ecr.2	security-control/ECR.2
service-managed-aws-control-Tower/v/1.0.0/ecr.3	security-control/ECR.3
service-managed-aws-control-Tower/v/1.0.0/ecs.1	security-control/ECS.1
service-managed-aws-control-Tower/v/1.0.0/ecs.2	security-control/ECS.2
service-managed-aws-control-Tower/v/1.0.0/ecs.3	security-control/ECS.3
service-managed-aws-control-Tower/v/1.0.0/ecs.4	security-control/ECS.4
service-managed-aws-control-Tower/v/1.0.0/ecs.5	security-control/ECS.5
service-managed-aws-control-Tower/v/1.0.0/ecs.8	security-control/ECS.8
service-managed-aws-control-Tower/v/1.0.0/ecs.10	security-control/ECS.10
service-managed-aws-control-Tower/v/1.0.0/ecs.12	security-control/ECS.12
service-managed-aws-control-Tower/v/1.0.0/efs.1	security-control/EFS.1
service-managed-aws-control-Tower/v/1.0.0/efs.2	security-control/EFS.2
service-managed-aws-control-Tower/v/1.0.0/efs.3	security-control/EFS.3

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/efs.4	security-control/EFS.4
service-managed-aws-control-Tower/v/1.0.0/eks.2	security-control/EKS.2
service-managed-aws-control-Tower/v/1.0.0/elb.2	security-control/ELB.2
service-managed-aws-control-Tower/v/1.0.0/elb.3	security-control/ELB.3
service-managed-aws-control-Tower/v/1.0.0/elb.4	security-control/ELB.4
service-managed-aws-control-Tower/v/1.0.0/elb.5	security-control/ELB.5
service-managed-aws-control-Tower/v/1.0.0/elb.6	security-control/ELB.6
service-managed-aws-control-Tower/v/1.0.0/elb.7	security-control/ELB.7
service-managed-aws-control-Tower/v/1.0.0/elb.8	security-control/ELB.8
service-managed-aws-control-Tower/v/1.0.0/elb.9	security-control/ELB.9
service-managed-aws-control-Tower/v/1.0.0/elb.10	security-control/ELB.10
service-managed-aws-control-Tower/v/1.0.0/elb.12	security-control/ELB.12
service-managed-aws-control-Tower/v/1.0.0/elb.13	security-control/ELB.13

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/elb.14	security-control/ELB.14
service-managed-aws-control-Tower/v/1.0.0/elbv2.1	security-control/ELBv2.1
service-managed-aws-control-Tower/v/1.0.0/emr.1	security-control/EMR.1
service-managed-aws-control-Tower/v/1.0.0/es.1	security-control/ES.1
service-managed-aws-control-Tower/v/1.0.0/es.2	security-control/ES.2
service-managed-aws-control-Tower/v/1.0.0/es.3	security-control/ES.3
service-managed-aws-control-Tower/v/1.0.0/es.4	security-control/ES.4
service-managed-aws-control-Tower/v/1.0.0/es.5	security-control/ES.5
service-managed-aws-control-Tower/v/1.0.0/es.6	security-control/ES.6
service-managed-aws-control-Tower/v/1.0.0/es.7	security-control/ES.7
service-managed-aws-control-Tower/v/1.0.0/es.8	security-control/ES.8
service-managed-aws-control-tower/v/1.0.0/ .1 ElasticBeanstalk	安全控制/ .1 ElasticBeanstalk
service-managed-aws-control-tower/v/1.0.0/ .2 ElasticBeanstalk	安全控制/ .2 ElasticBeanstalk

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-tower/v/1.0.0/ .1 GuardDuty	安全控制/ .1 GuardDuty
service-managed-aws-control-Tower/v/1.0.0/ iam.1	security-control/IAM.1
service-managed-aws-control-Tower/v/1.0.0/ iam.2	security-control/IAM.2
service-managed-aws-control-Tower/v/1.0.0/ iam.3	security-control/IAM.3
service-managed-aws-control-Tower/v/1.0.0/ iam.4	security-control/IAM.4
service-managed-aws-control-Tower/v/1.0.0/ iam.5	security-control/IAM.5
service-managed-aws-control-Tower/v/1.0.0/ iam.6	security-control/IAM.6
service-managed-aws-control-Tower/v/1.0.0/ iam.7	security-control/IAM.7
service-managed-aws-control-Tower/v/1.0.0/ iam.8	security-control/IAM.8
service-managed-aws-control-Tower/v/1.0.0/ iam.21	security-control/IAM.21
service-managed-aws-control-Tower/v/1.0.0/kinesis.1	security-control/Kinesis.1
service-managed-aws-control-Tower/v/1.0.0/ kms.1	security-control/KMS.1
service-managed-aws-control-Tower/v/1.0.0/ kms.2	security-control/KMS.2

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/kms.3	security-control/KMS.3
service-managed-aws-control-Tower/v/1.0.0/Lambda.1	security-control/Lambda.1
service-managed-aws-control-Tower/v/1.0.0/Lambda.2	security-control/Lambda.2
service-managed-aws-control-Tower/v/1.0.0/Lambda.5	security-control/Lambda.5
service-managed-aws-control-tower/v/1.0.0/ .3 NetworkFirewall	安全控制/ .3 NetworkFirewall
service-managed-aws-control-tower/v/1.0.0/ .4 NetworkFirewall	安全控制/ .4 NetworkFirewall
service-managed-aws-control-tower/v/1.0.0/ .5 NetworkFirewall	安全控制/ .5 NetworkFirewall
service-managed-aws-control-tower/v/1.0.0/ .6 NetworkFirewall	安全控制/ .6 NetworkFirewall
service-managed-aws-control-Tower/v/1.0.0/OpenSearch.	security-control/Opensearch.1
service-managed-aws-control-塔/v/1.0.0/OpenSearch.2	security-control/Opensearch.2
service-managed-aws-control-塔/v/1.0.0/OpenSearch.3	security-control/Opensearch.3
service-managed-aws-control-Tower/v/1.0.0/OpenSearch.4	security-control/Opensearch.4
service-managed-aws-control-Tower/v/1.0.0/OpenSearch.5	security-control/Opensearch.5

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/OpenSearch.6	security-control/Opensearch.6
service-managed-aws-control-Tower/v/1.0.0/OpenSearch.7	security-control/Opensearch.7
service-managed-aws-control-Tower/v/1.0.0/OpenSearch.8	security-control/Opensearch.8
service-managed-aws-control-Tower/v/1.0.0/rds.1	security-control/RDS.1
service-managed-aws-control-Tower/v/1.0.0/rds.2	security-control/RDS.2
service-managed-aws-control-Tower/v/1.0.0/rds.3	security-control/RDS.3
service-managed-aws-control-Tower/v/1.0.0/rds.4	security-control/RDS.4
service-managed-aws-control-Tower/v/1.0.0/rds.5	security-control/RDS.5
service-managed-aws-control-Tower/v/1.0.0/rds.6	security-control/RDS.6
service-managed-aws-control-Tower/v/1.0.0/rds.8	security-control/RDS.8
service-managed-aws-control-Tower/v/1.0.0/rds.9	security-control/RDS.9
service-managed-aws-control-Tower/v/1.0.0/rds.10	security-control/RDS.10
service-managed-aws-control-Tower/v/1.0.0/rds.11	security-control/RDS.11

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/rds.13	security-control/RDS.13
service-managed-aws-control-Tower/v/1.0.0/rds.17	security-control/RDS.17
service-managed-aws-control-Tower/v/1.0.0/rds.18	security-control/RDS.18
service-managed-aws-control-Tower/v/1.0.0/rds.19	security-control/RDS.19
service-managed-aws-control-Tower/v/1.0.0/rds.20	security-control/RDS.20
service-managed-aws-control-Tower/v/1.0.0/rds.21	security-control/RDS.21
service-managed-aws-control-Tower/v/1.0.0/rds.22	security-control/RDS.22
service-managed-aws-control-Tower/v/1.0.0/rds.23	security-control/RDS.23
service-managed-aws-control-Tower/v/1.0.0/rds.25	security-control/RDS.25
service-managed-aws-control-Tower/v/1.0.0/redshift.1	security-control/Redshift.1
service-managed-aws-control-Tower/v/1.0.0/redshift.2	security-control/Redshift.2
service-managed-aws-control-Tower/v/1.0.0/redshift.4	security-control/Redshift.4
service-managed-aws-control-Tower/v/1.0.0/redshift.6	security-control/Redshift.6

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-Tower/v/1.0.0/redshift.7	security-control/Redshift.7
service-managed-aws-control-Tower/v/1.0.0/redshift.8	security-control/Redshift.8
service-managed-aws-control-Tower/v/1.0.0/redshift.9	security-control/Redshift.9
service-managed-aws-control-Tower/v/1.0.0/s3.1	security-control/S3.1
service-managed-aws-control-Tower/v/1.0.0/s3.2	security-control/S3.2
service-managed-aws-control-Tower/v/1.0.0/s3.3	security-control/S3.3
service-managed-aws-control-Tower/v/1.0.0/s3.5	security-control/S3.5
service-managed-aws-control-Tower/v/1.0.0/s3.6	security-control/S3.6
service-managed-aws-control-Tower/v/1.0.0/s3.8	security-control/S3.8
service-managed-aws-control-Tower/v/1.0.0/s3.9	security-control/S3.9
service-managed-aws-control-Tower/v/1.0.0/s3.12	security-control/S3.12
service-managed-aws-control-Tower/v/1.0.0/s3.13	security-control/S3.13
service-managed-aws-control-tower/v/1.0.0/ .1 SageMaker	安全控制/ .1 SageMaker

开启整合的控件调查发现之前的生成器 ID	开启整合的控件调查发现后的生成器 ID
service-managed-aws-control-tower/v/1.0.0/ .1 SecretsManager	安全控制/ .1 SecretsManager
service-managed-aws-control-tower/v/1.0.0/ .2 SecretsManager	安全控制/ .2 SecretsManager
service-managed-aws-control-tower/v/1.0.0/ .3 SecretsManager	安全控制/ .3 SecretsManager
service-managed-aws-control-tower/v/1.0.0/ .4 SecretsManager	安全控制/ .4 SecretsManager
service-managed-aws-control-Tower/v/1.0.0/ sqs.1	security-control/SQS.1
service-managed-aws-control-Tower/v/1.0.0/ ssm.1	security-control/SSM.1
service-managed-aws-control-Tower/v/1.0.0/ ssm.2	security-control/SSM.2
service-managed-aws-control-Tower/v/1.0.0/ ssm.3	security-control/SSM.3
service-managed-aws-control-Tower/v/1.0.0/ ssm.4	security-control/SSM.4
service-managed-aws-control-Tower/v/1.0.0/ waf.2	security-control/WAF.2
service-managed-aws-control-Tower/v/1.0.0/ waf.3	security-control/WAF.3
service-managed-aws-control-Tower/v/1.0.0/ waf.4	security-control/WAF.4

整合如何影响控件 ID 和标题

整合的控件视图和整合的控件调查发现标准化了各类标准的控件 ID 和标题。安全控件 ID 和安全控件标题这两个术语是指这些与标准无关的值。下表显示了安全控件 ID 和标题与特定标准的控件 ID 和标题的映射。属于 AWS 基础安全最佳实践 (FSBP) 标准的控件的 ID 和标题不变。

无论您的账户中开启还是关闭了整合控制结果，Security Hub 控制台都会显示与标准无关的安全控制 ID 和安全控制标题。但是，如果您的账户中关闭了合并控制结果，则 Security Hub 调查结果将包含特定于标准的控制标题（适用于 PCI 和 CIS v1.2.0）。如果在您的账户中关闭了整合控制结果，Security Hub 的调查结果将包含特定于标准的控制 ID 和安全控制 ID。有关整合如何影响控件检查调查发现的更多信息，请参阅 控件调查发现样本。

对于属于服务管理标准:一部分的控件 AWS Control Tower，启用整合控制结果后，将从查找结果中的控件 ID 和标题中删除前缀CT.。

要在此表上运行您自己的脚本，将其下载为.csv 文件。

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.2.0	1.1 避免使用根用户	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
CIS v1.2.0	1.10 确保 IAM 密码策略阻止重复使用密码	[IAM.16] 确保 IAM 密码策略阻止重复使用密码
CIS v1.2.0	1.11 确保 IAM 密码策略使密码在 90 天或更短时间内失效	[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
CIS v1.2.0	1.12 确保不存在根用户访问密钥	[IAM.4] 不应存在 IAM 根用户访问密钥
CIS v1.2.0	1.13 确保为根用户启用 MFA	[IAM.9] 应为根用户启用 MFA
CIS v1.2.0	1.14 确保为根用户启用硬件 MFA	[IAM.6] 应该为根用户启用硬件 MFA
CIS v1.2.0	1.16 确保 IAM policy 仅附加到组或角色	[IAM.2] IAM 用户不应附加 IAM policy
CIS v1.2.0	1.2 确保为拥有控制台密码的所有 IAM 用户启用多重身份验证（MFA）	[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.2.0	1.20 确保已创建支持角色来管理事件 AWS Support	[IAM.18] 确保已创建支持角色来管理事件 AWS Support
CIS v1.2.0	1.22 确保未创建允许完全“*.*”管理权限的 IAM policy	[IAM.1] IAM policy 不应允许完整的“*”管理权限
CIS v1.2.0	1.3 确保禁用 90 天或更长时间未使用的凭证	[IAM.8] 应移除未使用的 IAM 用户凭证
CIS v1.2.0	1.4 确保访问密钥每 90 天或更短时间轮换一次	[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
CIS v1.2.0	1.5 确保 IAM 密码策略要求包含至少一个大写字母	[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
CIS v1.2.0	1.6 确保 IAM 密码策略要求包含至少一个小写字母	[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
CIS v1.2.0	1.7 确保 IAM 密码策略要求包含至少一个符号	[IAM.13] 确保 IAM 密码策略要求包含至少一个符号
CIS v1.2.0	1.8 确保 IAM 密码策略要求包含至少一个数字	[IAM.14] 确保 IAM 密码策略要求包含至少一个数字
CIS v1.2.0	1.9 确保 IAM 密码策略要求最短密码长度不低于 14	[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
CIS v1.2.0	2.1 确保 CloudTrail 在所有地区都已启用	[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
CIS v1.2.0	2.2 确保已启用 CloudTrail 日志文件验证	[CloudTrail.4] 应启用 CloudTrail 日志文件验证
CIS v1.2.0	2.3 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.2.0	2.4 确保 CloudTrail 跟踪与 CloudWatch 日志集成	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
CIS v1.2.0	2.5 确保 AWS Config 已启用	AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录
CIS v1.2.0	2.6 确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
CIS v1.2.0	2.7 确保使用 KMS CMK 对 CloudTrail 日志进行静态加密	[CloudTrail.2] CloudTrail 应该启用静态加密
CIS v1.2.0	2.8 确保为客户创建的 CMK 启用轮换	[KMS.4] 应启用 AWS KMS 密钥轮换
CIS v1.2.0	2.9 确保在所有 VPC 中启用 VPC 流日志记录	[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
CIS v1.2.0	3.1 确保存在关于未经授权的 API 调用的日志指标筛选条件和警报	[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报
CIS v1.2.0	3.10 确保存在关于安全组更改的日志指标筛选条件和警报	[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
CIS v1.2.0	3.11 确保存在关于网络访问控制列表 (NACL) 更改的日志指标筛选条件和警报	[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
CIS v1.2.0	3.12 确保存在关于网络网关更改的日志指标筛选条件和警报	[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
CIS v1.2.0	3.13 确保存在关于路由表更改的日志指标筛选条件和警报	[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
CIS v1.2.0	3.14 确保存在关于 VPC 更改的日志指标筛选条件和警报	[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.2.0	3.2 确保存在关于无 MFA 的管理控制台登录的日志指标筛选条件和警报	[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报
CIS v1.2.0	3.3 确保存在关于使用根用户的日志指标筛选条件和警报	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
CIS v1.2.0	3.4 确保存在关于 IAM policy 更改的日志指标筛选条件和警报	[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报
CIS v1.2.0	3.5 确保存在针对 CloudTrail 配置更改的日志指标筛选器和警报	[CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报
CIS v1.2.0	3.6 确保存在针对 AWS Managemen t Console 身份验证失败的日志指标筛选器和警报	[CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报
CIS v1.2.0	3.7 确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
CIS v1.2.0	3.8 确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报
CIS v1.2.0	3.9 确保存在 AWS Config 配置更改的日志指标筛选器和警报	[CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报
CIS v1.2.0	4.1 确保没有安全组允许从 0.0.0.0/0 到端口 22 的传入流量	[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
CIS v1.2.0	4.2 确保没有安全组允许从 0.0.0.0/0 到端口 3389 的传入流量	[EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.2.0	4.3 确保每个 VPC 的默认安全组限制所有流量	[EC2.2] VPC 默认安全组不应允许入站或出站流量
CIS v1.4.0	1.10 确保为拥有控制台密码的所有 IAM 用户启用多重身份验证（MFA）	[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
CIS v1.4.0	1.14 确保访问密钥每 90 天或更短时间轮换一次	[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
CIS v1.4.0	1.16 确保未附加的允许完全“*.*”管理权限的 IAM policy	[IAM.1] IAM policy 不应允许完整的“*”管理权限
CIS v1.4.0	1.17 确保已创建支持角色来管理事件 AWS Support	[IAM.18] 确保已创建支持角色来管理事件 AWS Support
CIS v1.4.0	1.4 确保不存在根用户账户访问密钥	[IAM.4] 不应存在 IAM 根用户访问密钥
CIS v1.4.0	1.5 确保为根用户账户启用 MFA	[IAM.9] 应为根用户启用 MFA
CIS v1.4.0	1.6 确保为根用户账户启用硬件 MFA	[IAM.6] 应该为根用户启用硬件 MFA
CIS v1.4.0	1.7 避免使用根用户执行管理和日常任务	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
CIS v1.4.0	1.8 确保 IAM 密码策略要求最短长度不低于 14	[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
CIS v1.4.0	1.9 确保 IAM 密码策略阻止重复使用密码	[IAM.16] 确保 IAM 密码策略阻止重复使用密码
CIS v1.4.0	2.1.2 确保 S3 存储桶策略设置为拒绝 HTTP 请求	[S3.5] S3 通用存储桶应要求请求使用 SSL
CIS v1.4.0	2.1.5.1 应启用 S3 阻止公有访问设置	[S3.1] S3 通用存储桶应启用阻止公共访问设置

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.4.0	2.1.5.2 应在存储桶级别启用 S3 阻止公有访问设置	[S3.8] S3 通用存储桶应阻止公共访问
CIS v1.4.0	2.2.1 确保启用 EBS 卷加密	[EC2.7] 应启用 EBS 默认加密
CIS v1.4.0	2.3.1 确保已为 RDS 实例启用加密	[RDS.3] RDS 数据库实例应启用静态加密
CIS v1.4.0	3.1 确保 CloudTrail 在所有地区都已启用	[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
CIS v1.4.0	3.2 确保已启用 CloudTrail 日志文件验证	[CloudTrail.4] 应启用 CloudTrail 日志文件验证
CIS v1.4.0	3.4 确保 CloudTrail 跟踪与 CloudWatch 日志集成	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
CIS v1.4.0	3.5 确保 AWS Config 在所有地区都已启用	AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录
CIS v1.4.0	3.6 确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
CIS v1.4.0	3.7 确保使用 KMS CMK 对 CloudTrail 日志进行静态加密	[CloudTrail.2] CloudTrail 应该启用静态加密
CIS v1.4.0	3.8 确保为客户创建的 CMK 启用轮换	[KMS.4] 应启用 AWS KMS 密钥轮换
CIS v1.4.0	3.9 确保在所有 VPC 中启用 VPC 流日志记录	[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
CIS v1.4.0	4.4 确保存在关于 IAM policy 更改的日志指标筛选条件和警报	[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.4.0	4.5 确保存在针对 CloudTrail 配置更改的日志指标筛选器和警报	[CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报
CIS v1.4.0	4.6 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报	[CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报
CIS v1.4.0	4.7 确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
CIS v1.4.0	4.8 确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报
CIS v1.4.0	4.9 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报	[CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报
CIS v1.4.0	4.10 确保存在关于安全组更改的日志指标筛选条件和警报	[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
CIS v1.4.0	4.11 确保存在关于网络访问控制列表 (NACL) 更改的日志指标筛选条件和警报	[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
CIS v1.4.0	4.12 确保存在关于网络网关更改的日志指标筛选条件和警报	[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
CIS v1.4.0	4.13 确保存在关于路由表更改的日志指标筛选条件和警报	[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
CIS v1.4.0	4.14 确保存在关于 VPC 更改的日志指标筛选条件和警报	[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

Standard	标准控件 ID 和标题	安全控制 ID 和标题
CIS v1.4.0	5.1 确保网络 ACL 不允许从 0.0.0.0/0 进入远程服务器管理端口	[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389
CIS v1.4.0	5.3 确保每个 VPC 的默认安全组限制所有流量	[EC2.2] VPC 默认安全组不应允许入站或出站流量
PCI DSS v3.2.1	PCI。 AutoScaling.1 与负载均衡器关联的 Auto Scaling 组应使用负载均衡器运行状况检查	[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
PCI DSS v3.2.1	PCI。 CloudTrail.1 CloudTrail 日志应使用 AWS KMS CMK 进行静态加密	[CloudTrail.2] CloudTrail 应该启用静态加密
PCI DSS v3.2.1	PCI。 CloudTrail CloudTrail 应该启用 .2	[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪
PCI DSS v3.2.1	PCI。 CloudTrail.3 应启用 CloudTrail 日志文件验证	[CloudTrail.4] 应启用 CloudTrail 日志文件验证
PCI DSS v3.2.1	PCI。 CloudTrail.4 CloudTrail 路径应与 Amazon CloudWatch 日志集成	[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
PCI DSS v3.2.1	PCI。 CodeBuild.1 CodeBuild GitHub 或 Bitbucket 源存储库网址应使用 OAuth	[CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
PCI DSS v3.2.1	PCI。 CodeBuild.2 CodeBuild 项目环境变量不应包含明文凭证	[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
PCI DSS v3.2.1	应该启用 pci.config.1 AWS Config	AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录
PCI DSS v3.2.1	PCI.CW.1 应具有有关“根”用户使用的日志指标筛选条件和警报	[CloudWatch.1] “root” 用户应有日志指标筛选器和警报
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service 复制实例不应公开	[DMS.1] Database Migration Service 复制实例不应公开

Standard	标准控件 ID 和标题	安全控制 ID 和标题
PCI DSS v3.2.1	PCI.EC2.1 不应公开还原 EBS 快照	[EC2.1] Amazon EBS 快照不应公开恢复
PCI DSS v3.2.1	PCI.EC2.2 VPC 默认安全组应禁止入站和出站流量	[EC2.2] VPC 默认安全组不应允许入站或出站流量
PCI DSS v3.2.1	PCI.EC2.4 应删除未使用的 EC2 EIP	[EC2.12] 应删除未使用的 Amazon EC2 EIP
PCI DSS v3.2.1	PCI.EC2.5 不允许安全组从 0.0.0.0/0 到端口 22 的入站流量	[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
PCI DSS v3.2.1	应在所有 VPC 中启用 PCI.EC2.6 VPC 流日志记录	[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
PCI DSS v3.2.1	PCI.ELBv2.1 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS	[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch 域应位于 VPC 中	[ES.2] Elasticsearch 域名不可供公共访问
PCI DSS v3.2.1	PCI.ES.2 Elasticsearch 域应启用静态加密	[ES.1] Elasticsearch 域应启用静态加密
PCI DSS v3.2.1	PCI。 GuardDuty.1 GuardDuty 应该启用	[GuardDuty.1] GuardDuty 应该启用
PCI DSS v3.2.1	PCI.IAM.1 IAM 根用户访问密钥不应存在	[IAM.4] 不应存在 IAM 根用户访问密钥
PCI DSS v3.2.1	PCI.IAM.2 IAM 用户不应附加 IAM policy	[IAM.2] IAM 用户不应附加 IAM policy
PCI DSS v3.2.1	PCI.IAM.3 IAM policy 不应允许完全“*”管理权限	[IAM.1] IAM policy 不应允许完整的“*”管理权限

Standard	标准控件 ID 和标题	安全控制 ID 和标题
PCI DSS v3.2.1	PCI.IAM.4 应该为根用户启用硬件 MFA	[IAM.6] 应该为根用户启用硬件 MFA
PCI DSS v3.2.1	PCI.IAM.5 应该为根用户启用虚拟 MFA	[IAM.9] 应为根用户启用 MFA
PCI DSS v3.2.1	PCI.IAM.6 应该为所有 IAM 用户启用 MFA	[IAM.19] 应为所有 IAM 用户启用 MFA
PCI DSS v3.2.1	如果未在预定义的天数内使用 PCI.IAM.7 IAM 用户凭证，则应禁用	[IAM.8] 应移除未使用的 IAM 用户凭证
PCI DSS v3.2.1	PCI.IAM.8 IAM 用户的密码策略应具有可靠的配置	[IAM.10] IAM 用户的密码策略应该有很长的持续时间 AWS Config
PCI DSS v3.2.1	PCI.KMS.1 应启用客户主密钥 (CMK) 轮换	[KMS.4] 应启用 AWS KMS 密钥轮换
PCI DSS v3.2.1	PCI.Lambda.1 Lambda 函数应禁止公开访问	[Lambda.1] Lambda 函数策略应禁止公共访问
PCI DSS v3.2.1	PCI.Lambda.2 Lambda 函数应位于 VPC 中	[Lambda.3] Lambda 函数应位于 VPC 中
PCI DSS v3.2.1	PCI.openSearch.1 OpenSearch 域名应该在 VPC 中	[Opensearch.2] OpenSearch 域名不应向公众开放
PCI DSS v3.2.1	PCI.Opensearch.2 不应公开还原 EBS 快照	[Opensearch.1] OpenSearch 域名应启用静态加密
PCI DSS v3.2.1	PCI.RDS.1 RDS 快照应为私有快照	[RDS.1] RDS 快照应为私有
PCI DSS v3.2.1	PCI.RDS.2 RDS 数据库实例应禁止公开访问	[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config
PCI DSS v3.2.1	PCI.Redshift.1 Amazon Redshift 集群应禁止公共访问	[Redshift.1] Amazon Redshift 集群应禁止公共访问

Standard	标准控件 ID 和标题	安全控制 ID 和标题
PCI DSS v3.2.1	PCI.S3.1 S3 存储桶应禁止公开写入访问	[S3.3] S3 通用存储桶应阻止公共写入权限
PCI DSS v3.2.1	PCI.S3.2 S3 存储桶应禁止公开读取访问	[S3.2] S3 通用存储桶应阻止公共读取权限
PCI DSS v3.2.1	PCI.S3.3 S3 存储桶应启用跨区域复制	[S3.7] S3 通用存储桶应使用跨区域复制
PCI DSS v3.2.1	PCI.S3.5 S3 存储桶应要求请求才能使用安全套接字层	[S3.5] S3 通用存储桶应要求请求使用 SSL
PCI DSS v3.2.1	PCI.S3.6 应启用 S3 阻止公有访问设置	[S3.1] S3 通用存储桶应启用阻止公共访问设置
PCI DSS v3.2.1	PCI。 SageMaker.1 Amazon SageMaker 笔记本实例不应直接访问互联网	[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
PCI DSS v3.2.1	PCI.SSM.1 由 Systems Manager 管理的 EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态	[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
PCI DSS v3.2.1	由 Systems Manager 管理的 PCI.SSM.2 EC2 实例的关联合规性的状态应为 COMPLIANT	[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
PCI DSS v3.2.1	PCI.SSM.3 EC2 实例应由以下人员管理 AWS Systems Manager	[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

更新工作流以进行整合。

如果工作流程不依赖于任何控件调查发现字段的特定格式，则无需执行任何操作。

如果您的工作流程依赖于表格中注明的任何控制查找字段的特定格式，则应更新工作流程。例如，如果您创建的 Amazon Events 规则触发了针对特定控 CloudWatch 件 ID 的操作（例如，如果控

件 ID 等于 CIS 2.7，则调用 AWS Lambda 函数），请将该规则更新为使用 CloudTrail .2（该控件的`Compliance.SecurityControlId`字段）。

如果您使用任何已更改的控件查找字段或值创建了自定义见解，请更新这些见解以使用当前字段或值。

ASFF 示例

以下各节包含 AWS 安全调查结果格式 (ASFF) 中必填属性和可选属性的示例，以及 ASFF 支持的每种资源的示例。

主题

必需的顶级属性

Security Hub 中的所有查找结果都必须具备以下 AWS 安全调查结果格式 (ASFF) 中的顶级属性。有关这些必需属性的更多信息，请参阅《AWS Security Hub API 参考》中的 AwsSecurityFinding。

AwsAccountId

调查结果适用的 AWS 账户 ID。

示例

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

CreatedAt

表示调查发现捕获到的潜在安全问题的创建时间。

示例

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

> **Note**
>
> Security Hub 会在最近更新后 90 天或创建日期后 90 天（如果没有发生更新）删除结果。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。

对于 Security Hub 生成的控件调查发现，此字段提供了对控件的描述。

如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

生成结果的特定于解决方案的组件（离散的逻辑单元）的标识符。

对于 Security Hub 生成的控件调查发现，如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"GeneratorId": "security-control/Config.1"
```

Id

结果的特定于产品的标识符。对于 Security Hub 生成的控件调查发现，该字段提供了调查发现的 Amazon 资源名称（ARN）。

如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956
```

```
"
```

ProductArn

由 Security Hub 生成的 Amazon 资源名称（ARN），用于在产品注册到 Security Hub 后唯一标识第三方结果产品。

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 AWS 服务，`company-id`必须`aws`是 “”，并且`product-id`必须是 AWS 公共服务名称。由于 AWS 产品和服务未与账户关联，所以 ARN 的`account-id`部分为空。AWS 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对象提供了一组资源数据类型，这些数据类型描述了调查结果所指的 AWS 资源。

示例

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
```

```
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
```

```
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
                "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                "Name": "1712be25e7c7f53c731fe464f1c869b8",
                "Count": 2,
```

```
                }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

格式化结果的架构版本。该字段的值必须为 AWS确定的官方发布版本之一。在当前版本中， AWS 安全调查结果格式架构版本为2018-10-08。

示例

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

严重性

定义调查发现的重要性。有关此对象的详细信息，请参阅 AWS Security Hub API 参考中的 Severity。

Severity 既是调查发现中的顶级对象，又嵌套在 FindingProviderFields 对象之下。

调查发现的顶级 Severity 对象的值只能由 BatchUpdateFindings API 更新。

要提供严重性信息，调查发现提供商在进行 BatchImportFindings API 请求时应更新 FindingProviderFields 下的 Severity 对象。
如果对新查找结果的BatchImportFindings请求仅提供Label或仅提供Normalized，则 Security Hub 会自动填充另一个字段的值。 也可以填充Product和Original字段。

如果顶级Finding.Severity对象存在但不存在，Finding.FindingProviderFieldsSecurity Hub 会创建该FindingProviderFields.Severity对象并将整个对象复制Finding.Severity object到其中。这样可以确保即使顶层Severity对象被覆盖，提供者提供的原始细节也能保留在FindingProviderFields.Severity结构中。

结果严重性不考虑涉及的资产或底层资源的严重性。严重性将定义为与结果关联的资源的重要性级别。例如，与任务关键型应用程序关联的资源比与非生产测试关联的资源具有更高的关键性。要捕获有关资源严重性的信息，请使用 Criticality 字段。

我们建议在将调查发现的本机严重性评分转换为 ASFF 中的 Severity.Label 值时使用以下指南。

- INFORMATIONAL——此类别可能包括 PASSED、WARNING、NOT AVAILABLE 的调查发现或敏感数据标识。
- LOW——可能导致未来受损的调查发现。例如，此类别可能包括漏洞、配置漏洞和泄露密码。
- MEDIUM——结果表明遭受活动攻击，但未指示攻击者已达成其目标 例如，此类别可能包括恶意软件活动、黑客活动和异常行为检测。

- HIGH 或 CRITICAL——指示攻击者达成目标（例如主动数据丢失或泄露、拒绝服务）的调查发现。

示例

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

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。

对于控件调查发现，此字段提供控件的标题。

如果您启用整合的控件调查发现，则此字段不会引用标准。

示例

```
"Title": "AWS Config should be enabled"
```

类型

一个或多个 *namespace*/*category*/*classifier* 格式的结果类型，用于对结果进行分类。如果您启用整合的控件调查发现，则此字段不会引用标准。

Types 只能使用 BatchUpdateFindings 进行更新。

调查发现提供商想要为 Types 提供值，应使用 FindingProviderFields 下面的 Types 属性。

在下面的列表中，顶级项目符号是命名空间，二级项目符号是类别，三级项目符号是分类器。我们建议调查发现提供商使用定义的命名空间来帮助对调查发现进行排序和分组。也可以使用定义的类别和分类器，但不是必需的。仅软件和配置检查命名空间定义了分类器。

您可以为命名空间/类别/分类器定义部分路径。例如，以下调查发现类型均有效：

- TTP
- TTP/Defense Evasion
- TTPS/逃避防御/ CloudTrailStopped

以下列表中的策略、技术和程序 (TTP) 类别与 MITRE ATT&CK MatrixTM 一致。Unusual Behaviours 命名空间反映一般异常行为，例如一般统计异常，并且与特定 TTP 不一致。但是，您可以使用 Unusual Behaviors 和 TTP 结果类型对结果进行分类。

命名空间、类别和分类器列表：

- Software and Configuration Checks
  - 漏洞
    - CVE
  - AWS 安全最佳实践
    - 网络可到达性
    - 运行时行为分析
  - 行业和法规标准
    - AWS 基础安全最佳实践
    - CIS 主机强化基准
    - 独联体 AWS 基金会基准
    - PCI-DSS
    - 云安全联盟控制
    - ISO 90001 控制
    - ISO 27001 控制
    - ISO 27017 控制
    - ISO 27018 控制
    - SOC 1
    - SOC 2
    - HIPAA 控制（美国）
    - NIST 800-53 控制（美国）
    - NIST CSF 控制（美国）
    - IRAP 控制（澳大利亚）
    - K-ISMS 控制（韩国）
    - MTCS 控制（新加坡）
    - FISC 控制（日本）
    - My Number Act 控制（日本）

    - ENS 控制（西班牙）
    - Cyber Essentials Plus 控制（英国）
    - G-Cloud 控制（英国）
    - C5 控制（德国）
    - IT-Grundschutz 控制（德国）
    - GDP 控制（欧洲）
    - TISAX 控制（欧洲）
  - 补丁管理
- TTP
  - 首次访问
  - Execution
  - Persistence
  - 权限提升
  - 躲避防御系统
  - 凭证访问
  - Discovery
  - 横向移动
  - 集合
  - 命令和控制
- 影响
  - 数据公开
  - 数据泄露
  - 数据销毁
  - 拒绝服务
  - 资源消耗
- 不寻常的行为
  - 应用程序
  - 网络流量
  - IP 地址
  - 用户

  - VM
  - 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

示例

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

UpdatedAt

表示调查发现提供商上次更新查找记录的时间。

此时间戳反映了上次或最近一次更新的调查发现记录的时间。因此，它可能与 `LastObservedAt` 时间戳不同，后者反映的是上次或最近观察到事件或漏洞的时间。

更新结果记录时，必须将该时间戳更新为当前时间戳。创建调查发现记录后，`CreatedAt` 和 `UpdatedAt` 时间戳必须相同。更新调查发现记录后，该字段的值必须比它包含的所有先前值更新。

请注意，`UpdatedAt` 无法使用 `BatchUpdateFindings` API 操作进行更新。您只能使用 `BatchImportFindings` 对其进行更新。

示例

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

> **Note**
>
> Security Hub 会在最近更新后 90 天或创建日期后 90 天（如果没有发生更新）删除结果。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 ，将结果路由到您的 S3 存储桶。

可选顶级属性

这些顶级属性在 AWS 安全调查结果格式 (ASFF) 中是可选的。有关这些属性的更多信息，请参阅 AWS Security Hub API 参考AwsSecurityFinding中的。

操作

该 `Action` 对象提供有关影响资源或已对资源采取的操作的详细信息。

示例

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
```

```
                    "Org": "ExampleOrg",
                    "Isp": "ExampleISP",
                    "Asn": 64496
                }
            }
        }
    ],
    "Blocked": false
  }
}
```

AwsAccountName

调查结果适用的 AWS 账户 名称。

示例

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

生成调查发现的产品的公司名称。对于基于控制的调查结果，该公司是。 AWS

Security Hub 会为每个调查发现自动填充此属性。您无法使用 `BatchImportFindings` 或 `BatchUpdateFindings` 对其进行更新。使用自定义集成是此规则的例外。请参阅 the section called “使用自定义产品集成”。

当您使用 Security Hub 控制台按公司名称筛选调查发现时，您可以使用此属性。当您使用 Security Hub API 按公司名称筛选调查发现时，将使用 `ProductFields` 下的 `aws/securityhub/CompanyName` 属性。Security Hub 不会同步这两个属性。

示例

```
"CompanyName": "AWS"
```

合规

`Compliance` 对象提供与控件相关的调查发现细节。对于从 Security Hub 控件生成的搜索结果和 AWS Config 发送到 Security Hub 的结果，将返回此属性。

示例

```
"Compliance": {
```

```
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

置信度

调查发现能够准确识别其理应识别的行为或问题的可能性。

Confidence 只能使用 BatchUpdateFindings 进行更新。

调查发现提供商想要为 Confidence 提供值，应使用 FindingProviderFields 下面的 Confidence 属性。请参阅 the section called “使用 FindingProviderFields”。

使用比例刻度按 0-100 分对 Confidence 进行评分。 0 表示置信度为 0%，100 表示置信度为 100%。例如，基于网络流量统计偏差的数据泄露检测的置信度较低，因为实际的泄露尚未得到验证。

示例

```
"Confidence": 42
```

严重性

分配给与调查发现关联的资源的重要性级别。

Criticality 只能通过调用 BatchUpdateFindings API 操作进行更新。不要使用 BatchImportFindings 更新此对象。

调查发现提供商想要为 Criticality 提供值，应使用 FindingProviderFields 下面的 Criticality 属性。请参阅 the section called “使用 FindingProviderFields”。

使用仅支持全整型的比例刻度以 0-100 为基础对 Criticality 进行评分。评分为 0 意味着底层资源不关键，对于最关键的资源，评分为 100。

对于每种资源，在分配 Criticality 时请考虑以下几点：

- 受影响的资源是否包含敏感数据（例如，具有 PII 的 S3 存储桶）？
- 受影响的资源是否使攻击者能够加深访问或扩展其能力以执行其他恶意活动（例如，受损的系统管理员账户）？
- 资源是否为业务关键型资产（例如，在受到攻击时可能会对收入造成重大影响的关键业务系统）？

您可以使用以下准则：

- 对于支持关键任务型系统或包含高度敏感数据的资源，评分范围为 75–100。
- 对于支持重要（但非关键）系统或包含中等重要程度数据的资源，评分范围为 25–74。
- 对于支持非重要系统或包含非敏感数据的资源，评分范围应 为 0–24。

示例

```
"Criticality": 99
```

FindingProviderFields

FindingProviderFields 包括以下属性：

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

前面的字段嵌套在FindingProviderFields对象下，但其名称与顶级 ASFF 字段的名称相同。当查找结果提供者将新发现发送到 Security Hub 时，如果FindingProviderFields对象为空，Security Hub 会根据相应的顶级字段自动填充该对象。

查找提供者FindingProviderFields可以通过使用 Security Hub API 的BatchImportFindings操作进行更新。查找提供者无法使用更新此对象BatchUpdateFindings。

有关 Security Hub 如何处理由 BatchImportFindings 到 FindingProviderFields，再到相应顶级属性的更新的详细信息，请参阅 the section called “使用 FindingProviderFields”。

客户可以使用BatchUpdateFindings操作更新顶级字段。客户无法更新FindingProviderFields。

示例

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
```

```
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

表示调查发现捕获到的潜在安全问题的首次观察时间。

此时间戳反映了首次观察到事件或漏洞的时间。因此，它可能与 CreatedAt 时间戳不同，后者反映了该调查发现记录的创建时间。

该时间戳在调查发现记录的更新之间应该是不可变的，但如果确定了更准确的时间戳，则可以更新。

示例

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

LastObservedAt

表示安全调查发现产品最近一次观察到由调查发现捕获的潜在安全问题的时间。

此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，后者反映了该调查发现记录的最后一次更新时间或最近更新的时间。

您可以提供此时间戳，但在首次观察时不需要此时间戳。如果您在首次观察时提供此字段，则此时间戳应与 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）

Network 对象提供有关调查发现的网络相关信息。

此对象已停用。要提供此数据，您可以将数据映射到 Resources 中的资源，也可以使用 Action 对象。

示例

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

NetworkPath 对象提供与调查发现相关的网络路径的相关信息。NetworkPath 中的每个条目都代表路径的一个组成部分。

示例

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
```

```
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
    }
]
```

备注

Note 对象指定了用户定义的注释，您可以将其添加到调查发现中。

结果提供商可以为结果提供初始注释，但不能在此之后添加注释。您只能使用 BatchUpdateFindings 更新注释。

示例

```
"Note": {
```

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

PatchSummary

PatchSummary 对象根据所选合规性标准提供实例的补丁合规性状态摘要。

示例

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

过程

Process 对象提供有关调查发现的过程相关详细信息。

例如：

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

指示 Security Hub 何时收到调查发现并开始对其进行处理。

与 CreatedAt 和 UpdatedAt 不同，这二者是必需的时间戳，与发现提供商与安全问题和调查发现的交互有关。ProcessedAt 时间戳指示 Security Hub 何时开始处理调查发现。处理完成后，调查发现会出现在用户的账户中。

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

一种数据类型，其中安全调查结果产品可以包含其他特定于解决方案的详细信息，这些详细信息不是定义 AWS 的安全调查结果格式的一部分。

有关由 Security Hub 控件生成的调查发现，ProductFields 包括有关控件的信息。请参阅 the section called “生成和更新控件调查发现”。

此字段不应包含冗余数据，也不得包含与 AWS 安全调查结果格式字段冲突的数据。

“aws/” 前缀仅代表为 AWS 产品和服务保留的命名空间，不得与第三方集成的发现一起提交。

虽然不是必需的，但产品应将字段名称格式化为 company-id/product-id/field-name，其中 company-id 和 product-id 与结果的 ProductArn 中提供的名称匹配。

当 Security Hub 存档现有调查发现时，将使用引用 Archival 的字段。例如，当您禁用控件或标准以及打开或关闭整合的控件调查发现时，Security Hub 会存档现有调查发现。

此字段还可能包含有关标准的信息，标准中包括产生调查发现的控件。

示例

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

提供生成调查发现的产品的名称。对于基于控件的调查发现，产品名称为 Security Hub。

Security Hub 会为每个调查发现自动填充此属性。您无法使用 `BatchImportFindings` 或 `BatchUpdateFindings` 对其进行更新。使用自定义集成是此规则的例外。请参阅 the section called “使用自定义产品集成”。

当您使用 Security Hub 控制台按产品名称筛选结果时，您可以使用此属性。

当您使用 Security Hub API 按产品名称筛选结果时，将使用 `ProductFields` 下面的 `aws/securityhub/ProductName` 属性。

Security Hub 不会同步这两个属性。

RecordState

提供调查发现的记录状态。

默认情况下，在最初由服务生成时，结果被视为 `ACTIVE`。

`ARCHIVED` 状态表示应从视图中隐藏结果。已存档的查找结果不会立即删除。您可以搜索、查看和报告这些结果。如果关联的资源被删除、资源不存在或控件被禁用，Security Hub 会自动存档基于控件的调查发现。

`RecordState` 适用于调查发现提供商，并且只能通过 `BatchImportFindings` 进行更新。您无法使用 `BatchUpdateFindings` 对其进行更新。

要跟踪调查发现的状态，请使用 `Workflow` 而不是 `RecordState`。

如果记录状态从 `ARCHIVED` 变为 `ACTIVE`，且调查发现的工作流程状态为 `NOTIFIED` 或 `RESOLVED`，则 Security Hub 会自动将工作流程状态设置为 `NEW`。

示例

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

区域

指定生成查找结果 AWS 区域 的依据。

Security Hub 会为每个调查发现自动填充此属性。您无法使用 BatchImportFindings 或 BatchUpdateFindings 对其进行更新。

示例

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

RelatedFindings

提供与当前发现相关的调查发现列表。

RelatedFindings 只能使用 BatchUpdateFindings API 操作进行更新。您不应使用 BatchImportFindings 更新此对象。

对于 BatchImportFindings 请求，调查发现提供商应使用 FindingProviderFields 下面的 RelatedFindings 对象。

要查看 RelatedFindings 属性的描述，请参阅 AWS Security Hub API 参考中的 RelatedFinding。

示例

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

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": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
```

```
}
```

样本

指定调查发现是否为调查发现样本。

```
"Sample": true
```

SourceUrl

SourceUrl 对象提供一个 URL，指向有关调查发现产品中当前调查发现的页面

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

ThreatIntelIndicators

ThreatIntelIndicator 对象提供与调查发现相关的威胁情报详细信息。

示例

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

威胁

Threats 对象提供调查发现所检测到的威胁的详细信息。

示例

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
```

```
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

提供与调查发现关联的名称/值字符串对的列表。这些是添加到结果的自定义用户定义字段。这些字段可以通过特定配置自动生成。

调查发现提供商不应将此字段用于产品生成的数据。相反，查找提供者可以将该`ProductFields`字段用于未映射到任何标准 AWS 安全查找格式字段的数据。

这些字段只能使用 `BatchUpdateFindings` 进行更新。

示例

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

提供调查发现的准确性。结果产品可以提供 `UNKNOWN` 作为该字段的值。如果在结果产品的系统中存在有意义的类比，则结果产品应该为该字段提供值。该字段通常由用户在对调查发现进行调查后做出的决定或操作填充。

结果提供商可以为此属性提供初始值，但在此之后无法更新它。您只能使用 `BatchUpdateFindings` 来更新此属性。

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

漏洞

`Vulnerabilities` 对象提供与调查发现相关的漏洞列表。

示例

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
```

```
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

工作流

`Workflow` 对象提供有关结果调查状态的信息。

此字段专供客户与修复、编排和票务工具配合使用。它不适用于结果提供商。

您只能使用 `BatchUpdateFindings` 更新 `Workflow` 字段。客户还可以从控制台更新它。请参阅 the section called “设置调查发现的工作流程状态”。

示例

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

WorkflowState （已退休）

此对象已停用，已被 `Workflow` 对象的 `Status` 字段所取代。

此字段提供调查发现的工作流程状态。结果产品可以提供 `NEW` 作为该字段的值。如果在结果产品的系统中存在有意义的类比，则结果产品可以为该字段提供值。

示例

```
"WorkflowState": "NEW"
```

Resources

`Resources` 对象提供有关结果中涉及的资源的信息。

它包含最多 32 个资源对象的数组。

要确定资源名称的格式，请参阅 AWS 安全调查结果格式 (ASFF) 语法。

有关每个资源对象的示例，请从以下列表中进行选择。

主题

- 资源属性
- AwsAmazonMQ
- AwsApiGateway
- AwsAppSync
- AwsAthena
- AwsAutoScaling
- AwsBackup
- AwsCertificateManager
- AwsCloudFormation
- AwsCloudFront
- AwsCloudTrail
- AwsCloudWatch
- AwsCodeBuild
- AwsDms
- AwsDynamoDB
- AwsEc2
- AwsEcr
- AwsEcs
- AwsEfs
- AwsEks

- AwsElasticBeanstalk
- AwsElasticSearch
- AwsElb
- AwsEventBridge
- AwsGuardDuty
- AwsIam
- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds
- AwsRedshift
- AwsRoute53
- AwsS3
- AwsSageMaker
- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

资源属性

以下是 AWS 安全调查结果格式 (ASFF) 中该`Resources`对象的描述和示例。有关这些字段的更多信息，请参阅资源。

ApplicationArn

确定调查发现中涉及的应用程序的 Amazon 资源名称（ARN）。

示例

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

确定调查发现中涉及的应用程序的名称。

示例

```
"ApplicationName": "SampleApp"
```

DataClassification

DataClassification 字段提供有关在资源上检测到的敏感数据的信息。

示例

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
```

```
                        "End": 10,
                        "StartColumn": 20
                    }
                ],
                "Pages": [],
                "Records": [],
                "Cells": []
            }
        },
        {
            "Count": 59,
            "Type": "EMAIL_ADDRESS",
            "Occurrences": {
                "Pages": [
                    {
                        "PageNumber": 1,
                        "OffsetRange": {
                            "Start": 1,
                            "End": 100,
                            "StartColumn": 10
                         },
                        "LineRange": {
                            "Start": 1,
                            "End": 100,
                            "StartColumn": 10
                        }
                    }
                ]
            }
        },
        {
            "Count": 2229,
            "Type": "URL",
            "Occurrences": {
               "LineRanges": [
                    {
                        "Start": 1,
                        "End": 13
                    }
               ]
            }
        },
        {
            "Count": 13826,
```

```
                    "Type": "NameDetection",
                    "Occurrences": {
                         "Records": [
                             {
                                 "RecordIndex": 1,
                                 "JsonPath": "$.ssn.value"
                             }
                         ]
                     }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
                "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                "Name": "1712be25e7c7f53c731fe464f1c869b8",
                "Count": 2,
            }
        ],
        "TotalCount": 2
    }
  }
}
```

详细信息

Details 字段使用相应对象提供有关单个资源的更多信息。必须在 Resources 对象中的单独资源对象中提供每个资源。

请注意，如果调查发现大小超过最大值 240 KB，则 Details 对象将从调查发现中移除。对于使用 AWS Config 规则的控制结果，您可以在 AWS Config 控制台上查看资源详细信息。

Security Hub 为其支持的资源类型提供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 Type 设置为 AwsS3Bucket 并在 AwsS3Bucket 对象中提供资源详细信息。

Other 对象允许您提供自定义字段和值。您在以下情况下使用 Other 对象：

- 资源类型（资源 Type 的值）没有对应的详细信息对象。要提供资源的详细信息，您可以使用 Other 对象。
- 资源类型的对象不包括您要填充的所有字段。在这种情况下，请使用资源类型的详细信息对象来填充可用字段。使用 Other 对象填充不在特定于类型的对象中的字段。
- 资源类型不是提供的类型之一。在此情况下，将 Resource.Type 设置为 Other，并使用 Other 对象填充详细信息。

示例

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
```

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

Id

给定资源类型的标识符。

对于 AWS 由 Amazon 资源名称 (ARN) 标识的资源，这是 ARN。

对于缺少 ARN 的 AWS 资源，这是创建资源的 AWS 服务所定义的标识符。

对于非AWS 资源，这是与资源关联的唯一标识符。

示例

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

分区

资源所在的分区。分区是一组 AWS 区域。每个分区的作用域 AWS 账户 仅限于一个分区。

支持以下分区：

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

示例

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

区域

此资源 AWS 区域 所在位置的代码。有关区域代码的列表，请参阅区域端点。

示例

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

ResourceRole

标识资源在调查发现中的作用。资源要么是调查发现活动的目标，要么是执行该活动的行为者。

示例

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

标签

您可以为采集到 Security Hub 的调查结果（包括来自集成产品 AWS 服务 和第三方产品的发现）添加资源标签。您可以为标记 API `GetResources` 操作支持的资源 AWS Resource Groups 添加标签。有关支持的资源列表，请参阅支持 Res ource Groups 标记 API 的服务。

添加标签会告诉您在处理查找结果时与资源关联的标签。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。

在调查结果中包含资源标签后，无需构建数据丰富管道或手动丰富安全发现的元数据。您还可以使用标签来搜索或筛选结果和见解，并创建自动化规则。

有关适用于标签的限制的信息，请参阅标签命名限制和要求。

您只能在此字段中提供 AWS 资源上存在的标签。要提供未在 AWS 安全调查结果格式中定义的数据，请使用`Other`详细信息子字段。

示例

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

类型

要为其提供详细信息的资源的类型。

如果可能，使用提供的资源类型之一，例如 `AwsEc2Instance` 或 `AwsS3Bucket`。

如果资源类型与提供的任何资源类型不匹配，则将资源 `Type` 设置为 `Other`，并使用 `Other` 详细信息子字段填写详细信息。

支持的值列在资源下。

示例

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

AwsAmazonMQ

以下是AwsAmazonMQ资源 AWS 的安全调查结果格式 (ASFF) 的示例。

AwsAmazonMQBroker

AwsAmazonMQBroker 提供有关 Amazon MQ 代理的信息，该代理是运行在 Amazon MQ 上的消息代理环境。

以下示例显示了 AwsAmazonMQBroker 对象的 ASFF。要查看AwsAmazonMQBroker属性的描述，请参阅 AWS Security Hub API 参考中的 AwsAmazonMQBroker。

示例

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
```

```
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

以下是AwsApiGateway资源 AWS 的安全调查结果格式的示例。

AwsApiGatewayRestApi

AwsApiGatewayRestApi 对象包含有关 Amazon API Gateway 版本 1 中的 REST API 的信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 AwsApiGatewayRestApi 调查发现示例。要查看AwsApiGatewayRestApi属性的描述，请参阅 AWS Security Hub API 参考AwsApiGatewayRestApiDetails中的。

示例

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
```

```
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

`AwsApiGatewayStage` 对象提供有关版本 1 的 Amazon API Gateway 阶段的信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 `AwsApiGatewayStage` 调查发现示例。要查看`AwsApiGatewayStage`属性的描述，请参阅 AWS Security Hub API 参考AwsApiGatewayStageDetails中的。

示例

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
```

```
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

`AwsApiGatewayV2Api` 对象包含有关 Amazon API Gateway 中版本 2 API 的信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 `AwsApiGatewayV2Api` 调查发现示例。要查看`AwsApiGatewayV2Api`属性的描述，请参阅《AWS Security Hub API 参考》ApiDetails中的 AwsApiGatewayV2。

示例

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

`AwsApiGatewayV2Stage` 包含有关 Amazon API Gateway 的版本 2 阶段的信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 `AwsApiGatewayV2Stage` 调查发现示例。要查看`AwsApiGatewayV2Stage`属性的描述，请参阅《AWS Security Hub API 参考》StageDetails中的 AwsApiGatewayV2。

示例

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
```

```
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync

以下是AwsAppSync资源 AWS 的安全调查结果格式 (ASFF) 的示例。

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi提供有关 AWS AppSync GraphQL API 的信息，该API是您的应用程序的顶级结构。

以下示例显示了 AwsAppSyncGraphQLApi 对象的 ASFF。要查看AwsAppSyncGraphQLApi属性的描述，请参阅《AWS Security Hub API 参考》中的 AwsAppSyncGraphqlaPi。

示例

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

以下是AwsAthena资源 AWS 的安全调查结果格式 (ASFF) 的示例。

AwsAthenaWorkGroup

AwsAthenaWorkGroup 提供了有关 Amazon Athena 工作组的信息。工作组可帮助您分离用户、团队、应用程序或工作负载。它还可以帮助您设置数据处理限制并跟踪成本。

以下示例显示了 AwsAthenaWorkGroup 对象的 ASFF。要查看AwsAthenaWorkGroup属性的描述，请参阅 AWS Security Hub API 参考AwsAthenaWorkGroup中的。

示例

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling

以下是AwsAutoScaling资源 AWS 的安全调查结果格式的示例。

AwsAutoScalingAutoScalingGroup

AwsAutoScalingAutoScalingGroup 对象提供有关自动扩展组的详细信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 AwsAutoScalingAutoScalingGroup 调查发现示例。要查看AwsAutoScalingAutoScalingGroup属性的描述，请参阅 AWS Security Hub API 参考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

`AwsAutoScalingLaunchConfiguration` 对象提供有关启动配置的详细信息。

以下是 AWS 安全`AwsAutoScalingLaunchConfiguration`调查结果格式 (ASFF) 中的示例发现。

要查看`AwsAutoScalingLaunchConfiguration`属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsBackupBackupPlan

AwsBackupBackupPlan 对象提供有关 AWS Backup 备份计划的信息。 AWS Backup 备份计划是一种策略表达式，用于定义何时以及如何备份 AWS 资源。

以下示例显示了AwsBackupBackupPlan对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsBackupBackupPlan属性的描述，请参阅 AWS Security Hub API 参考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

AwsBackupBackupVault 对象提供有关 AWS Backup 备份文件库的信息。 AWS Backup 备份保管库是一个用于存储和组织备份的容器。

以下示例显示了AwsBackupBackupVault对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsBackupBackupVault属性的描述，请参阅 AWS Security Hub API 参考AwsBackupBackupVault中的。

示例

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

AwsBackupRecoveryPoint 对象提供有关 AWS Backup 备份的信息，也称为恢复点。 AWS Backup 恢复点表示资源在指定时间的内容。

以下示例显示了AwsBackupRecoveryPoint对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsBackupBackupVault属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsCertificateManagerCertificate

AwsCertificateManagerCertificate 对象提供有关 AWS Certificate Manager (ACM) 证书的详细信息。

以下是 AWS 安全AwsCertificateManagerCertificate调查结果格式 (ASFF) 中的示例发现。要查看AwsCertificateManagerCertificate属性的描述，请参阅 AWS Security Hub API 参考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_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
```

```
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation

以下是AwsCloudFormation资源 AWS 的安全调查结果格式的示例。

AwsCloudFormationStack

AwsCloudFormationStack 对象提供有关在顶级模板中作为资源进行嵌套的 AWS CloudFormation 堆栈的详细信息。

以下示例显示了AwsCloudFormationStack对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsCloudFormationStack属性的描述，请参阅 AWS Security Hub API 参考AwsCloudFormationStackDetails中的。

示例

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
```

```
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront

以下是AwsCloudFront资源 AWS 的安全调查结果格式的示例。

AwsCloudFrontDistribution

该AwsCloudFrontDistribution对象提供有关 Amazon CloudFront 分配配置的详细信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 AwsCloudFrontDistribution 调查发现示例。要查看AwsCloudFrontDistribution属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsCloudTrailTrail

AwsCloudTrailTrail 对象提供有关 AWS CloudTrail 路径的详细信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 AwsCloudTrailTrail 调查发现示例。要查看AwsCloudTrailTrail属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsCloudWatchAlarm

该AwsCloudWatchAlarm对象提供有关 Amazon CloudWatch 警报的详细信息，这些警报会监视指标或在警报状态发生变化时执行操作。

以下示例显示了AwsCloudWatchAlarm对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsCloudWatchAlarm属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsCodeBuildProject

AwsCodeBuildProject 对象提供有关 AWS CodeBuild 项目的信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 AwsCodeBuildProject 调查发现示例。要查看AwsCodeBuildProject属性的描述，请参阅 AWS Security Hub API 参考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"]
    }
}
```

AwsDms

以下是AwsDms资源 AWS 的安全调查结果格式的示例。

AwsDmsEndpoint

该AwsDmsEndpoint对象提供有关 AWS Database Migration Service (AWS DMS) 端点的信息。端点提供有关数据存储的连接、数据存储类型和位置信息。

以下示例显示了AwsDmsEndpoint对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsDmsEndpoint属性的描述，请参阅 AWS Security Hub API 参考AwsDmsEndpointDetails中的。

示例

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

该AwsDmsReplicationInstance对象提供有关 AWS Database Migration Service (AWS DMS) 复制实例的信息。DMS 使用复制实例连接到源数据存储，读取源数据并设置数据格式以供目标数据存储使用。

以下示例显示了AwsDmsReplicationInstance对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsDmsReplicationInstance属性的描述，请参阅 AWS Security Hub API 参考AwsDmsReplicationInstanceDetails中的。

示例

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

该AwsDmsReplicationTask对象提供有关 AWS Database Migration Service (AWS DMS) 复制任务的信息。复制任务将一组数据从源端点移动到目标端点。

以下示例显示了AwsDmsReplicationInstance对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsDmsReplicationInstance属性的描述，请参阅 AWS Security Hub API 参考AwsDmsReplicationInstance中的。

示例


```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
```

```
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB

以下是AwsDynamoDB资源 AWS 的安全调查结果格式的示例。

AwsDynamoDbTable

AwsDynamoDbTable 对象提供有关 Amazon DynamoDB 表的详细信息。

以下是 AWS 安全调查发现格式 (ASFF) 中的 AwsDynamoDbTable 调查发现示例。要查看AwsDynamoDbTable属性的描述，请参阅 AWS Security Hub API 参考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",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
```

```
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
   ],
   "GlobalTableVersion": "V1",
   "ItemCount": 2705,
   "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
    ],
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
```

```
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

以下是AwsEc2资源 AWS 的安全调查结果格式的示例。

AwsEc2ClientVpnEndpoint

该AwsEc2ClientVpnEndpoint对象提供有关 AWS Client VPN 端点的信息。客户端 VPN 端点是您创建并配置以用于启用和管理客户端 VPN 会话的资源。这是所有 Client VPN 会话的终止点。

以下示例显示了AwsEc2ClientVpnEndpoint对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEc2ClientVpnEndpoint属性的描述，请参阅《AWS Security Hub API 参考》ClientVpnEndpointDetails中的 AwsEc2。

示例

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
```

```
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

`AwsEc2Eip` 对象提供有关弹性 IP 地址的信息。

以下示例显示了`AwsEc2Eip`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2Eip`属性的描述，请参阅《AWS Security Hub API 参考》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

`AwsEc2Instance` 对象提供有关 Amazon EC2 实例的详细信息。

以下示例显示了`AwsEc2Instance`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2Instance`属性的描述，请参阅《AWS Security Hub API 参考》InstanceDetails中的 AwsEc2。

示例

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
```

```
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

`AwsEc2LaunchTemplate` 对象包含有关指定实例配置信息的 Amazon Elastic Compute Cloud 启动模板的详细信息。

以下示例显示了`AwsEc2LaunchTemplate`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2LaunchTemplate`属性的描述，请参阅《AWS Security Hub API 参考》LaunchTemplateDetails中的 AwsEc2。

示例

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
```

```
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

`AwsEc2NetworkAcl` 对象包含有关 Amazon EC2 网络访问控制列表（ACL）的详细信息。

以下示例显示了`AwsEc2NetworkAcl`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2NetworkAcl`属性的描述，请参阅《AWS Security Hub API 参考》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

`AwsEc2NetworkInterface` 对象提供有关 Amazon EC2 网络接口的信息。

以下示例显示了`AwsEc2NetworkInterface`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2NetworkInterface`属性的描述，请参阅《AWS Security Hub API 参考》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
}
```

AwsEc2RouteTable

`AwsEc2RouteTable` 对象提供有关 Amazon EC2 路由表的信息。

以下示例显示了`AwsEc2RouteTable`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2RouteTable`属性的描述，请参阅《AWS Security Hub API 参考》RouteTableDetails中的AwsEc2。

示例

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

`AwsEc2SecurityGroup` 对象描述 Amazon EC2 安全组。

以下示例显示了`AwsEc2SecurityGroup`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2SecurityGroup`属性的描述，请参阅《AWS Security Hub API 参考》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

AwsEc2Subnet 对象提供有关 Amazon EC2 中子网的信息。

以下示例显示了AwsEc2Subnet对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEc2Subnet属性的描述，请参阅《AWS Security Hub API 参考》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 对象提供有关互连虚拟私有云 (VPC) 和本地网络的 Amazon EC2 中转网关的详细信息。

以下是 AWS 安全AwsEc2TransitGateway调查结果格式 (ASFF) 中的示例发现。要查看AwsEc2TransitGateway属性的描述，请参阅《AWS Security Hub API 参考》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

`AwsEc2Volume` 对象提供有关 Amazon EC2 卷的详细信息。

以下示例显示了`AwsEc2Volume`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2Volume`属性的描述，请参阅《AWS Security Hub API 参考》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/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

`AwsEc2Vpc` 对象提供有关 Amazon EC2 VPC 的详细信息。

以下示例显示了AwsEc2Vpc对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEc2Vpc属性的描述，请参阅《AWS Security Hub API 参考》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

AwsEc2VpcEndpointService 对象包含有关 VPC 端点服务的服务配置的详细信息。

以下示例显示了AwsEc2VpcEndpointService对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEc2VpcEndpointService属性的描述，请参阅《AWS Security Hub API 参考》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

`AwsEc2VpcPeeringConnection` 对象提供有关两个 VPC 之间网络连接的详细信息。

以下示例显示了`AwsEc2VpcPeeringConnection`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2VpcPeeringConnection`属性的描述，请参阅《AWS Security Hub API 参考》VpcPeeringConnectionDetails中的 AwsEc2。

示例

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
```

```
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

AwsEc2VpnConnection

`AwsEc2VpnConnection` 对象提供有关 Amazon EC2 VPN 连接的详细信息。

以下示例显示了`AwsEc2VpnConnection`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEc2VpnConnection`属性的描述，请参阅《AWS 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 AWS 的安全调查结果格式的示例。

AwsEcrContainerImage

AwsEcrContainerImage 对象提供 Amazon ECR 镜像的信息。

以下示例显示了AwsEcrContainerImage对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEcrContainerImage属性的描述，请参阅 AWS Security Hub API 参考AwsEcrContainerImageDetails中的。

示例

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

AwsEcrRepository 对象提供有关 Amazon Elastic Container Registry 存储库的信息。

以下示例显示了AwsEcrRepository对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEcrRepository属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsEcsCluster

AwsEcsCluster 对象提供有关 Amazon Elastic Container Service 集群的详细信息。

以下示例显示了AwsEcsCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEcsCluster属性的描述，请参阅 AWS Security Hub API 参考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

`AwsEcsContainer` 对象包含有关 Amazon ECS 容器的详细信息。

以下示例显示了`AwsEcsContainer`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEcsContainer`属性的描述，请参阅 AWS Security Hub API 参考[AwsEcsContainerDetails]中的。

示例

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

`AwsEcsService` 对象提供有关 Amazon ECS 集群内的服务的详细信息。

以下示例显示了`AwsEcsService`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsEcsService`属性的描述，请参阅 AWS Security Hub API 参考[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

AwsEcsTask 对象提供有关 Amazon ECS 任务的详细信息。

以下示例显示了AwsEcsTask对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEcsTask属性的描述，请参阅 AWS Security Hub API 参考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。

以下示例显示了AwsEcsTaskDefinition对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEcsTaskDefinition属性的描述，请参阅 AWS Security Hub API 参考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"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs

以下是`AwsEfs`资源 AWS 的安全调查结果格式的示例。

AwsEfsAccessPoint

`AwsEfsAccessPoint` 对象提供有关存储在 Amazon Elastic File System 中的文件的详细信息。

以下示例显示了`AwsEfsAccessPoint`对象 AWS 的安全调查结果格式 (ASFF)。
要查看`AwsEfsAccessPoint`属性的描述，请参阅 AWS Security Hub API 参考AwsEfsAccessPointDetails中的。

示例

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks

以下是AwsEks资源 AWS 的安全调查结果格式的示例。

AwsEksCluster

AwsEksCluster 对象提供有关 Amazon EKS 集群的详细信息。

以下示例显示了AwsEksCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEksCluster属性的描述，请参阅 AWS Security Hub API 参考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": {
```

```
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

以下是`AwsElasticBeanstalk`资源 AWS 的安全调查结果格式的示例。

AwsElasticBeanstalkEnvironment

`AwsElasticBeanstalkEnvironment` 对象包含有关 AWS Elastic Beanstalk 环境的详细信息。

以下示例显示了`AwsElasticBeanstalkEnvironment`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsElasticBeanstalkEnvironment`属性的描述，请参阅 AWS Security Hub API 参考[AwsElasticBeanstalkEnvironmentDetails](#)中的。

示例

```
"AwsElasticBeanstalkEnvironment": {
```

```
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
```

```
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

以下是AwsElasticSearch资源 AWS 的安全调查结果格式的示例。

AwsElasticSearchDomain

该AwsElasticSearchDomain对象提供有关亚马逊 OpenSearch 服务域的详细信息。

以下示例显示了AwsElasticSearchDomain对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsElasticSearchDomain属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsElbLoadBalancer

AwsElbLoadBalancer 对象包含有关经典负载均衡器的详细信息。

以下示例显示了AwsElbLoadBalancer对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsElbLoadBalancer属性的描述，请参阅 AWS Security Hub API 参考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。

以下示例显示了`AwsElbv2LoadBalancer`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsElbv2LoadBalancer`属性的描述，请参阅《AWS Security Hub API 参考》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"
                }
```

AwsEventBridge

以下是AwsEventBridge资源 AWS 的安全调查结果格式的示例。

AwsEventSchemasRegistry

该AwsEventSchemasRegistry对象提供有关 Amazon EventBridge 架构注册表的信息。架构定义了发送到的事件的结构 EventBridge。架构注册表是收集架构并对其进行逻辑分组的容器。

以下示例显示了AwsEventSchemasRegistry对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEventSchemasRegistry属性的描述，请参阅 AWS Security Hub API 参考AwsEventSchemasRegistry中的。

示例

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

该AwsEventsEndpoint对象提供有关 Amazon EventBridge 全局终端节点的信息。端点可以通过使其具有区域容错能力来提高应用程序的可用性。

以下示例显示了AwsEventsEndpoint对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEventsEndpoint属性的描述，请参阅 AWS Security Hub API 参考AwsEventsEndpointDetails中的。

示例

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

该AwsEventsEventbus对象提供有关 Amazon EventBridge 全局终端节点的信息。端点可以通过使其具有区域容错能力来提高应用程序的可用性。

以下示例显示了AwsEventsEventbus对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsEventsEventbus属性的描述，请参阅 AWS Security Hub API 参考AwsEventsEventbusDetails中的。

示例

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

以下是AwsGuardDuty资源 AWS 的安全调查结果格式的示例。

AwsGuardDutyDetector

该AwsGuardDutyDetector对象提供有关 Amazon GuardDuty 探测器的信息。探测器是代表 GuardDuty 服务的对象。需要探测器 GuardDuty 才能开始运行。

以下示例显示了AwsGuardDutyDetector对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsGuardDutyDetector属性的描述，请参阅 AWS Security Hub API 参考AwsGuardDutyDetector中的。

示例

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam

以下是AwsIam资源 AWS 的安全调查结果格式的示例。

AwsIamAccessKey

AwsIamAccessKey 对象包含与调查发现相关的 IAM 访问密钥的详细信息。

以下示例显示了AwsIamAccessKey对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsIamAccessKey属性的描述，请参阅 AWS Security Hub API 参考AwsIamAccessKeyDetails中的。

示例

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

AwsIamGroup 对象包含有关 IAM 组的详细信息。

以下示例显示了AwsIamGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsIamGroup属性的描述，请参阅 AWS Security Hub API 参考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

`AwsIamPolicy` 对象代表一个 IAM 权限策略。

以下示例显示了`AwsIamPolicy`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsIamPolicy`属性的描述，请参阅 AWS Security Hub API 参考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

AwsIamRole 对象包含有关 IAM 角色的信息，包括该角色的所有策略。

以下示例显示了AwsIamRole对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsIamRole属性的描述，请参阅 AWS Security Hub API 参考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": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
```

```
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

`AwsIamUser` 对象提供有关用户的信息。

以下示例显示了`AwsIamUser`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsIamUser`属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsKinesisStream

AwsKinesisStream 对象提供有关 Amazon Kinesis Data Streams 的详细信息。

以下示例显示了AwsKinesisStream对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsKinesisStream属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsKmsKey

该AwsKmsKey对象提供有关一个的详细信息 AWS KMS key。

以下示例显示了AwsKmsKey对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsKmsKey属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsLambdaFunction

AwsLambdaFunction 对象提供有关 Lambda 函数配置的详细信息。

以下示例显示了AwsLambdaFunction对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsLambdaFunction属性的描述，请参阅 AWS Security Hub API 参考AwsLambdaFunctionDetails中的。

示例

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
```

```
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

`AwsLambdaLayerVersion` 对象提供有关 Lambda 层版本的详细信息。

以下示例显示了`AwsLambdaLayerVersion`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsLambdaLayerVersion`属性的描述，请参阅 AWS Security Hub API 参考[AwsLambdaLayerVersionDetails](#)中的。

示例

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
```

```
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

以下是AwsMsk资源 AWS 的安全调查结果格式的示例。

AwsMskCluster

AwsMskCluster 对象提供有关 Amazon Managed Streaming for Apache Kafka (Amazon MSK) 集群的信息。

以下示例显示了AwsMskCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsMskCluster属性的描述，请参阅 AWS Security Hub API 参考AwsMskClusterDetails中的。

示例

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
```

```
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

以下是AwsNetworkFirewall资源 AWS 的安全调查结果格式的示例。

AwsNetworkFirewallFirewall

AwsNetworkFirewallFirewall 对象包含有关 AWS Network Firewall 防火墙的详细信息。

以下示例显示了AwsNetworkFirewallFirewall对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsNetworkFirewallFirewall属性的描述，请参阅 AWS Security Hub API 参考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

`AwsNetworkFirewallFirewallPolicy` 对象提供有关防火墙策略的详细信息。防火墙策略定义网络防火墙的行为。

以下示例显示了`AwsNetworkFirewallFirewallPolicy`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsNetworkFirewallFirewallPolicy`属性的描述，请参阅 AWS Security Hub API 参考[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

`AwsNetworkFirewallRuleGroup` 对象提供有关 AWS Network Firewall 规则组的详细信息。规则组用于检查和控制网络流量。无状态规则组适用于各个数据包。有状态规则组适用于其流量上下文中的数据包。

规则组在防火墙策略中引用。

以下示例显示了AwsNetworkFirewallRuleGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsNetworkFirewallRuleGroup属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsOpenSearchServiceDomain

该AwsOpenSearchServiceDomain对象包含有关亚马逊 OpenSearch 服务域的信息。

以下示例显示了AwsOpenSearchServiceDomain对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsOpenSearchServiceDomain属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsRdsDbCluster

AwsRdsDbCluster 对象提供有关 Amazon RDS 数据库集群的详细信息。

以下示例显示了AwsRdsDbCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsRdsDbCluster属性的描述，请参阅 AWS Security Hub API 参考AwsRdsDbClusterDetails中的。

示例

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
```

```
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

`AwsRdsDbClusterSnapshot` 对象包含有关 Amazon RDS DS集群快照的信息。

以下示例显示了`AwsRdsDbClusterSnapshot`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsRdsDbClusterSnapshot`属性的描述，请参阅 AWS Security Hub API 参考AwsRdsDbClusterSnapshotDetails中的。

示例

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

`AwsRdsDbInstance` 对象提供有关 Amazon RDS 数据库实例的详细信息。

以下示例显示了`AwsRdsDbInstance`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsRdsDbInstance`属性的描述，请参阅 AWS Security Hub API 参考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

`AwsRdsDbSecurityGroup` 对象包含有关 Amazon Relational Database Service 的信息

以下示例显示了`AwsRdsDbSecurityGroup`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsRdsDbSecurityGroup`属性的描述，请参阅 AWS Security Hub API 参考[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

AwsRdsDbSnapshot 对象包含有关 Amazon RDS DS集群快照的详细信息。

以下示例显示了AwsRdsDbSnapshot对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsRdsDbSnapshot属性的描述，请参阅 AWS Security Hub API 参考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。

以下示例显示了`AwsRdsEventSubscription`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsRdsEventSubscription`属性的描述，请参阅 AWS Security Hub API 参考[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 AWS 的安全调查结果格式的示例。

AwsRedshiftCluster

AwsRedshiftCluster 对象包含有关 Amazon Redshift 集群的详细信息。

以下示例显示了AwsRedshiftCluster对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsRedshiftCluster属性的描述，请参阅 AWS Security Hub API 参考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": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
```

```
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "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"
        }
    ]
}
```

AwsRoute53

以下是AwsRoute53资源 AWS 的安全调查结果格式的示例。

AwsRoute53HostedZone

AwsRoute53HostedZone 对象提供有关 Amazon Route 53 托管区域的信息，包括分配给托管区域的四个名称服务器。托管区域表示可统一管理的一组记录，属于单一父域名。

以下示例显示了AwsRoute53HostedZone对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsRoute53HostedZone属性的描述，请参阅《AWS Security Hub API 参考》HostedZoneDetails 中的 AwsRoute53。

示例

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

以下是AwsS3资源 AWS 的安全调查结果格式的示例。

AwsS3AccessPoint

AwsS3AccessPoint 提供有关 Amazon S3 接入点的信息。S3 接入点是附加到 S3 存储桶的具名网络端点，您可以使用这些存储桶执行 S3 对象操作。

以下示例显示了AwsS3AccessPoint对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsS3AccessPoint属性的描述，请参阅 AWS Security Hub API 参考AccessPointDetails中的awss3。

示例

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock` 提供了有关账户的 Amazon S3 公共访问屏蔽配置的信息。

以下示例显示了`AwsS3AccountPublicAccessBlock`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsS3AccountPublicAccessBlock`属性的描述，请参阅 AWS Security Hub API 参考 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。

以下示例显示了AwsS3Bucket对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsS3Bucket属性的描述，请参阅 AWS Security Hub API 参考BucketDetails中的 awss3。

示例

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
                           {
                               "Tag": {
                                   "Key": "ArchiveAge",
                                   "Value": "9m"
                               },
                               "Type": "LifecycleTagPredicate"
                           }
                       ],
                       "Type": "LifecycleAndOperator"
                   }
               },
               "ID": "Move rotated logs to Glacier",
               "NoncurrentVersionExpirationInDays": -1,
               "NoncurrentVersionTransitions": [
                   {
                       "Days": 2,
                       "StorageClass": "GLACIER"
                   }
```

```
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
    "FilterRules": [
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
     "Value": "pre"
    },
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
     "Value": "suf"
    },
    ]
   }
  },
  "Type": "LambdaConfiguration"
 }]
},
"BucketVersioningConfiguration": {
 "IsMfaDeleteEnabled": true,
 "Status": "Off"
```

```
    },
    "BucketWebsiteConfiguration": {
     "ErrorDocument": "error.html",
     "IndexDocumentSuffix": "index.html",
     "RedirectAllRequestsTo": {
      "HostName": "example.com",
      "Protocol": "http"
     },
     "RoutingRules": [{
      "Condition": {
       "HttpErrorCodeReturnedEquals": "Redirected",
       "KeyPrefixEquals": "index"
         },
      "Redirect": {
       "HostName": "example.com",
       "HttpRedirectCode": "401",
       "Protocol": "HTTP",
       "ReplaceKeyPrefixWith": "string",
       "ReplaceKeyWith": "string"
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
```

```
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
    }
}
```

AwsS3Object

`AwsS3Object` 对象提供有关 Amazon S3 对象的信息。

以下示例显示了`AwsS3Object`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsS3Object`属性的描述，请参阅 AWS Security Hub API 参考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": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

以下是`AwsSageMaker`资源 AWS 的安全调查结果格式的示例。

AwsSageMakerNotebookInstance

该`AwsSageMakerNotebookInstance`对象提供有关 Amazon SageMaker 笔记本实例的信息，该实例是一个运行 Jupyter 笔记本应用程序的机器学习计算实例。

以下示例显示了`AwsSageMakerNotebookInstance`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsSageMakerNotebookInstance`属性的描述，请参阅 AWS Security Hub API 参考AwsSageMakerNotebookInstanceDetails中的。

示例

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

以下是`AwsSecretsManager`资源 AWS 的安全调查结果格式的示例。

AwsSecretsManagerSecret

`AwsSecretsManagerSecret` 对象提供有关 Secrets Manager 密钥的详细信息。

以下示例显示了`AwsSecretsManagerSecret`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsSecretsManagerSecret`属性的描述，请参阅 AWS Security Hub API 参考[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 AWS 的安全调查结果格式的示例。

AwsSnsTopic

AwsSnsTopic 对象包含有关 Amazon Simple Notification Service 主题。

以下示例显示了AwsSnsTopic对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsSnsTopic属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsSqsQueue

AwsSqsQueue 对象包含有关 Amazon Simple Queue Service 队列的信息。

以下示例显示了AwsSqsQueue对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsSqsQueue属性的描述，请参阅 AWS Security Hub API 参考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 AWS 的安全调查结果格式的示例。

AwsSsmPatchCompliance

AwsSsmPatchCompliance 对象根据用于修补实例的补丁基准提供有关实例补丁状态的信息。

以下示例显示了AwsSsmPatchCompliance对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsSsmPatchCompliance属性的描述，请参阅 AWS Security Hub API 参考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"
        }
    }
}
```

AwsStepFunctions

以下是AwsStepFunctions资源 AWS 的安全调查结果格式的示例。

AwsStepFunctionStateMachine

AwsStepFunctionStateMachine 对象提供有关 AWS Step Functions 状态机的信息，状态机是一个由一系列事件驱动步骤组成的工作流程。

以下示例显示了AwsStepFunctionStateMachine对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsStepFunctionStateMachine属性的描述，请参阅 AWS Security Hub API 参考AwsStepFunctionStateMachine中的。

示例

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
```

```
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

以下是AwsWaf资源 AWS 的安全调查结果格式的示例。

AwsWafRateBasedRule

AwsWafRateBasedRule 对象包含有关 AWS WAF 基于速率的全局资源规则的详细信息。 AWS WAF 基于速率的规则提供设置，以指示何时允许、阻止或计算请求。基于速率的规则包括在指定时间段内到达的请求数。

以下示例显示了AwsWafRateBasedRule对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsWafRateBasedRule属性的描述，请参阅 AWS Security Hub API 参考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

AwsWafRegionalRateBasedRule 对象包含有关基于速率的区域性资源规则的详细信息。基于速率的规则提供设置，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指定时间段内到达的请求数。

以下示例显示了AwsWafRegionalRateBasedRule对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsWafRegionalRateBasedRule属性的描述，请参阅 AWS Security Hub API 参考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 AWS WAF 区域规则的详细信息。此规则标识您想要允许、阻止或计数的 Web 请求。

以下示例显示了AwsWafRegionalRule对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsWafRegionalRule属性的描述，请参阅 AWS Security Hub API 参考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

`AwsWafRegionalRuleGroup` 对象提供有关 AWS WAF 区域规则组的详细信息。规则组是添加到 Web 访问控制列表 (Web ACL) 的预定义规则的集合。

以下示例显示了`AwsWafRegionalRuleGroup`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsWafRegionalRuleGroup`属性的描述，请参阅 AWS Security Hub API 参考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 AWS WAF 区域 Web 访问控制列表 (Web ACL) 的详细信息。Web ACL 包含用于标识您要允许、阻止或计数的请求的规则。

以下是 AWS 安全调查发现格式 (ASFF) 中的 `AwsWafRegionalWebAcl` 调查发现示例。要查看`AwsApiGatewayV2Stage`属性的描述，请参阅 AWS Security Hub API 参考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 AWS WAF 规则的信息。 AWS WAF 规则标识您要允许、阻止或计数的 Web 请求。

以下是 AWS 安全AwsWafRule调查结果格式 (ASFF) 中的示例发现。要查看AwsApiGatewayV2Stage属性的描述，请参阅 AWS Security Hub API 参考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提供了有关 AWS WAF 规则组的信息。 AWS WAF 规则组是您添加到 Web 访问控制列表 (Web ACL) 中的预定义规则的集合。

以下是 AWS 安全AwsWafRuleGroup调查结果格式 (ASFF) 中的示例发现。要查看AwsApiGatewayV2Stage属性的描述，请参阅 AWS Security Hub API 参考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"
    }]
}
```

AwsWafv2RuleGroup

该AwsWafv2RuleGroup对象提供有关 AWS WAF V2 规则组的详细信息。

以下示例显示了AwsWafv2RuleGroup对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsWafv2RuleGroup属性的描述，请参阅《AWS Security Hub API 参考》RuleGroupDetails中的AwsWafv2。

示例

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

该`AwsWafWebAcl`对象提供有关 AWS WAF Web ACL 的详细信息。

以下示例显示了`AwsWafWebAcl`对象 AWS 的安全调查结果格式 (ASFF)。要查看`AwsWafWebAcl`属性的描述，请参阅 AWS Security Hub API 参考[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"
}
```

AwsWafv2WebAcl

该AwsWafv2WebAcl对象提供有关 AWS WAF V2 Web ACL 的详细信息。

以下示例显示了AwsWafv2WebAcl对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsWafv2WebAcl属性的描述，请参阅《AWS Security Hub API 参考》WebAclDetails中的AwsWafv2。

示例

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
```

```
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

以下是AwsXray资源 AWS 的安全调查结果格式的示例。

AwsXrayEncryptionConfig

该AwsXrayEncryptionConfig对象包含有关加密配置的信息 AWS X-Ray。

以下示例显示了AwsXrayEncryptionConfig对象 AWS 的安全调查结果格式 (ASFF)。要查看AwsXrayEncryptionConfig属性的描述，请参阅 AWS Security Hub API 参考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。

以下示例显示了Container对象 AWS 的安全调查结果格式 (ASFF)。要查看Container属性的描述，请参阅 AWS Security Hub API 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

Other 对象允许您提供自定义字段和值。您在以下情况下使用 Other 对象：

- 该资源类型没有对应的 Details 对象。要提供资源的详细信息，您可以使用 Other 对象。
- 资源类型的 Details 对象不包括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 Other 对象填充不在特定于类型的对象中的属性。
- 资源类型不是提供的类型之一。在本例中，将 Resource.Type 设置为 Other，并使用 Other 对象来填充详细信息。

类型：最多 50 个键/值对的映射

每个键-值对必须满足以下要求。

- 密钥包含的字符数必须少于 128 个。
- 该值包含的字符数必须少于 1024 个。

AWS Security Hub 中的见解

AWS Security Hub 见解是一系列相关调查发现。它确定了需要注意和干预的安全区域。例如，见解可能会指出 EC2 实例是检测出不良安全实践的调查发现的主题。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，如果洞察按资源标识符分组，则该洞察会生成资源标识符列表。可选的筛选条件用于识别与见解匹配的调查发现。例如，您可能希望仅查看来自特定提供商的调查发现或与特定类型的资源相关的调查发现。

Security Hub 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 AWS 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调查发现时，见解才返回结果。例如，托管见解 29. 仅当您启用 CIS AWS 基金会标准时，按失败的 CIS 检查次数排在首位的资源才会返回结果。

主题

查看和筛选见解列表

见解页面显示可用见解的列表。

默认情况下，该列表同时显示托管和自定义见解。要根据见解类型筛选见解列表，请从筛选字段旁边的下拉菜单中选择见解类型。

- 要显示所有可用的见解，请选择所有见解。这是默认选项。
- 要仅显示托管见解，请选择 Security Hub 托管见解。
- 要仅显示自定义见解，请选择自定义见解。

您还可以根据见解名称中的文本筛选见解列表。

在筛选字段中，键入用于筛选列表的文本。筛选不区分大小写。筛选器会查找在见解名称中任意位置包含文本的见解。

查看见解结果和调查结果并采取相应措施

对于每个见解，Sec AWS urity Hub 首先确定符合筛选条件的结果，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发现并采取相应措施。

如果您启用跨区域聚合，则在聚合区域中，托管见解的调查发现包括来自聚合区域和关联区域的调查发现。对于自定义见解结果，如果见解未按区域筛选，则结果将包括来自聚合区域和关联区域的调查发现。

在其他区域，见解结果仅适用于本区域。

有关如何配置跨区域聚合的信息，请参阅 跨区域聚合。

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，如果调查发现按资源标识符或资源类型分组，则结果将包括所有匹配调查发现中的资源。这包括与筛选条件中指定的资源类型不同的资源。例如，一个见解标识符与 S3 存储桶相关联的发现。如果匹配的调查发现同时包含 S3 存储桶资源和 IAM 访问密钥资源，则见解结果将列出这两个资源。

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。

- 严重性标签——每个严重性标签的调查发现数
- AWS 账户 ID — 匹配结果的前五个账户 ID
- 资源类型——匹配调查发现的前 5 个资源类型
- 资源 ID——匹配调查发现的前 5 个资源 ID
- 产品名称——匹配的调查发现的前 5 个调查发现提供商

如果您已配置自定义操作，则可以将选定结果发送到自定义操作。该操作必须与Security Hub Insight Results事件类型的 CloudWatch 规则相关联。请参阅 the section called “自动响应和补救”。

如果您尚未配置自定义操作，则操作菜单将被禁用。

显示见解结果列表并采取相应措施

1. 打开 S AWS ecurity Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Insights。
3. 要显示见解结果列表，请选择见解名称。
4. 选中要发送到自定义操作的每个结果的复选框。
5. 从 Actions (操作) 菜单中，选择自定义操作。

查看见解结果（Security Hub API, AWS CLI）

要查看见解结果，您可以使用 API 调用或 AWS Command Line Interface。

查看洞察结果（Security Hub API， AWS CLI）

- Security Hub API – 使用该 `GetInsightResults` 操作。要确定要返回结果的见解，您需要见解 ARN。要获取自定义见解的见解 ARN，请使用 `GetInsights` 操作。
- AWS 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"
```

查看见解结果的调查发现（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 S AWS ecurity Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

2. 在导航窗格中，选择 Insights。
3. 要显示见解结果列表，请选择见解名称。
4. 要显示见解结果的调查结果列表，请从结果列表中选择项目。

调查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
- 查看单个结果的详细信息
- 更新调查发现的工作流程状态
- 将结果发送到自定义操作

托管见解

AWS Security 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。您还可以将托管见解用作新的自定义见解的基础。

与所有见解一样，仅在启用了产品集成或安全标准来生成匹配的结果时，托管见解才返回结果。

对于按资源标识符分组的见解，结果包括匹配调查发现中所有资源的标识符。这包括与筛选条件中的资源类型不同的资源。例如，见解 2 可以识别与 Amazon S3 存储桶相关的调查发现。如果匹配的调查发现包含 S3 存储桶资源和 IAM 访问密钥资源，则见解结果将包括这两种资源。

Security Hub 提供了以下托管见解：

1. 具有最多结果的 AWS 资源

   ARN：`arn:aws:securityhub:::insight/securityhub/default/1`

   分组依据：资源标识符

   调查发现筛选条件：

   - 记录状态为 ACTIVE
   - 工作流程状态为 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

分组依据：资源标识符

调查发现筛选条件：

- 类型以 Effects/Data Exposure 开头
- 资源类型为 AwsS3Bucket
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：EC2 实例映像 ID

调查发现筛选条件：

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：资源 ID

调查发现筛选条件：

- 类型以 TTPs 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

5.访问密钥活动可疑的 AWS 主体

ARN：arn:aws:securityhub:::insight/securityhub/default/9

分组依据：IAM 访问密钥主体名称

调查发现筛选条件：

- 资源类型为 AwsIamAccessKey
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

6. 不符合安全标准/最佳实践的 AWS 资源实例

ARN：arn:aws:securityhub:::insight/securityhub/default/6

分组依据：资源 ID

调查发现筛选条件：

- 类型为 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

7. 与潜在数据泄露相关的 AWS 资源

ARN：arn:aws:securityhub:::insight/securityhub/default/7

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Effects/Data Exfiltration/ 开头
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

8. 与未经授权的资源使用相关的 AWS 资源

ARN：arn:aws:securityhub:::insight/securityhub/default/8

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Effects/Resource Consumption 开头
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：资源 ID

调查发现筛选条件：

- 资源类型为 AwsS3Bucket
- 类型为 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

10. 具有敏感数据的 S3 存储桶

ARN：arn:aws:securityhub:::insight/securityhub/default/12

分组依据：资源 ID

调查发现筛选条件：

- 资源类型为 AwsS3Bucket
- 类型以 Sensitive Data Identifications/ 开头
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

11. Credentials that may have leaked (可能泄露的凭证)

ARN：arn:aws:securityhub:::insight/securityhub/default/13

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Sensitive Data Identifications/Passwords/ 开头
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Software and Configuration Checks/Vulnerabilities/CVE 开头

- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

13. 具有一般异常行为的 EC2 实例

ARN：arn:aws:securityhub:::insight/securityhub/default/17

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Unusual Behaviors 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：资源 ID

调查发现筛选条件：

- 类型以 Software and Configuration Checks/AWS Security Best Practices/Network Reachability 开头
- 资源类型为 AwsEc2Instance
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：资源 ID

调查发现筛选条件：

- 类型以下列某个项开头：
  - Software and Configuration Checks/Industry and Regulatory Standards/

    - Software and Configuration Checks/AWS Security Best Practices
  - 资源类型为 AwsEc2Instance
  - 记录状态为 ACTIVE
  - 工作流程状态为 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

    分组依据：资源 ID

    调查发现筛选条件：

  - 类型以 Software and Configuration Checks/AWS Security Best Practices/Network Reachability 开头
  - 资源类型为 AwsEc2Instance
  - 记录状态为 ACTIVE
  - 工作流程状态为 NEW 或 NOTIFIED
17. 与攻击者侦测相关的 EC2 实例

    ARN：arn:aws:securityhub:::insight/securityhub/default/22

    分组依据：资源 ID

    调查发现筛选条件：

  - 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 AWS 资源

    ARN：arn:aws:securityhub:::insight/securityhub/default/23

    分组依据：资源 ID

    调查发现筛选条件：

  - 类型以下列某个项开头：
    - Effects/Data Exfiltration/Trojan

    - TTPs/Initial Access/Trojan
    - TTPs/Command and Control/Backdoor
    - TTPs/Command and Control/Trojan
    - Software and Configuration Checks/Backdoor
    - Unusual Behaviors/VM/Backdoor
  - 记录状态为 ACTIVE
  - 工作流程状态为 NEW 或 NOTIFIED

19. 与加密货币问题相关的 AWS 资源

    ARN：arn:aws:securityhub:::insight/securityhub/default/24

    分组依据：资源 ID

    调查发现筛选条件：

  - 类型以下列某个项开头：
    - Effects/Resource Consumption/Cryptocurrency
    - TTPs/Command and Control/CryptoCurrency
  - 记录状态为 ACTIVE
  - 工作流程状态为 NEW 或 NOTIFIED

20. 具有未经授权的访问尝试的 AWS 资源

    ARN：arn:aws:securityhub:::insight/securityhub/default/25

    分组依据：资源 ID

    调查发现筛选条件：

  - 类型以下列某个项开头：
    - TTPs/Command and Control/UnauthorizedAccess
    - TTPs/Initial Access/UnauthorizedAccess
    - Effects/Data Exfiltration/UnauthorizedAccess
    - Unusual Behaviors/User/UnauthorizedAccess
    - Effects/Resource Consumption/UnauthorizedAccess
  - 记录状态为 ACTIVE
  - 工作流程状态为 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

    调查发现筛选条件：

    - 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

    分组依据： AWS 账户 ID

    调查发现筛选条件：

    - 记录状态为 ACTIVE
    - 工作流程状态为 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

    分组依据：产品名称

    调查发现筛选条件：

    - 记录状态为 ACTIVE
    - 工作流程状态为 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

    分组依据：严重性标签

    调查发现筛选条件：

    - 记录状态为 ACTIVE
    - 工作流程状态为 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

    分组依据：资源 ID

    调查发现筛选条件：

- 资源类型为 AwsS3Bucket
- 记录状态为 ACTIVE
- 工作流程状态为 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

    分组依据：资源 ID

    调查发现筛选条件：

    - 资源类型为 AwsEc2Instance
    - 记录状态为 ACTIVE
    - 工作流程状态为 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

    分组依据：EC2 实例映像 ID

    调查发现筛选条件：

    - 资源类型为 AwsEc2Instance
    - 记录状态为 ACTIVE
    - 工作流程状态为 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

    分组依据：IAM 访问密钥 ID

    调查发现筛选条件：

    - 资源类型为 AwsIamAccessKey
    - 记录状态为 ACTIVE
    - 工作流程状态为 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

    分组依据：资源 ID

调查发现筛选条件：

- 生成器 ID 以 arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule 开头
- 已在最后一天更新
- 合规性状态为 FAILED
- 记录状态为 ACTIVE
- 工作流程状态为 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

分组依据：产品 ARN

调查发现筛选条件：

- 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

分组依据：资源 ID

调查发现筛选条件：

- 已在最后一天更新
- 合规性状态为 FAILED
- 记录状态为 ACTIVE
- 工作流程状态为 NEW 或 NOTIFIED

32. 有可疑活动的 IAM 用户

ARN：arn:aws:securityhub:::insight/securityhub/default/37

分组依据：IAM 用户

调查发现筛选条件：

- 资源类型为 AwsIamUser
- 记录状态为 ACTIVE

- 工作流程状态为 NEW 或 NOTIFIED

33. 具有最多 AWS Health 调查发现的资源

    ARN：arn:aws:securityhub:::insight/securityhub/default/38

    分组依据：资源 ID

    调查发现筛选条件：

    - ProductName 等于 Health

34. 具有最多 AWS Config 调查发现的资源

    ARN：arn:aws:securityhub:::insight/securityhub/default/39

    分组依据：资源 ID

    调查发现筛选条件：

    - ProductName 等于 Config

35. 调查发现最多的应用程序

    ARN：arn:aws:securityhub:::insight/securityhub/default/40

    分组依据: ResourceApplicationArn

    调查发现筛选条件：

    - RecordState 等于 ACTIVE
    - Workflow.Status 等于 NEW 或 NOTIFIED

自定义见解

除了 AWS Security Hub 托管见解之外，您还可以在 Security Hub 中创建自定义见解来跟踪特定于环境的问题。自定义见解提供了一种跟踪精选问题子集的方法。

以下是一些可能有助于设置的自定义见解示例：

- 如果您拥有管理员账户，则可以设置自定义见解来跟踪影响成员账户的关键和高严重性调查发现。
- 如果您依赖特定的集成 AWS 服务，则可以设置自定义见解来跟踪该服务的关键和高严重性调查发现。
- 如果您依赖第三方集成，您可以设置一个自定义见解来跟踪来自该集成产品的关键和高严重性结果。

您可以创建全新的自定义见解，也可以从现有的自定义见解或托管见解开始。

每个见解均配置了以下选项。

- 分组属性——分组属性确定了在见解结果列表中显示哪些项目。例如，如果分组属性是产品名称，则见解结果将显示与每个调查发现提供商关联的调查发现数。
- 可选筛选条件——筛选条件将缩小见解的匹配调查发现的范围。

  在查询结果时，Security Hub 会将 Boolean AND 逻辑应用于筛选条件集。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，如果筛选条件是“产品名称是 GuardDuty”和“资源类型是 `AwsS3Bucket`”，则匹配的调查发现必须同时符合这两个条件。

  不过，Security Hub 会对使用的属性相同但值不同的筛选条件应用 Boolean OR 逻辑。例如，如果筛选条件是“产品名称是 GuardDuty”和“产品名称是 Amazon Inspector”，则仅在调查发现由 GuardDuty 或 Amazon Inspector 生成时才被视为匹配的调查发现。

请注意，如果您使用资源标识符或资源类型作为分组属性，则见解结果将包括匹配调查发现中的所有资源。该列表不限于与资源类型筛选条件匹配的资源。例如，见解可以识别与 S3 存储桶关联的调查发现，并按资源标识符对这些调查发现进行分组。匹配的调查发现同时包含 S3 存储桶资源和 IAM 访问密钥资源。见解结果包括这两种资源。

创建自定义见解（控制台）

可以从控制台中创建全新的见解。

创建自定义见解

1. 打开 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Insights。
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选项。
   b. 选择 Group by (分组依据)。
   c. 选择要用于对与该见解关联的调查发现进行分组的属性。
   d. 选择 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，然后选择应用。

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（编程方式）

选择您的首选方法，然后按照以下步骤在 Security Hub 中以编程方式创建自定义见解。您可以指定筛选条件，将见解中的调查发现集合范围缩小到特定的子集。

以下选项卡包含几种语言的创建自定义见解的说明。有关其他语言的支持，请参阅在 AWS 上构建的工具。

Security Hub API

1. 运行CreateInsight操作。
2. 为自定义洞察输入 Name 参数名称。
3. 填充 Filters 参数以指定要在见解中包含哪些调查发现。
4. 填充 GroupByAttribute 参数以指定使用哪个属性对包含在见解中的调查发现进行分组。
5. 或者，填充 SortCriteria 参数以按特定字段对调查发现进行排序。

如果您启用了跨区域聚合并从聚合区域调用此 API，则该见解将应用于聚合和关联区域中的匹配调查发现。

AWS CLI

1. 在命令行处，运行 create-insight 命令。
2. 为自定义洞察输入 name 参数名称。
3. 填充 filters 参数以指定要在见解中包含哪些调查发现。
4. 填充 group-by-attribute 参数以指定使用哪个属性对包含在见解中的调查发现进行分组。

如果您启用了跨区域聚合并从聚合区域运行此命令，则该见解将应用于聚合和关联区域的匹配调查发现。

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

示例

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. 使用 New-SHUBInsight cmdlet。
2. 为自定义洞察输入 Name 参数名称。
3. 填充 Filter 参数以指定要在见解中包含哪些调查发现。
4. 填充 GroupByAttribute 参数以指定使用哪个属性对包含在见解中的调查发现进行分组。

如果您已启用跨区域聚合并使用聚合区域中的此 cmdlet，则该见解将应用于聚合和关联区域的匹配调查发现。

示例

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

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 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Insights。

3. 选择要修改的自定义见解。
4. 根据需要编辑见解配置。

   - 要更改用于对见解中的结果进行分组的属性，请执行以下操作：

     a. 要删除现有分组，请选择分组设置旁边的 X。

     b. 选择搜索框。

     c. 选择要用于分组的属性。

     d. 选择 Apply（应用）。
   - 要从见解中删除筛选条件，请选择筛选条件旁边带圆圈的 X。
   - 要将筛选条件添加到见解，请执行以下操作：

     a. 选择搜索框。

     b. 选择要用作筛选条件的属性和值。

     c. 选择 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（编程方式）

要修改自定义见解，请选择您的首选方法，然后按照说明操作。

Security Hub API

1. 运行UpdateInsight操作。
2. 要识别自定义见解，请提供见解的 Amazon 资源名称（ARN）。要获取自定义见解的 ARN，请运行 GetInsights 操作。
3. 根据需要更新参数 `Name`、`Filters` 和 `GroupByAttribute`。

AWS CLI

1. 在命令行处，运行 update-insight 命令。

2. 要识别自定义见解，请提供见解的 Amazon 资源名称（ARN）。要获取自定义见解的 ARN，请运行 get-insights 命令。
3. 根据需要更新参数 name、filters 和 group-by-attribute。

```
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-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. 使用 Update-SHUBInsight cmdlet。
2. 要识别自定义见解，请提供见解的 Amazon 资源名称（ARN）。要获取自定义见解的 ARN，请使用 Get-SHUBInsight cmdlet。
3. 根据需要更新参数 Name、Filter 和 GroupByAttribute。

示例

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

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 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Insights。
3. 选择要使用的托管见解。
4. 根据需要编辑见解配置。
   - 要更改用于对见解中的结果进行分组的属性，请执行以下操作：
     a. 要删除现有分组，请选择分组设置旁边的 X。
     b. 选择搜索框。
     c. 选择要用于分组的属性。
     d. 选择 Apply（应用）。
   - 要从见解中删除筛选条件，请选择筛选条件旁边带圆圈的 X。
   - 要将筛选条件添加到见解，请执行以下操作：
     a. 选择搜索框。
     b. 选择要用作筛选条件的属性和值。
     c. 选择 Apply（应用）。
5. 更新完成后，请选择 Create insight (创建见解)。
6. 在出现提示时，输入见解名称，然后选择创建见解。

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 AWS Security Hub 控制台，登陆：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（编程方式）

要删除自定义见解，请选择您的首选方法，然后按照说明操作。

Security Hub API

1. 运行DeleteInsight操作。
2. 要识别删除的自定义见解，请提供见解的 ARN。要获取自定义见解的 ARN，请运行 GetInsights 操作。

AWS CLI

1. 在命令行处，运行 delete-insight 命令。
2. 要识别自定义见解，请提供该见解的 ARN。要获取自定义见解的 ARN，请运行 get-insights 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"
```

PowerShell

1. 使用 Remove-SHUBInsight cmdlet。
2. 要识别自定义见解，请提供该见解的 ARN。要获取自定义见解的 ARN，请使用 Get-SHUBInsight cmdlet。

示例

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

自动化

Security Hub 自动化可以帮助您根据自己的规格快速修改和修复发现。

Security Hub 目前支持两种类型的自动化：

- 自动化规则 - 根据您定义的标准，近乎实时地自动更新和隐藏结果。
- 自动响应和补救 – 创建自定义的 EventBridge 规则，定义针对特定发现和洞察采取的自动措施。

自动规则优先于 EventBridge 规则。也就是说，在将调查发现发送到 EventBridge 之前，会触发自动规则并更新调查发现。然后，EventBridge 规则将应用于更新的调查发现。

在为安全控件设置自动化时，我们建议根据控件 ID 而不是标题或描述进行筛选。虽然 Security Hub 偶尔会更新控件标题和描述，但控件 ID 不会发生变更。

主题

自动化规则

自动化规则可用于自动更新 Security Hub 中的调查发现。提取调查发现时，Security Hub 可以应用各种规则操作，例如隐藏调查发现、更改其严重性以及在调查发现中添加注释。当调查发现符合您的指定标准（例如调查发现与哪个资源或账户 ID 或其标题相匹配时），此类规则操作就会生效。

自动化规则的使用案例示例包括：

- 如果调查发现的资源 ID 指的是业务关键型资源，则将调查发现的严重性提升为 `CRITICAL`。
- 如果调查发现影响特定生产账户中的资源，则将调查发现的严重性从 `HIGH` 提升到 `CRITICAL`。
- 分配具有 `SUPPRESSED` 工作流程状态 `INFORMATIONAL` 严重性的特定调查发现。

自动化规则可用于更新 AWS 安全查找格式 (ASFF) 中的选定查找字段。规则适用于新的和更新后的调查发现。

您可以从头开始创建自定义规则，也可以使用 Security Hub 提供的规则模板。如果您使用规则模板，则可以根据用例的需要对其进行修改。

自动化规则的工作原理

Security Hub 管理员可以通过定义规则标准来创建自动化规则。当调查发现与定义的条件相匹配时，Security Hub 会对其应用规则操作。有关可用条件和操作的更多信息，请参阅 可用的规则条件和规则操作。

只有 Security Hub 管理员账户可以创建、删除、编辑和查看自动化规则。管理员创建的规则适用于管理员账户和所有成员账户中的调查发现。通过提供成员账户 ID 作为规则标准，Security Hub 管理员还可以使用自动化规则来更新特定成员账户中的调查发现或对调查发现采取行动。

自动化规则仅适用于其创建时 AWS 区域 所在的。要在多个区域中应用规则，委托管理员必须在每个区域中创建规则。这可以通过 Security Hub 控制台、Security Hub API 或 AWS CloudFormation 完成。您也可以使用多区域部署脚本。

要获取自动化规则改变您的调查发现的历史记录，请参阅 查看发现历史记录。

> **Important**
>
> 自动化规则适用于 Security Hub 在您创建规则后生成或提取的新的和更新后的调查发现。Security Hub 每 12 至 24 小时或在关联资源状态发生变化时更新控件调查发现。有关更多信息，请参阅运行安全检查的计划。自动化规则评估提供商提供的原始查找字段。通过BatchUpdateFindings操作创建规则后，当您更新查找字段时，不会触发规则。

Security Hub 目前最多支持管理员账户的 100 条自动化规则。

规则顺序

创建自动化规则时，您可以为每条规则分配一个顺序。这决定了 Security Hub 应用您的自动化规则的顺序，当多个规则与同一个调查发现或调查发现字段相关时，这变得非常重要。

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

在 Security Hub 控制台中创建规则时，Security Hub 会根据规则的创建顺序自动分配规则顺序。最近创建的规则具有最低的规则顺序数值，因此首先适用。Security Hub 按升序应用后续规则。

当您通过 Security Hub API 或创建规则时 AWS CLI，Security Hub 会`RuleOrder`首先应用数值最低的规则。然后它按升序应用后续规则。如果多个调查发现有相同的 `RuleOrder`，则 Security Hub 会先为 `UpdatedAt` 字段应用具有较早值的规则（也就是说，最近编辑的规则应用在最后）。

您可以随时修改规则顺序。

规则顺序示例：

规则 A（规则顺序为 **1**）：

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

规则 B（规则顺序为 **2**）：

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

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

可用的规则条件和规则操作

目前支持以下 ASFF 字段作为自动化规则的条件。

ASFF 字段	筛选条件	字段类型
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS,	String

ASFF 字段	筛选条件	字段类型
	NOT_EQUALS, PREFIX_NOT_EQUALS	
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	选择：[FAILED、NOT_AVAILABLE 、PASSED、WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数字
CreatedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）

ASFF 字段	筛选条件	字段类型
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数字
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）

ASFF 字段	筛选条件	字段类型
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串

ASFF 字段	筛选条件	字段类型
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceType	Is, Is Not	选择（请参阅 ASFF 支持的资源）
SeverityLabel	Is, Is Not	选择：[CRITICAL、HIGH、MEDIUM、LOW、INFORMATIONAL]

ASFF 字段	筛选条件	字段类型
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字符串
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	日期（格式为 2022-12-01T21:47:39.269Z）
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	选择：[NEW、NOTIFIED、RESOLVED、SUPPRD]

目前支持以下 ASFF 字段作为自动化规则的操作：

- Confidence
- Criticality

- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

有关特定 ASFF 字段的更多信息，请参阅 AWS 安全调查发现格式（ASFF）语法和 ASFF 示例。

> **Tip**
>
> 如果您希望 Security Hub 停止为特定控件生成调查发现，我们建议您禁用该控件，而不是使用自动化规则。当您禁用某个控件时，Security Hub 会停止对其运行安全检查，并停止为其生成调查发现，因此您不会为该控件支付费用。对于符合定义条件的调查发现，我们建议使用自动化规则来更改特定 ASFF 字段的值。有关禁用控件的详细信息，请参阅 在所有标准中启用和禁用控件。

创建自动化规则

您可以从头开始创建自定义规则，也可以使用预先填充的 Security Hub 规则模板。

您一次只能创建一条自动化规则。要创建多个自动化规则，请多次遵循控制台过程，或者使用所需的参数多次调用 API 或命令。

您必须在您希望规则应用于调查发现的每个区域和账户中创建自动化规则。

当您在 Security Hub 控制台中创建自动化规则时，Security Hub 会显示您的规则所适用的调查发现预览。如果您的规则条件包含“CONTAINS”或“NOT_CONTAINS”筛选条件，则当前不支持预览。您可以为映射和字符串字段类型选择这些筛选条件。

> **Important**
>
> AWS 建议您不要在规则名称、描述或其他字段中包含个人身份、机密或敏感信息。

使用模板创建规则（仅限控制台）

目前，只有 Security Hub 控制台支持规则模板。这些模板反映了自动化规则的常见用例，可以帮助您开始使用该功能。完成以下步骤以在控制台中的模板创建自动化规则。

Console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   登录 Security Hub 管理员账户。
2. 在导航窗格中，选择 自动化。
3. 选择创建规则。在规则类型中，选择从模板创建规则。
4. 从下拉菜单中选择规则模板。
5. （可选）如果您的用例有需要，请修改规则、条件和自动操作部分。您必须指定至少一个规则条件和一个规则操作。

   如果您的选定条件支持，则控制台会显示符合您条件的调查发现预览。
6. 对于规则状态，请选择在规则创建后将其设置为启用或是禁用。
7. （可选）展开附加设置部分。如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请选择忽略符合这些条件的调查发现后续规则。
8. （可选）对于标签，请以键-值对的形式添加标签以帮助您轻松识别规则。
9. 选择创建规则。

创建自定义规则

选择您的首选方式，完成以下步骤以创建自定义自动化规则。

Console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   登录 Security Hub 管理员账户。
2. 在导航窗格中，选择 自动化。
3. 选择创建规则。对于规则类型，选择创建自定义规则。
4. 在规则部分，为您的规则提供唯一的规则名称和描述。
5. 对于条件，使用键、运算符和值下拉菜单来指定您的规则条件。您必须至少指定一项规则标准。

如果您的选定条件支持，则控制台会显示符合您条件的调查发现预览。

6. 对于自动操作，请使用下拉菜单，指定在调查发现符合规则条件时要更新的调查发现字段。您必须指定至少一个规则操作。
7. 对于规则状态，请选择在规则创建后将其设置为启用或是禁用。
8. （可选）展开附加设置部分。如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请选择忽略符合这些条件的调查发现后续规则。
9. （可选）对于标签，请以键-值对的形式添加标签以帮助您轻松识别规则。
10. 选择创建规则。

API

1. 从 Security Hub 管理员账户运行 `CreateAutomationRule`。此 API 使用特定的 Amazon 资源名称（ARN）创建规则。
2. 提供规则的名称和描述。
3. 如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请将 `IsTerminal` 参数设置为 `true`。
4. 对于 `RuleOrder` 参数，请提供规则的顺序。Security Hub 首先对该参数应用数值较小的规则。
5. 对于 `RuleStatus` 参数，请指定是否希望 Security Hub 启用该规则，并在创建后开始将规则应用于结果。如果未指定值，则默认值为 `ENABLED`。值为 `DISABLED` 表示规则在创建后暂停。
6. 对于 `Criteria` 参数，请提供您希望 Security Hub 用来筛选调查发现的条件。规则操作将适用于符合条件的调查发现。有关支持的标准的列表，请参阅 可用的规则条件和规则操作。
7. 对于 `Actions` 参数，请提供您希望 Security Hub 在调查发现与您定义的条件相匹配时采取的操作。有关受支持操作的列表，请参阅 可用的规则条件和规则操作。

API 请求示例：

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
```

```
            },
            "Note": {
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
    },
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. 从 Security Hub 管理员账户运行 `create-automation-rule` 命令。此命令创建具有特定 Amazon 资源名称（ARN）的规则。
2. 提供规则的名称和描述。

3. 如果您希望此规则成为应用于符合规则条件调查发现的最后一条规则，请包括 `is-terminal` 参数。否则，请包含 `no-is-terminal` 参数。
4. 对于 `rule-order` 参数，请提供规则的顺序。Security Hub 首先对该参数应用数值较小的规则。
5. 对于 `rule-status` 参数，请指定是否希望 Security Hub 启用该规则，并在创建后开始将规则应用于结果。如果未指定值，则默认值为 `ENABLED`。值为 `DISABLED` 表示规则在创建后暂停。
6. 对于 `criteria` 参数，请提供您希望 Security Hub 用来筛选调查发现的条件。规则操作将适用于符合条件的调查发现。有关支持的标准的列表，请参阅 可用的规则条件和规则操作。
7. 对于 `actions` 参数，请提供您希望 Security Hub 在调查发现与您定义的条件相匹配时采取的操作。有关受支持操作的列表，请参阅 可用的规则条件和规则操作。

命令示例：

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

查看自动化规则

选择您的首选方法，然后按照步骤查看您的自动化规则和每条规则的详细信息。

Console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   登录 Security Hub 管理员账户。
2. 在导航窗格中，选择 自动化。
3. 选择规则名称。或者，选择一条规则。
4. 选择操作和视图。

API

1. 要查看您账户的自动化规则，请从 Security Hub 管理员账户运行 `ListAutomationRules`。此 API 会为您的规则返回规则 ARN 和其他元数据。此 API 不需要输入参数，但您可以选择提供 `MaxResults` 以限制结果数量和 `NextToken` 作为分页参数。`NextToken` 的初始值应为 `NULL`。

   API 请求示例：

   ```
   {
    "MaxResults": 50,
    "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
   }
   ```
2. 有关其他规则详细信息，包括规则的条件和操作，请从 Security Hub 管理员账户中运行 `BatchGetAutomationRules`。

   API 请求示例：

   ```
   {
       "AutomationRulesArns": [
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   ```

```
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. 要查看您账户的自动化规则，请从 Security Hub 管理员账户运行 `list-automation-rules` 命令。此命令返回规则 ARN 和规则的其他元数据。此命令不需要输入参数，但您可以选择提供 `max-results` 以限制结果数量和 `next-token` 作为分页参数。

   命令示例：

   ```
   aws securityhub list-automation-rules  \
   --max-results 5 \
   --next-token cVpdnSampleTokenYcXgTockBW44c \
   --region us-east-1
   ```

2. 有关其他规则详细信息，包括规则的标准和操作，请从 Security Hub 管理员账户运行 `batch-get-automation-rules` 命令。

   命令示例：

   ```
   aws securityhub batch-get-automation-rules \
   --automation-rules-arns '["arn:aws:securityhub:us-
   east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
   cdef-EXAMPLE22222"]' \
   --region us-east-1
   ```

编辑自动化规则

当您编辑自动化规则时，更改将应用于规则编辑后 Security Hub 生成或提取的新增的或更新后的调查发现。

选择您的首选方式，按照步骤编辑自动化规则的内容。您只需一个请求即可编辑一条或多条规则。有关编辑规则顺序的说明，请参阅 编辑规则顺序。

Console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   登录 Security Hub 管理员账户。
2. 在导航窗格中，选择 自动化。
3. 选择您要编辑的规则。选择操作和编辑。
4. 根据需要更改规则，然后选择保存更改。

API

1. 从 Security Hub 管理员账户运行 `BatchUpdateAutomationRules`。
2. 对于 `RuleArn` 参数，请提供要编辑的规则的 ARN。
3. 为要编辑的参数提供新值。除 `RuleArn` 之外，您可以编辑任何参数。

API 请求示例：

```
{
    "UpdateAutomationRulesRequestItems": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. 从 Security Hub 管理员账户运行 `batch-update-automation-rules` 命令。
2. 对于 `RuleArn` 参数，请提供要编辑的规则的 ARN。
3. 为要编辑的参数提供新值。除 `RuleArn` 之外，您可以编辑任何参数。

命令示例：

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

编辑规则顺序

在某些情况下，您可能希望保持规则条件和操作不变，但要更改 Security Hub 应用自动化规则的顺序。选择您喜欢的方法，然后按照步骤编辑规则顺序。

Console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   登录 Security Hub 管理员账户。
2. 在导航窗格中，选择 自动化。

3. 选择要更改其顺序的规则。选择编辑优先级。
4. 选择向上移动可将规则的优先级提高一个单位。选择下移可将规则优先级降低一个单位。选择移至顶部，将规则的顺序分配为 1（这使规则优先于其他现有规则）。

> **Note**
>
> 在 Security Hub 控制台中创建规则时，Security Hub 会根据规则的创建顺序自动分配规则顺序。最近创建的规则具有最低的规则顺序数值，因此首先适用。

API

1. 从 Security Hub 管理员账户运行 `BatchUpdateAutomationRules`。
2. 对于 `RuleArn` 参数，请提供要编辑其顺序的规则的 ARN。
3. 修改 `RuleOrder` 字段的值。

> **Note**
>
> 如果多个规则具有相同的 `RuleOrder`，Security Hub 会先为该 `UpdatedAt` 字段应用具有较早值的规则（也就是说，最后应用最近编辑的规则）。

AWS CLI

1. 从 Security Hub 管理员账户运行 `batch-update-automation-rules` 命令。
2. 对于 `RuleArn` 参数，请提供要编辑其顺序的规则的 ARN。
3. 修改 `RuleOrder` 字段的值。

> **Note**
>
> 如果多个规则具有相同的 `RuleOrder`，Security Hub 会先为该 `UpdatedAt` 字段应用具有较早值的规则（也就是说，最后应用最近编辑的规则）。

删除自动化规则

当您删除自动化规则时，Security Hub 会将其从您的账户中删除，并且不再将该规则应用于调查发现。

选择您的首选方法，然后按照步骤删除自动化规则。您可以在单个请求中删除一个或多个规则。

> **Tip**
>
> 除了删除之外，您还可以禁用规则。这会保留该规则以备将来使用，但是在您启用该规则之前，Security Hub 不会将该规则应用于任何匹配的调查发现。

Console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   登录 Security Hub 管理员账户。
2. 在导航窗格中，选择 自动化。
3. 选择您要删除的规则。选择操作和删除（要保留规则，但暂时将其禁用，请选择禁用）。
4. 确认您的选择，然后选择删除。

API

1. 从 Security Hub 管理员账户运行 `BatchDeleteAutomationRules`。
2. 对于 `AutomationRulesArns` 参数，请提供要删除的规则的 ARN（要保留规则，但暂时将其禁用，请提供 `RuleStatus` 参数的 `DISABLED`）。

   API 请求示例：

```
{
    "AutomationRulesArns": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
```

```
    ]
}
```

AWS CLI

1. 从 Security Hub 管理员账户运行 batch-delete-automation-rules 命令。
2. 对于 automation-rules-arns 参数，请提供要删除的规则的 ARN（要保留规则，但暂时将其禁用，请提供 RuleStatus 参数的 DISABLED）。

命令示例：

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

自动化规则示例

本节包括常见用例的一些自动化规则示例。这些示例与 Security Hub 控制台中的规则模板相对应。

当特定资源（例如 S3 存储桶）面临风险时，将严重性提升为“严重”

在本示例中，当 ResourceId 在调查发现中的对象是特定的 Amazon Simple Storage Service（Amazon S3）存储桶时，匹配规则条件。规则操作是将匹配调查发现的严重性更改为 CRITICAL。您可以修改此模板以应用于其他资源。

API 请求示例：

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
```

```
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

示例 CLI 命令：

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
```

```
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

提高与生产账户中资源相关调查发现的严重性

在此示例中，当在特定的生产账户中生成 HIGH 严重级别的调查发现时，匹配规则条件。规则操作是将匹配调查发现的严重性更改为 CRITICAL。

API 请求示例：

```
{
```

```
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
```

```
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

示例 CLI 命令：

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
```

```
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

隐藏信息性结果

在此示例中，与从亚马逊发送到 Security Hub 的INFORMATIONAL严重性调查结果的规则标准相匹配 GuardDuty。规则操作是将匹配调查发现的工作流程状态更改为 SUPPRESSED。

API 请求示例：

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
```

```
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

示例 CLI 命令：

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
```

```
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

自动响应和补救

借助 Amazon EventBridge，您可以自动化您的 AWS 服务，以自动响应系统事件，例如应用程序可用性问题或资源更改。来自 AWS 服务的事件会近乎实时且有保证地传送到 EventBridge。您可以编写简单的规则来指示您对哪些事件感兴趣，以及当事件与规则匹配时要采取哪些自动操作。可自动触发的操作包括：

- 调用 AWS Lambda 函数
- 调用 Amazon EC2 运行命令
- 将事件中继到 Amazon Kinesis Data Streams
- 激活 AWS Step Functions 状态机
- 通知 Amazon SNS 主题或 Amazon SQS 队列
- 将结果发送到第三方票证、聊天、SIEM 或事件响应和管理工具

Security Hub 自动将所有新发现以及现有发现的所有更新作为 EventBridge 事件发送到 EventBridge。您还可以创建自定义操作，以便将选定的发现和见解结果发送到 EventBridge。

然后，您可以配置 EventBridge 规则来响应每种类型的事件。

有关使用 EventBridge 的更多信息，请参阅 Amazon EventBridge 用户指南。

> **Note**
>
> 作为最佳实践，请确保授予用户访问 EventBridge 的权限使用仅授予所需权限的最低权限 IAM policy。
> 有关更多信息，请参阅 Amazon EventBridge 中的身份和访问管理。

AWS 解决方案中还提供了一组用于跨账户自动响应和补救的模板。这些模板利用了 EventBridge 事件规则和 Lambda 函数。您可以使用 AWS CloudFormation 和 AWS Systems Manager 部署解决方案。该解决方案可以创建完全自动化的响应和补救措施操作。它还可以使用 Security Hub 自定义操作来创建用户触发的响应和补救措施操作。有关如何配置和使用解决方案的详细信息，请参阅 AWS 解决方案页面上的自动安全响应。

主题

Security Hub 与 EventBridge 集成的类型

Security Hub 使用以下 EventBridge 事件类型来支持以下与 EventBridge 的集成类型。

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

所有结果（Security Hub Findings - Imported）

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

每个 `BatchImportFindings` 和 `BatchUpdateFindings` 请求都会触发一个 Security Hub Findings - Imported 事件。

对于管理员账号，EventBridge 中的事件源包括其账号和成员账号中调查发现的事件。

在聚合区域中，事件源包括来自聚合区域和关联区域的调查发现的事件。跨区域调查发现几乎实时地包含在事件源中。有关如何配置调查发现聚合的信息，请参阅 跨区域聚合。

您可以在 EventBridge 中定义规则，自动将结果路由到 Amazon S3 存储桶、补救工作流程或第三方工具。这些规则可以包括筛选条件，使仅在调查发现具有特定属性值时才应用规则。

您可以使用此方法自动将所有结果或具有特定特征的所有结果发送到响应或补救工作流程。

请参阅the section called “配置自动发送调查发现的规则”。

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调查发现作为 Security Hub Findings - Custom Action 事件发送到 EventBridge。

这对于使用 Security Hub 控制台的分析师非常有用（他们需要将特定调查发现或一小组调查发现发送到响应或修复工作流程）。您可以每次为最多 20 个结果选择自定义操作。每项调查发现都作为单独的 EventBridge 事件发送到 EventBridge。

创建自定义操作时，您可以为其分配一个自定义操作 ID。您可以使用此 ID 创建一条 EventBridge 规则，该规则在收到与该自定义操作 ID 关联的调查发现后执行指定操作。

请参阅the section called “配置和使用自定义操作”。

例如，您可以在 Security Hub 中创建一个名为 `send_to_ticketing` 的自定义操作。然后，您在 EventBridge 中创建一个规则，将在 EventBridge 收到包含 `send_to_ticketing` 自定义操作 ID 的调查发现时触发该规则。该规则包括将结果发送到票证系统的逻辑。然后，您可以在 Security Hub 中选择结果，并在 Security Hub 中使用自定义操作将结果手动发送到票证系统。

有关如何将 Security Hub 调查发现发送给 EventBridge 进行进一步处理的示例，请参阅AWS合作伙伴网络 (APN) 博客上的如何将 AWS Security Hub 自定义操作与 PagerDuty 集成以及如何启用 AWS Security Hub 中的自定义操作。

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集作为 Security Hub Insight Results 事件发送到 EventBridge。洞察结果是与洞察相匹配的资源。请注意，当您将见解结果发送到 EventBridge 时，您并未将结果发送到 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。

与调查发现的自定义操作类似，您首先在 Security Hub 中创建自定义操作，然后在 EventBridge 中创建规则。

请参阅the section called “配置和使用自定义操作”。

例如，假设你看到了一个你感兴趣的特定洞察结果，想与同事分享。在这种情况下，您可以使用自定义操作通过聊天或票务系统将洞察结果发送给同事。

Security Hub 的 EventBridge 事件格式

Security Hub Findings - Imported、Security Findings - Custom Action 和 Security Hub Insight Results 事件类型使用以下事件格式。

事件格式是 Security Hub 向 EventBridge 发送事件时使用的格式。

Security Hub Findings - Imported

Security Hub Findings - Imported 从 Security Hub 发送到 EventBridge 的事件使用以下格式。

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

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

有关调查发现属性的完整列表，请参阅 AWS 安全调查结果格式 (ASFF)。

有关如何配置由这些事件触发的 EventBridge 规则的信息，请参阅 the section called “配置自动发送调查发现的规则”。

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action 从 Security Hub 发送到 EventBridge 的事件使用以下格式。每项调查发现均在单独的事件中发送。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

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

有关调查发现属性的完整列表，请参阅 AWS 安全调查结果格式 (ASFF)。

有关如何配置由这些事件触发的 EventBridge 规则的信息，请参阅 the section called “配置和使用自定义操作”。

Security Hub Insight Results

Security Hub Insight Results 从 Security Hub 发送到 EventBridge 的事件使用以下格式。

```
{
  "version": "0",
```

```
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

有关如何创建由这些事件触发的 EventBridge 规则的信息，请参阅 the section called “配置和使用自定义操作”。

配置 EventBridge 规则以自动发送调查发现

您可以在 EventBridge 中创建规则，该规则定义在收到 Security Hub Findings - Imported 事件时要采取的操作。Security Hub Findings - Imported 事件由 `BatchImportFindings` 和 `BatchUpdateFindings` 的更新触发。

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

然后，该规则确定了规则目标。目标是 EventBridge 收到 Security Hub 结果 - 已导入 事件并且调查发现与筛选条件匹配时要采取的操作。

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

您还可以使用 EventBridge API 的 PutRule API 操作。但是，如果您使用 EventBridge API，则必须创建基于资源的策略。有关所需策略的详细信息，请参阅《Amazon EventBridge 用户指南》中的 CloudWatch Logs 日志权限。

事件模式的格式

Security Hub 结果 - 已导入事件的事件模式格式如下：

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

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

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

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

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

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

当您提供属性值时，它必须反映该属性在 AWS 安全调查发现格式 (ASFF) 结构中的位置。

> **Tip**
>
> 筛选控件调查发现时，我们建议使用 SecurityControlId 或 SecurityControlArn ASFF 字段作为筛选条件，而不是 Title 或 Description。后面的字段偶尔会发生变化，而控件 ID 和 ARN 是静态标识符。

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

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

创建事件规则

您可以使用预定义的事件模式或自定义的事件模式在 EventBridge 中创建规则。如果您选择预定义的模式，EventBridge 会自动填充 source 和 detail-type。EventBridge 还提供了用于为以下调查发现属性指定筛选值的字段：

- AwsAccountId
- Compliance.Status
- Criticality
- ProductArn
- RecordState
- ResourceId

- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

创建 EventBridge 规则

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

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

使用...构建事件模式	请执行此操作...

性筛选结果，请使用自定义模式。）	<pre>{
	  "source": [
	  "aws.secu
	rityhub"
	  ],
	  "detail-type": [
	  "Security
	 Hub Findings -
	 Imported"
	  ],
	  "detail": {
	  "findings": {
	  "<attribut
	e name> ":
	 ["<value1>",
	 "<value2>"]
	  }
	  }
	}</pre>
	• 更新事件模式以包含要用作筛选器的属性和属性值。
	
	例如，要将规则应用于验证状态为 TRUE_POSITIVE 的调查发现，请使用以下模式示例：
	
	<pre>{
	  "source": [
	  "aws.secu
	rityhub"
	  ],
	  "detail-type": [
	  "Security
	 Hub Findings -
	 Imported"
	  ],</pre>

使用...构建事件模式	请执行此操作...

	<pre>"detail": {
	"findings": {
	"Verifica
	tionState":
	["TRUE_POSITIVE"]
	}
	}
	}</pre>

- 对于目标类型，选择 AWS 服务，对于选择目标，选择一个目标，例如 Amazon SNS 主题或 AWS Lambda 函数。在收到与规则中定义的事件模式匹配的事件时将触发目标。

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

使用自定义操作将调查发现和洞察结果发送到 EventBridge

要使用 Security Hub 自定义操作将调查发现或洞察结果发送到 EventBridge，您需要先在 Security Hub 中创建自定义操作。然后，在 EventBridge 中定义适用于您的自定义操作的规则。

您最多可以创建 50 个自定义操作。

如果您启用了跨区域聚合并在聚合区域管理结果，则须在聚合区域中创建自定义操作。

EventBridge 中的规则使用自定义操作中的 ARN。

创建自定义操作（控制台）

当您创建自定义操作时，您指定名称、描述和唯一标识符。

要在 Security Hub（控制台）中创建自定义操作

1. 通过以下网址打开AWS 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。

每个 AWS 账户的自定义操作 ID 必须是唯一的。

5. 选择 Create custom action (创建自定义操作)。
6. 记下自定义操作 ARN。在 EventBridge 中创建与此操作关联的规则时，您需要使用 ARN。

创建自定义操作 (Security Hub API, AWS CLI)

要创建自定义操作，您可以使用 API 调用或 AWS Command Line Interface。

要创建自定义操作 (Security Hub API, AWS CLI)

- Security Hub API – 使用该 `CreateActionTarget` 操作。创建自定义操作时，您需要提供名称、描述和自定义操作标识符。
- AWS CLI – 在命令行中，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 EventBridge 中定义规则

要处理自定义操作，您必须在 EventBridge 中创建相应的规则。规则定义包括自定义操作的 ARN。

Security Hub 结果 - 自定义操作事件的事件模式采用以下格式：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
```

```
}
```

Security Hub 洞察结果事件的事件模式采用以下格式：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

在这两种模式中，*<custom action ARN>* 都是自定义操作的 ARN。您可以配置适用于多个自定义操作的规则。

此处提供的说明适用于 EventBridge 控制台。当您使用控制台时，EventBridge 会自动创建所需的基于资源的策略，使 EventBridge 能够写入 CloudWatch Logs 日志。

您还可以使用 EventBridge API 的 `PutRule` API 操作。但是，如果您使用 EventBridge API，则必须创建基于资源的策略。有关所需策略的详细信息，请参阅《Amazon EventBridge 用户指南》中的 CloudWatch Logs 日志权限。

要在 EventBridge 中定义规则

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。
5. 对于事件总线，请选择要与此规则关联的事件总线。如果您希望此规则对来自您自己的账户的匹配事件触发，请选择默认。当您账户中的某个 AWS 服务发出一个事件时，它始终会发送到您账户的默认事件总线。
6. 对于规则类型，选择具有事件模式的规则。
7. 选择下一步。
8. 对于事件源，选择 AWS 事件。
9. 对于事件模式，选择事件模式表。
10. 对于事件源，选择AWS 服务。

11. 要获得 AWS 服务，请选择 Security Hub。
12. 对于 Event type (事件类型)，执行以下操作之一：
    - 要创建在将结果发送到自定义操作时要应用的规则，请选择 Security Hub 结果 - 自定义操作。
    - 要创建在向自定义操作发送洞察结果时要应用的规则，请选择 Security Hub 洞察结果。
13. 选择特定自定义操作 ARN，添加自定义操作 ARN。

    如果该规则适用于多个自定义操作，请选择添加以添加更多自定义操作 ARN。
14. 选择下一步。
15. 在选择目标下，选择并配置匹配此规则时要调用的目标。
16. 选择下一步。
17. （可选）为规则输入一个或多个标签。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 标签。
18. 选择下一步。
19. 查看规则详细信息并选择创建规则。

    当您对账户中的发现或见解结果执行自定义操作时，EventBridge 中会生成事件。

为调查发现和洞察结果选择自定义操作

创建 Security Hub 自定义操作和 EventBridge 规则后，您可以将调查发现和见解结果发送到 EventBridge 以进行进一步管理和处理。

事件仅在它们被查看的账户中发送到 EventBridge。如果您使用管理员账户查看调查发现，则该事件将以管理员账户发送到 EventBridge。

要使 AWS API 调用生效，目标代码的实现必须将角色切换到成员账户。这也意味着您切换到的角色必须部署到需要采取行动的每个成员。

将调查发现发送到 EventBridge

1. 通过以下网址打开AWS Security Hub控制台：https://console.aws.amazon.com/securityhub/。
2. 显示调查发现列表：
    - 在调查发现中，您可以查看所有已启用的产品集成和控件的调查发现。
    - 从安全标准中，您可以导航到从选定控件生成的调查发现列表。请参阅the section called “查看控件的详细信息”。

- 从集成中，您可以导航到已启用的集成生成的调查发现列表。请参阅the section called “查看来自集成的结果”。
- 从见解中，您可以导航到见解结果的调查发现列表。请参阅the section called “查看见解结果和调查结果”。

3. 选择要发送到 EventBridge 的调查发现。您一次最多可选择 20 个结果。
4. 从操作中，选择与要应用的 EventBridge 规则一致的自定义操作。

   Security Hub 会为每个调查发现单独发送一个 Security Hub 调查发现 - 自定义操作事件。

将洞察结果发送到 EventBridge

1. 通过以下网址打开AWS Security Hub控制台：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Insights。
3. 在见解页面上，选择包含要发送到 EventBridge 的结果的见解。
4. 选择要发送到 EventBridge 的洞察结果。您一次最多可以选择 20 个结果。
5. 从操作中，选择与要应用的 EventBridge 规则一致的自定义操作。

AWS Security Hub 中的产品集成

AWS Security Hub 可以聚合来自多个 AWS 服务和受支持的 AWS 合作伙伴网络 (APN) 安全解决方案的安全调查发现数据。聚合提供了整个 AWS 环境的安全性和合规性的全面视图。

您还可以发送从您自己的自定义安全产品生成的结果。

> **Important**
>
> 从支持的 AWS 和合作伙伴产品集成中，Security Hub 仅接收并合并您在 AWS 账户 账户中启用 Security Hub 后生成的调查发现。
> 服务不会以追溯方式接收和合并在启用 Security Hub 前生成的安全调查发现。

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

中的集成页面 AWS Management Console 提供对所有可用 AWS 和第三方产品集成的访问权限。S AWS ecurity Hub API 还提供了允许您管理集成的操作。

> **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，则不会在集成页面上列出该集成。
> 另请参阅 the section called “中国（北京）和中国（宁夏）区域支持的集成” 和 the section called “AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）支持的集成”。

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 S AWS ecurity Hub 控制台，网址为 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 AWS 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

您可以从以下字段中输入文本来筛选列表。

- 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， AWS CLI）

要查看有关产品集成的信息，您可以使用“API 调用”或 AWS Command Line Interface。您可以显示有关所有产品集成的信息，也可以显示有关您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, AWS CLI)

- Security Hub API – 使用该 `DescribeProducts` 操作。要确定要返回的特定产品集成，请使用 `ProductArn` 参数提供集成 ARN。

- AWS 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, AWS CLI)

- Security Hub API – 使用该 ListEnabledProductsForImport 操作。
- AWS 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 AWS 服务的大多数集成，唯一需要的步骤就是启用其他服务。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调查发现。

对于第三方产品集成，您可能需要从购买集成 AWS Marketplace，然后配置集成。集成信息提供了用于执行这些任务的链接。

如果产品有多个版本可用 AWS Marketplace，请选择要订阅的版本，然后选择 “继续订阅”。例如，有些产品提供标准版本和 AWS GovCloud (US) 版本。

启用产品集成时，将向该产品订阅自动附加资源策略。该资源策略定义 Security Hub 从该产品接收调查发现所需的权限。

禁用和启用来自集成的结果流（控制台）

在集成页面上，对于发送调查发现的集成，状态信息指示您当前是否正在接受调查发现。

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)。

禁用集成的结果流（Security Hub API， AWS CLI）

要禁用来自集成的调查发现流，您可以使用“API 调用”或 AWS Command Line Interface。

禁用集成的结果流（Security Hub API， AWS CLI）

- Security Hub API – 使用该 DisableImportFindingsForProduct 操作。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 操作。
- AWS 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"
```

启用集成（Security Hub API， AWS CLI）中的发现流

要启用来自集成的调查发现流，您可以使用“API 调用”或 AWS Command Line Interface。

启用集成（Security Hub API， AWS CLI）中发现的结果流

- Security Hub API – 使用该 EnableImportFindingsForProduct 操作。要允许 Security Hub 接收来自集成的调查发现，您需要产品 ARN。要获取可用集成的 ARN，请使用 DescribeProducts 操作。
- AWS 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

对于您接受其调查发现的集成（状态为正在接受调查发现），要查看调查发现列表，请选择查看调查发现。

结果列表显示了工作流程状态为 NEW 或 NOTIFIED 的所选集成的活动结果。

如果您启用跨区域聚合，则在聚合区域中，列表将包括来自聚合区域和启用集成的关联区域的调查发现。Security Hub 不会根据跨区域聚合配置自动启用集成。

在其他区域，集成的查找调查发现列表仅包含来自当前区域的调查发现。

有关如何配置跨区域聚合的信息，请参阅 跨区域聚合。

从调查结果列表中，您可以执行以下操作。

- 更改列表的筛选条件和分组
- 查看单个结果的详细信息
- 更新调查发现的工作流程状态
- 将结果发送到自定义操作

AWS 服务 与 Sec AWS urity Hub 的集成

AWS Security Hub 支持与其他 AWS 服务几个集成。

> **Note**
>
> 某些集成仅在精选 AWS 区域版本中可用。
> 如果特定区域不支持某个集成，则该集成不会在 Security Hub 控制台的集成页面上列出。
> 有关更多信息，请参阅 中国（北京）和中国（宁夏）区域支持的集成 和 AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）支持的集成。

除非下文另有说明，否则在您启 AWS 服务 用 Security Hub 后，将自动激活将发现结果发送到 Security Hub 的集成。接收 Security Hub 调查发现的集成可能需要额外的激活步骤。查看有关每个集成的信息以了解更多信息。

与 Security Hub 的 AWS 服务集成概述

以下是将调查结果发送到 Security Hub 或从 Security Hub 接收发现结果的 AWS 服务的概述。

综合 AWS 服务	方向
AWS Config	发送调查发现
AWS Firewall Manager	发送调查发现
Amazon GuardDuty	发送调查发现
AWS Health	发送调查发现
AWS Identity and Access Management Access Analyzer	发送调查发现
Amazon Inspector	发送调查发现
AWS IoT Device Defender	发送调查发现
Amazon Macie	发送调查发现
AWS Systems Manager Patch Manager	发送调查发现
AWS Audit Manager	接收调查发现
AWS Chatbot	接收调查发现
Amazon Detective	接收调查发现
Amazon Security Lake	接收调查发现
AWS Systems Manager 探险家和 OpsCenter	接收和更新调查发现

综合 AWS 服务	方向	
AWS Trusted Advisor	接收调查发现	

AWS 将调查结果发送到 Security Hub 的服务

通过向 Security Hub 发送调查结果，以下 AWS 服务与 Security Hub 集成。Security Hub 将调查发现转换为 AWS 安全调查发现格式。

AWS Config （发送调查结果）

AWS Config 是一项允许您评估、审核和评估 AWS 资源配置的服务。 AWS Config 持续监控和记录您的 AWS 资源配置，并允许您根据所需的配置自动评估记录的配置。

通过与集成 AWS Config，您可以在 Security Hub 中将 AWS Config 托管和自定义规则评估的结果作为发现结果进行查看。这些结果可以与 Security Hub 的其他发现一起查看，提供您的安全态势的全面概述。

AWS Config 使用亚马逊 EventBridge 向 Security Hub 发送 AWS Config 规则评估。Security Hub 将规则评估转换成遵循 AWS 安全调查发现格式的调查发现。然后，Security Hub 通过获取有关受影响资源的更多信息（例如 Amazon 资源名称（ARN）和创建日期），尽最大努力丰富调查发现。 AWS Config 规则评估中的资源标签不包含在 Security Hub 的调查结果中。

有关此集成的更多信息，请参阅以下部分：

如何 AWS Config 将调查结果发送到 Security Hub

Security Hub 中的所有调查发现都使用 ASFF 的标准 JSON 格式。ASFF 包括有关发现的来源、受影响的资源以及发现的当前状态的详细信息。 AWS Config 通过向 Security Hub 发送托管和自定义规则评估 EventBridge。Security Hub 将规则评估转化为遵循 ASFF 的调查发现，并尽最大努力丰富调查发现。

AWS Config 发送到 Security Hub 的发现类型

激活集成后， AWS Config 会向 Security Hub 发送所有 AWS Config 托管规则和自定义规则的评估结果。仅排除来自服务相关 AWS Config 规则的评估，例如用于对安全控制进行检查的评估。

将 AWS Config 调查结果发送到 Security Hub

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 AWS Config。Security Hub 使用 service-to-service 级别权限，为您提供一种安全的方式来激活此集成并 AWS Config 通过亚马逊导入调查结果 EventBridge。

发送调查发现的延迟

AWS Config 创建新发现时，您通常可以在五分钟内在 Security Hub 中查看该发现。

Security Hub 不可用时重试

AWS Config 尽最大努力将调查结果发送到 Security Hub。 EventBridge如果事件未成功传送到 Security Hub， EventBridge则会重试投递最多 24 小时或 185 次，以先到者为准。

更新 Security Hub 中的现有 AWS Config 发现

将调查结果 AWS Config 发送到 Security Hub 后，它可以向 Security Hub 发送同一发现的更新，以反映对发现活动的其他观察结果。仅针对 `ComplianceChangeNotification` 事件发送更新。如果没有发生合规性变化，则不会向 Security Hub 发送更新。Security Hub 会在最近一次更新后的 90 天或（如果没有更新）创建后的 90 天删除结果。

AWS Config 即使您删除了关联的资源，Security Hub 也不会存档从中发送的结果。

存在 AWS Config 调查结果的地区

AWS Config 调查结果以区域为基础出现。 AWS Config 将发现结果发送到发现结果所在的一个或多个区域的 Security Hub。

在 Security Hub 中查看 AWS Config 调查结果

要查看您的 AWS 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 AWS Config 结果，请在搜索栏下拉列表中选择产品名称。输入Config，然后选择应用。

解释在 Security Hub 中 AWS Config 查找的名字

Security Hub 将 AWS Config 规则评估转化为遵循的AWS 安全调查结果格式 (ASFF)结果。 AWS Config 与 ASFF 相比，规则评估使用不同的事件模式。下表将 AWS Config 规则评估字段映射到它们在 Security Hub 中显示的 ASFF 对应字段。

Config 规则评估调查发现类型	ASFF 结果类型	硬编码值
细节。 awsAccountId	AwsAccountId	

Config 规则评估调查发现类型	ASFF 结果类型	硬编码值
细节。 newEvaluationResult。resultRecordedTime	CreatedAt	
细节。 newEvaluationResult。resultRecordedTime	UpdatedAt	
	ProductArn	"arn:<partition>:securityhub:<region>::product/aws/config"
	ProductName	"Config"
	CompanyName	"AWS"
	区域	"eu-central-1"
configRuleArn	GeneratorId, ProductFields	
细节。 ConfigRuleARN/Finding/Hash	Id	
细节。 configRuleName	标题 ， ProductFields	
细节。 configRuleName	描述	“此调查发现是针对配置规则的资源合规性更改而创建的：${detail.ConfigRuleName} ”
配置项目“ARN”或 Security Hub 计算的 ARN	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	"eu-central-1"
配置项目“配置”	Resources[i].Details	

Config 规则评估调查发现类型	ASFF 结果类型	硬编码值
	SchemaVersion	"2018-10-08"
	Severity.Label	请参阅下面的“解释严重性标签”
	类型	[“软件和配置检查”]
细节。 newEvaluationResult. 合规类型	Compliance.Status	"FAILED", "NOT_AVAILABLE", "PASSED", or "WARNING"
	Workflow.Status	如果生成的 “合规性” 状态为 “已通过”，或者合规状态从 “失败” 变为 “已通过”，则为 “已解决”。 AWS Config 否则，Workflow.Status 将为“NEW”。您可以通过 BatchUpdateFindingsAPI 操作更改此值。

解释严重性标签

AWS Config 规则评估的所有发现在 ASFF 中都有一个默认的严重性标签为 MEDIUM。您可以通过 `BatchUpdateFindings` API 操作更新调查发现的严重性标签。

来自的典型发现 AWS Config

Security Hub 将 AWS Config 规则评估转化为遵循 ASFF 的调查结果。以下是ASFF中典型发现 AWS Config 的示例。

> **Note**
>
> 如果描述超过 1024 个字符，则它将被截断至 1024 个字符，并在结尾处显示“（截断）”。

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

```
 "Id": "arn:aws: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": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
```

```
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

启用和配置集成

启用 Security Hub 后，此集成将自动激活。 AWS Config 立即开始向 Security Hub 发送调查结果。

停止向 Security Hub 发布调查发现

要停止向 Security Hub 发送调查发现,可以使用 Security Hub 控制台、Security Hub API 或 AWS CLI。

请参阅 禁用和启用来自集成的结果流（控制台） 或 禁用集成的结果流（Security Hub API， AWS CLI）。

AWS Firewall Manager（发送调查结果）

当 web application firewall (WAF) 策略或 Web 访问控制列表 (Web ACL) 规则不合规时，Firewall Manager 将调查发现发送到 Security Hub。F AWS Shield Advanced irewall Manager 还会在未保护资源或发现攻击时发送调查结果。

启用 Security Hub 后，此集成将自动激活。Firewall Manager 会立即开始向 Security Hub 发送调查发现。

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 的更多信息，请参阅 AWS WAF 开发人员指南。

亚马逊 GuardDuty （发送调查结果）

GuardDuty 将其生成的所有发现结果发送到 Security Hub。

来自 GuardDuty 的新发现将在五分钟内发送到 Security Hub。调查结果的更新是根据设置 EventBridge 中亚马逊的 “更新调查结果 GuardDuty ” 设置发送的。

当您使用 GuardDuty “设置” 页面生成 GuardDuty 示例查找结果时，Security Hub 会接收样本查找结果并省略查找结果类型`[Sample]`中的前缀。例如，中的样本查找结果类型显示 GuardDuty `[SAMPLE]` `Recon:IAMUser/ResourcePermissions`为 Securit `Recon:IAMUser/ResourcePermissions` y Hub。

启用 Security Hub 后，此集成将自动激活。 GuardDuty 立即开始向 Security Hub 发送调查结果。

有关 GuardDuty 集成的更多信息，请参阅《亚马逊 GuardDuty 用户指南》中的与 Sec AWS urity Hub 集成。

AWS Health （发送调查结果）

AWS Health 提供对您的资源性能以及 AWS 服务和账户可用性的持续可见性。您可以使用 AWS Health 事件来了解服务和资源更改会如何影响正在 AWS运行的应用程序。

与的集成 AWS Health 不起作用`BatchImportFindings`。而是 AWS Health 使用 service-to-service 事件消息将发现结果发送到 Security Hub。

有关此集成的更多信息，请参阅以下部分：

如何 AWS Health 将调查结果发送到 Security Hub

在 Security Hub 中，安全问题按调查结果进行跟踪。一些发现来自其他 AWS 服务或第三方合作伙伴检测到的问题。Security Hub 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 管理和查看查找结果的详细信息和历史记录。您还可以跟踪调查发现的调查状态。请参阅 对调查结果采取行动 AWS Security Hub。

Security Hub 中的所有结果都使用标准的 JSON 格式，称为 AWS 安全调查结果格式 (ASFF)。ASFF 包括有关问题根源、受影响资源以及调查发现当前状态的详细信息。

AWS Health 是将发现结果发送到 Security Hub 的 AWS 服务之一。

AWS Health 发送到 Security Hub 的发现类型

启用集成后， AWS Health 会将其生成的所有与安全相关的结果发送到 Security Hub。使用 AWS 安全调查结果格式 (ASFF) 将调查发现发送到 Security Hub。与安全相关的调查发现定义如下：

- 任何与 AWS 安全服务相关的发现
- 任何在 AWS Health T ypeCode `certificate` 中带有`securityabuse`、或字样的搜索结果
- 发现 AWS Health 服务在哪里，`risk`或 `abuse`

将 AWS Health 调查结果发送到 Security Hub

当您选择接受来自的调查结果时 AWS Health，Security Hub 将自动分配从中接收调查结果所需的权限 AWS Health。Security Hub 使用 service-to-service 级别权限，为您提供一种安全、简便的方法来启用此集成并 EventBridge 代表您 AWS 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 使用其中的查找结果的权限 AWS Health。

发送调查发现的延迟

AWS Health 创建新发现时，通常会在五分钟内将其发送到 Security Hub。

Security Hub 不可用时重试

AWS Health 尽最大努力将调查结果发送到 Security Hub。 EventBridge如果事件未成功传送到 Security Hub， EventBridge则会在 24 小时内重试发送该事件。

更新 Security Hub 中的现有 结果

将调查结果 AWS Health 发送到 Security Hub 后，它可以将同一发现的更新发送给 Security Hub，以反映对发现活动的其他观察结果。

存在调查发现的区域

对于全局事件，以 us-east-1（分区）、cn-northwest-1（中国分区）和 -1 AWS （分区） AWS Health 将发现结果发送到 Security Hub。 gov-us-west GovCloud AWS Health 将特定于区域的事件发送到事件发生地相同的一个或多个区域的 Security Hub。

在 Security Hub 中查看 AWS Health 调查结果

要在 Security Hub 中查看您的 AWS Health 发现，请从导航面板中选择调查结果。要筛选结果以仅显示搜索 AWS Health 结果，请从 “产品名称” 字段中选择 “Heal th”。

解释在 Security Hub 中 AWS Health 查找的名字

AWS Health 使用将发现结果发送到 Security Hub AWS 安全调查结果格式 (ASFF)。 AWS 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 AWS Health 查找字段及其在 Security Hub 中显示的 ASFF 对应字段。

健康调查发现类型	ASFF 结果类型	硬编码值
account	AwsAccountId	
detail.startTime	CreatedAt	
detail.eventDescription.latestDescription	描述	
细节。 eventTypeCode	GeneratorId	
detail.eventArn（包括账户）+ detail.startTime 的 hash	Id	
"arn:aws:securityhub:<region>::product/aws/health"	ProductArn	
账户或 resourceId	Resources[i].id	
	Resources[i].Type	“其他”
	SchemaVersion	"2018-10-08"
	Severity.Label	请参阅下面的“解释严重性标签”
“AWS Health -” 详情。eventTypeCode	Title	
-	类型	[“软件和配置检查”]
event.time	UpdatedAt	
Health 控制台上事件的 URL	SourceUrl	

解释严重性标签

ASFF 调查发现中的严重性标签是使用以下逻辑确定的：

- 如果满足以下条件，则严重性为危急。
  - AWS Health 调查结果中的`service`字段具有值 `Risk`
  - AWS Health 调查结果中的`typeCode`字段具有值 `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - AWS Health 调查结果中的`typeCode`字段具有值 `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - AWS Health 调查结果中的`typeCode`字段具有值 `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  严重性为高，如果：
  - AWS Health 调查结果中的`service`字段具有值 `Abuse`
  - AWS Health 调查结果中的`typeCode`字段包含值 `SECURITY_NOTIFICATION`
  - AWS Health 调查结果中的`typeCode`字段包含值 `ABUSE_DETECTION`

  如果满足以下条件，则严重性为中。
  - 调查发现中的 `service` 字段为以下任意字段：`ACM`、`ARTIFACT`、`AUDITMANAGER`、`BACKUP`、`CLOUDENDURE`、`CLOUDHSM`、`CLOUDTRAIL`、`CLOU` 或 `WAF`
  - AWS Health 调查发现中的typeCode字段包含值 `CERTIFICATE`
  - AWS Health 调查发现中的typeCode字段包含值 `END_OF_SUPPORT`

来自的典型发现 AWS Health

AWS Health 使用将发现结果发送到 Security Hub AWS 安全调查结果格式 (ASFF)。以下是来自的典型发现的示例 AWS Health。

> **Note**
>
> 如果描述超过 1024 个字符，则它将被截断至 1024 个字符，并在结尾处显示（截断）。

```
{
```

```
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
```

```
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

启用和配置集成

启用 Security Hub 后，此集成将自动激活。 AWS Health 立即开始向 Security Hub 发送调查结果。

停止向 Security Hub 发布调查发现

要停止向 Security Hub 发送调查结果，你可以使用 Security Hub 控制台、Security Hub API 或 AWS CLI。

请参阅 禁用和启用来自集成的结果流（控制台） 或 禁用集成的结果流（Security Hub API， AWS CLI）。

AWS Identity and Access Management Access Analyzer （发送调查结果）

借助 IAM Access Analyzer，所有结果都会发送到 Security Hub。

IAM Access Analyzer 使用基于逻辑的推理来分析应用于您账户中受支持资源的基于资源的策略。IAM Access Analyzer 在检测到允许外部主体访问您账户中资源的策略语句时生成一个调查发现。

在 IAM Access Analyzer 中，只有管理员账户才能看到适用于组织的分析器的调查发现。对于组织分析器，`AwsAccountId` ASFF 字段反映管理员账户 ID。在 `ProductFields` 下方，`ResourceOwnerAccount` 字段表示调查发现被发现的账户。如果您为每个账户单独启用分析器，Security Hub 会生成多个结果：一个用于标识管理员账户 ID，另一个用于标识资源账户 ID。

有关更多信息，请参阅《IAM 用户指南》中的与 AWS Security Hub 集成。

Amazon Inspector（发送调查发现）

Amazon Inspector 是一项漏洞管理服务，可持续扫描您的 AWS 工作负载中是否存在漏洞。Amazon Inspector 可以自动发现并扫描驻留在 Amazon 弹性容器注册表中的 Amazon EC2 实例和容器映像。扫描会查找软件漏洞和意外网络暴露。

启用 Security Hub 后，此集成将自动激活。Amazon Inspector 立即开始将其生成的所有结果发送到 Security Hub。

有关集成的更多信息，请参阅 Amazon Inspector 用户指南中的与 Sec AWS urity Hub 集成。

Security Hub 还可以接收来自 Amazon Inspector Classic 的调查发现。Amazon Inspector Classic 会把通过评测生成的调查发现发送到 Security Hub，这一评测运行于所有支持的规则包。

有关集成的更多信息，请参阅 Amazon Inspector Classic 用户指南中的与 Sec AWS urity Hub 集成。

Amazon Inspector 和 Amazon Inspector Classic 的调查发现使用相同的产品 ARN。Amazon Inspector 的调查发现在 `ProductFields` 中有以下条目：

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender（发送调查结果）

AWS IoT Device Defender 是一项安全服务，可审核您的物联网设备的配置，监控连接的设备以检测异常行为，并帮助降低安全风险。

同时启用两者 AWS IoT Device Defender 和 Security Hub 后，请访问 Sec urity Hub 控制台的 “集成” 页面，然后选择 “接受审计”、“检测” 或 “两者” 的调查结果。 AWS IoT Device Defender “审计和检测” 开始将所有发现结果发送到 Security Hub。

AWS IoT Device Defender 审计将支票摘要发送到 Security Hub，其中包含特定审计检查类型和审计任务的一般信息。 AWS IoT Device Defender 检测将机器学习 (ML)、统计和静态行为的违规发现发送到 Security Hub。审计还会将调查发现更新发送到 Security Hub。

有关此集成的更多信息，请参阅《AWS IoT 开发者指南》中的 “与 S AWS ecurity Hub 集成”。

Amazon Macie（发送调查发现）

Macie 的调查发现可以指示存在潜在的策略违规，或者组织存储在 Amazon S3 中的数据中存在敏感数据，例如个人身份信息(PII)。

启用 Security Hub 后，Macie 会自动开始向 Security Hub 发送策略调查发现。您可以对集成进行配置，将敏感数据结果也发送到 Security Hub。

在 Security Hub 中，策略或敏感数据调查发现的调查发现类型更改为与 ASFF 兼容的值。例如，Macie 中的 `Policy:IAMUser/S3BucketPublic` 调查发现类型在 Security Hub 中显示为 `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`。

Macie 还会将生成的调查发现样本发送到 Security Hub。对于调查发现样本，受影响资源的名称为 `macie-sample-finding-bucket`，`Sample` 字段的值为 `true`。

有关更多信息，请参阅 Amazon Macie 用户指南中的与 AWS Security Hub 集成。

AWS Systems Manager 补丁管理器（发送调查结果）

AWS Systems Manager 当客户队列中的实例不符合其补丁合规性标准时，Patch Manager 会将发现结果发送给 Security Hub。

Patch Manager 能够使用安全相关更新及其他更新类型自动执行修补托管实例的过程。

启用 Security Hub 后，此集成将自动激活。Systems Manager Patch Manager 立即开始将结果发送到 Security Hub。

有关使用 Patch Manager 的更多信息，请参阅 AWS Systems Manager 用户指南中的 AWS Systems Manager Patch Manager。

AWS 从 Security Hub 接收调查结果的服务

以下 AWS 服务与 Security Hub 集成并接收来自 Security Hub 的调查结果。如有注明，集成服务也可能更新调查发现。在这种情况下，您在集成服务中进行的调查发现更新也将反映在 Security Hub 中。

AWS Audit Manager（接收调查结果）

AWS Audit Manager 接收来自 Security Hub 的调查结果。这些调查发现有助于 Audit Manager 用户为审计做好准备。

要了解有关 Audit Manager 的更多信息，请参阅 Au AWS dit Manager 用户指南。AWSAWS Audit Manager支持的 Security Hub 检查列出了 Security Hub 向 Audit Manager 发送调查发现的控件。

AWS Chatbot（接收调查结果）

AWS Chatbot 是一个交互式代理，可帮助您监控 Slack 频道和 Amazon Chime 聊天室中的 AWS 资源并与之互动。

AWS Chatbot 接收来自 Security Hub 的调查结果。

要了解有关与 Security Hub 集 AWS Chatbot 成的更多信息，请参阅《AWS Chatbot 管理员指南》中的 Sec urity Hub 集成概述。

Amazon Detective（接收调查发现）

Detective 会自动从您的 AWS 资源中收集日志数据，并使用机器学习、统计分析和图论来帮助您实现可视化，并更快、更高效地进行安全调查。

Security Hub 与 Detective 的集成允许你从亚马逊在 Security Hub 中的 GuardDuty 发现转向侦探。然后，您可以使用 Detective 工具和可视化功能调查它们。该集成不需要在 Security Hub 或 Detective 中进行任何其他配置。

对于从其他人那里收到的调查结果 AWS 服务，Security Hub 控制台上的调查结果详细信息面板包括“侦探调查” 小节。该小节包含指向 Detective 的链接，您可以在其中进一步调查调查发现所标记的安全问题。您还可以根据 Security Hub 的调查发现在 Detective 中构建行为图，以进行更有效的调查。要了解更多信息，请参阅《Amazon Detective 管理指南》中的AWS 安全调查发现。

如果启用了跨区域聚合，则当您从聚合区域进行转向时，Detective 将在调查发现的来源区域中打开。

如果链接无效，请参阅对转换进行故障排除以了解故障排除建议。

Amazon Security Lake（接收调查发现）

Security Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 自动将来自云、本地和自定义源的安全数据集中到存储在您账户中的数据湖中。订阅用户可以使用 Security Lake 中的数据进行调查和分析用例。

要激活此集成，您必须启用这两项服务，并在 Security Lake 控制台、Security Lake API 或中将 Security Hub 添加为来源 AWS CLI。完成这些步骤后，Security Hub 开始将所有的调查发现发送到 Security Lake。

Security Lake 会自动对 Security Hub 的调查发现进行标准化，并将其转换为名为开放网络安全架构框架 (OCSF) 的标准化开源架构。在 Security Lake 中，你可以添加一个或多个订阅者来使用 Security Hub 的调查发现。

有关此集成的更多信息，包括有关将 Security Hub 添加为来源和创建订阅者的说明，请参阅 Amazon Sec AWS urity Lake 用户指南中的与 Secur ity Hub 集成。

AWS Systems Manager Explorer 和 OpsCenter（接收和更新调查结果）

AWS Systems Manager 浏览并 OpsCenter 接收来自 Security Hub 的调查结果，然后在 Security Hub 中更新这些发现。

Explorer 为您提供可自定义的控制面板，提供有关您 AWS 环境运营状况和性能的关键见解和分析。

OpsCenter 为您提供查看、调查和解决操作工作项的中心位置。

有关 Explorer 和的更多信息 OpsCenter，请参阅《AWS Systems Manager 用户指南》中的操作管理。

AWS Trusted Advisor（接收调查结果）

Trusted Advisor 借鉴了从为成千上万的 AWS 客户提供服务中学到的最佳实践。 Trusted Advisor 检查您的 AWS 环境，然后在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。

当你同时启用两者 Trusted Advisor 并启用 Security Hub 时，集成会自动更新。

Security Hub 将其 AWS 基础安全最佳实践检查结果发送至。 Trusted Advisor

有关 Security Hub 与集成的更多信息 Trusted Advisor，请参阅《AWS 支持用户指南》 AWS Trusted Advisor中的 “查看 Sec AWS urity Hub 控件”。

可用的第三方合作伙伴产品集成

AWS Security Hub 可与多个第三方合作伙伴产品集成。集成可以执行以下一项或多项操作：

- 将其生成的调查发现发送到 Security Hub。
- 接收来自 Security Hub 的调查发现。
- 更新 Security Hub 中的调查发现。

所有将结果发送到 Security Hub 的集成，都有一个 Amazon 资源名称（ARN）。

> **Note**
>
> 某些集成仅在精选 AWS 区域版本中可用。
> Security Hub 控制台的集成页面列出了当前区域支持的所有集成。
> 有关更多信息，请参阅 中国（北京）和中国（宁夏）区域支持的集成 和 AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）支持的集成。

如果您有安全解决方案并有兴趣成为 Security Hub 合作伙伴，<######## securityhub-partners@amazon.com>。有关更多信息，请参阅 AWS Security Hub 合作伙伴集成指南。

第三方与 Security Hub 的集成概述

以下是将调查发现发送到 Security Hub 或从 Security Hub 接收调查发现的第三方集成的概述。

集成	方向	ARN（如果适用）
3CORESec – 3CORESec NTA	发送调查发现	arn:aws:securityhub: *<REGION>*::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	发送调查发现	arn:aws:securityhub: *<REGION>*:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	发送调查发现	arn:aws:securityhub: *<REGION>*::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	发送调查发现	arn:aws:securityhub: *<REGION>*::product/aqua-security/kube-bench
Armor – Armor Anywhere	发送调查发现	arn:aws:securityhub: *<REGION>*:679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	发送调查发现	arn:aws:securityhub: *<REGION>*::product

集成	方向	ARN（如果适用）
		/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	发送调查发现	arn:aws:securityhub: <REGION>:151784055945:product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	发送调查发现	arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	发送调查发现	arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws
Capitis Solutions – C2VS	发送调查发现	arn:aws:securityhub: <REGION>::product/capitis/c2vs
Check Point – CloudGuard IaaS	发送调查发现	arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	发送调查发现	arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc

集成	方向	ARN（如果适用）
Claroty – xDome	发送调查发现	arn:aws:securityhub: *<REGION>*::product/claroty/xdome
Cloud Storage Security – Antivirus for Amazon S3	发送调查发现	arn:aws:securityhub: *<REGION>*::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	发送调查发现	arn:aws:securityhub: *<REGION>*::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	发送调查发现	arn:aws:securityhub: *<REGION>*:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	发送调查发现	arn:aws:securityhub: *<REGION>*:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	发送调查发现	arn:aws:securityhub: *<REGION>*::product/data-theorem/api-cloud-web-secure
Drata	发送调查发现	arn:aws:securityhub: *<REGION>*::product/drata/drata-integration

集成	方向	ARN（如果适用）
Forcepoint – Forcepoint CASB	发送调查发现	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	发送调查发现	arn:aws:securityhub: *<REGION>*::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	发送调查发现	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	发送调查发现	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	发送调查发现	arn:aws:securityhub: *<REGION>*::product/fugue/fugue
Guardicore – Centra 4.0	发送调查发现	arn:aws:securityhub: *<REGION>*::product/guardicore/guardicore

集成	方向	ARN（如果适用）
HackerOne – Vulnerability Intelligence	发送调查发现	arn:aws:securityhub: *<REGION>*::product/hackerone/vulnerability-intelligence
JFrog – Xray	发送调查发现	arn:aws:securityhub: *<REGION>*::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	发送调查发现	arn:aws:securityhub: *<REGION>*::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	发送调查发现	arn:aws:securityhub: *<REGION>*::product/k9-security/access-analyzer
Lacework – Lacework	发送调查发现	arn:aws:securityhub: *<REGION>*::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	发送调查发现	arn:aws:securityhub: *<REGION>*::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	发送调查发现	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator

集成	方向	ARN（如果适用）
Palo Alto Networks – Prisma Cloud Compute	发送调查发现	arn:aws:securityhub: *<REGION>*:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	发送调查发现	arn:aws:securityhub: *<REGION>*:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	发送调查发现	arn:aws:securityhub: *<REGION>*::product/plerion/cloud-security-platform
Prowler – Prowler	发送调查发现	arn:aws:securityhub: *<REGION>*::product/prowler/prowler
Qualys – Vulnerability Management	发送调查发现	arn:aws:securityhub: *<REGION>*:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	发送调查发现	arn:aws:securityhub: *<REGION>*:336818582268:product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	发送调查发现	arn:aws:securityhub: *<REGION>*::product/securecloudddb/securecloudddb

集成	方向	ARN（如果适用）
SentinelOne – SentinelOne	发送调查发现	arn:aws:securityhub: *<REGION>*::product/sentinelone/endpoint-protection
Snyk	发送调查发现	arn:aws:securityhub: *<region>*::product/snyk/snyk
Sonrai Security – Sonrai Dig	发送调查发现	arn:aws:securityhub: *<REGION>*::product/sonrai-security/sonrai-dig
Sophos – Server Protection	发送调查发现	arn:aws:securityhub: *<REGION>*:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	发送调查发现	arn:aws:securityhub: *<REGION>*::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	发送调查发现	arn:aws:securityhub: *<REGION>*:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	发送调查发现	arn:aws:securityhub: *<REGION>*:754237914691:product/symantec-corp/symantec-cwp

集成	方向	ARN（如果适用）
Tenable – Tenable.io	发送调查发现	arn:aws:securityhub: *<REGION>*:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	发送调查发现	arn:aws:securityhub: *<REGION>*::product/trend-micro/cloud-one
Vectra – Cognito Detect	发送调查发现	arn:aws:securityhub: *<REGION>*:978576646331:product/vectra-ai/cognito-detect
Wiz	发送调查发现	arn:aws:securityhub: *<REGION>*::product/wiz-security/wiz-security
Atlassian - Jira Service Management	接收和更新调查发现	不适用
Atlassian - Jira Service Management Cloud	接收和更新调查发现	不适用
Atlassian – Opsgenie	接收调查发现	不适用
Fortinet – FortiCNP	接收调查发现	不适用
IBM – QRadar	接收调查发现	不适用
Logz.io Cloud SIEM	接收调查发现	不适用
MetricStream	接收调查发现	不适用

集成	方向	ARN（如果适用）
MicroFocus – MicroFocus Arcsight	接收调查发现	不适用
New Relic Vulnerability Management	接收调查发现	不适用
PagerDuty – PagerDuty	接收调查发现	不适用
Palo Alto Networks – Cortex XSOAR	接收调查发现	不适用
Palo Alto Networks – VM-Series	接收调查发现	不适用
Rackspace Technology – Cloud Native Security	接收调查发现	不适用
Rapid7 – InsightConnect	接收调查发现	不适用
RSA – RSA Archer	接收调查发现	不适用
ServiceNow – ITSM	接收和更新调查发现	不适用
Slack – Slack	接收调查发现	不适用
Splunk – Splunk Enterprise	接收调查发现	不适用
Splunk – Splunk Phantom	接收调查发现	不适用
ThreatModeler	接收调查发现	不适用
Trellix – Trellix Helix	接收调查发现	不适用
Caveonix – Caveonix Cloud	发送和接收调查发现	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`

集成	方向	ARN（如果适用）
Cloud Custodian – Cloud Custodian	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/disruptops-inc/disruptops
Kion	发送和接收调查发现	arn:aws:securityhub: *<REGION>*::product/cloudtamerio/cloudtamerio
Turbot – Turbot	发送和接收调查发现	arn:aws:securityhub: *<REGION>*:453761072151:product/turbot/turbot

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 将调查发现转换为 AWS 安全调查发现格式。

3CORESec – 3CORESec NTA

集成类型：发送

产品 ARN：arn:aws:securityhub:*<REGION>*::product/3coresec/3coresec

3CORESec 为本地和 AWS 系统提供托管检测服务。它们与 Security Hub 的集成允许查看恶意软件、权限升级、横向移动和不当网络分段等威胁。

产品链接

合作伙伴文档

Alert Logic – SIEMless Threat Management

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

获得适当的覆盖级别：漏洞和资产可见性、威胁检测和事件管理 AWS WAF，以及分配的 SOC 分析师选项。

产品链接

合作伙伴文档

Aqua Security – Aqua Cloud Native Security Platform

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) 为基于容器的无服务器应用程序提供从 CI/CD 管道到运行时生产环境的完整生命周期安全性。

产品链接

合作伙伴文档

Aqua Security – Kube-bench

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench 是一款开源工具，可针对您的环境运行 Center for Internet Security (CIS) Kubernetes 基准。

产品链接

合作伙伴文档

Armor – Armor Anywhere

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere为。提供托管的安全性和合规性 AWS。

产品链接

合作伙伴文档

AttackIQ – AttackIQ

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform 模拟与 MITRE ATT&CK 框架一致的真实对抗行为，以帮助验证和改善您的整体安全状况。

产品链接

合作伙伴文档

Barracuda Networks – Cloud Security Guardian

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry 帮助组织在公共云中构建应用程序并将工作负载迁移到公共云时保持安全。

AWS 商城链接

产品链接

BigID – BigID Enterprise

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform 帮助公司管理和保护其所有系统中的敏感数据（PII）。

产品链接

合作伙伴文档

Blue Hexagon— Blue Hexagon 对于 AWS

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon 是一个实时威胁检测平台。它使用深度学习原理来检测已知和未知威胁，包括恶意软件和网络异常。

AWS 商城链接

合作伙伴文档

Capitis Solutions – C2VS

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VS 是一个可定制的合规性解决方案，旨在自动识别特定于应用程序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>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard轻松将全面的威胁防御安全扩展到， AWS 同时保护云中的资产。

产品链接

合作伙伴文档

Check Point – CloudGuard Posture Management

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

一个 SaaS 平台，提供可验证的云网络安全、高级 IAM 保护以及全面的合规性和治理。

产品链接

合作伙伴文档

Claroty – xDome

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome 帮助组织在工业（OT）、医疗保健（IoMT）和企业（IoT）环境中通过扩展物联网（XioT）保护其网络物理系统。

产品链接

合作伙伴文档

Cloud Storage Security – Antivirus for Amazon S3

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security为 Amazon S3 对象提供云原生防恶意软件和防病毒扫描。

Antivirus for Amazon S3 提供对 Amazon S3 中对象和文件的实时和计划扫描，以发现恶意软件和威胁。它为问题文件和受感染文件提供了可见性和补救措施。

产品链接

合作伙伴文档

Contrast Security – Contrast Assess

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess 是一款 IAST 工具，可在 Web 应用程序、API 和微服务中提供实时漏洞检测。Contrast Assess 与 Security Hub 集成，有助于为所有工作负载提供集中可见性和响应能力。

产品链接

合作伙伴文档

CrowdStrike – CrowdStrike Falcon

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

CrowdStrike Falcon 的单一的轻量级传感器统一了下一代防病毒、端点检测和响应，以及通过云进行全天候托管威胁搜寻。

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>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics 收集、检测、警报和响应特权账户的高风险活动和行为，以遏制正在进行的攻击。

产品链接

合作伙伴文档

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，寻找安全漏洞和数据隐私漏洞，防止 AppSec 数据泄露。

产品链接

合作伙伴文档

Drata

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata 是一个合规性自动化平台，可帮助您实现和保持与各种框架（例如 SOC2、ISO 和 GDPR）的合规性。Drata 和 Security Hub 之间的集成可帮助您将安全调查发现集中在一个位置。

AWS 商城链接

合作伙伴文档

Forcepoint – Forcepoint CASB

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB 允许您发现云应用程序的使用情况、分析风险并对 SaaS 和自定义应用程序实施适当的控制。

产品链接

合作伙伴文档

Forcepoint – 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 是一项融合云安全服务，无论用户身在何处，都能为用户和数据提供可见性、控件和威胁防护。

产品链接

合作伙伴文档

Forcepoint – Forcepoint DLP

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP 通过员工工作的任何地方和数据所在的任何地方的可见性和控制来解决以人为中心的风险。

产品链接

合作伙伴文档

Forcepoint – Forcepoint NGFW

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW允许您将 AWS 环境连接到企业网络，提供管理网络和应对威胁所需的可扩展性、保护和洞察力。

产品链接

合作伙伴文档

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，可使用相同的策略自动对 infrastructure-as-code 云运行时环境进行持续验证。

产品链接

合作伙伴文档

Guardicore – Centra 4.0

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra 为现代数据中心和云中的工作负载提供流量可视化、微分段和违规检测。

产品链接

合作伙伴文档

HackerOne – Vulnerability Intelligence

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOne 平台与全球黑客社区合作，发现最相关的安全问题。Vulnerability Intelligence 让您的组织能够超越自动扫描的局限。它共享 HackerOne 道德黑客已经验证的漏洞，并提供了重现步骤。

AWS 市场链接

合作伙伴文档

JFrog – Xray

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray 是一款通用的应用程序安全软件组成分析 (SCA) 工具，可持续扫描二进制文件中的许可证合规性和安全漏洞，以便您可以运行安全的软件供应链。

AWS 商城链接

合作伙伴文档

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、安全的 SD-WAN、强大的网络和内置的自动化功能。

AWS 商城链接

合作伙伴文档

产品链接

k9 Security – Access Analyzer

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security当您的 AWS Identity and Access Management 帐户发生重要的访问权限更改时，会通知您。借k9 Security助，您可以了解用户和 IAM 角色对关键数据 AWS 服务 和您的数据的访问权限。

k9 Security专为持续交付而构建，允许您通过可操作的访问审计和针对 Terraform 的简单策略自动化来实施 IAM。 AWS CDK

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 可实现大规模云安全自动化，因此您可以快速、安全地进行创新。

产品链接

合作伙伴文档

McAfee – MVISION 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) 为您的 AWS 环境提供云安全状态管理（CSPM）和云工作负载保护平台（CWPP）。

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>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute 是一种云原生网络安全平台，可为虚拟机、容器和无服务器平台提供保护。

产品链接

合作伙伴文档

Palo Alto Networks – Prisma Cloud Enterprise

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

通过云安全分析、高级威胁检测和合规性监控来保护您的 AWS 部署。

产品链接

合作伙伴文档

Plerion – Cloud Security Platform

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion 是一个云安全平台，采用以威胁为导向、以风险驱动的独特方法，可针对您的工作负载提供预防、检测和纠正措施。与 Security Hub Plerion 之间的集成使客户能够将他们的安全调查发现集中到一个地方，并据此采取行动。

AWS 商城链接

合作伙伴文档

Prowler – Prowler

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler是一种开源安全工具，用于执行与安全最佳实践、强化和持续监控相关的 AWS 检查。

产品链接

合作伙伴文档

Qualys – Vulnerability Management

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) 持续扫描和识别漏洞，保护您的资产。

产品链接

合作伙伴文档

Rapid7 – InsightVM

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM 为现代环境提供漏洞管理，使您能够有效地查找、确定优先级和修复漏洞。

产品链接

合作伙伴文档

SecureCloudDB – SecureCloudDB

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/securecloudd b/securecloudd b`

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，并针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 ARN：`arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne 是一个自主扩展检测和响应（XDR）平台，包括基于人工智能的预防、检测、响应和跨端点、容器、云工作负载和物联网设备搜寻。

AWS 商城链接

产品链接

Snyk

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk 提供了一个安全平台，用于扫描在 AWS上运行的工作负载中应用组件的安全风险。这些风险作为发现结果发送到 Security Hub，帮助开发人员和安全团队对其余 AWS 安全发现进行可视化并确定其优先级。

AWS 商城链接

合作伙伴文档

Sonrai Security – Sonrai Dig

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig 监控和修复云端配置错误和策略违规行为，因此您可以改善安全性和合规性。

产品链接

合作伙伴文档

Sophos – Server Protection

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection使用综合 defense-in-depth 技术保护组织核心的关键应用程序和数据。

产品链接

合作伙伴文档

StackRox – StackRox Kubernetes Security

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox 通过在整个容器生命周期（构建、部署和运行）中强制执行合规性和安全策略，帮助企业大规模保护其容器和 Kubernetes 部署。

产品链接

合作伙伴文档

Sumo Logic – Machine Data Analytics

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic 是一个安全的机器数据分析平台，使开发和安全运营团队能够构建、运行和保护其 AWS 应用程序。

产品链接

合作伙伴文档

Symantec – Cloud Workload Protection

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection 通过反恶意软件、入侵防御和文件完整性监控为您的 Amazon EC2 实例提供全面的保护。

产品链接

合作伙伴文档

Tenable – Tenable.io

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

准确识别、调查漏洞并确定其优先级。托管在云中。

产品链接

合作伙伴文档

Trend Micro – Cloud One

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One 在正确的时间和地点为团队提供正确的安全信息。这种集成可将安全发现实时发送到 Security Hub，从而增强了 Security Hub 中 AWS 资源和Trend Micro Cloud One事件详细信息的可见性。

AWS 商城链接

合作伙伴文档

Vectra – Cognito Detect

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra 正在改变网络安全领域，它通过应用先进的 AI 检测和应对隐藏的网络攻击者，以防止其窃取信息或造成损害。

AWS 商城链接

合作伙伴文档

Wiz – Wiz Security

集成类型：发送

产品 ARN：`arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz持续分析您 AWS 账户的、用户和工作负载中的配置、漏洞、网络、IAM 设置、密钥等，以发现构成实际风险的关键问题。将 Wiz 与 Security Hub 集成，可视化并响应 Wiz 从 Security Hub 控制台检测到的问题。

AWS 商城链接

合作伙伴文档

接收来自 Security Hub 的调查发现的第三方集成

以下第三方合作伙伴产品集成从 Security Hub 获得调查发现。如有说明，产品还可能更新调查发现。在这种情况下，您在合作伙伴产品中所做的调查发现更新也将反映在 Security Hub 中。

Atlassian - Jira Service Management

集成类型：接收和更新

f AWS 服务管理连接器 or 将发现结果从 Security Hub Jira 发送到Jira。 Jira问题是根据调查结果创建的。当 Jira 问题更新时，Security Hub 中相应的调查发现也会更新。

该集成仅支持 Jira 服务器和 Jira 数据中心。

有关集成及其工作原理的概述，请观看视频 AWS Security Hub - 与 Atlassian Jira Service Management 的双向集成。

产品链接

合作伙伴文档

Atlassian - Jira Service Management Cloud

集成类型：接收和更新

Jira Service Management Cloud 是 Jira 服务管理的云组件。

f AWS 服务管理连接器 or 将发现结果从 Security Hub Jira 发送到Jira。这些结果引发 Jira Service Management Cloud 中的问题产生。当您在 Jira Service Management Cloud 中更新这些问题时，Security Hub 中也会更新相应的调查发现。

产品链接

合作伙伴文档

Atlassian – Opsgenie

集成类型：接收

Opsgenie 是一种现代事件管理解决方案，用于运营始终在线的服务，使开发和运营团队能够规划服务中断并在事件期间保持控制。

与 Security Hub 集成可确保将与安全相关的关键任务事件路由到适当的团队以立即解决。

产品链接

合作伙伴文档

Fortinet – FortiCNP

集成类型：接收

FortiCNP 是一款云原生防护产品，可将安全调查发现汇总为切实可行的见解，并根据风险评分确定安全见解的优先级，以减少警报疲劳并加快补救速度。

AWS 商城链接

合作伙伴文档

IBM – QRadar

集成类型：接收

IBM QRadar SIEM 让安全团队能够快速、准确地检测威胁并确定其优先级，然后调查和响应威胁。

产品链接

合作伙伴文档

Logz.io Cloud SIEM

集成类型：接收

Logz.io 是一家提供 Cloud SIEM 的提供商，它提供日志和事件数据高级关联，可帮助安全团队实时检测、分析和应对安全威胁。

产品链接

合作伙伴文档

MetricStream – CyberGRC

集成类型：接收

MetricStream CyberGRC 帮助您管理、衡量和降低网络安全风险。通过收到 Security Hub 的调查发现，CyberGRC 让您可以更清楚地了解这些风险，因此您可以优先考虑网络安全投资并遵守 IT 策略。

AWS 商城链接

产品链接

MicroFocus – MicroFocus Arcsight

集成类型：接收

ArcSight 实时加速有效的威胁检测和响应，将事件关联以及受监督和无监督的分析与响应自动化和编排相结合。

产品链接

合作伙伴文档

New Relic Vulnerability Management

集成类型：接收

New Relic Vulnerability Management 接收来自 Security Hub 的安全调查发现，因此您可以集中查看整个堆栈中情境的安全情况以及性能遥测数据。

AWS 商城链接

合作伙伴文档

PagerDuty – PagerDuty

集成类型：接收

PagerDuty 的数字运营管理平台让团队能够自动将任何信号转化为适当的见解和操作，从而主动缓解影响客户的问题。

AWS 用户可以放心地使用这PagerDuty组 AWS 集成来扩展其 AWS 和混合环境。

与 Security Hub 聚合和组织的安全警报结合使用时，PagerDuty 让团队自动化威胁响应流程并快速设置自定义操作以防止潜在问题。

正在进行云迁移项目的 PagerDuty 用户可以快速迁移，同时减少整个迁移生命周期中发生的问题的影响。

产品链接

合作伙伴文档

Palo Alto Networks – Cortex XSOAR

集成类型：接收

Cortex XSOAR 是一种安全编排、自动化和响应 (SOAR) 平台，可与您的整个安全产品堆栈集成，以加快事件响应和安全操作。

产品链接

合作伙伴文档

Palo Alto Networks – VM-Series

集成类型：接收

Palo Alto VM-Series 与 Security Hub 集成可收集威胁情报，并将其作为自动安全策略更新发送到 VM-Series 下一代防火墙，从而阻止恶意 IP 地址活动。

产品链接

合作伙伴文档

Rackspace Technology – Cloud Native Security

集成类型：接收

Rackspace Technology 在本机 AWS 安全产品之上提供托管安全服务，通过 Rackspace SOC 进行 24x7x365 监控、高级分析和威胁修复。

产品链接

Rapid7 – InsightConnect

集成类型：接收

Rapid7 InsightConnect 是一种安全编排和自动化解决方案，使您的团队无需编写代码即可优化 SOC 操作。

产品链接

合作伙伴文档

RSA – RSA Archer

集成类型：接收

RSA Archer IT 和安全风险管理让您可以确定哪些资产对您的业务至关重要，制定和传达安全策略和标准，检测和应对攻击，识别和修复安全缺陷，并建立明确的 IT 风险管理最佳实践。

产品链接

合作伙伴文档

ServiceNow – ITSM

集成类型：接收和更新

ServiceNow 与 Security Hub 的集成允许在 ServiceNow ITSM 内部查看 Security Hub 的安全调查发现。您也可以配置 ServiceNow 以在收到来自 Security Hub 的调查发现时自动创建事件或问题。

对这些事件和问题的任何更新都会导致 Security Hub 中的调查发现更新。

有关集成及其工作原理的概述，请观看视频 AWS Security Hub-与 ServiceNow ITSM 的双向集成。

产品链接

合作伙伴文档

Slack – Slack

集成类型：接收

Slack 是业务技术堆栈中的一层，它将人员、数据和应用程序组合在一起。它可让人员有效地协同工作、查找重要信息和访问数十万种关键应用程序和服务，以取得最佳的工作成果。

产品链接

合作伙伴文档

Splunk – Splunk Enterprise

集成类型：接收

Splunk使用 Amazon E CloudWatch vents 作为 Security Hub 调查结果的使用者。将您的数据发送到 Splunk 以进行高级安全分析和 SIEM。

产品链接

合作伙伴文档

Splunk – Splunk Phantom

集成类型：接收

使用 Sec AWS urity Hub 的Splunk Phantom应用程序，可以将发现结果发送到以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，可保护和扩展企业软件和云开发生命周期。

产品链接

合作伙伴文档

Trellix – Trellix Helix

集成类型：接收

Trellix Helix 是一个云托管的安全操作平台，可让组织控制从警报到修复的任何事件。

产品链接

合作伙伴文档

第三方集成向 Security Hub 发送调查发现并从 Security Hub 接收调查发现

以下第三方合作伙伴产品集成会向 Security Hub 发送调查发现并从中接收调查发现。

Caveonix – Caveonix Cloud

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix 基于人工智能的平台可自动执行混合云中的可见性、评估和缓解措施，涉及的对象涵盖云原生服务、虚拟机和容器。与 Sec AWS urity Hub 集成，可Caveonix合并 AWS 数据和高级分析，以深入了解安全警报和合规性。

AWS 商城链接

合作伙伴文档

Cloud Custodian – Cloud Custodian

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian 使用户能够在云端得到良好的管理。简单的 YAML DSL 允许轻松定义规则，以实现安全且成本优化的管理良好的云基础设施。

产品链接

合作伙伴文档

DisruptOps, Inc. – DisruptOPS

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps 的安全运营平台通过使用自动化护栏，帮助企业在云中维护最佳安全实践。

产品链接

合作伙伴文档

Kion

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion（前身为 cloudtamer.io）是一款完整的云治理解决方案。 AWSKion让利益相关者了解云运营情况，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

Turbot – Turbot

集成类型：发送和接收

产品 ARN：`arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot 可确保您的云基础设施安全、合规、可扩展且保持最优成本。

产品链接

合作伙伴文档

使用定制产品集成将发现结果发送到 Sec AWS urity Hub

除了集成 AWS 服务和第三方产品生成的调查结果外，Security Hub 还可以使用其他定制安全产品生成的调查结果。

您可以使用 `BatchImportFindings`API 操作将这些发现手动发送到 Security Hub。

设置自定义集成时，请使用《Security Hub 合作伙伴集成指南》中提供的指南和清单。

从自定义安全产品发送结果的要求和建议

在成功调用 `BatchImportFindings` API 操作之前，您必须启用 Security Hub。

您必须使用 the section called “结果格式” 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，会在当前账户中为 Security Hub 生成一个默认的产品 Amazon 资源名称（ARN）。

该产品 ARN 具有以下格式：`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`。例如，`arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`。

调用 `BatchImportFindings` API 操作时，请使用此产品 ARN 作为 `ProductArn` 属性的值。

定义公司和产品名称

您可以使用 `BatchImportFindings` 为将调查发现发送到 Security Hub 的自定义集成设置首选公司名称和产品名称。

您指定的名称将替换预先配置的公司名称和产品名称（分别称为“个人名称”和“默认名称”），并显示在 Security Hub 控制台和每个调查发现的 JSON 中。请参阅 使用 BatchImportFindings 创建和更新结果。

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。

每个新发现都应有一个唯一的发现 ID。如果定制产品发送了多个具有相同查找 ID 的搜索结果，则 Security Hub 仅处理第一个查找结果。

设置账户 ID

您必须使用 `AwsAccountId` 属性指定您自己的账户 ID。

设置创建日期和更新日期

您必须为 `CreatedAt` 和 `UpdatedAt` 属性提供您自己的时间戳。

更新来自自定义产品的结果

除了从自定义产品发送新结果以外，您还可以使用 `BatchImportFindings` API 操作更新来自自定义产品的现有结果。

要更新现有结果，请使用现有结果 ID（通过 `Id` 属性）。使用请求中更新的相应信息（包括修改后的 `UpdatedAt` 时间戳）重新发送完整的结果。

示例自定义集成

您可以使用以下示例自定义产品集成作为指南来创建您自己的自定义解决方案。

将 Chef InSpec 扫描结果发送到 Security Hub

您可以创建一个 AWS CloudFormation 模板来运行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 Chef InSpec 和 AWS Security Hub 进行持续合规性监控》。

将 Trivy 检测到的容器漏洞发送到 Security Hub

您可以创建一个用于扫描容器中是否存在漏洞的 AWS CloudFormation 模板，然后将这些漏洞发现发送到 Security Hub。AquaSecurity Trivy

有关更多详细信息，请参阅如何使用Trivy和 Sec AWS urity Hub 构建用于容器漏洞扫描的 CI/CD 管道。

Security Hub 中的 AWS 安全控制和标准

AWS Security Hub 使用、汇总和分析来自各种受支持产品 AWS 和第三方产品的安全发现。

Security Hub 还可以根据规则运行自动和持续的安全检查，从而生成自己的调查发现。这些规则由安全控件来表示。反过来，可以在一个或多个安全标准中启用这些控件。这些控件可帮助您确定是否满足标准中的要求。

针对控制措施进行安全检查会生成调查结果，您可以使用这些发现来监控您的安全状况并识别需要注意的特定资源 AWS 账户 或资源。每个控件都与一项 AWS 服务和资源相关。例如，针对 CloudTrail.4 控件的安全检查可确定您是否已在日志中配置了日志文件验证。 AWS CloudTrail 有关控件的详细信息，请参阅 查看和管理安全控件。

您可以在一个或多个已启用的 Security Hub 标准中启用控件。当您启用标准时，Security Hub 会自动启用适用于该标准的控件。安全标准使您能够专注于特定的合规性框架。Security Hub 定义了适用于每个标准的控件。有关安全标准的更多信息，请参阅 查看和管理安全标准。

根据安全检查的结果，Security Hub 计算总体安全评分和特定标准的安全评分。这些分数可帮助您了解安全状况。有关分数的更多信息，请参阅 安全评分是如何计算的。

有关 Security Hub 安全检查定价的信息，请参阅 Security Hub 定价。

主题

用于配置标准和控件的 IAM 权限

要查看有关安全控制的信息以及启用和禁用标准中的安全控制，用于访问的 AWS Identity and Access Management (IAM) 角色 AWS Security Hub 需要调用以下 API 操作的权限。如果不为这些操作添加权限，则无法调用这些 API。要获得必要的权限，您可以使用 Security Hub 托管策略。或者，您可以更

新自定义 IAM policy 以包含这些操作的权限。自定义策略还应包括 DescribeStandardsControls 和 UpdateStandardsControl API 的权限。

- **BatchGetSecurityControls**— 返回有关当前账户和的一批安全控制措施的信息 AWS 区域。
- **ListSecurityControlDefinitions**——返回有关适用于指定标准的安全控件的信息。
- **ListStandardsControlAssociations**——确定账户中每个启用的标准中当前是启用还是禁用了安全控件。
- **BatchGetStandardsControlAssociations**——对于一批安全控件，标识每个控件当前是在指定标准中启用还是禁用。
- **BatchUpdateStandardsControlAssociations**——用于在包含该控件的标准中启用安全控件，或禁用标准中的控件。如果管理员不想允许成员账户启用或禁用控件，则可以批量替代现有 UpdateStandardsControl API。

除了前面的 API 之外，您还应该添加调用 **BatchGetControlEvaluations** 的权限至 IAM 角色。要在 Security Hub 控制台上查看控件的启用和合规性状态、控件的调查发现计数以及控件的总体安全评分，需要此权限。由于只有控制台调用 **BatchGetControlEvaluations**，因此此 IAM 权限并不直接对应于公开记录的 Security Hub API 或 AWS CLI 命令。

有关控件和标准相关的 API 的更多信息，请参阅 AWS Security Hub API 参考。

Security Hub 中的安全检查和安全评分

对于您启用的每个控件，都会 AWS Security Hub 运行安全检查。安全检查可确定您的 AWS 资源是否符合控件中包含的规则。

有些检查是定期进行的。其他检查仅在资源状态发生更改时运行。有关更多信息，请参阅 the section called “有关运行安全检查的计划”。

许多安全检查使用 AWS Config 托管或自定义规则来确定合规性要求。要运行这些检查，必须进行设置 AWS Config。有关更多信息，请参阅 the section called “AWS Config 规则和安全检查”。其他人则使用自定义 Lambda 函数，这些函数由 Security Hub 管理，并且对客户不可见。

当 Security Hub 运行安全检查时，它会生成调查发现并为其分配合规性状态。有关合规状态的更多信息，请参阅 调查结果的合规状态值。

Security Hub 使用控件调查发现的合规性状态来确定总体控件状态。Security Hub 还会计算所有已启用的控件和特定标准的安全分数。有关更多信息，请参阅 the section called “合规状态和控制状态” 和 the section called “确定安全分数”。

如果您开启了整合的控件调查发现，即使一个控件与多个标准相关联，Security Hub 也会生成一个调查发现。有关更多信息，请参阅 整合的控件调查发现。

主题

Security Hub 如何使用 AWS Config 规则进行安全检查

要对环境的资源进行安全检查， AWS Security Hub 要么使用标准指定的步骤，要么使用特定的 AWS Config 规则。有些规则是托管规则，由 AWS Config管理。其他规则是 Security Hub 开发的自定义规则。

AWS Config Security Hub 用于控制的规则被称为服务相关规则，因为它们由 Security Hub 服务启用和控制。

要启用对这些 AWS Config 规则的检查，您必须先 AWS Config 为您的账户启用并启用所需资源的资源记录。有关如何启用的信息 AWS Config，请参阅正在配置 AWS Config。有关所需资源记录的信息，请参阅 AWS Config 生成控制结果所需的资源

Security Hub 如何生成服务相关规则

对于使用 AWS Config 服务相关规则的每个控件，Security Hub 都会在您的 AWS 环境中创建所需规则的实例。

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。服务相关规则在原始规则名称前添加一个 `securityhub`，并在规则名称后添加一个唯一标识符。例如，对于原始 AWS Config 托管规则`vpc-flow-logs-enabled`，与服务相关的规则名称将类似`securityhub-vpc-flow-logs-enabled-12345`于。

可用于评估控件的 AWS Config 规则数量有限制。Security Hub 创建的自定义 AWS Config 规则不计入该限制。即使您的账户中已达到托管规则的 AWS Config 限制，也可以启用安全标准。要了解有关 AWS Config 规则限制的更多信息，请参阅《AWS Config 开发者指南》中的服务限制。

查看有关控件 AWS Config 规则的详细信息

对于使用 AWS Config 托管规则的控件，控件描述包括指向 AWS Config 规则详细信息的链接。自定义规则未从控件描述中链接。有关控件的说明，请参见 Security Hub 控件参考。从列表中选择一个控件以查看其描述。

对于通过这些控件生成的调查结果，查找结果详细信息包括指向关联 AWS Config 规则的链接。请注意，要通过查找详细信息导航到 AWS 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 AWS Config。

调查发现页面、见解页面和集成页面上的调查发现详细信息包括指向 AWS Config 规则详细信息的规则链接。请参阅 查看发现详情。

在控件详细信息页面上，调查结果列表的 “调查” 列包含指向 AWS Config 规则详细信息的链接。请参阅 查看查找资源的 AWS Config 规则。

AWS Config 生成控制结果所需的资源

AWS Security Hub 通过对 Security Hub 控件执行安全检查来生成控制结果。一些控制使用 AWS Config 规则来评估对特定资源的合规性。要让 Security Hub 为具有变更触发计划类型的控件生成调查发现，您必须在 AWS Config中开启所需资源的记录。对于大多数具有定期计划类型的控件，您无需记录资源。但是，一些定期控制需要记录资源以检测合规性变化。

此页面提供了各类标准所需资源的列表以及按标准划分的所需资源列表。第一张表还列出了使用每种资源的 Security Hub 控件。

如果调查结果是由基于 AWS Config 规则的安全检查生成的，则查找结果详细信息将包括指向关联规则的 AWS Config 规则链接。要导航到 AWS Config 规则，您的账户必须具有 AWS Identity and Access Management (IAM) 权限才能查看 AWS Config 规则。

> **Note**
>
> AWS 区域 如果控件不可用，则相应的资源在中不可用 AWS Config。有关 Security Hub 控件的区域限制列表，请参阅 按地区划分的控件可用性。

AWS Config 所有控制所需的资源

要让 Security Hub 为启用的 Security Hub 更改触发的使用 AWS Config 规则的控件生成调查结果，您必须将这些资源记录在中 AWS Config。此表还指出了哪些控件需要特定的资源。控件可能需要多个资源。

服务	所需资源	相关控件
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5
AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`	备份。5
	`AWS::Backup::BackupVault`	备份。3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	备份。4
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3

服务	所需资源	相关控件
Amazon Athena	`AWS::Athena::DataCatalog`	雅典娜.2
	`AWS::Athena::WorkGroup`	雅典娜.3
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17

服务	所需资源	相关控件
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
Amazon Detective	`AWS::Detective::Graph`	侦探。1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2

	`AWS::DMS::Endpoint`	`DMS.9`
		`DMS.10`
		`DMS.11`
		`DMS.12`

	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5

服务	所需资源	相关控件
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamodB.5 DynamodB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::EIP`	EC2.12 EC2.37
	`AWS::EC2::FlowLog`	EC2.48

服务	所需资源	相关控件
	AWS::EC2::Instance	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	AWS::EC2::InternetGateway	EC2.39
	AWS::EC2::LaunchTemplate	EC2.25
	AWS::EC2::NatGateway	EC2.40
	AWS::EC2::NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2::NetworkInterface	EC2.22 EC2.35
	AWS::EC2::RouteTable	EC2.42

服务	所需资源	相关控件
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache.7
	AWS::EC2::TransitGateway	EC2.23 EC2.52
	AWS::EC2::TransitGatewayAttachment	EC2.33
	AWS::EC2::TransitGatewayRouteTable	EC2.34
	AWS::EC2::Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46

服务	所需资源	相关控件
	AWS::EC2::VPCEndpointService	EC2.47
	AWS::EC2::VPCPeeringConnection	EC2.49
	AWS::EC2::VPNConnection	EC2.20
	AWS::EC2::VPNGateway	EC2.50
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	AWS::AutoScaling::LaunchConfiguration	AutoScaling.3 Autoscaling.5
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance	SSM.3
	AWS::SSM::ManagedInstanceInventory	SSM.1

服务	所需资源	相关控件
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15

服务	所需资源	相关控件
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
Amazon Elastic Kubernetes Service(Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14

服务	所需资源	相关控件
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	AWS::Elasticsearch::Domain	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EventBridge	AWS::Events::EventBus	EventBridge.2 EventBridge.3
	AWS::Events::Endpoint	EventBridge.4
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator.1

服务	所需资源	相关控件
AWS Glue	AWS::Glue::Job	胶水。1
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty.4
	AWS::GuardDuty::Filter	GuardDuty.2
	AWS::GuardDuty::IPSet	GuardDuty.3
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	IAM.24 IAM.27 KMS.2

服务	所需资源	相关控件
	AWS::IAM::User	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	IAM.23
AWS IoT	AWS::IoT::Authorizer	IoT.4
	AWS::IoT::Dimension	IoT.3
	AWS::IoT::MitigationAction	IoT.2
	AWS::IoT::Policy	IoT.6
	AWS::IoT::RoleAlias	IoT.5

服务	所需资源	相关控件
	`AWS::IoT::SecurityProfile`	IoT.1
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 S3.17
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6

服务	所需资源	相关控件
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 OpenSearch.9 Opensearch.10 打开搜索。11

服务	所需资源	相关控件
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

服务	所需资源	相关控件
	AWS::RDS::DBClusterSnapshot	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29
	AWS::RDS::DBInstance	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RDS.30

服务	所需资源	相关控件
	AWS::RDS::DBSecurityGroup	RDS.31
	AWS::RDS::DBSnapshot	RDS.1 RDS.4 RDS.32
	AWS::RDS::DBSubnetGroup	RDS.33
	AWS::RDS::EventSubscription	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	AWS::Redshift::Cluster	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 Redshift.11

服务	所需资源	相关控件
	AWS::Redshift::ClusterParameterGroup	Redshift.2
	AWS::Redshift::ClusterSnapshot	Redshift.13
	AWS::Redshift::ClusterSubnetGroup	Redshift.14
	AWS::Redshift::EventSubscription	Redshift.12
Amazon Route 53	AWS::Route53::HostedZone	Route53.2
	AWS::Route53::HealthCheck	53.1 号公路
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::AccountPublicAccessBlock	S3.2 S3.3

服务	所需资源	相关控件
	AWS::S3::Bucket	S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog.1

服务	所需资源	相关控件
Amazon Simple Email Service（Amazon SES）	`AWS::SES::ConfigurationSet`	SES.2
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Transfer Family	`AWS::Transfer::Workflow`	转账。1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7

服务	所需资源	相关控件
	AWS::WAF::WebACL	WAF.1 WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFv2::RuleGroup	WAF.12
	AWS::WAFv2::WebACL	WAF.10 WAF.11

FSBP 标准所需的资源

为了让 Security Hub 准确报告已启用的 AWS 基础安全最佳实践 (FSBP) 变更触发的使用 AWS Config 规则的控件的调查结果，您必须将这些资源记录在中。 AWS Config有关此标准的更多信息，请参阅 AWS 基础安全最佳实践 (FSBP) 标准。

服务	所需的 资源
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint

服务	所需的 资源
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

服务	所需的 资源

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry（Amazon ECR）	`AWS::ECR::Repository`

Amazon Elastic Container Service（Amazon ECS）	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System（Amazon EFS）	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

服务	所需的 资源
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`

服务	所需的 资源

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`
	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::Bucket`

Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

服务	所需的 资源

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

CIS AWS 基金会基准测试所需的资源

要对适用于互联网安全中心 (CIS) AWS 基金会基准测试的已启用控件进行安全检查，Security Hub 要么按照保护 Amazon Web Services 中为检查规定的确切审计步骤运行，要么使用特定的 AWS Config 托管规则。

有关此标准的更多信息，请参阅 CIS AWS 基金会基准。

CIS v3.0.0 所需的资源

为使 Security Hub 能够准确报告已启用 CIS v3.0.0 更改触发的使用 AWS Config 规则的控件的发现结果，您必须将这些资源记录在中。 AWS Config

服务	所需的 资源

Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`

服务	所需的 资源

	`AWS::IAM::User`
	
	`AWS::IAM::Role`

Amazon Relational Database Service（Amazon RDS）	`AWS::RDS::DBInstance`
Amazon Simple Storage Service（Amazon S3）	`AWS::S3::Bucket`

CIS v1.4.0 所需的 资源

为了让 Security Hub 准确报告已启用 CIS v1.4.0 更改触发的使用 AWS Config 规则的控件的发现，您必须在中记录这些资源。 AWS Config

服务	所需的 资源

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::NetworkAcl`
	
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Policy`
	
	`AWS::IAM::User`

Amazon Relational Database Service（Amazon RDS）	`AWS::RDS::DBInstance`
Amazon Simple Storage Service（Amazon S3）	`AWS::S3::Bucket`

CIS v1.2.0 所需的 资源

为了让 Security Hub 准确报告已启用 CIS v1.2.0 更改触发的使用 AWS Config 规则的控件的发现，您必须在中记录这些资源。 AWS Config

服务	所需的 资源
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

NIST SP 800-53 修订版 5 所需的资源

为了让 Security Hub 准确报告已启用的美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5 使用 AWS Config 规则的变更触发控件的调查结果，您必须将这些资源记录在中。 AWS Config您只需要记录已触发计划类型变更的控件的资源即可。有关此标准的更多信息，请参阅 美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5。

服务	所需的 资源
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

服务	所需的 资源
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry（Amazon ECR）	`AWS::ECR::Repository`

Amazon Elastic Container Service（Amazon ECS）	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System（Amazon EFS）	`AWS::EFS::AccessPoint`

服务	所需的 资源
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

服务	所需的 资源

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::AccessPoint`
	`AWS::S3::Bucket`

AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`

服务	所需的 资源

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

PCI DSS v3.2.1 所需的资源

为了让 Security Hub 准确报告使用 AWS Config 规则的已启用的支付卡行业数据安全标准 (PCI DSS) 控件的调查结果，您必须将这些资源记录在中。 AWS Config有关此标准的更多信息，请参阅 支付卡行业数据安全标准 (PCI DSS)。

服务	所需的 资源
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::EIP`

服务	所需的 资源
	AWS::EC2::Instance AWS::EC2::SecurityGroup
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy AWS::IAM::User
AWS Lambda	AWS::Lambda::Function
亚马逊 OpenSearch 服务	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::Bucket
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance

资源标签标准 AWS 版所需的资源

AWS 资源标签标准中的所有控件都是变更触发的，并使用 AWS Config 规则。为了让 Security Hub 准确报告这些控件的调查结果，您必须在中记录以下资源 AWS Config。您只需要记录已触发计划类型变更的控件的资源即可。有关此标准的更多信息，请参阅 AWS 资源标签标准。

服务	所需的 资源
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` `AWS::Athena::WorkGroup`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`
	`AWS::Backup::BackupVault`
	`AWS::Backup::RecoveryPlan`
	`AWS::Backup::ReportPlan`

AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon Detective	`AWS::Detective::Graph`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`
	`AWS::DMS::EventSubscription`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationSubnetGroup`

服务	所需的 资源
Amazon DynamoDB	`AWS::DynamoDB::Trail`

服务	所需的 资源
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::CustomerGateway AWS::EC2::EIP AWS::EC2::FlowLog AWS::EC2::Instance AWS::EC2::InternetGateway AWS::EC2::NatGateway AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::RouteTable AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::TransitGatewayAttachment AWS::EC2::TransitGatewayRouteTable AWS::EC2::Volume AWS::EC2::VPC AWS::EC2::VPCEndpointService AWS::EC2::VPCPeeringConnection AWS::EC2::VPNGateway

服务	所需的 资源
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry（Amazon ECR）	`AWS::ECR::PublicRepository`

Amazon Elastic Container Service（Amazon ECS）	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System（Amazon EFS）	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service（Amazon EKS）	`AWS::EKS::Cluster` `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk （Elastic Beanstalk）	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`

Amazon GuardDuty	`AWS::GuardDuty::Detector`
	`AWS::GuardDuty::Filter`
	`AWS::GuardDuty::IPSet`

AWS Identity and Access Management (IAM)	`AWS::IAM::Role` `AWS::IAM::User`

服务	所需的 资源
AWS Identity and Access Management Access Analyzer（ IAM 访问分析器 ）	`AWS::AccessAnalyzer::Analyzer`

AWS IoT	`AWS::IoT::Authorizer`
	`AWS::IoT::Dimension`
	`AWS::IoT::MitigationAction`
	`AWS::IoT::Policy`
	`AWS::IoT::RoleAlias`
	`AWS::IoT::SecurityProfile`

Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` `AWS::NetworkFirewall::FirewallPolicy`
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`

Amazon Relational Database Service	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSecurityGroup`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::DBSubnetGroup`

服务	所需的 资源

Amazon Redshift	`AWS::Redshift::Cluster`
	`AWS::Redshift::ClusterSnapshot`
	`AWS::Redshift::ClusterSubnetGroup`
	`AWS::Redshift::EventSubscription`

Amazon Route 53	`AWS::Route53::HealthCheck`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service（Amazon SES）	`AWS::SES::ConfigurationSet` `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Transfer Family	`AWS::Transfer::Workflow`

服务管理标准版所需的资源： AWS Control Tower

为了让 Security Hub 准确报告已启用的服务管理标准：使用 AWS Config 规则的 AWS Control Tower 变更触发控件的发现，您必须在中 AWS Config记录以下资源。有关此标准的更多信息，请参阅 服务管理标准： AWS Control Tower。

服务	所需的 资源
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`

服务	所需的 资源
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry（Amazon ECR）	`AWS::ECR::Repository`

Amazon Elastic Container Service（Amazon ECS）	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System（Amazon EFS）	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

服务	所需的 资源
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`

服务	所需的 资源

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

有关运行安全检查的计划

启用安全标准后，将在两小时内 AWS Security Hub 开始运行所有检查。大多数检查会在 25 分钟内开始运行。Security Hub 通过评估控件底层的规则来运行检查。在控件完成其第一次检查之前，其状态为无数据。

启用新标准后，Security Hub 最多可能需要 24 小时才能为使用与其他启用标准中的已启用控件相同的底层 AWS Config 服务关联规则的控件生成调查结果。例如，如果您在 AWS 基础安全最佳实践 (FSBP) 标准中启用 Lambda.1，Security Hub 将创建与服务相关的规则，并且通常会在几分钟内生成结果。此后，如果您在支付卡行业数据安全标准 (PCI DSS) 中启用 Lambda.1，Security Hub 最多可能需要 24 小时才能生成此控件的调查发现，因为它使用的服务关联规则与 Lambda.1 相同。

初始检查后，每个控件的计划可以是定期的，也可以是更改触发的。

- 定期检查：这些检查会在最近一次运行后的 12 或 24 小时内自动运行。Security Hub 决定周期性，您无法对其进行更改。定期控制反映了检查运行时的评估。如果您更新了定期控件调查发现的工作流状态，然后在下次检查中该调查发现的合规性状态保持不变，则工作流状态将保持其已修改状态。例如，如果您的 KMS.4 发现失败，则应启用 AWS KMS key 轮换，然后修复发现结果，Security Hub 会将工作流程状态从更改为。`NEW` `RESOLVED`如果您在下次定期检查之前禁用 KMS 密钥轮换，则调查发现的工作流程状态将保持 `RESOLVED` 不变。
- 变更触发的检查 — 这些检查在关联的资源状态发生变化时运行。 AWS Config 允许您在连续记录资源状态变化和每日记录之间进行选择。如果您选择每日记录，则在资源状态发生变化时，会在每 24 小时结束时 AWS Config 提供资源配置数据。如果没有任何更改，则不会传送任何数据。这可能会导致 Security Hub 调查发现生成延迟，直到 24 小时周期结束。无论您选择哪个录制时段，Security Hub 都会每 18 小时检查一次，以确保 AWS Config 没有错过任何资源更新。

通常，Security Hub 尽可能使用更改触发的规则。要使资源使用变更触发的规则，它必须支持 AWS Config 配置项目。

对于基于托管 AWS Config 规则的控件，控件描述中包含指向《AWS Config 开发人员指南》中规则描述的链接。该描述包括规则是更改触发的还是定期性的。

使用 Security Hub 自定义 Lambda 函数的检查始终是定期的。

生成和更新控件调查发现

AWS Security Hub 通过对安全控制进行检查来生成调查结果。这些发现使用 AWS 安全调查结果格式 (ASFF)。请注意，如果调查发现大小超过最大值 240 KB，则 `Resource.Details` 对象将被移除。对于由 AWS Config 资源支持的控件，您可以在 AWS Config 控制台上查看资源详细信息。

Security Hub 通常会对控件的每项安全检查收费。但是，如果多个控件使用相同的 AWS Config 规则，那么 Security Hub 只会 AWS Config 根据该规则对每一次检查收取一次费用。如果您启用整合的控件调查发现，即使该控件包含在多个启用的标准中，Security Hub 也会生成一个用于安全检查的调查发现。

例如，互联网安全中心 (CIS) AWS 基金会基准标准和基础安全最佳实践标准中的多个控件都使用该 AWS Config 规则`iam-password-policy`。每次 Security Hub AWS Config 根据该规则运行检查时，它会为每个相关控件生成一个单独的调查结果，但只对检查收取一次费用。

整合的控件调查发现

在账户中启用整合的控件调查发现后，Security Hub 会为控件的每项安全检查生成一个新调查发现或调查发现更新，即使某项控件适用于多个启用的标准。要查看控件列表及其适用的标准，请参阅 Security Hub 控件参考。您可以开启或关闭整合的控件调查发现。我们建议将其开启以减少调查发现中的噪音。

如果您在 2023 年 2 月 23 日 AWS 账户 之前启用了 Security Hub，则必须按照本节后面的说明打开合并控制结果。如果 2023 年 2 月 23 日当天或之后启用 Security Hub，则账户中将自动启用整合的控件调查发现。但是，如果您通过手动邀请流程使用 Security Hub 集成 AWS Organizations或邀请成员账户，则只有在管理员账户中启用了整合的控件调查发现后，才会在成员账户中启用整合的控件调查发现。如果该功能在管理员账户中关闭，则在成员账户中也会关闭。此行为适用于新的和现有的成员账户。

如果您在账户中关闭了整合的控件调查发现，Security Hub 会为每项包含控件的已启用标准生成每项安全检查的单独调查发现。例如，如果四个启用的标准共享一个具有相同基础 AWS Config 规则的控件，则在对该控件进行安全检查后，您会收到四个不同的结果。如果启用整合的控件调查发现，则只会收到一个调查发现。有关整合如何影响调查发现的更多信息，请参阅 控件调查发现样本。

开启整合的控件调查发现后，Security Hub 会创建与标准无关的新调查发现，并存档基于标准的原始调查发现。某些控件调查发现字段和值会发生变化，并可能影响现有的工作流程。有关这些更改的更多信息，请参阅整合的控件调查发现——ASFF 的变化。

启用整合的控件调查发现还可能影响第三方集成从 Security Hub 收到的调查发现。AWS v2.0.0 上的自动安全响应支持整合的控制结果。

开启整合的控件调查发现

要启用整合的控件调查发现，您必须登录管理员账户或独立账户。

> **Note**
>
> 开启整合的控件调查发现后，Security Hub 最多可能需要 24 小时才能生成新的整合调查发现并存档基于标准的原始调查发现。在此期间，您可能会在账户中看到一系列与标准无关的和基于标准的调查发现。

Security Hub console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Settings（设置）。
3. 选择常规选项卡。
4. 对于控件，打开整合的控件调查发现。
5. 选择保存。

Security Hub API

1. 运行 UpdateSecurityHubConfiguration。
2. 设置 ControlFindingGenerator 等于 SECURITY_CONTROL。

   请求示例：

```
{
   "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

AWS CLI

1. 运行 update-security-hub-configuration 命令。
2. 设置 control-finding-generator 等于 SECURITY_CONTROL。

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

关闭合并的控件调查发现

要关闭整合的控件调查发现，您必须登录管理员账户或独立账户。

> **Note**
>
> 关闭整合的控件调查发现后，Security Hub 最多可能需要 24 小时才能生成新的基于标准的调查发现并存档合并的调查发现。在此期间，您可能会在账户中看到各种基于标准的和合并的调查发现。

Security Hub console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择 Settings（设置）。
3. 选择常规选项卡。
4. 对于控件，选择编辑，然后关闭整合的控件调查发现。
5. 选择保存。

Security Hub API

1. 运行 UpdateSecurityHubConfiguration。
2. 设置 ControlFindingGenerator 等于 STANDARD_CONTROL。

   请求示例：

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
}
```

AWS CLI

1. 运行 update-security-hub-configuration 命令。
2. 设置 control-finding-generator 等于 STANDARD_CONTROL。

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Compliance 控件调查发现的详细信息

对于控制措施安全检查生成的调查结果，AWS 安全调查结果格式 (ASFF) 中的Compliance字段包含与控制结果相关的详细信息。Compliance 字段包含以下信息。

AssociatedStandards

启用控件的启用标准。

RelatedRequirements

所有启用标准中控件的相关要求清单。这些要求来自第三方安全框架的控制，例如支付卡行业数据安全标准 (PCI DSS)。

SecurityControlId

Security Hub 支持的各类安全标准控制的标识符。

Status

Security Hub 针对给定控件运行的最新检查的结果。之前检查的结果将保持存档状态 90 天。

StatusReasons

包含 Compliance.Status 值的原因列表。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说明。补救步骤取决于哪个控件生成了带有原因代码的调查发现。从 Security Hub 控件参考 中选择一个控件以查看该控件的修复步骤。

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 CloudTrail 跟踪不存在指标筛选条件。
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	该账户没有具有所需配置的多区域 CloudTrail 跟踪。

原因代码	Compliance.Status	描述
CLOUDTRAIL_REGION_INVAILD	WARNING	多区域 CloudTrail 跟踪不在当前区域中。
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	不存在有效的警报操作。
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch 账户中不存在警报。
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config 状态是 ConfigError	AWS Config 访问被拒绝。 验证 AWS Config 是否已启用并已被授予足够的权限。
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config 根据规则评估了您的资源。 该规则不适用于其范围内的 AWS 资源，指定的资源已被删除，或者评估结果被删除。
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	合规性状态NOT_AVAILABLE 是因为 AWS Config 返回的状态为 “不适用”。 AWS Config 未提供该状态的原因。以下是不适用状态的一些可能原因： • 该资源已从 AWS Config 规则的范围中移除。 • 该 AWS Config 规则已删除。 • 资源已删除。 • AWS Config 规则逻辑可能会生成 “不适用” 状态。

原因代码	Compliance.Status	描述
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config 状态是 ConfigError	此原因代码用于几种不同类型的评估错误。 描述提供了具体的原因信息。 错误类型可以是以下类型之一： • 由于缺乏权限而无法执行评估。描述提供缺少的特定权限。 • 参数缺少值或值无效。描述提供参数和参数值的要求。 • 从 S3 存储桶读取时出错。描述标识存储桶并提供特定错误。 • 缺少 AWS 订阅。 • 评估时出现一般超时。 • 账户暂停。
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config 状态是 ConfigError	该 AWS Config 规则正在创建中。
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	出现未知错误。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub 无法对自定义 Lambda 运行时系统执行检查。

原因代码	Compliance.Status	描述
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	该调查发现处于 WARNING 状态，因为与此规则关联的 S3 存储桶位于不同的区域或账户中。 此规则不支持跨区域或跨账户检查。 建议您在此区域或账户中禁用此控制。仅在资源所在的区域或账户中运行它。
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch 日志指标筛选条件没有有效的 Amazon SNS 订阅。
SNS_TOPIC_CROSS_ACCOUNT	WARNING	该调查发现处于一种 WARNING 状态。 与此规则关联的 SNS 主题由其他账户拥有。当前账户无法获取订阅信息。 拥有 SNS 主题的账户必须向当前账户授予访问 SNS 主题的 sns:ListSubscriptionsByTopic 权限。
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	该调查发现处于 WARNING 状态，因为与此规则关联的 SNS 主题位于不同的区域或账户中。 此规则不支持跨区域或跨账户检查。 建议您在此区域或账户中禁用此控制。仅在资源所在的区域或账户中运行它。
SNS_TOPIC_INVALID	FAILED	与此规则关联的 SNS 主题无效。
THROTTLING_ERROR	NOT_AVAILABLE	相关 API 操作超出了允许的速率。

`ProductFields` 控件调查发现的详细信息

当 Security Hub 运行安全检查并生成控件调查发现时，ASFF 中的 `ProductFields` 属性包括以下字段：

`ArchivalReasons:0/Description`

描述 Security Hub 为何对现有调查发现进行存档。

例如，当您禁用控件或标准以及打开或关闭整合的控件调查发现时，Security Hub 会存档现有调查发现。

`ArchivalReasons:0/ReasonCode`

提供了 Security Hub 存档现有调查发现的原因。

例如，当您禁用控件或标准以及打开或关闭整合的控件调查发现时，Security Hub 会存档现有调查发现。

`StandardsGuideArn` 或 `StandardsArn`

与控件关联的标准的 ARN。

对于 CIS AWS 基金会基准标准，字段为`StandardsGuideArn`。

对于 PCI DSS 和 AWS 基础安全最佳实践标准，字段为。`StandardsArn`

如果您启用整合的控件调查发现，这些字段将被 `Compliance.AssociatedStandards` 替代。

`StandardsGuideSubscriptionArn` 或 `StandardsSubscriptionArn`

账户订阅该标准的 ARN。

对于 CIS AWS 基金会基准标准，字段为`StandardsGuideSubscriptionArn`。

对于 PCI DSS 和 AWS 基础安全最佳实践标准，字段为。`StandardsSubscriptionArn`

如果您启用整合的控件调查发现，则这些字段将被删除。

`RuleId` 或 `ControlId`

控件的标识符。

对于 CIS AWS 基金会基准标准，字段为`RuleId`。

对于其他标准，该字段为 `ControlId`。

如果您启用整合的控件调查发现，这些字段将被 Compliance.SecurityControlId 替代。

RecommendationUrl

控件修正信息的 URL。如果您启用整合的控件调查发现，这些字段将被 Remediation.Recommendation.Url 替代。

RelatedAWSResources:0/name

与调查发现关联的资源的名称。

RelatedAWSResource:0/type

与控件关联的资源类型。

StandardsControlArn

控件的 ARN。如果您启用整合的控件调查发现，则会删除此字段。

aws/securityhub/ProductName

对于基于控件的调查发现，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。 AWS

aws/securityhub/annotation

对控件所发现问题的描述。

aws/securityhub/FindingId

调查发现的标识符。如果您启用整合的控件调查发现，则此字段不会引用标准。

为控件调查发现分配严重性

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对照调查发现的严重性标签。

严重性条件

控制的严重程度是根据对以下标准的评估来确定的：

- 威胁行为者利用与控制相关的配置弱点有多困难？

  难度取决于利用弱点执行威胁场景所需的复杂程度。

- 这种弱点导致你的 AWS 账户 资源受损的可能性有多大？

  您的资源泄露意味着您的数据 AWS 账户 或 AWS 基础架构的机密性、完整性或可用性在某种程度上受到损害。

  入侵的可能性表明威胁情景导致您的 AWS 服务或资源中断或泄露的可能性有多大。

例如，考虑以下配置缺点：

- 用户访问密钥不是每 90 天轮换一次。
- IAM 根用户密钥存在。

对于攻击者来说，这两个弱点同样难以利用。在这两种情况下，攻击者都可以使用凭证盗窃或其他方法来获取用户密钥。然后，他们可以使用它以未经授权的方式访问您的资源。

但是，如果威胁行为者获取了根用户访问密钥，则受到损害的可能性会更高，因为这为他们提供了更大的访问权限。因此，根用户密钥漏洞的严重性更高。

严重性未考虑底层资源的重要程度。严重性是指与调查发现关联的资源的重要性级别。例如，与任务关键型应用程序关联的资源比与非生产测试关联的资源更重要。要获取资源重要性信息，请使用 AWS 安全调查结果格式 (ASFF) 的`Criticality`字段。

下表将漏洞利用的难度和受损的可能性映射到安全标签。

	极有可能受损	可能受损	不太可能受损	受损的可能性极小
非常容易被利用	重大	重大	高	中
有点容易被利用	重大	高	中	中
有点难以利用	高	中	中	低
很难被利用	中	中	低	低

严重性定义

严重性标签的定义如下：

严重——应立即修复问题以避免问题升级。

例如，开放的 S3 存储桶被视为具有“严重”严重性的结果。由于许多威胁行为者会扫描开放的 S3 存储桶，因此暴露的 S3 存储桶中的数据很可能会被其他人发现和访问。

一般而言，公开访问的资源被视为关键的安全问题。您应该以最紧迫的态度对待关键结果。您还应该考虑资源的重要程度。

高——该问题必须作为近期优先事项予以解决。

例如，如果默认 VPC 安全组对入站和出站流量开放，则其被视为高严重性。使用这种方法，威胁行为者很容易入侵 VPC。一旦资源进入 VPC，威胁行为者也有可能破坏或泄露资源。

Security Hub 建议您将高严重性结果视为近期优先事项。您应该立即采取补救措施。您还应该考虑资源的重要程度。

中度——该问题应作为中期优先事项加以解决。

例如，对传输中数据缺乏加密被认为是中等严重性的调查发现。要利用这个弱点，需要进行复杂的 man-in-the-middle 攻击。换句话说，这有点困难。如果威胁情景成功，某些数据可能会被泄露。

Security Hub 建议您尽早调查受影响的资源。您还应该考虑资源的重要程度。

低——无需针对问题执行任何操作。

例如，未能收集取证信息被视为严重性较低。这种控制可以帮助防止未来的受损，但是缺乏取证并不能直接导致受损。

您无需对低严重性结果立即采取操作，但是当您将这些结果与其他问题关联时，它们可以提供背景信息。

信息——未结果任何配置漏洞。

换言之，状态为 `PASSED`、`WARNING` 或 `NOT AVAILABLE`。

没有建议的操作。信息性结果可帮助客户证明其处于合规状态。

更新控件调查发现的规则

针对给定规则的后续检查可能会生成新结果。例如，“避免使用根用户”的状态可能会从 `FAILED` 更改为 `PASSED`。在这种情况下，将生成包含最新调查发现的新调查发现。

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。

如果关联的资源被删除、资源不存在或控件被禁用，Security Hub 会自动存档控件的调查发现。由于当前未使用关联的服务，资源可能不再存在。结果将根据以下条件之一自动存档：

- 该调查发现在三至五天内不会更新（请注意，这是尽最大努力的结果且无法保证）。
- 相关的 AWS Config 评估结果已返回NOT_APPLICABLE。

合规状态和控制状态

AWS 安全调查结果格式的Compliance.Status字段描述了控制结果的结果。Security Hub 使用控件调查发现的合规性状态来确定总体控件状态。控件状态显示在 Security Hub 控制台上控件的详细信息页面上。

对于管理员帐户，控制状态反映了管理员帐户和成员帐户中的控制状态。具体而言，如果控件在管理员帐户或任何成员帐户中有一个或多个失败的发现结果，则该控件的总体状态将显示为 “失败”。如果您设置了聚合区域，则聚合区域中的控制状态将反映聚合区域和链接区域中的控制状态。具体而言，如果控件在聚合区域或任何关联区域中有一个或多个失败的发现结果，则该控件的总体状态将显示为 “失败”。

Security Hub 通常会在您首次访问 Security Hub 控制台的 “摘要” 页面或 “安全标准” 页面后 30 分钟内生成初始控制状态。您必须配置AWS Config 资源记录才能显示控制状态。首次生成控制状态后，Security Hub 会根据前 24 小时的发现每 24 小时更新一次控制状态。控件详细信息页面上的时间戳表示上次更新控件状态的时间。

> **Note**
>
> 启用控件后，最长可能需要 24 小时才能在中国地区和 AWS GovCloud (US) Region生成首次控件状态。

调查结果的合规状态值

为每个发现的合规性状态分配了以下值之一：

- PASSED— 表示控件已通过此发现的安全检查。自动将 Security Hub 设置Workflow.Status为RESOLVED。

  如果Compliance.Status查找结果从变PASSED为FAILEDWARNING、或，并且Workflow.Status是NOTIFIED或 NOT_AVAILABLERESOLVED，则 Security Hub 会自动设置Workflow.Status为NEW。

如果您没有与控件对应的资源，Security Hub 会在账户级别生成PASSED调查结果。如果您有与控件对应的资源，但随后删除了该资源，Security Hub 会创建NOT_AVAILABLE查找结果并立即将其存档。18 小时后，您会收到一个PASSED发现，因为您不再拥有与该控件对应的资源。

- FAILED— 表示控件未通过此发现的安全检查。
- WARNING— 表示检查已完成，但是 Security Hub 无法确定资源是否处于PASSED或FAILED状态。
- NOT_AVAILABLE— 表示无法完成检查，原因是服务器出现故障、资源已删除或 AWS Config 评估结果失败NOT_APPLICABLE。

  如果 AWS Config 评估结果为NOT_APPLICABLE，Security Hub 会自动将结果存档。

控制状态的值

Security Hub 根据控制结果的合规状态得出总体控制状态。在确定控制状态时，Security Hub 会忽略具有为RecordState的发现结果ARCHIVED和具有为Workflow.Status的SUPPRESSED结果。

控制状态被分配以下值之一：

- 已通过 — 表示所有发现的合规状态均为PASSED。
- 失败 — 表示至少有一个查找结果的合规状态为FAILED。
- 未知-表示至少有一个发现的合规状态为WARNING或NOT_AVAILABLE。没有发现的合规状态为FAILED。
- 无数据——表示控件没有结果。例如，新启用的控件在 Security Hub 开始为其生成发现结果之前一直处于此状态。如果所有发现结果均为SUPPRESSED或在当前区域不可用，则控件也将处于此状态。
- 已禁用 — 表示当前账户和区域中的控件已禁用。当前未对当前账户和地区中的此控件进行安全检查。但是，禁用对照的发现可能对禁用后最长 24 小时的合规状态具有价值。

确定安全分数

Security Hub 控制台的摘要页面和控制页面显示所有已启用标准的安全分数摘要。在安全标准页面上，Security Hub 还会显示每个启用的标准的安全分数，介于 0-100% 之间。

首次启用 Security Hub 时，Security Hub 会在您首次访问 Security Hub 控制台上的摘要页面或安全标准页面后 30 分钟内计算出摘要安全分数和标准安全分数。仅针对您访问这些页面时启用的标准生成分数。要查看当前启用的标准列表，请调用 GetEnabledStandards API 操作。此外，必须配置 AWS Config 资源记录才能显示分数。摘要安全评分是标准安全评分的平均值。

首次生成分数后，Security Hub 每 24 小时更新一次安全分数。Security Hub 显示时间戳以指示安全评分上次更新的时间。

> **Note**
>
> 在中国地区和 AWS GovCloud (US) Region生成首次获得安全评分最多可能需要 24 小时。

如果您启用整合的控件调查发现，则最长可能需要 24 小时才能更新安全评分。此外，启用新的聚合区域或更新关联区域会重置现有的安全分数。Security Hub 最多可能需要 24 小时才能生成包含来自更新区域的数据的新安全分数。

安全评分是如何计算的

安全分数表示通过的控件与已启用的控件的比例。分数显示为四舍五入到最接近的整数的百分比。

Security Hub 会计算您启用的所有标准的摘要安全分数。Security Hub 还会计算每个启用的标准的安全分数。为了计算分数，启用的控件包括状态为通过、失败和未知的控件。状态为无数据的控件将排除在分数计算之外。

在计算控件状态时，Security Hub 会忽略已存档和隐藏的调查发现。这可能会影响安全分数。例如，如果您隐藏控件的所有失败的调查发现，则其状态将变为已通过，这反过来可以提高安全分数。有关控件状态的详细信息，请参阅 合规状态和控制状态。

评分示例：

Standard	已通过的控件	失败的控件	未知控件	标准分数
AWS 基础安全最佳实践 v1.0.0	168	22	0	88%
独联体 AWS 基金会基准测试 v1.4.0	8	29	0	22%
独联体 AWS 基金会基准测试 v1.2.0	6	35	0	15%

Standard	已通过的控件	失败的控件	未知控件	标准分数
NIST 特别出版物 800-53 第 5 版	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

在计算摘要安全分数时，Security Hub 在各类标准中只计算每个控件一次。例如，如果您启用了一个适用于三个启用标准的控件，则出于评分目的，它仅算作一个启用的控件。

在此示例中，虽然跨已启用标准的已启用控件总数为 528 个，但出于评分目的，Security Hub 仅对每个唯一控件进行一次计数。唯一启用的控件的数量可能低于 528。如果我们假设唯一启用的控件的数量为 515，并且唯一通过的控件的数量为 357，则汇总分数为 69%。该分数的计算方法是将唯一通过的控件数量除以唯一启用的控件数量。

即使您在当前地区的账户中只启用了一个标准，摘要分数也可能与标准安全分数不同。如果您登录到管理员账户并且成员账户启用了其他标准或不同的标准，则可能会发生这种情况。如果您正在查看聚合区域的分数并且在链接的区域中启用了其他标准或不同的标准，也可能会发生这种情况。

管理员账户的安全评分

如果您登录了管理员账户，则摘要安全分数和标准分数会说明管理员账户和所有成员账户中的控件状态。

如果一个成员账户中的控件状态为失败，则管理员账户中的控件状态为失败，这会影响管理员账户的分数。

如果您已登录管理员账户并正在查看聚合区域的分数，则安全分数会考虑所有成员账户和所有关联区域中的控件状态。

安全分数（如果您已设置聚合区域）

如果您设置了聚合 AWS 区域，则摘要安全分数和标准分数将全部考虑控制状态 关联区域。

即使在一个关联区域中，控件的状态也为失败，则其在聚合区域中的状态为 失败，这会影响聚合区域分数。

如果您已登录管理员账户并正在查看聚合区域的分数，则安全分数会考虑所有成员账户和所有关联区域中的控件状态。

Security Hub 标准参考

AWS Security Hub 目前支持本节中详述的安全标准。

选择一个标准以查看有关它的更多详细信息以及适用于它的控制措施。

Security Hub 的标准和控件并不能保证遵守任何监管框架或审计。相反，这些控件提供了一种监视 AWS 账户 和资源当前状态的方法。

支持的标准

- AWS 基础安全最佳实践 (FSBP) 标准
- CIS AWS 基金会基准
- 美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5
- 支付卡行业数据安全标准 (PCI DSS)
- AWS 资源标签标准
- 服务托管标准

AWS 基础安全最佳实践 (FSBP) 标准

AWS 基础安全最佳实践标准是一组控制措施，用于检测您的 AWS 账户 和资源何时偏离安全最佳实践。

该标准允许您持续评估所有 AWS 账户 和工作负载，以快速确定偏离最佳实践的领域。它提供了有关如何改进和维护组织的安全状况的可操作的规范性指导。

这些控件包括多个 AWS 服务资源的安全最佳实践。每个控件还分配有一个类别，反映其适用的安全功能。有关更多信息，请参阅 the section called “控件类别”。

适用于 FSBP 标准的控件

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

[ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度

[ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录

[APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证

[APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能

[APIGateway.4] API Gateway 应与 WAF Web ACL 关联

[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密

[APIGateway.8] API Gateway 路由应指定授权类型

[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

[AppSync.2] AWS AppSync 应该启用字段级日志记录

[AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

[AutoScaling.2] Amazon EC2 Auto Scaling 组应覆盖多个可用区

[AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)

[Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址

[AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型

[AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板

[Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密

[CloudFront.1] CloudFront 发行版应配置默认根对象

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

[CloudFront.4] CloudFront 发行版应配置源站故障转移

[CloudFront.5] CloudFront 发行版应启用日志记录

[CloudFront.6] CloudFront 发行版应启用 WAF

[CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书

[CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

[CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

[CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

[CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

[CloudFront.13] CloudFront 发行版应使用源站访问控制

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

[CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

[DataFirehose.1] Firehose 传输流应在静态状态下进行加密

[DMS.1] Database Migration Service 复制实例不应公开

[DMS.6] DMS 复制实例应启用自动次要版本升级

[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录

[DMS.8] 源数据库的 DMS 复制任务应启用日志记录

[DMS.9] DMS 端点应使用 SSL

[DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权

[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

[DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS

[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密

[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期

[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护

[DynamoDB.1] DynamoDB 表应根据需求自动扩展容量

[DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time

[DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密

[DynamodB.6] DynamoDB 表应启用删除保护

[DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密

[EC2.1] Amazon EBS 快照不应公开恢复

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.3] 挂载的 Amazon EBS 卷应进行静态加密

[EC2.4] 停止的 EC2 实例应在指定时间段后删除

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

[EC2.7] 应启用 EBS 默认加密

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)

[EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址

[EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点

[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址

[EC2.16] 应删除未使用的网络访问控制列表

[EC2.17] Amazon EC2 实例不应使用多个 ENI

[EC2.18] 安全组应只允许授权端口不受限制的传入流量

[EC2.19] 安全组不应允许不受限制地访问高风险端口

[EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态

[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389

[EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求

[EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

[EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录

[ECR.1] ECR 私有存储库应配置图像扫描

[ECR.2] ECR 私有存储库应配置标签不可变性

[ECR.3] ECR 存储库应至少配置一个生命周期策略

[ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。

[ECS.2] ECS 服务不应自动分配公有 IP 地址

[ECS.3] ECS 任务定义不应共享主机的进程命名空间

[ECS.4] ECS 容器应以非特权身份运行

[ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。

[ECS.8] 密钥不应作为容器环境变量传递

[ECS.9] ECS 任务定义应具有日志配置

[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行

[ECS.12] ECS 集群应该使用容器详情

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

[EFS.2] Amazon EFS 卷应包含在备份计划中

[EFS.3] EFS 接入点应强制使用根目录

[EFS.4] EFS 接入点应强制使用用户身份

[EFS.6] EFS 挂载目标不应与公有子网关联

[EKS.1] EKS 集群端点不应公开访问

[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行

[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

[EKS.8] EKS 集群应启用审核日志记录

[ElastiCache.1] ElastiCache Redis 集群应启用自动备份

[ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级

[ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移

[ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密

[ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密

[ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证

[ElastiCache.7] ElastiCache 群集不应使用默认子网组

[ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

[ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新

[ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

[ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager

[ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止

[ELB.4] 应将应用程序负载均衡器配置为删除 http 标头

[ELB.5] 应启用应用程序和经典负载均衡器日志记录

[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护

[ELB.7] 经典负载均衡器应启用连接耗尽功能

[ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

[ELB.9] 经典负载均衡器应启用跨区域负载均衡器

[ELB.10] 经典负载均衡器应跨越多个可用区

[ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

[ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置

[ES.1] Elasticsearch 域应启用静态加密

[ES.2] Elasticsearch 域名不可供公共访问

[ES.3] Elasticsearch 域应加密节点之间发送的数据

[ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志

[ES.5] Elasticsearch 域名应该启用审核日志

[ES.6] Elasticsearch 域应拥有至少三个数据节点

[ES.7] 应将 Elasticsearch 域配置为至少三个专用的主节点

[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密

[EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

[fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷

[fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份

[GuardDuty.1] GuardDuty 应该启用

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.7] IAM 用户的密码策略应具有可靠的配置

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作

[Kinesis.1] Kinesis 直播应在静态状态下进行加密

[KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作

[KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

AWS KMS keys 不应无意中删除 [KMS.3]

[Lambda.1] Lambda 函数策略应禁止公共访问

[Lambda.2] Lambda 函数应使用受支持的运行时系统

[Lambda.5] VPC Lambda 函数应在多个可用区内运行

[Macie.1] 应该启用亚马逊 Macie

[Macie.2] 应启用 Macie 自动发现敏感数据

[MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch

[MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级

[MSK.1] MSK 集群应在代理节点之间传输时进行加密

[Neptune.1] 应对 Neptune 数据库集群进行静态加密

[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

[Neptune.3] Neptune 数据库集群快照不应公开

[Neptune.4] Neptune 数据库集群应启用删除保护

[Neptune.5] Neptune 数据库集群应启用自动备份

[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密

[Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证

[Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照

[NetworkFirewall.2] 应启用 Network Firewall 日志记录

[NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

[NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包

[NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

[NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

[Opensearch.1] OpenSearch 域名应启用静态加密

[Opensearch.2] OpenSearch 域名不应向公众开放

[Opensearch.3] OpenSearch 域应加密节点之间发送的数据

[Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

[Opensearch.5] OpenSearch 域应启用审核日志

[Opensearch.6] OpenSearch 域名应至少有三个数据节点

[Opensearch.7] OpenSearch 域名应启用精细的访问控制

[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密

[Opensearch.10] OpenSearch 域名应安装最新的软件更新

[PCA.1] 应禁用 AWS Private CA 根证书颁发机构

[Route53.2] Route 53 公有托管区域应记录 DNS 查询

[RDS.1] RDS 快照应为私有

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config

[RDS.3] RDS 数据库实例应启用静态加密

[RDS.4] RDS 集群快照和数据库快照应进行静态加密

[RDS.5] RDS 数据库实例应配置多个可用区

[RDS.6] 应为 RDS 数据库实例配置增强监控

[RDS.7] RDS 集群应启用删除保护

[RDS.8] RDS 数据库实例应启用删除保护

[RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch

[RDS.10] 应为 RDS 实例配置 IAM 身份验证

[RDS.11] RDS 实例应启用自动备份

[RDS.12] 应为 RDS 集群配置 IAM 身份验证

[RDS.13] 应启用 RDS 自动次要版本升级

[RDS.14] Amazon Aurora 集群应启用回溯功能

[RDS.15] 应为多个可用区配置 RDS 数据库集群

[RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照

[RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照

[RDS.18] RDS 实例应部署在 VPC 中

[RDS.19] 应为关键集群事件配置现有 RDS 事件通知订阅

[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

[RDS.22] 应为关键数据库安全组事件配置 RDS 事件通知订阅

[RDS.23] RDS 实例不应使用数据库引擎的默认端口

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

[RDS.27] 应对 RDS 数据库集群进行静态加密

[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch

[RDS.35] RDS 数据库集群应启用自动次要版本升级

[Redshift.1] Amazon Redshift 集群应禁止公共访问

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

[Redshift.3] Amazon Redshift 集群应启用自动快照

[Redshift.4] Amazon Redshift 集群应启用审核日志记录

[Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能

[Redshift.7] Redshift 集群应使用增强型 VPC 路由

[Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名

[Redshift.9] Redshift 集群不应使用默认的数据库名称

[Redshift.10] Redshift 集群应在静态状态下进行加密

[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口

[S3.1] S3 通用存储桶应启用阻止公共访问设置

[S3.2] S3 通用存储桶应阻止公共读取权限

[S3.3] S3 通用存储桶应阻止公共写入权限

[S3.5] S3 通用存储桶应要求请求使用 SSL

[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户

[S3.8] S3 通用存储桶应阻止公共访问

[S3.9] S3 通用存储桶应启用服务器访问日志记录

[S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限

[S3.13] S3 通用存储桶应具有生命周期配置

[S3.19] S3 接入点已启用屏蔽公共访问权限设置

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限

[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

[SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换

[SecretsManager.3] 移除未使用的 Secrets Manager 密钥

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享

[SQS.1] 应对 Amazon SQS 队列进行静态加密

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

[SSM.4] SSM 文档不应公开

[StepFunctions.1] Step Functions 状态机应该开启日志功能

[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

[WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录

[WAF.2] AWS WAF 经典区域规则应至少有一个条件

[WAF.3] AWS WAF 经典区域规则组应至少有一条规则

[WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组

[WAF.6] AWS WAF 经典全局规则应至少有一个条件

[WAF.7] AWS WAF 经典全局规则组应至少有一条规则

[WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

[WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组

[WAF.12] AWS WAF 规则应启用指标 CloudWatch

CIS AWS 基金会基准

互联网安全中心 (CIS) AWS 基金会基准测试是一组安全配置最佳实践 AWS。这些业界认可的最佳实践为您提供了清晰的 step-by-step 实施和评估程序。从操作系统到云服务和网络设备，此基准测试中的控件可帮助您保护组织使用的特定系统。

AWS Security Hub 支持 CIS AWS 基金会基准测试 v3.0.0、1.4.0 和 v1.2.0。

本页列出了每个版本支持的安全控制，并提供了版本对比。

独联体 AWS 基金会基准测试 v3.0.0

Security Hub 支持 CIS AWS 基金会基准测试的 3.0.0 版。

Security Hub 已满足 CIS 安全软件认证的要求，并已根据以下 CIS 基准获得 CIS 安全软件认证：

- CIS AWS 基金会基准测试基准，v3.0.0，第 1 级
- CIS AWS 基金会基准测试基准，v3.0.0，第 2 级

适用于 CIS AWS 基金会基准测试 v3.0.0 的控件

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

[EC2.7] 应启用 EBS 默认加密

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)

[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389

[EC2.53] EC2 安全组不应允许从 0.0.0.0/0 进入远程服务器管理端口

[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.9] 应为根用户启用 MFA

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.18] 确保已创建支持角色来管理事件 AWS Support

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

[IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书

[IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess

[IAM.28] 应启用 IAM 访问分析器外部访问分析器

[KMS.4] 应启用 AWS KMS 密钥轮换

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config

[RDS.3] RDS 数据库实例应启用静态加密

[RDS.13] 应启用 RDS 自动次要版本升级

[S3.1] S3 通用存储桶应启用阻止公共访问设置

[S3.5] S3 通用存储桶应要求请求使用 SSL

[S3.8] S3 通用存储桶应阻止公共访问

[S3.20] S3 通用存储桶应启用 MFA 删除

[S3.22] S3 通用存储桶应记录对象级写入事件

[S3.23] S3 通用存储桶应记录对象级读取事件

独联体 AWS 基金会基准测试 v1.4.0

Security Hub 支持 CIS AWS 基金会基准测试的 v1.4.0。

适用于 CIS AWS 基金会基准测试 v1.4.0 的控件

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

[CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报

[CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报

[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报

[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

[CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报

[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报

[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报

[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报

[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

[EC2.7] 应启用 EBS 默认加密

[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.9] 应为根用户启用 MFA

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.18] 确保已创建支持角色来管理事件 AWS Support

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

[KMS.4] 应启用 AWS KMS 密钥轮换

[RDS.3] RDS 数据库实例应启用静态加密

[S3.1] S3 通用存储桶应启用阻止公共访问设置

[S3.5] S3 通用存储桶应要求请求使用 SSL

[S3.8] S3 通用存储桶应阻止公共访问

[S3.20] S3 通用存储桶应启用 MFA 删除

Center for Internet Security（CIS）AWS 基金会基准 v1.2.0

Security Hub 支持 CIS AWS 基金会基准测试的 1.2.0 版。

Security Hub 已满足 CIS 安全软件认证的要求，并已根据以下 CIS 基准获得 CIS 安全软件认证：

- CIS AWS 基金会基准测试基准，v1.2.0，第 1 级
- CIS AWS 基金会基准测试基准，v1.2.0，第 2 级

适用于 CIS AWS 基金会基准测试 v1.2.0 的控件

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报

[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报

[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

[CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报

[CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报

[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报

[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

[CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报

[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报

[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报

[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报

[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量

[EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.9] 应为根用户启用 MFA

[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母

[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母

[IAM.13] 确保 IAM 密码策略要求包含至少一个符号

[IAM.14] 确保 IAM 密码策略要求包含至少一个数字

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效

[IAM.18] 确保已创建支持角色来管理事件 AWS Support

[KMS.4] 应启用 AWS KMS 密钥轮换

CIS AWS 基金会基准测试的版本比较

本节总结了互联网安全中心 (CIS) AWS 基金会基准测试 v3.0.0、v1.4.0 和 v1.2.0 之间的区别。

Security Hub 支持这些版本的 CIS AWS 基金会基准测试，但我们建议使用 v3.0.0 来了解最新的安全最佳实践。您可以同时启用多个版本的标准。有关更多信息，请参阅 启用和禁用安全标准。如果要升级到 v3.0.0，最好先将其启用，然后再禁用旧版本。如果您使用与 Security Hub 的集成 AWS

Organizations 来集中管理多个账户，AWS 账户 并且想要在所有账户中批量启用 v3.0.0，则可以使用集中配置。

将控件映射到每个版本中的 CIS 要求

了解每个版本的 CIS AWS 基金会基准测试支持的控件。

控件 ID 和标题	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[Account.1] 应为以下人员提供安全联系信息 AWS 账户	1.2	1.2	1.18
[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	3.1	3.1	2.1
[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	3.1	3.1	2.1
[CloudTrail.2] CloudTrail 应该启用静态加密	3.5	3.7	2.7
[CloudTrail.4] 应启用 CloudTrail 日志文件验证	3.2	3.2	2.2
[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成	不支持 — CIS 删除了此要求	3.4	2.4
[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	不支持 — CIS 删除了此要求	3.3	2.3
[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录	3.4	3.6	2.6
[CloudWatch.1] “root” 用户应有日志指标筛选器和警报	不支持-手动检查	4.3	3.3

控件 ID 和标题	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报	不支持-手动检查	不支持-手动检查	3.1
[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报	不支持-手动检查	不支持-手动检查	3.2
[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报	不支持-手动检查	4.4	3.4
[CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报	不支持-手动检查	4.5	3.5
[CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报	不支持-手动检查	4.6	3.6
[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报	不支持-手动检查	4.7	3.7
[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报	不支持-手动检查	4.8	3.8
[CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报	不支持-手动检查	4.9	3.9
[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报	不支持-手动检查	4.10	3.10
[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报	不支持-手动检查	4.11	3.11

控件 ID 和标题	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报	不支持-手动检查	4.12	3.12
[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报	不支持-手动检查	4.13	3.13
[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报	不支持-手动检查	4.14	3.14
AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录	3.3	3.5	2.5
[EC2.2] VPC 默认安全组不应允许入站或出站流量	5.4	5.3	4.3
[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录	3.7	3.9	2.9
[EC2.7] 应启用 EBS 默认加密	2.2.1	2.2.1	不支持
[EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)	5.6	不支持	不支持
[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量	不支持 — 取而代之的是要求 5.2 和 5.3	不支持 — 取而代之的是要求 5.2 和 5.3	4.1
[EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量	不支持 — 取而代之的是要求 5.2 和 5.3	不支持 — 取而代之的是要求 5.2 和 5.3	4.2
[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389	5.1	5.1	不支持
[EC2.53] EC2 安全组不应允许从 0.0.0.0/0 进入远程服务器管理端口	5.2	不支持	不支持

控件 ID 和标题	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口	5.3	不支持	不支持
[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS	2.4.1	不支持	不支持
[IAM.1] IAM policy 不应允许完整的“*”管理权限	不支持	1.16	1.22
[IAM.2] IAM 用户不应附加 IAM policy	1.15	不支持	1.16
[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次	1.14	1.14	1.4
[IAM.4] 不应存在 IAM 根用户访问密钥	1.4	1.4	1.12
[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA	1.10	1.10	1.2
[IAM.6] 应该为根用户启用硬件 MFA	1.6	1.6	1.14
[IAM.8] 应移除未使用的 IAM 用户凭证	不支持 — [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证改为参见	不支持 — [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证改为参见	1.3
[IAM.9] 应为根用户启用 MFA	1.5	1.5	1.13
[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母	不支持 — CIS 删除了此要求	不支持 — CIS 删除了此要求	1.5
[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母	不支持 — CIS 删除了此要求	不支持 — CIS 删除了此要求	1.6

控件 ID 和标题	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[IAM.13] 确保 IAM 密码策略要求包含至少一个符号	不支持 — CIS 删除了此要求	不支持 — CIS 删除了此要求	1.7
[IAM.14] 确保 IAM 密码策略要求包含至少一个数字	不支持 — CIS 删除了此要求	不支持 — CIS 删除了此要求	1.8
[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14	1.8	1.8	1.9
[IAM.16] 确保 IAM 密码策略阻止重复使用密码	1.9	1.9	1.10
[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效	不支持 — CIS 删除了此要求	不支持 — CIS 删除了此要求	1.11
[IAM.18] 确保已创建支持角色来管理事件 AWS Support	1.17	1.17	1.2
[IAM.20] 避免使用根用户	不支持 — CIS 删除了此要求	不支持 — CIS 删除了此要求	1.1
[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证	1.12	1.12	不支持 — CIS 在更高版本中添加了此要求
[IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书	1.19	不支持 — CIS 在更高版本中添加了此要求	不支持 — CIS 在更高版本中添加了此要求
[IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess	1.22	不支持 — CIS 在更高版本中添加了此要求	不支持 — CIS 在更高版本中添加了此要求
[IAM.28] 应启用 IAM 访问分析器外部访问分析器	1.20	不支持 — CIS 在更高版本中添加了此要求	不支持 — CIS 在更高版本中添加了此要求

控件 ID 和标题	CIS v3.0.0 要求	CIS v1.4.0 要求	CIS v1.2.0 要求
[KMS.4] 应启用 AWS KMS 密钥轮换	3.6	3.8	2.8
[Macie.1] 应该启用亚马逊 Macie	不支持-手动检查	不支持 — 手动检查	不支持 — 手动检查
[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config	2.3.3	不支持 — CIS 在更高版本中添加了此要求	不支持 — CIS 在更高版本中添加了此要求
[RDS.3] RDS 数据库实例应启用静态加密	2.3.1	2.3.1	不支持 — CIS 在更高版本中添加了此要求
[RDS.13] 应启用 RDS 自动次要版本升级	2.3.2	不支持 — CIS 在更高版本中添加了此要求	不支持 — CIS 在更高版本中添加了此要求
[S3.1] S3 通用存储桶应启用阻止公共访问设置	2.1.4	2.1.5	不支持 — CIS 在更高版本中添加了此要求
[S3.5] S3 通用存储桶应要求请求使用 SSL	2.1.1	2.1.2	不支持 — CIS 在更高版本中添加了此要求
[S3.8] S3 通用存储桶应阻止公共访问	2.1.4	2.1.5	不支持 — CIS 在更高版本中添加了此要求
[S3.20] S3 通用存储桶应启用 MFA 删除	2.1.2	2.1.3	不支持 — CIS 在更高版本中添加了此要求

独联体 AWS 基金会的 ARN 基准测试

启用一个或多个版本的 CIS AWS Foundations Benchmark 后，您将开始收到 AWS 安全调查结果格式 (ASFF) 中的调查结果。在 ASFF 中，每个版本都使用以下亚马逊资源名称 (ARN)：

独联体 AWS 基金会基准测试 v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

独联体 AWS 基金会基准测试 v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

独联体 AWS 基金会基准测试 v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

您可以使用 Security Hub API 的GetEnabledStandards操作来找出已启用标准的 ARN。

前面的值适用于StandardsArn。但是，StandardsSubscriptionArn是指 Security Hub BatchEnableStandards在您通过调用某个区域来订阅标准时创建的标准订阅资源。

> **Note**
>
> 启用 CIS AWS Foundations Benchmark 版本时，Security Hub 最多可能需要 18 小时才能为使用与其他已启用标准中的已启用控件相同的 AWS Config 服务关联规则的控件生成调查结果。有关更多信息，请参阅 有关运行安全检查的计划。

如果启用合并控制结果，则查找字段会有所不同。有关这些区别的更多信息，请参阅 合并对 ASFF 字段和值的影响。有关样本对照结果，请参阅控件调查发现样本。

Security Hub 不支持的 CIS 要求

如上表所述，Security Hub并不支持每个版本的CIS AWS 基金会基准测试中的所有CIS要求。许多不受支持的要求只能通过查看您的 AWS 资源状态来手动评估。

美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 是由美国商务部下属机构美国国家标准与技术研究院 (NIST) 开发的网络安全和合规框架。此合规性框架可帮助您保护信息系统和关键资源的可用性、机密性和完整性。美国联邦政府机构和承包商必须遵守 NIST SP 800-53 来保护其系统，但私营公司可以自愿将其用作降低网络安全风险的指导框架。

Security Hub 提供支持选定 NIST SP 800-53 要求的控件。这些控件通过自动安全检查进行评估。Security Hub 控件不支持需要手动检查的 NIST SP 800-53 要求。此外，Security Hub 控件仅支持自动化 NIST SP 800-53 要求，这些要求在每个控件的详细信息中列为相关要求。从以下列表中选择一个控件以查看其详细信息。Security Hub 目前不支持控件细节中未提及的相关要求。

与其他框架不同，NIST SP 800-53 没有规定如何评估其需求。相反，该框架提供了指导方针，Security Hub NIST SP 800-53 控件代表了服务对它们的理解。

如果您使用与 Security Hub 的集成 AWS Organizations 来集中管理多个帐户，并且想要在所有账户中批量启用 NIST SP 800-53，则可以从管理员帐户运行 Sec urity Hub 多账户脚本。

有关 NIST SP 800-53 Rev. 5 的更多信息，请参阅 NIST 计算机安全资源中心。

适用于 NNIST SP 800-53 Rev. 5 的控件

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

[账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分

[ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

[ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录

[APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证

[APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能

[APIGateway.4] API Gateway 应与 WAF Web ACL 关联

[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密

[APIGateway.8] API Gateway 路由应指定授权类型

[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

[AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

[AutoScaling.2] Amazon EC2 Auto Scaling 组应覆盖多个可用区

[AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)

[Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址

[AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型

[AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板

[Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密

[CloudFront.1] CloudFront 发行版应配置默认根对象

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

[CloudFront.4] CloudFront 发行版应配置源站故障转移

[CloudFront.5] CloudFront 发行版应启用日志记录

[CloudFront.6] CloudFront 发行版应启用 WAF

[CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书

[CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

[CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

[CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

[CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudWatch.15] CloudWatch 警报应配置指定操作

[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留

[CloudWatch.17] 应激 CloudWatch 活警报动作

[CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

[CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

[DataFirehose.1] Firehose 传输流应在静态状态下进行加密

[DMS.1] Database Migration Service 复制实例不应公开

[DMS.6] DMS 复制实例应启用自动次要版本升级

[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录

[DMS.8] 源数据库的 DMS 复制任务应启用日志记录

[DMS.9] DMS 端点应使用 SSL

[DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权

[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

[DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS

[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密

[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期

[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护

[DynamoDB.1] DynamoDB 表应根据需求自动扩展容量

[DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time

[DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密

[DynamoDB.4] 备份计划中应有 DynamoDB 表

[DynamodB.6] DynamoDB 表应启用删除保护

[DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密

[EC2.1] Amazon EBS 快照不应公开恢复

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.3] 挂载的 Amazon EBS 卷应进行静态加密

[EC2.4] 停止的 EC2 实例应在指定时间段后删除

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

[EC2.7] 应启用 EBS 默认加密

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)

[EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址

[EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点

[EC2.12] 应删除未使用的 Amazon EC2 EIP

[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量

[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址

[EC2.16] 应删除未使用的网络访问控制列表

[EC2.17] Amazon EC2 实例不应使用多个 ENI

[EC2.18] 安全组应只允许授权端口不受限制的传入流量

[EC2.19] 安全组不应允许不受限制地访问高风险端口

[EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态

[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389

[EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求

[EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

[EC2.28] 备份计划应涵盖 EBS 卷

[EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录

[ECR.1] ECR 私有存储库应配置图像扫描

[ECR.2] ECR 私有存储库应配置标签不可变性

[ECR.3] ECR 存储库应至少配置一个生命周期策略

[ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。

[ECS.2] ECS 服务不应自动分配公有 IP 地址

[ECS.3] ECS 任务定义不应共享主机的进程命名空间

[ECS.4] ECS 容器应以非特权身份运行

[ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。

[ECS.8] 密钥不应作为容器环境变量传递

[ECS.9] ECS 任务定义应具有日志配置

[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行

[ECS.12] ECS 集群应该使用容器详情

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

[EFS.2] Amazon EFS 卷应包含在备份计划中

[EFS.3] EFS 接入点应强制使用根目录

[EFS.4] EFS 接入点应强制使用用户身份

[EFS.6] EFS 挂载目标不应与公有子网关联

[EKS.1] EKS 集群端点不应公开访问

[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行

[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

[EKS.8] EKS 集群应启用审核日志记录

[ElastiCache.1] ElastiCache Redis 集群应启用自动备份

[ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级

[ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移

[ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密

[ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密

[ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证

[ElastiCache.7] ElastiCache 群集不应使用默认子网组

[ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

[ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

[ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager

[ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止

[ELB.4] 应将应用程序负载均衡器配置为删除 http 标头

[ELB.5] 应启用应用程序和经典负载均衡器日志记录

[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护

[ELB.7] 经典负载均衡器应启用连接耗尽功能

[ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

[ELB.9] 经典负载均衡器应启用跨区域负载均衡器

[ELB.10] 经典负载均衡器应跨越多个可用区

[ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

[ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式

[ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置

[ES.1] Elasticsearch 域应启用静态加密

[ES.2] Elasticsearch 域名不可供公共访问

[ES.3] Elasticsearch 域应加密节点之间发送的数据

[ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志

[ES.5] Elasticsearch 域名应该启用审核日志

[ES.6] Elasticsearch 域应拥有至少三个数据节点

[ES.7] 应将 Elasticsearch 域配置为至少三个专用的主节点

[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密

[EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

[EventBridge.4] EventBridge 全局端点应启用事件复制

[fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷

[fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份

[GuardDuty.1] GuardDuty 应该启用

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.7] IAM 用户的密码策略应具有可靠的配置

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.9] 应为根用户启用 MFA

[IAM.19] 应为所有 IAM 用户启用 MFA

[IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作

[Kinesis.1] Kinesis 直播应在静态状态下进行加密

[KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作

[KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

AWS KMS keys 不应无意中删除 [KMS.3]

[KMS.4] 应启用 AWS KMS 密钥轮换

[Lambda.1] Lambda 函数策略应禁止公共访问

[Lambda.2] Lambda 函数应使用受支持的运行时系统

[Lambda.3] Lambda 函数应位于 VPC 中

[Lambda.5] VPC Lambda 函数应在多个可用区内运行

[Macie.1] 应该启用亚马逊 Macie

[Macie.2] 应启用 Macie 自动发现敏感数据

[MSK.1] MSK 集群应在代理节点之间传输时进行加密

[MSK.2] MSK 集群应配置增强型监控

[MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch

[MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级

[MQ.5] ActiveMQ 代理应使用主动/备用部署模式

[MQ.6] RabbitMQ 代理应该使用集群部署模式

[Neptune.1] 应对 Neptune 数据库集群进行静态加密

[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

[Neptune.3] Neptune 数据库集群快照不应公开

[Neptune.4] Neptune 数据库集群应启用删除保护

[Neptune.5] Neptune 数据库集群应启用自动备份

[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密

[Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证

[Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照

[Neptune.9] Neptune 数据库集群应跨多个可用区部署

[NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中

[NetworkFirewall.2] 应启用 Network Firewall 日志记录

[NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

[NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包

[NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

[NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

[Opensearch.1] OpenSearch 域名应启用静态加密

[Opensearch.2] OpenSearch 域名不应向公众开放

[Opensearch.3] OpenSearch 域应加密节点之间发送的数据

[Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

[Opensearch.5] OpenSearch 域应启用审核日志

[Opensearch.6] OpenSearch 域名应至少有三个数据节点

[Opensearch.7] OpenSearch 域名应启用精细的访问控制

[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密

[Opensearch.10] OpenSearch 域名应安装最新的软件更新

[Opensearch.11] OpenSearch 域名应至少有三个专用的主节点

[PCA.1] 应禁用 AWS Private CA 根证书颁发机构

[RDS.1] RDS 快照应为私有

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config

[RDS.3] RDS 数据库实例应启用静态加密

[RDS.4] RDS 集群快照和数据库快照应进行静态加密

[RDS.5] RDS 数据库实例应配置多个可用区

[RDS.6] 应为 RDS 数据库实例配置增强监控

[RDS.7] RDS 集群应启用删除保护

[RDS.8] RDS 数据库实例应启用删除保护

[RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch

[RDS.10] 应为 RDS 实例配置 IAM 身份验证

[RDS.11] RDS 实例应启用自动备份

[RDS.12] 应为 RDS 集群配置 IAM 身份验证

[RDS.13] 应启用 RDS 自动次要版本升级

[RDS.14] Amazon Aurora 集群应启用回溯功能

[RDS.15] 应为多个可用区配置 RDS 数据库集群

[RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照

[RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照

[RDS.18] RDS 实例应部署在 VPC 中

[RDS.19] 应为关键集群事件配置现有 RDS 事件通知订阅

[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

[RDS.22] 应为关键数据库安全组事件配置 RDS 事件通知订阅

[RDS.23] RDS 实例不应使用数据库引擎的默认端口

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

[RDS.26] RDS 数据库实例应受备份计划保护

[RDS.27] 应对 RDS 数据库集群进行静态加密

[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch

[RDS.35] RDS 数据库集群应启用自动次要版本升级

[Redshift.1] Amazon Redshift 集群应禁止公共访问

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

[Redshift.3] Amazon Redshift 集群应启用自动快照

[Redshift.4] Amazon Redshift 集群应启用审核日志记录

[Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能

[Redshift.7] Redshift 集群应使用增强型 VPC 路由

[Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名

[Redshift.9] Redshift 集群不应使用默认的数据库名称

[Redshift.10] Redshift 集群应在静态状态下进行加密

[Route53.2] Route 53 公有托管区域应记录 DNS 查询

[S3.1] S3 通用存储桶应启用阻止公共访问设置

[S3.2] S3 通用存储桶应阻止公共读取权限

[S3.3] S3 通用存储桶应阻止公共写入权限

[S3.5] S3 通用存储桶应要求请求使用 SSL

[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户

[S3.7] S3 通用存储桶应使用跨区域复制

[S3.8] S3 通用存储桶应阻止公共访问

[S3.9] S3 通用存储桶应启用服务器访问日志记录

[S3.10] 启用版本控制的 S3 通用存储桶应具有生命周期配置

[S3.11] S3 通用存储桶应启用事件通知

[S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限

[S3.13] S3 通用存储桶应具有生命周期配置

[S3.14] S3 通用存储桶应启用版本控制

[S3.15] S3 通用存储桶应启用对象锁定

[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys

[S3.19] S3 接入点已启用屏蔽公共访问权限设置

[S3.20] S3 通用存储桶应启用 MFA 删除

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限

[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

[SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换

[SecretsManager.3] 移除未使用的 Secrets Manager 密钥

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享

[SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS

[SQS.1] 应对 Amazon SQS 队列进行静态加密

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

[SSM.4] SSM 文档不应公开

[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

[WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录

[WAF.2] AWS WAF 经典区域规则应至少有一个条件

[WAF.3] AWS WAF 经典区域规则组应至少有一条规则

[WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组

[WAF.6] AWS WAF 经典全局规则应至少有一个条件

[WAF.7] AWS WAF 经典全局规则组应至少有一条规则

[WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

[WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组

[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

[WAF.12] AWS WAF 规则应启用指标 CloudWatch

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) 为处理持卡人数据提供了一套 AWS 安全最佳实践。您可以使用此标准来发现处理持卡人数据的资源中的安全漏洞。Security Hub 当前将控制范围限制到账户级别。我们建议您在拥有存储、处理或传输持卡人数据资源的所有账户中启用这些控件。

该标准已通过 AWS 安全保障服务有限责任公司（AWS SAS）的验证，该小组由经过认证的合格安全评估员（QSA）组成，可提供PCI DSS指导和PCI DSS安全标准委员会（PCI SSC）的评估。 AWS SAS 已确认，自动检查可以帮助客户为 PCI DSS 评估做准备。

此页面列出了安全控件 ID 和标题。在 AWS GovCloud (US) Region 和中国区域，使用特定于标准的控件 ID 和标题。有关安全控件 ID 和标题与特定标准的控件 ID 和标题的映射，请参阅 整合如何影响控件 ID 和标题。

适用于 PCI DSS 的控件

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

[CloudTrail.2] CloudTrail 应该启用静态加密

[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

[CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

[DMS.1] Database Migration Service 复制实例不应公开

[EC2.1] Amazon EBS 快照不应公开恢复

[EC2.2] VPC 默认安全组不应允许入站或出站流量

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

[EC2.12] 应删除未使用的 Amazon EC2 EIP

[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

[ES.1] Elasticsearch 域应启用静态加密

[ES.2] Elasticsearch 域名不可供公共访问

[GuardDuty.1] GuardDuty 应该启用

[IAM.1] IAM policy 不应允许完整的“*”管理权限

[IAM.2] IAM 用户不应附加 IAM policy

[IAM.4] 不应存在 IAM 根用户访问密钥

[IAM.6] 应该为根用户启用硬件 MFA

[IAM.8] 应移除未使用的 IAM 用户凭证

[IAM.9] 应为根用户启用 MFA

[IAM.10] IAM 用户的密码策略应该有很长的持续时间 AWS Config

[IAM.19] 应为所有 IAM 用户启用 MFA

[KMS.4] 应启用 AWS KMS 密钥轮换

[Lambda.1] Lambda 函数策略应禁止公共访问

[Lambda.3] Lambda 函数应位于 VPC 中

[Opensearch.1] OpenSearch 域名应启用静态加密

[Opensearch.2] OpenSearch 域名不应向公众开放

[RDS.1] RDS 快照应为私有

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config

[Redshift.1] Amazon Redshift 集群应禁止公共访问

[S3.1] S3 通用存储桶应启用阻止公共访问设置

[S3.2] S3 通用存储桶应阻止公共读取权限

[S3.3] S3 通用存储桶应阻止公共写入权限

[S3.5] S3 通用存储桶应要求请求使用 SSL

[S3.7] S3 通用存储桶应使用跨区域复制

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

AWS 资源标签标准

本节提供有关 AWS 资源标签标准的信息。

> **Note**
>
> AWS 资源标签标准不适用于加拿大西部（卡尔加里）、中国和。 AWS GovCloud (US)

什么是 AWS 资源标签标准？

标签是键和值对，用作组织 AWS 资源的元数据。对于大多数 AWS 资源，您可以选择在创建资源时或创建后添加标签。资源示例包括亚马逊 CloudFront 分配、亚马逊弹性计算云 (Amazon EC2) 实例或中的密钥。 AWS Secrets Manager

标签可帮助您管理、识别、组织、搜索和筛选资源。

每个标签具有两个部分：

- 标签键（例如，`CostCenter`、`Environment` 或 `Project`）。标签键区分大小写。
- 标签值（例如`111122223333`或`Production`）。与标签键一样，标签值区分大小写。

您可使用标签，按用途、所有者、环境或其他标准对资源进行分类。

有关为 AWS 资源添加标签的说明，请参阅 Sec AWS urity Hub 用户指南中的如何向 AWS 资源添加标签。

由 Sec AWS urity Hub 开发的 AWS 资源标签标准可帮助您快速识别是否有任何 AWS 资源缺少标签密钥。您可以自定义`requiredTagKeys`参数以指定控件检查的特定标签密钥。如果未提供特定的标签，则控件只需检查是否存在至少一个标签密钥即可。

启用 AWS 资源标记标准后，您将开始以 AWS 安全调查结果格式 (ASFF) 接收结果。

> **Note**
>
> 启用 AWS 资源标记标准后，Security Hub 最多可能需要 18 小时才能为使用与其他已启用标准中的已启用控件相同的 AWS Config 服务关联规则的控件生成结果。有关更多信息，请参阅 有关运行安全检查的计划。

该标准具有以下亚马逊资源名称 (ARN)：。`arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`

您还可以使用 Security Hub API 的GetEnabledStandards操作来找出已启用标准的 ARN。

AWS 资源标签标准中的控件

AWS 资源标签标准包括以下控件。选择一个控件可查看其详细描述。

- [ACM.3] 应标记 ACM 证书
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.9] CloudTrail 路径应加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [Detective.1] 应标记侦探行为图

- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DynamodB.5] 应标记 DynamoDB 表
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关
- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL
- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应给亚马逊 VPC 加标签
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接进行标记
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.52] 应标记 EC2 传输网关
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [EFS.5] 应标记 EFS 接入点
- [EKS.6] 应标记 EKS 集群

- [EKS.7] 应标记 EKS 身份提供商配置
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.23] 应标记 IAM 访问分析器分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.2] Kinesis 直播应该被标记
- [Lambda.6] 应标记 Lambda 函数
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [Redshift.11] 应该标记 Redshift 集群

- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Route53.1] 应标记 Route53 运行状况检查
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SNS.3] 应标记 SNS 话题
- [SQS.2] 应标记 SQS 队列
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程

服务托管标准

服务管理标准是其他人 AWS 服务 管理的安全标准。例如，服务管理标准： AWS Control Tower是一种管理的服务管理标准。 AWS Control Tower 服务托管标准与 AWS Security Hub 托管的安全标准在以下方面有所不同：

- 标准创建和删除——您可以使用托管服务的控制台或 API 或使用 AWS CLI创建和删除服务托管标准。在您通过其中一种方式在托管服务中创建标准之前，该标准不会出现在 Security Hub 控制台中，也无法通过 Security Hub API 或 AWS CLI进行访问。
- 不自动启用控件——创建服务托管标准时，Security Hub 和管理服务不会自动启用适用于该标准的控件。此外，当 Security Hub 发布标准的新控件时，新控件不会自动启用。这与 Security Hub 托管的标准有所不同。有关在 Security Hub 中配置控件的常用方法的更多信息，请参阅 查看和管理安全控件。
- 启用和禁用控件——我们建议在托管服务中启用和禁用控件，以避免出现偏差。
- 控件的可用性——托管服务选择哪些控件可作为服务托管标准的一部分。可用控件可能包括所有或部分现有的 Security Hub 控件。

管理服务创建服务托管标准并为其提供控件后，您可以在 Security Hub 控制台、Security Hub API 或 AWS CLI中访问控件调查发现、控件状态和标准安全分数。在托管服务中也可能提供部分或全部信息。

从以下列表中选择服务托管标准可查看有关它的更多详细信息。

服务托管标准

- 服务管理标准： AWS Control Tower

服务管理标准： AWS Control Tower

本节提供有关服务管理标准的信息: AWS Control Tower.

什么是服务管理标准： AWS Control Tower？

该标准专为 Sec AWS urity Hub 和 AWS Control Tower. 它允许您在 AWS Control Tower 服务中配置 Security Hub 的主动控制 AWS Control Tower 以及侦探控制。

主动控制有助于确保您 AWS 账户 保持合规性，因为它们会标记可能导致违反策略或配置错误的操作。侦探控件可检测您内部的资源不合规（例如，配置错误）。 AWS 账户通过为您的 AWS 环境启用主动和侦测控制，您可以在不同的开发阶段增强您的安全状况。

> **Tip**
>
> 服务管理标准与 Sec AWS urity Hub 管理的标准不同。例如，您必须在托管服务中创建和删除服务托管标准。有关更多信息，请参阅 服务托管标准。

在 Security Hub 控制台和 API 中，您可以查看服务管理标准： AWS Control Tower 以及其他 Security Hub 标准。

创建标准

仅当您在中创建标准时，该标准才可用 AWS Control Tower。 AWS Control Tower 使用以下方法之一首次启用适用的控件时创建标准：

- AWS Control Tower 控制台
- AWS Control Tower API（调用 `EnableControl`API）
- AWS CLI （运行`enable-control`命令）

Security Hub 控件在 AWS Control Tower 控制台中被标识为 SH。 ***`controlID`***（例如，SH. CodeBuild.1)。

在创建标准时，如果您尚未启用 Security Hub， AWS Control Tower 还会为您启用 Security Hub。

如果您尚未设置 AWS Control Tower，则无法在 Security Hub 控制台、Security Hub API 或中查看或访问此标准 AWS CLI。即使您已经进行了设置 AWS Control Tower，也无法在 Security Hub 中查看或访问此标准，除非先 AWS Control Tower 使用上述方法之一创建该标准。

该标准仅在可用AWS 区域 的地方可 AWS Control Tower 用，包括 AWS GovCloud (US)。

在标准中启用和禁用控件

在 AWS Control Tower 控制台中创建标准后，可以在两个服务中查看该标准及其可用控件。

首次创建标准后，没有任何自动启用的控件。此外，当 Security Hub 添加新控件时，这些控件不会自动启用服务托管标准： AWS Control Tower。您应使用以下方法之一启用和禁用标准中的 AWS Control Tower 控件：

- AWS Control Tower 控制台
- AWS Control Tower API（调用`EnableControl`和 `DisableControl`API）
- AWS CLI（运行`enable-control`和`disable-control`命令）

当您在中更改控件的启用状态时 AWS Control Tower，更改也会反映在 Security Hub 中。

但是，在 Security Hub 中禁用已启用的控件会 AWS Control Tower 导致控制偏差。中的控件状态 AWS Control Tower 显示为`Drifted`。您可以通过在 AWS Control Tower 控制台中选择 “重新注册 OU”，或者 AWS Control Tower 使用上述方法之一禁用并重新启用中的控件来解决这种偏差。

在中完成启用和禁用操作 AWS Control Tower 可帮助您避免控制偏差。

当您在中启用或禁用控件时 AWS Control Tower，该操作将应用于所有账户和区域。如果您在 Security Hub 中启用和禁用控制（不建议用于此标准），则该操作仅适用于当前账户和区域。

> **Note**
>
> 中央配置不能用于管理服务管理标准: AWS Control Tower. 如果您使用中央配置，则只能使用该 AWS Control Tower 服务为集中管理的账户启用和禁用本标准中的控件。

查看启用状态和控件状态

您可以使用以下方法之一查看控件的启用状态：

- Security Hub 控制台、Security Hub API 或 AWS CLI

- AWS Control Tower 控制台
- AWS Control Tower 用于查看已启用控件列表的 API（调用 ListEnabledControlsAPI）
- AWS CLI 查看已启用的控件列表（运行list-enabled-controls命令）

除非您在 Security Hub 中明确启用 AWS Control Tower 该控件，否则您在Disabled中禁用的控件在 Security Hub 中的启用状态为。

Security Hub 根据控件调查发现的工作流程状态和合规性状态来计算控件状态。有关启用状态和控件状态的更多信息，请参阅 查看控件的详细信息。

根据控制状态，Security Hub 计算服务管理标准的安全分数：。 AWS Control Tower此分数仅在 Security Hub 中可用。此外，您只能在 Security Hub 中查看控件调查发现。中没有标准安全评分和控制结果 AWS Control Tower。

> **Note**
>
> 启用服务管理标准:的控件后 AWS Control Tower，Security Hub 最多可能需要 18 小时才能为使用现有 AWS Config 服务关联规则的控件生成调查结果。如果您在 Security Hub 中启用了其他标准和控件，则可能已有与服务相关的规则。有关更多信息，请参阅 有关运行安全检查的计划。

删除标准

您可以使用以下方法之一禁 AWS Control Tower 用所有适用的控件，从而在中删除此标准：

- AWS Control Tower 控制台
- AWS Control Tower API（调用 DisableControlAPI）
- AWS CLI （运行disable-control命令）

禁用所有控件会删除 AWS Control Tower中所有托管账户和受管辖区域中的标准。 AWS Control Tower 删除中的标准会将其从 Security Hub 控制台的 “标准” 页面中删除，并且您无法再使用 Security Hub API 或访问该标准 AWS CLI。

> **Note**
>
> 在 Security Hub 中禁用标准中的所有控件并不能禁用或删除该标准。

禁用 Security Hub 服务会移除服务管理标准： AWS Control Tower 以及您已启用的任何其他标准。

服务管理标准的查找字段格式： AWS Control Tower

创建服务管理标准： AWS Control Tower 并对其启用控制后，您将开始在 Security Hub 中收到控制结果。Security Hub 在 AWS 安全调查结果格式 (ASFF) 中报告控件调查发现。以下是本标准的 Amazon 资源名称（ARN）的 ASFF 值，以及 `GeneratorId`：

- 标准 ARN——*`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

有关服务托管标准:的调查结果示例 AWS Control Tower，请参阅控件调查发现样本。

适用于服务管理标准的控制措施： AWS Control Tower

服务管理标准： AWS Control Tower 支持 AWS 基础安全最佳实践 (FSBP) 标准中的一部分控件。从下表中选择一个控件以查看有关该控件的信息，包括失败的调查发现的补救步骤。

以下列表显示了服务管理标准的可用控件: AWS Control Tower. 对控件的区域限制与 FSBP 标准中对相关控件的区域限制相符。此列表显示了与标准无关的安全控件 ID。在 AWS Control Tower 控制台中，控件 ID 的格式为 SH。 ***`controlID`*** （例如 SH. CodeBuild.1）。在 Security Hub 中，如果在账户中关闭了整合的控件调查发现，则 `ProductFields.ControlId` 字段将使用基于标准的控件 ID。基于标准的对照 ID 的格式为 CT。 ***`ControlId`*** （例如，CT。 CodeBuild.1）。

- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.5] API Gateway REST API 缓存数据应进行静态加密
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证

- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [AutoScaling.2] Amazon EC2 Auto Scaling 组应覆盖多个可用区
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板
- [CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
- [CloudTrail.2] CloudTrail 应该启用静态加密
- [CloudTrail.4] 应启用 CloudTrail 日志文件验证
- [CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.9] DMS 端点应使用 SSL
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [DynamoDB.1] DynamoDB 表应根据需求自动扩展容量
- [DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [EC2.1] Amazon EBS 快照不应公开恢复
- [EC2.2] VPC 默认安全组不应允许入站或出站流量
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
- [EC2.7] 应启用 EBS 默认加密
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)

- [EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址
- [EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.19] 安全组不应允许不受限制地访问高风险端口
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.2] ECS 服务不应自动分配公有 IP 地址
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应该使用容器详情
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移

- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头
- [ELB.5] 应启用应用程序和经典负载均衡器日志记录
- [ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护
- [ELB.7] 经典负载均衡器应启用连接耗尽功能
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.9] 经典负载均衡器应启用跨区域负载均衡器
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [ES.5] Elasticsearch 域名应该启用审核日志
- [ES.6] Elasticsearch 域应拥有至少三个数据节点
- [ES.7] 应将 Elasticsearch 域配置为至少三个专用的主节点
- [ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [GuardDuty.1] GuardDuty 应该启用
- [IAM.1] IAM policy 不应允许完整的“*”管理权限

- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- AWS KMS keys 不应无意中删除 [KMS.3]
- [KMS.4] 应启用 AWS KMS 密钥轮换
- [Lambda.1] Lambda 函数策略应禁止公共访问
- [Lambda.2] Lambda 函数应使用受支持的运行时系统
- [Lambda.3] Lambda 函数应位于 VPC 中
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [RDS.1] RDS 快照应为私有
- [RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config
- [RDS.3] RDS 数据库实例应启用静态加密
- [RDS.4] RDS 集群快照和数据库快照应进行静态加密
- [RDS.5] RDS 数据库实例应配置多个可用区
- [RDS.6] 应为 RDS 数据库实例配置增强监控
- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.11] RDS 实例应启用自动备份
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照
- [RDS.18] RDS 实例应部署在 VPC 中
- [RDS.19] 应为关键集群事件配置现有 RDS 事件通知订阅
- [RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅
- [RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅
- [RDS.22] 应为关键数据库安全组事件配置 RDS 事件通知订阅

- [RDS.23] RDS 实例不应使用数据库引擎的默认端口
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.4] Amazon Redshift 集群应启用审核日志记录
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.9] Redshift 集群不应使用默认的数据库名称
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.2] S3 通用存储桶应阻止公共读取权限
- [S3.3] S3 通用存储桶应阻止公共写入权限
- [S3.5] S3 通用存储桶应要求请求使用 SSL
- [S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.9] S3 通用存储桶应启用服务器访问日志记录
- [S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SecretsManager.1] Secrets Manager 密钥应启用自动轮换
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组

有关此标准的更多信息，请参阅 AWS Control Tower 用户指南中的 Security Hub 控件。

查看和管理安全标准

安全标准包括一组用于确定是否符合监管框架、行业最佳实践或公司政策的要求。 AWS Security Hub 将这些要求映射到控制措施，并对控制措施进行安全检查，以评估是否符合标准的要求。可以在一个或多个标准中启用控件。如果您启用整合的控件调查发现，即使控件属于多个已启用标准，Security Hub 也会为每项安全检查生成一个安全检查。有关更多信息，请参阅 整合的控件调查发现。

有关可用标准和适用于这些标准的控件列表，请参阅 标准参考。Security Hub 控制台上的安全标准页面还显示 Security Hub 中支持的所有安全标准及其启用状态。对于在您的账户中启用的每项安全标准（或者如果您在组织中的至少一个账户中使用与 AWS Organizations集成），您可以查看以下信息：

- 不同 Security Hub 配置策略中标准的启用状态（如果您使用中心配置）
- 对任何禁用标准的描述
- 标准中当前已启用的控件清单，以及这些控件的总体状态（基于其调查发现的合规状态）
- 适用于标准但当前已禁用的控件列表
- 标准的安全评分

Security Hub 为每个标准生成一个安全评分。管理员账户可以查看其成员账户的聚合安全评分和控件状态。如果您设置了聚合区域，则安全分数将反映所有关联区域中控件的合规性状态。有关更多信息，请参阅 安全评分是如何计算的。

主题

- 启用和禁用安全标准

- 查看标准的详细信息
- 在特定标准中启用和禁用控件

启用和禁用安全标准

您可以启用或禁用 Security Hub 中可用的每个安全标准。

在启用任何安全标准之前，请确保已启用 AWS Config 并配置资源记录。否则，Security Hub 可能无法为适用于标准的控件生成调查发现。有关更多信息，请参阅 正在配置 AWS Config。

> **Note**
>
> 启用和禁用标准的说明因您是否使用中心配置而异。本部分介绍其中的区别。集成 Security Hub 和的用户可以使用中央配置 AWS Organizations。我们建议使用中心配置来简化在多账户、多区域环境中启用和禁用标准的过程。

启用安全标准

在启用安全标准时，适用于该标准的所有控件都会在其中自动启用。Security Hub 还将开始为适用于该标准的控件生成调查发现。

然后，您可以选择每个标准中要启用和禁用的控件。禁用控件会阻止生成该控件的调查发现，并且在计算安全分数时会忽略该控件。

启用 Security Hub 后，Security Hub 会在您首次访问 Security Hub 控制台上的摘要页面或安全标准页面后 30 分钟内计算标准的初始安全分数。在中国地区和 AWS GovCloud (US) Region生成首次获得安全评分最多需要 24 小时。仅针对您访问这些页面时启用的标准生成分数。此外，必须配置 AWS Config 资源记录才能显示分数。首次生成分数后，Security Hub 每 24 小时更新一次安全分数。Security Hub 显示时间戳以指示安全评分上次更新的时间。要查看账户中当前启用的标准的列表，请调用 GetEnabledStandards API。

跨多个账户和区域启用标准

要在多个账户和之间启用安全标准 AWS 区域，必须使用集中配置。

使用中心配置时，委托管理员可以创建启用一个或多个标准的 Security Hub 配置策略。然后，您可以将配置策略与特定的账户和组织单元（OU）或根相关联。配置策略在您的主区域（也称为聚合区域）和所有关联区域中生效。

配置策略可自定义。例如，您可以选择在一个 OU 中仅启用 AWS 基础安全最佳实践 (FSBP)，也可以选择在另一个 OU 中启用 FSBP 和互联网安全中心 (CIS) Foundations Benchmark v1. AWS 4.0。有关创建启用了指定标准的配置策略的说明，请参阅创建和关联 Security Hub 配置策略

如果您使用中心配置，Security Hub 不会在新账户或现有账户中自动启用任何标准。相反，在创建配置策略时，委托管理员会定义要在不同账户中启用哪些标准。Security Hub 提供了一种推荐的配置策略，在该策略中仅启用 FSBP。有关更多信息，请参阅 配置策略的类型。

> **Note**
>
> 授权的管理员可以创建配置策略来启用除服务管理标准之外的任何标准： AWS Control Tower。您只能在 AWS Control Tower 服务中启用此标准。如果您使用中心配置，则只能在 AWS Control Tower中为集中管理的账户启用和禁用本标准中的控件。

如果您希望某些账户自行配置标准而不是由委托管理员配置，则委托管理员可以将这些账户指定为自行管理。自行管理账户必须在每个区域单独配置标准。

在单个账户和区域中启用标准

如果您不使用中心配置或者您是自行管理账户，则无法使用配置策略在多个账户和区域中集中启用标准。但是，您可以使用以下步骤在单个账户和区域中启用标准。

Security Hub console

要在一个账户和区域中启用标准

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 确认您正在要启用该标准的区域中使用 Security Hub。
3. 在 Security Hub 导航窗格中，选择安全标准。
4. 对于要启用的标准，请选择 Enable（启用）。这也启用了该标准中的所有控件。
5. 在您要在其中启用标准的每个区域中重复这些步骤。

Security Hub API

要在一个账户和区域中启用标准

1. 调用 BatchEnableStandards API。

2. 提供您要启用的标准的 Amazon 资源名称（ARN）。要获取标准 ARN，请调用 DescribeStandards API。
3. 在您要在其中启用标准的每个区域中重复这些步骤。

AWS CLI

要在一个账户和区域中启用标准

1. 运行 batch-enable-standards 命令。
2. 提供您要启用的标准的 Amazon 资源名称（ARN）。要获取标准 ARN，请运行 describe-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"}'
```

3. 在您要在其中启用标准的每个区域中重复这些步骤。

自动启用默认安全标准

如果您不使用中心配置，Security Hub 会在新账户加入您的组织时自动启用默认安全标准。作为默认标准一部分的所有控件也会自动启用。当前，自动启用的默认安全标准是 AWS 基础安全最佳实践 (FSBP) 和互联网安全中心 (CIS) AWS 基金会基准 v1.2.0。如果您希望在新账户中手动启用标准，您可以关闭自动启用的标准。

如果您使用中心配置，则可以创建启用默认标准的配置策略并将此策略与根相关联。您的所有组织账户和 OU 都将继承此配置策略，除非它们与其他策略关联，或是自行管理账户。

关闭自动启用的标准

以下步骤仅在与中央配置集成 AWS Organizations 但不使用中央配置时适用。如果您不使用 Organizations 集成，则可以在首次启用 Security Hub 时关闭默认标准，也可以按照禁用标准的步骤操作。

Security Hub console

关闭自动启用的标准

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用管理员账户的凭证登录。
2. 在 Security Hub 导航窗格中的设置下，选择配置。
3. 在账户部分中，关闭自动启用默认标准。

Security Hub API

关闭自动启用的标准

1. 通过 Security Hub 管理员账户调用 UpdateOrganizationConfiguration API。
2. 要在新成员账户中关闭自动启用的标准，将 `AutoEnableStandards` 的值设置为 `NONE`。

AWS CLI

关闭自动启用的标准

1. 运行 update-organization-configuration 命令。
2. 包括用于在新成员账户中关闭自动启用的标准的 `auto-enable-standards` 参数。

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

禁用安全标准

在 Security Hub 中禁用安全标准时，会发生以下情况：

- 适用于该标准的所有控件也将被禁用，除非它们与另一个标准关联。
- 不再执行对禁用控件的检查，并且不会为禁用控件生成其他结果。
- 已禁用控件的现有调查发现将在大约 3-5 天后自动存档。
- Security Hub 为禁用的控件创建的 AWS Config 规则已删除。

  这通常会在您禁用标准后的几分钟内发生，但可能需要更长的时间。如果删除规则的第一个请求失败， AWS Config 则 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，那么 Security Hub 将无法重试该请求，这意味着它无法删除 AWS Config 规则。如果发生这种情况，并且您需要删除 AWS Config 规则，请联系 AWS Support。

在多个账户和区域中禁用标准

要在多个账户和区域禁用安全标准，必须使用中心配置。

使用中心配置时，委托管理员可以创建禁用一个或多个标准的配置策略。您可以将配置策略与特定账户和 OU 或根相关联。配置策略在您的主区域（也称为聚合区域）和所有关联区域中生效。

配置策略可自定义。例如，您可以选择在一个 OU 中禁用支付卡行业数据安全标准（PCI DSS），也可以选择在另一个 OU 中禁用 PCI DSS 和美国国家标准与技术研究所（NIST）SP 800-53 Rev. 5。有关创建禁用指定标准的配置策略的说明，请参阅创建和关联 Security Hub 配置策略。

> **Note**
>
> 授权的管理员可以创建配置策略来禁用除服务管理标准之外的任何标准: AWS Control Tower。您只能在 AWS Control Tower 服务中禁用此标准。如果您使用中心配置，则只能在 AWS Control Tower中为集中管理的账户启用和禁用本标准中的控件。

如果您希望某些账户自行配置标准而不是由委托管理员配置，则委托管理员可以将这些账户指定为自行管理。自行管理账户必须在每个区域单独配置标准。

在单个账户和区域中禁用标准

如果您不使用中心配置或您是自行管理账户，则无法使用配置策略在多个账户和区域中集中禁用标准。但是，您可以使用以下步骤在单个账户和区域中禁用标准。

Security Hub console

在一个账户和区域中禁用标准

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 确认您正在要禁用该标准的区域中使用 Security Hub。
3. 在 Security Hub 导航窗格中，选择安全标准。
4. 对于要禁用的标准，请选择 Disable（禁用）。
5. 在您要禁用标准的每个区域中重复此操作。

Security Hub API

在一个账户和区域中禁用标准

1. 调用 BatchDisableStandards API。
2. 对于您要禁用的每个标准，请提供标准订阅 ARN。要获取已启用标准的订阅 ARN，请调用 GetEnabledStandards API。
3. 在您要禁用标准的每个区域中重复此操作。

AWS CLI

在一个账户和区域中禁用标准

1. 运行 batch-disable-standards 命令。
2. 对于您要禁用的每个标准，请提供标准订阅 ARN。要获取已启用标准的订阅 ARN，请运行 get-enabled-standards 命令。

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard
 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"
```

3. 在您要禁用标准的每个区域中重复此操作。

查看标准的详细信息

在 AWS Security Hub 控制台上，标准的详细信息页面包含以下信息：

- 标准安全评分和标准中启用的控件安全检查的视觉摘要 如果您与集成 AWS Organizations，则在至少一个组织账户中启用的控件将被视为已启用。
- 启用或禁用适用于标准的控件的设置
- 适用于该标准的控件列表。根据启用状态，控件分为不同的选项卡。全部启用列中的控件数是失败、未知、无数据和通过列中控件的总和。

您还可以使用 Security Hub API 和 AWS CLI 来检索标准的详细信息。以下部分说明如何获取标准的详细信息。

显示已启用标准的详细信息页面（控制台）

在安全标准页面上，您可以显示已启用标准的详细信息页面。

如果您以管理员账户登录，则可以查看至少一个成员账户中启用的任何标准的详细信息。

1. 打开 AWS Security Hub 控制台，网址为 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。

标准安全评分和安全检查摘要

标准详细信息页面的顶部是标准的安全评分。分数是通过的控件相对于标准启用的控件（具有数据）数量的百分比。

Security Hub 通常会在您首次访问 Security Hub 控制台上的摘要页面或安全标准页面后 30 分钟内计算出初始安全分数。仅针对您访问这些页面时启用的标准生成分数。要查看当前启用的标准列表，请使用 `GetEnabledStandards` API 操作。此外，必须配置 AWS Config 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 显示时间戳以指示安全评分上次更新的时间。有关更多信息，请参阅 the section called “确定安全分数”。

> **Note**
>
> 在中国地区和 AWS GovCloud (US) Region生成首次获得安全评分最多需要 24 小时。

分数旁边是一个图表，该图表汇总了针对该标准启用的控件的安全检查。该图表显示了未通过和通过安全检查的百分比。当您在图表上停下来时，弹出窗口会显示以下内容：

- 每种严重性的控件的安全检查失败次数
- 状态为未知的控件的安全检查数量
- 已通过安全检查的数量

对于管理员账户，标准分数和图表是在跨管理员账户和所有成员账户之间汇总的。

除非您设置了聚合区域，否则安全标准详细信息页面上的所有数据都特定于当前区域。如果您设置了聚合区域，则安全分数适用于各个区域，并包括所有关联区域的调查发现。标准详细信息页面上控件的合规性状态也反映了来自关联区域的调查发现，安全检查的数量包括来自关联区域的调查发现。

查看已启用的标准中的控件

当您访问标准的详细信息页面时，可以查看适用于该标准的安全控件列表。此列表根据控件的合规性状态和分配给每个控件的严重性进行排序。Security Hub 每 24 小时更新一次控件状态和安全检查计数。每个选项卡上的时间戳表示控件状态和安全检查计数最近更新的时间。有关更多信息，请参阅 the section called “合规状态和控制状态”。

对于管理员账户，控制合规性状态和安全检查数量是在管理员账户和所有成员账户之间汇总的。

全部启用选项卡列出了标准中当前启用的所有控件。对于管理员账户，全部启用选项卡包括标准中在其账户或至少一个成员账户中启用的控件。

在失败、未知、无数据和通过选项卡上，全部启用选项卡中的控件经过筛选，仅包括具有特定状态的已启用控件。

已禁用选项卡包含标准中禁用的控件列表。对于管理员账户，已禁用选项卡包括标准中在其账户和所有成员账户中禁用的控件。

对于每个控件，选项卡显示以下信息：

- 控件的状态（请参阅 the section called “合规状态和控制状态”）
- 分配给控件的严重性等级
- 控件 ID 和标题
- 活跃结果总数中失败的活跃结果数。如果适用，检查失败列还会列出状态为未知的调查发现数量。

除了每个选项卡上的搜索筛选条件外，您还可以根据以下字段对列表进行排序：

- Compliance Status
- 严重性
- ID
- 标题
- 检查失败

您可以使用任何列对每个列表进行排序。默认情况下，会对全部启用选项卡进行排序，使失败的控件位于列表的顶部。这可以帮助您立即关注需要修复的问题。

在其余选项卡上，控件默认按严重性降序排序。换句话说，首先是严重的控件，然后是高等级的控件，接着是中等级的控件，最后是低等级的控件。

选择您首选的访问方法，然后按照步骤显示已启用标准的可用控件。您也可以使用 DescribeStandardsControlAPI 操作来代替这些说明。

Security Hub console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中选择安全标准。
3. 对于标准，选择查看结果。页面底部列出了适用于该标准的控件（按选项卡划分）。

Security Hub API

1. 运行 ListSecurityControlDefinitions 并提供标准的 Amazon 资源名称（ARN）以获取该标准的控件 ID 列表。要获取标准 ARN，请运行 DescribeStandards。如果您不提供标准 ARN，此 API 将返回所有 Security Hub 控制 ID。此 API 返回与标准无关的安全控件 ID，而不是特定于标准的控件 ID。

   请求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 运行 ListStandardsControlAssociations 以查看您在账户中启用的每个标准中是否都启用了控件。
3. 通过提供 SecurityControlId 或 SecurityControlArn 来识别控件。分页参数是可选的。

   请求示例：

   ```
   {
       SecurityControlId: Config.1
       NextToken: lkeyusdlk-sdlflsnd-ladfterb
       MaxResults: 5
   ```

```
}
```

AWS CLI

1. 运行 list-security-control-definitions 命令，并提供一个或多个标准 ARN 以获取控件 ID 列表。要获取标准 ARN，请运行 describe-standards 命令。如果您不提供标准 ARN，则此命令会返回所有 Security Hub 控件 ID。此命令返回与标准无关的安全控件 ID，而不是特定于标准的控件 ID。

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --
   standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0"
   ```

2. 运行 list-standards-control-associations 命令以了解您在账户中启用的每个标准中是否启用了控件。

3. 通过提供 security-control-id 或 security-control-arn 来识别控件。

   命令示例：

   ```
   aws securityhub --region us-east-1 list-standards-control-associations --
   security-control-id Config.1
   ```

正在下载控件列表

您可以将控件列表的当前页面下载到 .csv 文件中。

如果您筛选了控件列表，则下载的文件仅包含与筛选条件设置匹配的控件。

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。

要下载控件列表的当前页面或当前选定的控件，请选择下载。

在特定标准中启用和禁用控件

当您在中启用标准时 AWS Security Hub，适用于该标准的所有控件都会自动启用该标准中的所有控件（服务管理标准除外）。然后，您可以禁用并重新启用标准中的特定控件。但是，我们建议您在所有已启用的标准中调整控件的启用状态。

> **Note**
>
> 如果您使用 Security Hub 中心配置，则委托管理员可以在所有已启用的标准下启用和禁用针对组织账户的控件。我们建议采用这种方法，以便控件的启用状态在不同标准之间保持一致。但是，委托管理员可以将账户指定为自行管理，这意味着这些账户能够自行启用和禁用特定标准中的控件。有关更多信息，请参阅 中央配置的工作原理。

标准的详细信息页面包含该标准的适用控件列表，以及有关该标准当前启用和禁用哪些控件的信息。

在标准详细信息页面上，您还可以启用和禁用特定标准中的控件。您必须在每个 AWS 账户 和中分别启用和禁用控件 AWS 区域。当您启用或禁用控件时，它只会影响当前账户和区域。

您可以使用 Security Hub 控制台、Security Hub API 或在每个区域启用和禁用控件 AWS CLI。如果您设置了聚合区域，您将看到来自所有关联区域的控件。如果某个控件在关联区域中可用，但在聚合区域中不可用，则无法在聚合区域启用或禁用该控件。有关多账户和多区域控件禁用脚本，请参阅在多账户环境中禁用 Security Hub 控件。

启用特定标准中的控件

要启用标准中的控件，您必须首先启用至少一个该控件适用的标准。有关启用标准的更多信息，请参阅 启用和禁用安全标准。当您在标准中启用控件时， AWS Security Hub 会开始生成该控件的结果。Security Hub 还在总体安全分数和标准安全分数的计算中包括控件状态。即使您在多个标准中启用了控件，但如果您开启整合的控件调查发现，您也将收到一个各类标准的安全检查调查发现。有关更多信息，请参阅 Consolidated control findings。

要启用标准中的控件，该控件必须在您当前的区域中可用。有关更多信息，请参阅根据区域的控件可用性。

请按照以下步骤启用特定标准中的 Security Hub 控件。除了以下步骤之外，您还可以使用 `UpdateStandardsControl` API 操作来启用特定标准中的控件。有关在所有标准中启用控件的说明，请参阅 在单个账户和区域中启用所有标准的控件。

Security Hub console

要启用特定标准中的控件

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 从导航窗格中选择安全标准。

3. 对于相关标准，选择查看结果。
4. 选择控件。
5. 选择启用控制（对于已启用的控件，此选项不会出现）。选择启用进行确认。

Security Hub API

要启用特定标准中的控件

1. 运行 ListSecurityControlDefinitions 并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 DescribeStandards。此 API 返回与标准无关的安全控件 ID，而不是特定于标准的控件 ID。

   请求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 运行 ListStandardsControlAssociations，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

   请求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. 运行 BatchUpdateStandardsControlAssociations。提供您想要在其中启用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 ENABLED。

   请求示例：

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
   }
   ```

AWS CLI

要启用特定标准中的控件

1. 运行 list-security-control-definitions 命令并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 describe-standards。此命令返回与标准无关的安全控件 ID，而不是特定于标准的控件 ID。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. 运行 list-standards-control-associations 命令，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. 运行 batch-update-standards-control-associations 命令。提供您想要在其中启用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 ENABLED。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

禁用特定标准中的控件

当您在标准中禁用某个控件时，Security Hub 将停止为该控件生成调查发现。控件状态不再用于计算标准的安全评分。

禁用控件的一种方法是禁用该控件适用的所有标准。禁用标准时，所有适用于该标准的控件都将被禁用（但是，这些控件在其他标准中可能仍处于启用状态）。有关禁用标准的信息，请参阅 the section called “启用和禁用标准”。

当您通过禁用某个控件所适用的标准来禁用该控件时，会发生以下情况：

- 不再针对该标准执行控件的安全检查。这意味着控件状态不会影响标准安全分数（如果在其他标准中启用了控件，Security Hub 将继续运行控件的安全检查）。
- 不会为该控制生成任何其他结果。
- 现有调查发现将在 3-5 天后自动存档（请注意，这是尽最大努力的结果且无法保证）。
- Security Hub 创建的相关 AWS Config 规则已删除。

当您禁用标准时，Security Hub 不会跟踪哪些控件被禁用。如果您随后再次启用该标准，则所有适用于该标准的控件都会自动启用。此外，禁用控件是一次性操作。假设您禁用一个控件，然后启用一个先前禁用的标准。如果标准包含该控件，它将在该标准中启用。当您在 Security Hub 中启用标准时，适用于该标准的所有控件都会自动启用。

您可以仅在一个或多个特定标准中禁用该控件，而不是通过禁用该控件适用的标准来禁用该控件。

为了减少调查发现噪音，禁用与环境无关的控件可能会很有用。有关禁用哪些控件的建议，请参阅[您可能希望禁用的 Security Hub 控件]。

按照以下步骤禁用特定标准中的控件。除了以下步骤之外，您还可以使用 `UpdateStandardsControl` API 操作来禁用特定标准中的控件。有关在所有标准中禁用控件的说明，请参阅 [在所有标准中启用和禁用控件]。

Security Hub console

要禁用特定标准中的控件

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 从导航窗格中选择安全标准。对于相关标准，选择查看结果。
3. 选择控件。
4. 选择禁用控制（对于已禁用的控件，此选项不会出现）。
5. 提供禁用控件的原因，然后选择禁用进行确认。

Security Hub API

要禁用特定标准中的控件

1. 运行 `ListSecurityControlDefinitions` 并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 `DescribeStandards`。此 API 返回与标准无关的安全控件 ID，而不是特定于标准的控件 ID。

请求示例：

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. 运行 ListStandardsControlAssociations，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

   请求示例：

```
{
    "SecurityControlId": "IAM.1"
}
```

3. 运行 BatchUpdateStandardsControlAssociations。提供您要在其中禁用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已禁用的控件执行以下步骤，API 将返回 HTTP 状态代码 200 响应。

   请求示例：

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to environment"}]
}
```

AWS CLI

要禁用特定标准中的控件

1. 运行 list-security-control-definitions 命令并提供标准 ARN 以获取特定标准的可用控件列表。要获取标准 ARN，请运行 describe-standards。此命令返回与标准无关的安全控件 ID，而不是特定于标准的控件 ID。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. 运行 list-standards-control-associations 命令，并提供特定的控件 ID 以返回每个标准中控件的当前启用状态。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. 运行 batch-update-standards-control-associations 命令。提供您要在其中禁用控件的标准的 ARN。
4. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已启用的控件执行这些步骤，该命令将返回 HTTP 状态代码 200 响应。

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Security Hub 控件参考

此控件参考提供了可用 AWS Security Hub 控件的列表，以及指向有关每个控件的更多信息的链接。概览表按控件 ID 按字母顺序显示控件。此处仅包含 Security Hub 正在使用的控件。已停用的控件不在此列表中。该表提供了每个控件的以下信息：

- 安全控制 ID — 此 ID 适用于所有标准，并表示该控件所涉及的 AWS 服务 和资源。无论账户中开启还是关闭了整合的控件调查发现，Security Hub 控制台都会显示安全控件 ID。但是，只有在账户中启用了整合的控件调查发现时，Security Hub 的调查发现才会引用安全控件 ID。如果在账户中关闭了整合的控件调查发现，则控件调查发现中的某些控件 ID 可能会因标准而异。有关特定于标准的控件 ID 与安全控件 ID 的映射，请参阅 整合如何影响控件 ID 和标题。

  如果您想为安全控件设置自动化，我们建议您根据控件 ID 而不是标题或描述进行筛选。尽管 Security Hub 偶尔会更新控件标题或描述，但控件 ID 保持不变。

  控件 ID 可能会跳过数字。这些是未来控件的占位符。

- 适用标准——指明控件适用于哪些标准。选择一个控件以查看第三方合规性框架的具体要求。
- 安全控件标题——此标题适用于各类标准。无论账户中开启还是关闭了整合的控件调查发现，Security Hub 控制台都会显示安全控件标题。但是，只有在账户中启用了整合的控件调查发现时，Security Hub 的调查发现才会引用安全控件标题。如果在账户中关闭了整合的控件调查发现，则控件调查发现中的某些控件标题可能会因标准而异。有关特定于标准的控件 ID 与安全控件 ID 的映射，请参阅 整合如何影响控件 ID 和标题。
- 严重性——从安全角度来看，控制的严重性确定了其重要性。有关 Security Hub 如何确定控制严重性的信息，请参阅 为控件调查发现分配严重性。
- 计划类型——指明何时评估控件。有关更多信息，请参阅 有关运行安全检查的计划。
- 支持自定义参数-指示控件是否支持一个或多个参数的自定义值。选择一个控件以查看参数的详细信息。有关更多信息，请参阅 自定义控制参数。

选择一个控件以查看更多详细信息。控件按服务名称的字母顺序列出。

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Account.1	应为以下人员提供安全联系信息 AWS 账户	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	定期
Account.2	AWS 账户 应该是 AWS Organizations 组织的一部分	NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期
ACM.1	导入的证书和 ACM 颁发的证书应在指定时间段后更新	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发且定期进行

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ACM.2	由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度	AWS 基础安全最佳实践 v1.0.0	HIGH（高）	 否	变更已触发
ACM.3	应标记 ACM 证书	AWS 资源标签标准	低	是	变更已触发
APIGateway.1	应启用 API Gateway REST 和 WebSocket API 执行日志记录	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
APIGateway.2	API Gateway REST API 阶段应配置为使用 SSL 证书进行后端身份验证	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
APIGateway.3	API Gateway REST API 阶段应启用 AWS X-Ray 跟踪	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
APIGateway.4	API Gateway 应与 WAF Web ACL 关联	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
APIGateway.5	API Gateway REST API 缓存数据应静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
APIGateway.8	API Gateway 路由应指定授权类型	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	定期
APIGateway.9	应为 API Gateway V2 阶段配置访问日志记录	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
AppSync.2	AWS AppSync 应该启用字段级日志记录	AWS 基础安全最佳实践 v1.0.0	中	 是	变更已触发
AppSync.4	AWS AppSync 应标记 GraphQL API	AWS 资源标签标准	低	是	变更已触发
AppSync.5	AWS AppSync 不应使用 API 密钥对 GraphQL API 进行身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
雅典娜.2	应标记 Athena 数据目录	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
雅典娜.3	应标记 Athena 工作组	AWS 资源标签标准	低	是	变更已触发
AutoScaling.1	与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查	AWS 基础安全最佳实践，服务管理标准：，PCI DSS v3.2.1 AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
AutoScaling.2	Amazon EC2 自动扩缩组应覆盖多个可用区	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
AutoScaling.3	自动扩缩组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (IMDSv2)	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
Autoscaling.5	使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
AutoScaling.6	自动扩缩组组应在多个可用区中使用多种实例类型	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
AutoScaling.9	EC2 自动扩缩组应使用 EC2 启动模板	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
AutoScaling.10	应标记 EC2 Auto Scaling 群组	AWS 资源标签标准	低	是	变更已触发
Backup.1	AWS Backup 恢复点应在静态状态下进行加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Backup.2	AWS Backup 应标记恢复点	AWS 资源标签标准	低	是	变更已触发
备份。3	AWS Backup 应给保管库加标签	AWS 资源标签标准	低	是	变更已触发
备份。4	AWS Backup 报告计划应加标签	AWS 资源标签标准	低	是	变更已触发
备份。5	AWS Backup 应标记备份计划	AWS 资源标签标准	低	是	变更已触发
CloudFormation.2	CloudFormation 堆栈应该加标签	AWS 资源标签标准	低	 是	变更已触发
CloudFront.1	CloudFront 发行版应配置默认根对象	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudFront.3	CloudFront 发行版在传输过程中应要求加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
CloudFront.4	CloudFront 发行版应配置源站故障转移	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	 否	变更已触发
CloudFront.5	CloudFront 发行版应该启用日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
CloudFront.6	CloudFront 发行版应启用 WAF	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
CloudFront.7	CloudFront 发行版应使用自定义 SSL/TLS 证书	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
CloudFront.8	CloudFront 发行版应使用 SNI 来处理 HTTPS 请求	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	 否	变更已触发
CloudFront.9	CloudFront 发行版应加密发往自定义来源的流量	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudFront.10	CloudFront 发行版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
CloudFront.12	CloudFront 发行版不应指向不存在的 S3 来源	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期
CloudFront.13	CloudFront 发行版应使用源站访问控制	AWS 基础安全最佳实践 v1.0.0	中	 否	变更已触发
CloudFront.14	CloudFront 应该给发行版加标签	AWS 资源标签标准	低	是	变更已触发
CloudTrail.1	CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	CIS AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1.4.0、AWS 基础安全最佳实践 v1.0.0、服务管理标准：，NIST SP 800-53 修订版 5 AWS Control Tower	HIGH（高）	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudTrail.2	CloudTrail 应该启用静态加密	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIST SP 800-53 修订版 5 AWS	中	 否	定期
CloudTrail.3	至少应启用一条 CloudTrail 跟踪	PCI DSS v3.2.1	HIGH（高）	 否	定期
CloudTrail.4	CloudTrail 应启用日志文件验证	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIST SP 800-53 修订版 5 AWS	低	 否	定期
CloudTrail.5	CloudTrail 应将跟踪与 Amazon CloudWatch 日志集成	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIST SP 800-53 修订版 5 AWS	低	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudTrail.6	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	关键	否	变更已触发且定期进行
CloudTrail.7	确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	否	定期
CloudTrail.9	CloudTrail 路径应该被标记	AWS 资源标签标准	低	是	变更已触发
CloudWatch.1	应具有有关“根”用户使用的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0、PCI DSS v3.2.1、CIS 基金会基准 v1.4.0 AWS	低	否	定期
CloudWatch.2	确保存在关于未经授权的 API 调用的日志指标筛选条件和警报	独联体 AWS 基金会基准测试 v1.2.0	低	否	定期
CloudWatch.3	确保存在关于无 MFA 的管理控制台登录的日志指标筛选条件和警报	独联体 AWS 基金会基准测试 v1.2.0	低	否	定期
CloudWatch.4	确保存在关于 IAM 策略更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudWatch.5	确保存在 CloudTrail 配置更改的日志指标筛选器和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.6	确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.7	确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.8	确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.9	确保存在 AWS Config 配置更改的日志指标筛选器和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.10	确保存在关于安全组更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.11	确保存在关于网络访问控制列表 (NACL) 更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CloudWatch.12	确保存在关于网络网关更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.13	确保存在关于路由表更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.14	确保存在关于 VPC 更改的日志指标筛选条件和警报	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
CloudWatch.15	CloudWatch 警报应配置指定的操作	NIST SP 800-53 Rev. 5	HIGH（高）	 是	变更已触发
CloudWatch.16	CloudWatch 日志组应在指定的时间段内保留	NIST SP 800-53 Rev. 5	中	 是	定期
CloudWatch.17	CloudWatch 应启用警报操作	NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
CodeArtifact.1	CodeArtifact 存储库应该被标记	AWS 资源标签标准	低	 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
CodeBuild.1	CodeBuild Bitbucket 源存储库网址不应包含敏感凭据	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	变更已触发
CodeBuild.2	CodeBuild 项目环境变量不应包含明文凭证	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	变更已触发
CodeBuild.3	CodeBuild 应对 S3 日志进行加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
CodeBuild.4	CodeBuild 项目环境应该有日志配置	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Config.1	AWS Config 应该启用并使用服务相关角色进行资源记录	CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准 v1.2.0、AWS 基础安全最佳实践、NIST SP 800-53 修订版 5、PCI DSS v3.2.1	中	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DataFirehose.1	Firehose 传输流应在静态状态下进行加密	AWS 基础安全最佳实践 NIST SP 800-53 修订版 5	中	 否	定期
侦探。1	应标记 Detective 行为图	AWS 资源标签标准	低	是	变更已触发
DMS.1	Database Migration Service 复制实例不应公开	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	定期
DMS.2	应标记 DMS 证书	AWS 资源标签标准	低	是	变更已触发
DMS.3	应标记 DMS 活动订阅	AWS 资源标签标准	低	是	变更已触发
DMS.4	应标记 DMS 复制实例	AWS 资源标签标准	低	是	变更已触发
DMS.5	应标记 DMS 复制子网组	AWS 资源标签标准	低	是	变更已触发
DMS.6	DMS 复制实例应启用自动次要版本升级	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DMS.7	目标数据库的 DMS 复制任务应启用日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DMS.8	源数据库的 DMS 复制任务应启用日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DMS.9	DMS 端点应使用 SSL	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DMS.10	Neptune 数据库的 DMS 终端节点应启用 IAM 授权	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	 否	变更已触发
DMS.11	MongoDB 的 DMS 端点应启用身份验证机制	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	 否	变更已触发
DMS.12	适用于 Redis 的 DMS 终端节点应启用 TLS	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DocumentDB.1	Amazon DocumentDB 集群应进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 否	变更已触发
DocumentDB.2	Amazon DocumentDB 集群应有足够的备份保留期	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 是	变更已触发
DocumentDB.3	Amazon DocumentDB 手动集群快照不应公开	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	关键	 否	变更已触发
DocumentDB.4	Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DocumentDB.5	Amazon DocumentDB 集群应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DynamoDB.1	DynamoDB 表应根据需求自动扩展容量	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
DynamoDB 2	DynamoDB 表应该启用恢复功能 point-in-time	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DynamoDB 3	DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
DynamoDB 4	备份计划中应有 DynamoDB 表	NIST SP 800-53 Rev. 5	中	 是	定期
DynamodB 5	应标记 DynamoDB 表	AWS 资源标签标准	低	是	变更已触发
DynamodB 6	DynamoDB 表应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
DynamodB 7	DynamoDB 加速器集群应在传输过程中进行加密	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.1	不应公开还原 EBS 快照	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	定期
EC2.2	VPC 默认安全组不应允许入站或出站流量	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIS T SP 800-53 修订版 5 AWS	HIGH（高）	 否	变更已触发
EC2.3	挂载的 EBS 卷应进行静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
EC2.4	停止的 EC2 实例应在指定时间段后删除	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.6	应在所有 VPC 中启用 VPC 流日志记录	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIS T SP 800-53 修订版 5 AWS	中	 否	定期
EC2.7	EBS 默认加密应该为已启用。	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，CIS Foundations Benchmark v1.4.0 AWS Control Tower，NIST SP 8 AWS 00-53 Rev. 5	中	 否	定期
EC2.8	EC2 实例应使用实例元数据服务版本 2 (IMDSv2)	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
EC2.9	EC2 实例不应拥有公有 IPv4 地址	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.10	应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	定期
EC2.12	应删除未使用的 EC2 EIP	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	否	变更已触发
EC2.13	安全组不应允许从 0.0.0.0/0 或:: /0 进入端口 22	CIS F AWS oundations Benchmark v1.2.0、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	HIGH（高）	否	变更已触发
EC2.14	安全组不应允许从 0.0.0.0/0 或:: /0 进入端口 3389	独联体 AWS 基金会基准测试 v1.2.0	HIGH（高）	否	变更已触发
EC2.15	EC2 子网不应自动分配公有 IP 地址	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发
EC2.16	应删除未使用的网络访问控制列表	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.17	EC2 实例不应使用多个 ENI	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
EC2.18	安全组应仅允许授权端口不受限制的传入流量	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 是	变更已触发
EC2.19	安全组不应允许无限制地访问高风险端口	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	关键	 否	变更已触发
EC2.20	AWS 站点到站点 VPN 连接的两个 VPN 隧道都应处于开启状态	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
EC2.21	网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389	AWS 基础安全最佳实践 v1.0.0，服务管理标准： ，CIS Foundations Benchmark v1.4.0 AWS Control Tower，NIST SP 8 AWS 00-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.22	应删除未使用的 EC2 安全组	服务管理标准： AWS Control Tower	中	 否	定期
EC2.23	EC2 中转网关不应自动接受 VPC 附件请求	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
EC2.24	不应使用 EC2 半虚拟化实例类型	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
EC2.25	EC2 启动模板不应将公共 IP 分配给网络接口	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
EC2.28	EBS 卷应包含在备份计划中	NIST SP 800-53 Rev. 5	低	 是	定期
EC2.33	应标记 EC2 传输网关附件	AWS 资源标签标准	低	是	变更已触发
EC2.34	应标记 EC2 传输网关路由表	AWS 资源标签标准	低	是	变更已触发
EC2.35	应标记 EC2 网络接口	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.36	应标记 EC2 客户网关	AWS 资源标签标准	低	是	变更已触发
EC2.37	应标记 EC2 弹性 IP 地址	AWS 资源标签标准	低	是	变更已触发
EC2.38	应标记 EC2 实例	AWS 资源标签标准	低	是	变更已触发
EC2.39	应标记 EC2 互联网网关	AWS 资源标签标准	低	是	变更已触发
EC2.40	应标记 EC2 NAT 网关	AWS 资源标签标准	低	是	变更已触发
EC2.41	应标记 EC2 网络 ACL	AWS 资源标签标准	低	是	变更已触发
EC2.42	应标记 EC2 路由表	AWS 资源标签标准	低	是	变更已触发
EC2.43	应标记 EC2 安全组	AWS 资源标签标准	低	是	变更已触发
EC2.44	应标记 EC2 子网	AWS 资源标签标准	低	是	变更已触发
EC2.45	应标记 EC2 卷	AWS 资源标签标准	低	是	变更已触发
EC2.46	应该给亚马逊 VPC 加标签	AWS 资源标签标准	低	是	变更已触发
EC2.47	应标记 Amazon VPC 终端节点服务	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EC2.48	应标记 Amazon VPC 流日志	AWS 资源标签标准	低	是	变更已触发
EC2.49	应标记 Amazon VPC 对等连接	AWS 资源标签标准	低	是	变更已触发
EC2.50	应标记 EC2 VPN 网关	AWS 资源标签标准	低	是	变更已触发
EC2.51	EC2 Client VPN 端点应启用客户端连接日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	 否	变更已触发
EC2.52	应标记 EC2 传输网关	AWS 资源标签标准	低	是	变更已触发
EC2.53	EC2 安全组不应允许从 0.0.0.0/0 进入远程服务器管理端口	独联体 AWS 基金会基准测试 v3.0.0	HIGH（高）	 否	定期
EC2.54	EC2 安全组不应允许从:: /0 进入远程服务器管理端口	独联体 AWS 基金会基准测试 v3.0.0	HIGH（高）	 否	定期
ECR.1	ECR 私有存储库应配置图像扫描	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ECR.2	ECR 私有存储库应配置标签不可变性	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ECR.3	ECR 存储库应至少配置一项生命周期策略	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ECR.4	应标记 ECR 公共存储库	AWS 资源标签标准	低	是	变更已触发
ECS.1	Amazon ECS 任务定义应具有安全网络模式和用户定义。	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
ECS.2	ECS 服务不应自动分配公共 IP 地址	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
ECS.3	ECS 任务定义不应共享主机的进程命名空间	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ECS.4	ECS 容器应以非特权身份运行	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
ECS.5	ECS 容器应限制为仅对根文件系统具有只读访问权限。	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
ECS.8	密钥不应作为容器环境变量传递	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
ECS.9	ECS 任务定义应具有日志配置	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
ECS.10	ECS Fargate 服务应在最新的 Fargate 平台版本上运行	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ECS.12	ECS 集群应该使用容器详情	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ECS.13	应标记 ECS 服务	AWS 资源标签标准	低	是	变更已触发
ECS.14	应标记 ECS 集群	AWS 资源标签标准	低	是	变更已触发
ECS.15	应标记 ECS 任务定义	AWS 资源标签标准	低	是	变更已触发
EFS.1	弹性文件系统应配置为使用以下方法加密静态文件数据 AWS KMS	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	定期
EFS.2	Amazon EFS 卷应包含在备份计划中	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	定期
EFS.3	EFS 接入点应强制使用根目录	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
EFS.4	EFS 接入点应强制使用用户身份	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EFS.5	应标记 EFS 接入点	AWS 资源标签标准	低	是	变更已触发
EFS.6	EFS 挂载目标不应与公有子网关联	AWS 基础安全最佳实践	中	否	定期
EKS.1	EKS 集群端点不应公开访问	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	否	定期
EKS.2	EKS 集群应在受支持的 Kubernetes 版本上运行	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	否	变更已触发
EKS.3	EKS 集群应该使用加密的 Kubernetes 密钥	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	否	定期
EKS.6	应标记 EKS 集群	AWS 资源标签标准	低	是	变更已触发
EKS.7	应标记 EKS 身份提供商配置	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EKS.8	EKS 集群应启用审核日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
ElastiCache.1	ElastiCache Redis 集群应启用自动备份	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 是	定期
ElastiCache.2	ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期
ElastiCache.3	ElastiCache 复制组应启用自动故障切换	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
ElastiCache.4	ElastiCache 复制组应该已 encryption-at-rest 启用	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
ElastiCache.5	ElastiCache 复制组应该已 encryption-in-transit 启用	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
ElastiCache.6	ElastiCache 早期 Redis 版本的复制组应启用 Redis 身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ElastiCache.7	ElastiCache 群集不应使用默认子网组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期
ElasticBeanstalk.1	Elastic Beanstalk 环境应启用增强型运行状况报告	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
ElasticBeanstalk.2	应启用 Elastic Beanstalk 托管平台更新	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 是	变更已触发
ElasticBeanstalk.3	Elastic Beanstalk 应该将日志流式传输到 CloudWatch	AWS 基础安全最佳实践 v1.0.0	HIGH（高）	 是	变更已触发
ELB.1	应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS	AWS 基础安全最佳实践 v1.0.0，服务管理标准： ，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	中	 否	定期
ELB.2	带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由 AWS Certificate Manager 提供的证书	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ELB.3	应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.4	应将应用程序负载均衡器配置为删除 http 标头	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.5	应启用应用程序和经典负载均衡器日志记录	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.6	应用程序、网关和网络负载均衡器应启用删除保护	AWS 基础安全最佳实践，服务管理标准： ，NIST SP 800-AWS Control Tower 53 Rev. 5	中	 否	变更已触发
ELB.7	经典负载均衡器应启用连接耗尽功能	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.8	具有 SSL 侦听器的经典负载均衡器应使用具有强大配置的预定义安全策略	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ELB.9	经典负载均衡器应启用跨区域负载均衡器	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.10	经典负载均衡器应跨越多个可用区	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
ELB.12	应用程序负载均衡器应配置为防御性或最严格的异步缓解模式	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.13	应用程序、网络和网关负载均衡器应跨越多个可用区	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
ELB.14	经典负载均衡器应配置为防御性或最严格的异步缓解模式	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ELB.16	应用程序负载均衡器应与 AWS WAF Web ACL 关联	NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EMR.1	Amazon EMR 集群主节点不应有公有 IP 地址	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期
EMR.2	应启用 Amazon EMR 屏蔽公共访问权限设置	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	关键	 否	定期
ES.1	Elasticsearch 域应启用静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： ，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	中	 否	定期
ES.2	Elasticsearch 域名不可供公共访问	AWS 基础安全最佳实践 v1.0.0，服务管理标准： ，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	定期
ES.3	Elasticsearch 域应加密节点之间发送的数据	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
ES.4	应启用 Elasticsearch 域名错误 CloudWatch 日志记录到日志	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ES.5	Elasticsearch 域名应该启用审核日志	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ES.6	Elasticsearch 域应拥有至少三个数据节点	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ES.7	Elasticsearch 域应配置至少三个专用主节点	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
ES.8	与 Elasticsearch 域的连接应使用最新的 TLS 安全策略进行加密	AWS 基础安全最佳实践，服务管理标准： ，NIST SP 800- AWS Control Tower 53 Rev. 5	中	 否	变更已触发
ES.9	应标记 Elasticsearch 域名	AWS 资源标签标准	低	是	变更已触发
EventBridge.2	EventBridge 应标记活动总线	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
EventBridge.3	EventBridge 自定义事件总线应附加基于资源的策略	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	否	变更已触发
EventBridge.4	EventBridge 全局端点应启用事件复制	NIST SP 800-53 Rev. 5	中	否	变更已触发
fsx.1	应将 FSx for OpenZFS 文件系统配置为将标签复制到备份和卷	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	否	变更已触发
fsx.2	应将 FSx for Lustre 文件系统配置为将标签复制到备份	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	低	否	变更已触发
胶水。1	AWS Glue 应该给工作加标签	AWS 资源标签标准	低	是	变更已触发
GlobalAccelerator.1	应标记全球加速器加速器	AWS 资源标签标准	低	是	变更已触发
GuardDuty.1	GuardDuty 应该启用	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	HIGH（高）	否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
GuardDuty.2	GuardDuty 应该给过滤器加标签	AWS 资源标签标准	低	是	变更已触发
GuardDuty.3	GuardDuty 应标记 IP 集	AWS 资源标签标准	低	是	变更已触发
GuardDuty.4	GuardDuty 应给探测器加标签	AWS 资源标签标准	低	是	变更已触发
IAM.1	IAM policy 不应允许完全“*”管理权限	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIST SP 800-53 修订版 5 AWS	HIGH（高）	 否	变更已触发
IAM.2	IAM 用户不应附加 IAM policy	CIS AWS Foundations Benchmark v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	低	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.3	IAM 用户访问密钥应每 90 天或更短时间轮换一次	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，CIS AWS 基金会基准 v1.4.0，NIST SP 8 AWS Control Tower 00-53 修订版 5	中	 否	定期
IAM.4	不应存在 IAM 根用户访问密钥	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIS T SP 800-53 修订版 5 AWS	关键	 否	定期
IAM.5	应为拥有控制台密码的所有 IAM 用户启用 MFA	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，CIS AWS 基金会基准 v1.4.0，NIST SP 8 AWS Control Tower 00-53 修订版 5	中	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.6	应该为根用户启用硬件 MFA	CIS AWS 基金会基准 v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，CIS 基金会基准 v1.4.0 AWS Control Tower，NIST SP 800-53 修订版 5 AWS	关键	 否	定期
IAM.7	IAM 用户的密码策略应具有可靠的配置	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	定期
IAM.8	应移除未使用的 IAM 用户凭证	CIS AWS Foundations Benchmark v1.2.0， AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，PCI DSS v3.2.1，NIST SP 800-53 Rev. 5	中	 否	定期
IAM.9	应为根用户启用 MFA	CIS AWS 基金会基准 v1.2.0、PCI DSS v3.2.1、CIS AWS 基金会基准 v1.4.0、NIST SP 800-53 修订版 5	关键	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.10	IAM 用户的密码策略应具有可靠的配置	PCI DSS v3.2.1	中	 否	定期
IAM.11	确保 IAM 密码策略要求包含至少一个大写字母	独联体 AWS 基金会基准测试 v1.2.0	中	 否	定期
IAM.12	确保 IAM 密码策略要求包含至少一个小写字母	独联体 AWS 基金会基准测试 v1.2.0	中	 否	定期
IAM.13	确保 IAM 密码策略要求包含至少一个符号	独联体 AWS 基金会基准测试 v1.2.0	中	 否	定期
IAM.14	确保 IAM 密码策略要求包含至少一个数字	独联体 AWS 基金会基准测试 v1.2.0	中	 否	定期
IAM.15	确保 IAM 密码策略要求最短密码长度不低于 14	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	中	 否	定期
IAM.16	确保 IAM 密码策略阻止重复使用密码	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.17	确保 IAM 密码策略使密码在 90 天或更短时间内失效	独联体 AWS 基金会基准测试 v1.2.0	低	 否	定期
IAM.18	确保已创建支持角色来管理事件 AWS Support	独联体 AWS 基金会基准 v1.2.0，独联体 AWS 基金会基准 v1.4.0	低	 否	定期
IAM.19	应该为所有 IAM 用户启用 MFA	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 否	定期
IAM.21	您创建的 IAM 客户管理型策略不应允许对服务执行通配符操作	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
IAM.22	应移除在 45 天内未使用的 IAM 用户凭证	独联体 AWS 基金会基准测试 v1.4.0	中	 否	定期
IAM.23	应标记 IAM 访问分析器分析器	AWS 资源标签标准	低	 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IAM.24	应标记 IAM 角色	AWS 资源标签标准	低	 是	变更已触发
IAM.25	应标记 IAM 用户	AWS 资源标签标准	低	 是	变更已触发
IAM.26	应移除在 IAM 中管理的过期 SSL/TLS 证书	独联体 AWS 基金会基准测试 v3.0.0	中	 否	定期
IAM.27	IAM 身份不应附加 AWSCloudShellFullAccess 策略	独联体 AWS 基金会基准测试 v3.0.0	中	 否	变更已触发
IAM.28	应启用 IAM 访问分析器外部访问分析器	独联体 AWS 基金会基准测试 v3.0.0	HIGH（高）	 否	定期
IoT.1	AWS IoT Core 应标记安全配置文件	AWS 资源标签标准	低	是	变更已触发
IoT.2	AWS IoT Core 应标记缓解措施	AWS 资源标签标准	低	是	变更已触发
IoT.3	AWS IoT Core 应给尺寸加标签	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
IoT.4	AWS IoT Core 应给授权者加标签	AWS 资源标签标准	低	是	变更已触发
IoT.5	AWS IoT Core 应标记角色别名	AWS 资源标签标准	低	是	变更已触发
IoT.6	AWS IoT Core 策略应该被标记	AWS 资源标签标准	低	是	变更已触发
Kinesis.1	Kinesis 直播应在静态状态下进行加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Kinesis.2	应标记 Kinesis 直播内容	AWS 资源标签标准	低	是	变更已触发
KMS.1	IAM 客户管理型策略不应允许对所有 KMS 密钥执行解密操作	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
KMS.2	IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
KMS.3	AWS KMS keys 不应无意中删除	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	关键	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
KMS.4	AWS KMS key 应该启用旋转	CIS AWS 基金会基准 v1.2.0、PCI DSS v3.2.1、CIS AWS 基金会基准 v1.4.0、NIST SP 800-53 修订版 5	中	 否	定期
Lambda.1	Lambda 函数策略应禁止公共访问	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	变更已触发
Lambda.2	Lambda 函数应使用受支持的运行时系统	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Lambda.3	Lambda 函数应位于 VPC 中	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 否	变更已触发
Lambda.5	VPC Lambda 函数应在多个可用区内运行	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
Lambda.6	应标记 Lambda 函数	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Macie.1	应该启用 Amazon Macie	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
Macie.2	应启用 Macie 自动发现敏感数据	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	HIGH（高）	 否	定期
MSK.1	MSK 集群应在代理节点之间传输时进行加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
MSK.2	MSK 集群应配置增强监控	NIST SP 800-53 Rev. 5	低	 否	变更已触发
MQ.2	ActiveMQ 代理应将审计日志流式传输到 CloudWatch	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	 否	变更已触发
MQ.3	亚马逊 MQ 代理应启用自动次要版本升级	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	低	 否	变更已触发
MQ.4	应给亚马逊 MQ 经纪人贴上标签	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
MQ.5	ActiveMQ 代理应使用主动/备用部署模式	NIST SP 800-53 修订版 5，服务管理标准：AWS Control Tower	低	 否	变更已触发
MQ.6	RabbitMQ 代理应该使用集群部署模式	NIST SP 800-53 修订版 5，服务管理标准：AWS Control Tower	低	 否	变更已触发
Neptune.1	应对 Neptune 数据库集群进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 否	变更已触发
Neptune.2	Neptune 数据库集群应将审核日志发布到日志 CloudWatch	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 否	变更已触发
Neptune.3	Neptune 数据库集群快照不应公开	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	关键	 否	变更已触发
Neptune.4	Neptune 数据库集群应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	低	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Neptune.5	Neptune 数据库集群应启用自动备份	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 是	变更已触发
Neptune.6	应对 Neptune 数据库集群快照进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 否	变更已触发
Neptune.7	Neptune 数据库集群应启用 IAM 数据库身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 否	变更已触发
Neptune.8	应将 Neptune 数据库集群配置为将标签复制到快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	低	 否	变更已触发
Neptune.9	Neptune 数据库集群应部署在多个可用区中	NIST SP 800-53 Rev. 5	中	 否	变更已触发
NetworkFirewall.1	Network Firewall 防火墙应跨多个可用区部署	NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
NetworkFirewall.2	应启用 Network Firewall 日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	定期
NetworkFirewall.3	Network Firewall 策略应至少关联一个规则组	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
NetworkFirewall.4	Network Firewall 策略的默认无状态操作应为丢弃或转发完整数据包	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
NetworkFirewall.5	Network Firewall 策略的默认无状态操作应为丢弃或转发分段数据包	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
NetworkFirewall.6	无状态网络防火墙规则组不应为空	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
NetworkFirewall.7	应标记 Network Firewall 防火墙	AWS 资源标签标准	低	是	变更已触发
NetworkFirewall.8	应标记 Network Firewall 防火墙策略	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
NetworkFirewall.9	Network Firewall 防火墙应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	否	变更已触发
Opensearch.1	OpenSearch 域应启用静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	中	否	变更已触发
Opensearch.2	OpenSearch 域名不应该可供公众访问	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	否	变更已触发
Opensearch.3	OpenSearch 域应加密节点之间发送的数据	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发
Opensearch.4	OpenSearch 应该启用记录到 CloudWatch 日志的域错误	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Opensearch.5	OpenSearch 域应启用审核日志	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发
Opensearch.6	OpenSearch 域应至少有三个数据节点	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发
Opensearch.7	OpenSearch 域名应启用细粒度访问控制	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	否	变更已触发
Opensearch.8	应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密	AWS 基础安全最佳实践，服务管理标准：，NIST SP 800-AWS Control Tower 53 Rev. 5	中	否	变更已触发
打开搜索。9	OpenSearch 域名应该被标记	AWS 资源标签标准	低	是	变更已触发
Opensearch.10	OpenSearch 域名应安装最新的软件更新	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
打开搜索。11	OpenSearch 域应至少有三个专用的主节点	NIST SP 800-53 Rev. 5	中	 否	定期
PCA.1	AWS Private CA 应禁用根证书颁发机构	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	 否	定期
RDS.1	RDS 快照应为私有快照	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	变更已触发
RDS.2	根据 PubliclyA ccessible 配置，RDS 数据库实例应禁止公共访问	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	变更已触发
RDS.3	RDS 数据库实例应启用静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，CIS Foundations Benchmark v1.4.0 AWS Control Tower，NIST SP 8 AWS 00-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.4	RDS 集群快照和数据库快照应进行静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.5	RDS 数据库实例应配置多个可用区	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.6	应为 RDS 数据库实例配置增强监控	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 是	变更已触发
RDS.7	RDS 集群应启用删除保护	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.8	RDS 数据库实例应启用删除保护	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.9	RDS 数据库实例应将日志发布到 CloudWatch 日志	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.10	应为 RDS 实例配置 IAM 身份验证	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.11	RDS 实例应启用自动备份	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
RDS.12	应为 RDS 集群配置 IAM 身份验证	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.13	应启用 RDS 自动次要版本升级	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
RDS.14	Amazon Aurora 集群应启用回溯功能	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 是	变更已触发
RDS.15	应为多个可用区配置 RDS 数据库集群	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.16	应将 RDS 数据库集群配置为将标签复制到快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.17	应将 RDS 数据库实例配置为将标签复制到快照	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.18	RDS 实例应部署在 VPC 中	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
RDS.19	应为关键集群事件配置现有 RDS 事件通知订阅	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.20	应为关键数据库实例事件配置现有 RDS 事件通知订阅	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.21	应为关键数据库参数组事件配置 RDS 事件通知订阅	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.22	应为关键数据库安全组事件配置 RDS 事件通知订阅	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.23	RDS 实例不应使用数据库引擎的默认端口	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	低	 否	变更已触发
RDS.24	RDS 数据库集群应使用自定义管理员用户名	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.25	RDS 数据库实例应使用自定义管理员用户名	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.26	RDS 数据库实例应受备份计划保护	NIST SP 800-53 Rev. 5	中	 是	定期
RDS.27	应对 RDS 数据库集群进行静态加密	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 修订版 5，服务管理标准： AWS Control Tower	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
RDS.28	应标记 RDS 数据库集群	AWS 资源标签标准	低	是	变更已触发
RDS.29	应标记 RDS 数据库集群快照	AWS 资源标签标准	低	是	变更已触发
RDS.30	应标记 RDS 数据库实例	AWS 资源标签标准	低	是	变更已触发
RDS.31	应标记 RDS 数据库安全组	AWS 资源标签标准	低	是	变更已触发
RDS.32	应标记 RDS 数据库快照	AWS 资源标签标准	低	是	变更已触发
RDS.33	应标记 RDS 数据库子网组	AWS 资源标签标准	低	是	变更已触发
RDS.34	Aurora MySQL 数据库集群应将审计日志发布到 CloudWatch 日志	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
RDS.35	RDS 数据库集群应启用自动次要版本升级	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.1	Amazon Redshift 集群应禁止公共访问	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	关键	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Redshift.2	与 Amazon Redshift 集群的连接应在传输过程中加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.3	Amazon Redshift 集群应启用自动快照	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 是	变更已触发
Redshift.4	Amazon Redshift 集群应启用审核日志记录	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.6	Amazon Redshift 应该启用自动升级到主要版本的功能	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.7	Redshift 集群应使用增强型 VPC 路由	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.8	Amazon Redshift 集群不应使用默认管理员用户名	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Redshift.9	Redshift 集群不应使用默认数据库名称	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.10	Redshift 集群应静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
Redshift.11	应该标记 Redshift 集群	AWS 资源标签标准	低	是	变更已触发
Redshift.12	应标记 Redshift 事件订阅通知	AWS 资源标签标准	低	是	变更已触发
Redshift.13	应标记 Redshift 集群快照	AWS 资源标签标准	低	是	变更已触发
Redshift.14	应标记 Redshift 集群子网组	AWS 资源标签标准	低	是	变更已触发
redshift.15	Redshift 安全组应仅允许从受限来源进入集群端口	AWS 基础安全最佳实践	HIGH（高）	 否	定期
53.1 号公路	应标记 Route 53 运行状况检查	AWS 资源标签标准	低	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
Route53.2	Route 53 公共托管区域应记录 DNS 查询	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
S3.1	S3 通用存储桶应启用阻止公共访问设置	AWS 基础安全最佳实践，服务管理标准：，PCI DSS v3.2.1 AWS Control Tower，CIS Foundations Benchmark v1.4.0，NIS AWS T SP 800-53 Rev. 5	中	 否	定期
S3.2	S3 通用存储桶应阻止公共读取权限	AWS 基础安全最佳实践，服务管理标准：，PCI DSS v3.2.1 AWS Control Tower，NIST SP 800-53 Rev. 5	关键	 否	变更已触发且定期进行
S3.3	S3 通用存储桶应阻止公共写入权限	AWS 基础安全最佳实践，服务管理标准：，PCI DSS v3.2.1 AWS Control Tower，NIST SP 800-53 Rev. 5	关键	 否	变更已触发且定期进行

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
S3.5	S3 通用存储桶应要求请求使用 SSL	AWS 基础安全最佳实践，服务管理标准：，PCI DSS v3.2.1 AWS Control Tower，CIS Foundations Benchmark v1.4.0，NIS AWS TSP 800-53 Rev. 5	中	 否	变更已触发
S3.6	S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户	AWS 基础安全最佳实践，服务管理标准：，NIST SP 800-AWS Control Tower 53 Rev. 5	HIGH（高）	 否	变更已触发
S3.7	S3 通用存储桶应使用跨区域复制	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 否	变更已触发
S3.8	S3 通用存储桶应阻止公共访问	AWS 基础安全最佳实践，服务管理标准：，CIS Foundations Benchmark v1.4.0 AWS Control Tower，NIS AWS TSP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
S3.9	S3 通用存储桶应启用服务器访问日志记录	AWS 基础安全最佳实践，服务管理标准：，NIST SP 800-AWS Control Tower 53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
S3.10	启用版本控制的 S3 通用存储桶应具有生命周期配置	NIST SP 800-53 Rev. 5	中	 否	变更已触发
S3.11	S3 通用存储桶应启用事件通知	NIST SP 800-53 Rev. 5	中	 是	变更已触发
S3.12	不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限	AWS 基础安全最佳实践，服务管理标准：，NIST SP 800-AWS Control Tower 53 Rev. 5	中	 否	变更已触发
S3.13	S3 通用存储桶应具有生命周期配置	AWS 基础安全最佳实践，服务管理标准：，NIST SP 800-AWS Control Tower 53 Rev. 5	低	 是	变更已触发
S3.14	S3 通用存储桶应启用版本控制	NIST SP 800-53 Rev. 5	低	 否	变更已触发
S3.15	S3 通用存储桶应启用对象锁定	NIST SP 800-53 Rev. 5	中	 是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
S3.17	S3 通用存储桶应使用静态加密 AWS KMS keys	服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
S3.19	S3 接入点应启用屏蔽公共访问权限设置	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	关键	 否	变更已触发
S3.20	S3 通用存储桶应启用 MFA 删除功能	CIS AWS 基金会基准 v1.4.0，NIST SP 800-53 Rev. 5	低	 否	变更已触发
S3.22	S3 通用存储桶应记录对象级写入事件	独联体 AWS 基金会基准测试 v3.0.0	中	 否	定期
S3.23	S3 通用存储桶应记录对象级读取事件	独联体 AWS 基金会基准测试 v3.0.0	中	 否	定期
SageMaker.1	Amazon SageMaker 笔记本实例不应直接访问互联网	AWS 基础安全最佳实践 v1.0.0，服务管理标准： ，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	HIGH（高）	 否	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SageMaker.2	SageMaker 笔记本实例应在自定义 VPC 中启动	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
SageMaker.3	用户不应拥有 SageMaker 笔记本实例的 root 访问权限	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	HIGH（高）	 否	变更已触发
SageMaker.4	SageMaker 端点生产变体的初始实例数应大于 1	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	 否	定期
SecretsManager.1	Secrets Manager 密钥应启用自动轮换	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	变更已触发
SecretsManager.2	配置自动轮换的 Secrets Manager 密钥应成功轮换	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
SecretsManager.3	移除未使用 Secrets Manager 密钥	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	定期

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SecretsManager.4	Secrets Manager 密钥应在指定的天数内轮换	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 是	定期
SecretsManager.5	应标记 Secrets Manager 的机密	AWS 资源标签标准	低	是	变更已触发
ServiceCatalog.1	Service Catalog 产品组合只能在 AWS 组织内部共享	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	HIGH（高）	 否	定期
SES.1	应标记 SES 联系人列表	AWS 资源标签标准	低	是	变更已触发
SES.2	应标记 SES 配置集	AWS 资源标签标准	低	是	变更已触发
SNS.1	SNS 主题应使用以下方法进行静态加密 AWS KMS	NIST SP 800-53 Rev. 5	中	 否	变更已触发
SNS.3	应标记 SNS 话题	AWS 资源标签标准	低	是	变更已触发
SQS.1	应对 Amazon SQS 队列进行静态加密	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
SQS.2	应标记 SQS 队列	AWS 资源标签标准	低	是	变更已触发
SSM.1	EC2 实例应由以下人员管理 AWS Systems Manager	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	中	否	变更已触发
SSM.2	由 Systems Manager 管理的 EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	HIGH（高）	否	变更已触发
SSM.3	由 Systems Manager 管理的 EC2 实例的关联合规性的状态应为 COMPLIANT	AWS 基础安全最佳实践 v1.0.0，服务管理标准：，PCI DSS v3.2.1，NIST S AWS Control Tower P 800-53 Rev. 5	低	否	变更已触发
SSM.4	SSM 文档不应公开	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	关键	否	定期
StepFunctions.1	Step Functions 状态机应该开启日志功能	AWS 基础安全最佳实践	中	是	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
StepFunctions.2	应标记 Step Functions 活动	AWS 资源标签标准	低	是	变更已触发
转账。1	应标记 Transfer Family 工作流程	AWS 资源标签标准	低	是	变更已触发
转账。2	Transfer Family 服务器不应使用 FTP 协议进行端点连接	AWS 基础安全最佳实践，NIST SP 800-53 修订版 5	中	否	定期
WAF.1	AWS WAF 应启用经典全局 Web ACL 日志记录	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	否	定期
WAF.2	AWS WAF 经典区域规则应至少有一个条件	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发
WAF.3	AWS WAF 经典区域规则组应至少有一条规则	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发
WAF.4	AWS WAF 经典区域 Web ACL 应至少有一个规则或规则组	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	否	变更已触发

安全控件 ID	安全控件标题	适用标准	严重性	支持自定义参数	计划类型
WAF.6	AWS WAF 经典全局规则应至少有一个条件	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
WAF.7	AWS WAF 经典全局规则组应至少有一条规则	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
WAF.8	AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发
WAF.10	AWS WAF Web ACL 应至少有一个规则或规则组	AWS 基础安全最佳实践 v1.0.0，服务管理标准： AWS Control Tower，NIST SP 800-53 Rev. 5	中	 否	变更已触发
WAF.11	AWS WAF 应启用 Web ACL 日志记录	NIST SP 800-53 Rev. 5	低	 否	定期
WAF.12	AWS WAF 规则应启用 CloudWatch 指标	AWS 基础安全最佳实践 v1.0.0，NIST SP 800-53 Rev. 5	中	 否	变更已触发

主题

- AWS 账户 控件

- AWS Certificate Manager 控件
- Amazon API Gateway 控件
- AWS AppSync 控件
- Amazon Athena 控件
- AWS Backup 控件
- AWS CloudFormation 控件
- 亚马逊 CloudFront 控制
- AWS CloudTrail 控件
- 亚马逊 CloudWatch 控制
- AWS CodeArtifact 控件
- AWS CodeBuild 控件
- AWS Config 控件
- 亚马逊 Data Firehose 控件
- 亚马逊 Detective 控件
- AWS Database Migration Service 控件
- Amazon DocumentDB 控件
- Amazon DynamoDB 控件
- Amazon Elastic Container Registry 控件
- Amazon ECS 控件
- Amazon Elastic Compute Cloud 控件
- Amazon EC2 Auto Scaling 控件
- Amazon EC2 Systems Manager 控件
- Amazon Elastic File System 控件
- Amazon Elastic Kubernetes Service 控件
- 亚马逊 ElastiCache 控制
- AWS Elastic Beanstalk 控件
- 弹性负载均衡控件
- Amazon EMR 控件
- Elasticsearch 控件

- 亚马逊 EventBridge 控制
- Amazon FSx 控件
- AWS Global Accelerator 控件
- AWS Glue 控件
- 亚马逊 GuardDuty 控制
- AWS Identity and Access Management 控件
- AWS IoT 控件
- Amazon Kinesis 控件
- AWS Key Management Service 控件
- AWS Lambda 控件
- Amazon Macie 控件
- Amazon MSK 控件
- Amazon MQ 控件
- Amazon Neptune 控件
- AWS Network Firewall 控件
- 亚马逊 OpenSearch 服务控制
- AWS Private Certificate Authority 控件
- Amazon Relational Database Service 控件
- Amazon Redshift 控件
- Amazon Route 53 控制
- Amazon Simple Storage Service 控制
- 亚马逊 SageMaker 控制
- AWS Secrets Manager 控件
- AWS Service Catalog 控件
- Amazon 简单电子邮件服务控件
- Amazon Simple Notification Service 控件
- Amazon Simple Queue Service 控件
- AWS Step Functions 控件
- AWS Transfer Family 控件
- AWS WAF 控件

AWS 账户 控件

这些控件与有关 AWS 账户。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Account.1] 应为以下人员提供安全联系信息 AWS 账户

相关要求：NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`security-account-information-provided`

计划类型：定期

参数：无

此控件可检查 Amazon Web Services (AWS) 账户是否有安全联系信息。如果未提供账户的安全联系信息，则控制失败。

备用安全联系人 AWS 允许您就您的账户问题联系其他人，以防万一您不在场。有关与您的 AWS 账户使用情况相关的安全相关主题的通知可以来自 AWS Support其他 AWS 服务 团队。

修复

要将备用联系人作为安全联系人添加到您的联系人 AWS 账户，请参阅《B AWS illing and Cost Management 用户指南》中的添加、更改或删除备用联系人。

[账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分

类别：保护 > 安全访问管理 > 访问控制

相关要求：NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`account-part-of-organizations`

计划类型：定期

参数：无

此控件检查是否 AWS 账户 是通过管理的组织的一部分 AWS Organizations。如果账户不属于组织，则控制失败。

随着工作负载的扩展，Organizations 可帮助你集中管理环境 AWS。您可以使用多个 AWS 账户 来隔离具有特定安全要求的工作负载，或者符合 HIPAA 或 PCI 等框架。通过创建组织，您可以将多个账户作为一个单位进行管理，并集中管理其对资源的访问权限 AWS 服务、资源和区域。

修复

要创建新组织并自动 AWS 账户 添加到该组织，请参阅《AWS Organizations 用户指南》中的创建组织。要向现有组织添加帐户，请参阅AWS Organizations 用户指南中的AWS 账户 邀请加入您的组织。

AWS Certificate Manager 控件

这些控件与 ACM 资源相关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订

相关要求：NIST.800-53.r5 SC-28(3), NIST.800-53.r5 SC-7(16)

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ACM::Certificate`

AWS Config 规则：`acm-certificate-expiration-check`

计划类型：已触发变更和定期更改

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`daysToExpiration`	必须续订 ACM 证书的天数	整数	`14` 到 `365`	`30`

此控件检查 AWS Certificate Manager (ACM) 证书是否在指定的时间段内续订。它会检查导入的证书和 ACM 提供的证书。如果证书未在指定的时间段内续订，则控制失败。除非您为续订期提供自定义参数值，否则 Security Hub 将使用默认值即 30 天。

ACM 可以自动续订使用 DNS 验证的证书。对于使用电子邮件验证的证书，您必须回复域验证电子邮件。ACM 不会自动续订您导入的证书。您必须手动续订导入的证书。

修复

ACM 为 Amazon 颁发的 SSL/TLS 证书提供托管续订。这意味着 ACM 要么自动续订您的证书（如果您使用 DNS 验证），要么在证书即将到期时向您发送电子邮件通知。对于公有和私有 ACM 证书，都提供这些服务。

对于通过电子邮件验证的域

当证书到期 45 天后，ACM 会向域所有者发送一封针对每个域名的电子邮件。要验证域名并完成续订，您必须回复电子邮件通知。

有关更多信息，请参阅 AWS Certificate Manager 用户指南中的续订通过电子邮件验证的域。

对于通过 DNS 验证的域

ACM 自动续订使用 DNS 验证的证书。 到期前 60 天，ACM 验证证书是否可以续订。

如果无法验证域名，ACM 会发送需要手动验证的通知。它会在到期前 45 天、30 天、7 天和 1 天发送这些通知。

有关详细信息，请参阅 AWS Certificate Manager 用户指南中的通过 DNS 验证的域的续订。

[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度

类别：识别 > 库存 > 库存服务

严重性：高

资源类型：`AWS::ACM::Certificate`

AWS Config 规则：`acm-certificate-rsa-check`

计划类型：已触发变更

参数：无

此控件检查管理的 RSA 证书是否 AWS Certificate Manager 使用至少 2,048 位的密钥长度。如果密钥长度小于 2,048 位，则控制失败。

加密的强度与密钥大小直接相关。我们建议密钥长度至少为 2,048 位，以保护您的 AWS 资源，因为计算能力变得越来越便宜，服务器也变得更加先进。

修复

ACM 颁发的 RSA 证书的最小密钥长度已经是 2,048 位。有关使用 ACM 颁发新 RSA 证书的说明，请参阅 AWS Certificate Manager 用户指南中的颁发和管理证书。

虽然 ACM 允许您导入密钥长度较短的证书，但您必须使用至少 2,048 位的密钥才能通过此控制。导入证书后，您无法变更密钥长度。相反，您必须删除密钥长度小于 2,048 位的证书。有关将证书导入到 ACM 的更多信息，请参阅 AWS Certificate Manager 用户指南中的导入证书的先决条件。

[ACM.3] 应标记 ACM 证书

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ACM::Certificate`

AWS Config 规则：`tagged-acm-certificate`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Certificate Manager (ACM) 证书是否具有参数`requiredTagKeys`中定义的特定密钥的标签。如果证书没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果证书未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ACM 证书添加标签，请参阅AWS Certificate Manager 用户指南中的标记 AWS Certificate Manager 证书。

Amazon API Gateway 控件

这些控件与 API Gateway 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ApiGateway::Stage`、`AWS::ApiGatewayV2::Stage`

AWS Config 规则：`api-gw-execution-logging-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`loggingLevel`	Logging level（日志记录级别）	枚举	`ERROR`, `INFO`	`No default value`

此控件会检查 Amazon API Gateway REST 或 WebSocket API 的所有阶段是否都启用了日志记录。如果对于 API 的所有阶段 `loggingLevel` 不是 `ERROR` 或者 `INFO`，则控制失败。除非您提供自定义参数值来指示应启用特定的日志类型，否则如果日志记录级别为 `ERROR` 或 `INFO`，Security Hub 会生成通过的调查发现。

API Gateway REST 或 WebSocket API 阶段应启用相关日志。API Gateway REST 和 WebSocket API 执行日志提供了向 API Gateway REST 和 WebSocket API 阶段发出的请求的详细记录。这些阶段包括 API 集成后端响应、Lambda 授权方响应和集成终端节点`requestId`。 AWS

修复

要启用 REST 和 WebSocket API 操作的日志记录，请参阅《AP CloudWatch I Gateway 开发者指南》中的使用 API Gateway 控制台设置 API 日志记录。

[APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ApiGateway::Stage`

AWS Config 规则：`api-gw-ssl-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon API Gateway REST API 阶段是否配置了 SSL 证书。后端系统使用这些证书来验证传入的请求是否来自 API Gateway。

API Gateway REST API 阶段应配置 SSL 证书，以允许后端系统对请求是否来自 API Gateway 进行身份验证。

修复

有关如何生成和配置 API Gateway REST API SSL 证书的详细说明，请参阅 API Gateway 开发人员指南中的生成和配置用于后端身份验证的 SSL 证书。

[APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能

相关要求：NIST.800-53.r5 CA-7

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::ApiGateway::Stage`

AWS Config 规则：`api-gw-xray-enabled`

计划类型：已触发变更

参数：无

此控件检查您的 Amazon API Gateway REST API 阶段是否启用了 AWS X-Ray 主动跟踪。

X-Ray 主动跟踪可以更快速地响应底层基础设施的性能变化。性能变化可能会导致 API 的可用性不足。X-Ray 主动跟踪提供流经 API Gateway REST API 操作和关联服务的用户请求实时指标。

修复

有关如何为 API Gateway REST API 操作启用 X-REST 主动跟踪的详细说明，请参阅 AWS X-Ray 开发人员指南中的Amazon API Gateway 对 AWS X-Ray的主动跟踪支持。

[APIGateway.4] API Gateway 应与 WAF Web ACL 关联

相关要求：NIST.800-53.r5 AC-4(21)

类别：保护 > 防护服务

严重性：中

资源类型：AWS::ApiGateway::Stage

AWS Config 规则：api-gw-associated-with-waf

计划类型：已触发变更

参数：无

此控件检查 API Gateway 阶段是否使用 AWS WAF Web 访问控制列表 (ACL)。如果 AWS WAF Web ACL 未连接到 REST API Gateway 阶段，则此控件将失败。

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 API 免受攻击。它使您能够配置 ACL，这是一组规则，可根据您定义的可自定义 Web 安全规则和条件来允许、阻止或计数 Web 请求。确保您的 API Gateway 阶段与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。

修复

有关如何使用 API Gateway 控制台将 AWS WAF 区域 Web ACL 与现有 API Gateway API 阶段关联的信息，请参阅《API Gatewa y 开发者指南》中的使用 AWS WAF 保护您的 API。

[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 静态数据加密

严重性：中

资源类型：AWS::ApiGateway::Stage

AWS Config 规则：api-gw-cache-encrypted（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查 API Gateway REST API 阶段中启用缓存的所有方法是否都已加密。如果 API Gateway REST API 阶段中的任何方法配置为缓存并且缓存未加密，则控制将失败。仅当为特定方法启用缓存时，Security Hub 才会评估该方法的加密。

对静态数据进行加密可降低存储在磁盘上的数据被未经身份验证的用户访问的风险。 AWS它添加了另一组访问控制来限制未经授权的用户访问数据的能力。例如，需要 API 权限才能解密数据，然后才能读取数据。

API Gateway REST API 缓存应静态加密，以增加安全性。

修复

要为某个阶段配置 API 缓存，请参阅 API Gateway 开发人员指南中的启用 Amazon API Gateway 缓存。在缓存设置中，选择加密缓存数据。

[APIGateway.8] API Gateway 路由应指定授权类型

相关要求：NIST.800-53.r5 AC-3、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::ApiGatewayV2::Route`

AWS Config 规则：`api-gwv2-authorization-type-configured`

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`authorizationType`	API 路由的授权类型	枚举	`AWS_IAM`, `CUSTOM`, `JWT`	无默认值

此控件检查 Amazon API Gateway 路由是否具有授权类型。如果 API 网关路由未指定任何授权类型，则控制失败。或者，如果您希望仅在路径使用 `authorizationType` 参数中指定的授权类型时才通过控件，则可以提供自定义参数值。

API Gateway 支持多种用于控制和管理对 API 的访问的机制：通过指定授权类型，您可以将对 API 的访问限制为仅授权用户或进程。

修复

要为 HTTP API 设置授权类型，请参阅 API Gateway 开发人员指南中的在 API Gateway 中控制和管理对 HTTP API 的访问。要为 API 设置授权类型，请参阅《 WebSocket API Gatew ay 开发者指南》中的 WebSocket API Gateway 中控制和管理对 API 的访问权限。

[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ApiGatewayV2::Stage`

AWS Config 规则：`api-gwv2-access-logs-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon API Gateway V2 阶段是否配置了访问日志记录。如果未定义访问日志设置，则控制失败。

API Gateway访问日志提供有关谁访问了您的 API 以及调用方访问 API 的方式的详细信息。这些日志对于安全和访问审核以及取证调查等应用程序非常有用。启用这些访问日志来分析流量模式并解决问题。

有关其他最佳实践，请参阅《API Gateway 开发者指南》中的监控 REST API。

修复

要设置访问日志，请参阅《 CloudWatch API Gateway 开发者指南》中的 “使用 API Gateway 控制台设置 API 日志”。

AWS AppSync 控件

这些控制措施与 AWS AppSync 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AppSync.2] AWS AppSync 应该启用字段级日志记录

类别：识别 > 日志记录

严重性：中

资源类型：AWS::AppSync::GraphQLApi

AWS Config 规则：appsync-logging-enabled

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
fieldLoggingLevel	字段日志记录级别	枚举	ERROR, ALL	No default value	

此控件检查 AWS AppSync API 是否开启了字段级日志记录。如果字段解析器日志级别设置为无，则控制失败。除非您提供自定义参数值来指示应启用特定的日志类型，否则如果字段解析器日志级别为 ERROR 或 ALL，Security Hub 会生成通过的调查发现。

您可以使用日志记录和指标来识别、优化 GraphQL 查询和排除其问题。启用 AWS AppSync GraphQL 的日志记录功能可帮助您获取有关 API 请求和响应的详细信息、识别和响应问题以及遵守监管要求。

修复

要开启登录功能 AWS AppSync，请参阅《AWS AppSync 开发者指南》中的设置和配置。

[AppSync.4] 应标记 AWS AppSync GraphQL API

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::AppSync::GraphQLApi

AWS Config 规则：tagged-appsync-graphqlapi（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS AppSync GraphQL API 是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果 GraphQL API 没有任何标签密钥或参数中没有指定的所有密钥，则控件将失败。`requiredTagKeys`如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果 GraphQL API 未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 AWS AppSync GraphQL API 添加标签，请参阅 AP AWS AppSync I 参考TagResource中的。

[AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：高

资源类型：AWS::AppSync::GraphQLApi

AWS Config 规则：appsync-authorization-check

计划类型：已触发变更

参数：

- AllowedAuthorizationTypes： AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS（不可自定义）

此控件可检查您的应用程序是否使用 API 密钥与 AWS AppSync GraphQL API 进行交互。如果使用 API 密钥对 AWS AppSync GraphQL API 进行了身份验证，则控制失败。

API 密钥是应用程序中的硬编码值，在您创建未经身份验证的 GraphQL 端点时由 AWS AppSync 服务生成。如果此 API 密钥遭到泄露，您的端点很容易受到意外访问。除非您支持可公开访问的应用程序或网站，否则我们不建议使用 API 密钥进行身份验证。

修复

要为您的 AWS AppSync GraphQL API 设置授权选项，请参阅AWS AppSync 开发者指南中的授权和身份验证。

Amazon Athena 控件

这些控制与 Athena 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Athena.1] Athena 工作组应进行静态加密

> **Important**
>
> Security Hub 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub 控件的更改日志。

类别：保护 > 数据保护 > 静态数据加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

严重性：中

资源类型：`AWS::Athena::WorkGroup`

AWS Config 规则：`athena-workgroup-encrypted-at-rest`

计划类型：已触发变更

参数：无

此控件检查 Athena 工作组是否处于静态加密状态。如果 Athena 工作组未静态加密，则控制失败。

在 Athena 中，您可以创建工作组来运行团队、应用程序或不同工作负载的查询。每个工作组都有对所有查询启用加密的设置。您可以选择对亚马逊简单存储服务 (Amazon S3) 托管密钥使用服务器端加密、使用 () 密钥使用服务器端加密或使用客户托管的 KMS 密钥 AWS Key Management Service 进行 AWS KMS客户端加密。静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。

修复

要为 Athena 工作组启用静态加密，请参阅 Amazon Athena 用户指南中的编辑工作组。在查询结果配置部分，选择加密查询结果。

[Athena.2] 应标记 Athena 数据目录

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Athena::DataCatalog`

AWS Config 规则：`tagged-athena-datacatalog`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 Amazon Athena 数据目录是否具有参数中定义的特定密钥的标签。requiredTagKeys如果数据目录没有任何标签键或者没有参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果数据目录未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Athena 数据目录添加标签，请参阅亚马逊 Athena 用户指南中的为 Athena 资源添加标签。

[Athena.3] 应标记 Athena 工作组

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Athena::WorkGroup

AWS Config 规则：`tagged-athena-workgroup`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon Athena 工作组是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果工作组没有任何标签密钥或者没有参数`requiredTagKeys`中指定的所有密钥，则控件将失败。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果工作组未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Athena 工作组添加标签，请参阅 A mazon Athena 用户指南中的在单个工作组中添加和删除标签。

AWS Backup 控件

这些控制措施与 AWS Backup 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密

相关要求：NIST.800-53.r5 CP-9(8)、NIST.800-53.r5 SI-12

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Backup::RecoveryPoint`

AWS Config 规则：`backup-recovery-point-encrypted`

计划类型：已触发变更

参数：无

此控件检查 AWS Backup 恢复点是否处于静态加密状态。如果未对恢复点进行静态加密，则控制失败。

AWS Backup 恢复点是指在备份过程中创建的特定数据副本或快照。它代表备份数据的特定时刻，可作为恢复点，以防原始数据丢失、损坏或无法访问。对备份恢复点进行加密可增加额外的保护层来阻止未经授权的访问。加密是保护备份数据的机密性、完整性和安全性的最佳实践。

修复

要加密 AWS Backup 恢复点，请参阅《AWS Backup 开发人员指南》 AWS Backup中的备份加密。

[Backup.2] 应标记 AWS Backup 恢复点

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::RecoveryPoint`

AWS Config规则：`tagged-backup-recoverypoint`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Backup 恢复点是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果恢复点没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果未使用任何密钥标记恢复点，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向 AWS Backup 恢复点添加标签

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份计划。
3. 从列表中选择一个备份计划。

4. 在 Backup 计划标签部分，选择管理标签。
5. 输入标签的键和值。为其他键值对选择 “添加新标签”。
6. 完成添加标签后，选择保存。

[Backup.3] 应 AWS Backup 标记文件库

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::BackupVault`

AWS Config规则：`tagged-backup-backupvault`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Backup 文件库是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果恢复点没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果未使用任何密钥标记恢复点，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向 AWS Backup 文件库添加标签

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 从列表中选择一个备份存储库。
4. 在 Backup 保管库标签部分，选择管理标签。
5. 输入标签的键和值。为其他键值对选择 “添加新标签”。
6. 完成添加标签后，选择保存。

[Backup.4] 应 AWS Backup 标记报告计划

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::ReportPlan`

AWS Config规则：`tagged-backup-reportplan`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Backup 报告计划是否包含参数中定义的特定键的标签`requiredTagKeys`。如果报告计划没有任何标签密钥或者没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果报告计划未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向 AWS Backup 报告计划添加标签

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。
2. 在导航窗格中，选择备份保管库。
3. 从列表中选择一个备份存储库。
4. 在 Backup 保管库标签部分，选择管理标签。
5. 选择添加新标签。输入标签的键和值。对于其他键值对，重复此操作。
6. 完成添加标签后，选择保存。

[Backup.5] 应 AWS Backup 标记备份计划

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Backup::BackupPlan`

AWS Config规则：`tagged-backup-backupplan`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Backup 备份计划是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果备份计划没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果备份计划未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向 AWS Backup 备份计划添加标签

1. 打开 AWS Backup 控制台，网址为 https://console.aws.amazon.com/backup。

2. 在导航窗格中，选择备份保管库。
3. 从列表中选择一个备份存储库。
4. 在 Backup 保管库标签部分，选择管理标签。
5. 选择添加新标签。输入标签的键和值。对于其他键值对，重复此操作。
6. 完成添加标签后，选择保存。

AWS CloudFormation 控件

这些控制措施与 CloudFormation 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudFormation.1] CloudFormation 堆栈应与简单通知服务 (SNS) 集成 Simple Notification Service

> **Important**
>
> Security Hub 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::CloudFormation::Stack`

AWS Config 规则：`cloudformation-stack-notification-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon Simple Notification Service 通知是否与 AWS CloudFormation 堆栈集成。如果没有与 CloudFormation 堆栈相关联的 SNS 通知，则该堆栈的控制将失败。

在堆栈中配置 SNS 通知有助于立即将 CloudFormation 堆栈中发生的任何事件或更改通知利益相关者。

修复

要集成堆 CloudFormation 栈和 SNS 主题，请参阅AWS CloudFormation 用户指南中的直接更新堆栈。

[CloudFormation.2] 应 CloudFormation 标记堆栈

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CloudFormation::Stack`

AWS Config 规则：`tagged-cloudformation-stack`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS CloudFormation 堆栈是否具有参数中定义的特定键的标签`requiredTagKeys`。如果堆栈没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果堆栈未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 CloudFormation 堆栈添加标签，请参阅 AWS CloudFormation API 参考CreateStack中的。

亚马逊 CloudFront 控制

这些控制措施与 CloudFront 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudFront.1] CloudFront 发行版应配置默认根对象

相关要求：NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)。

类别：保护 > 安全访问管理 > 不可公开访问的资源

严重性：高

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-default-root-object-configured`

计划类型：已触发变更

参数：无

此控件检查 Amazon CloudFront 分配是否配置为返回默认根对象的特定对象。如果 CloudFront 发行版未配置默认根对象，则控件将失败。

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，指定默认根对象可以帮助您避免暴露 Web 分发的内容。

修复

要为 CloudFront 分配配置默认根对象，请参阅 Amazon CloudFront 开发者指南中的如何指定默认根对象。

[CloudFront.3] CloudFront 发行版在传输过程中应要求加密

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-viewer-policy-https`

计划类型：已触发变更

参数：无

此控件可检查 Amazon CloudFront 分配是否要求查看者直接使用 HTTPS 或是否使用重定向。如果 `ViewerProtocolPolicy` 对于 `defaultCacheBehavior` 或 `cacheBehaviors` 设置为 `allow-all`，则控制失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试应用程序，以了解性能概况和 TLS 的影响。

修复

要对传输中的 CloudFront 分配进行加密，请参阅《亚马逊 CloudFront 开发者指南》中的 “需要 HTTPS 才能 CloudFront在查看者之间进行通信”。

[CloudFront.4] CloudFront 发行版应配置源站故障转移

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-origin-failover-enabled`

计划类型：已触发变更

参数：无

此控件会检查 Amazon CloudFront 配送是否配置了具有两个或更多来源的起源组。

CloudFront 源站故障转移可以提高可用性。如果主源不可用或返回特定的 HTTP 响应状态代码，则源失效转移会自动将流量重定向到辅助源。

修复

要为 CloudFront 分配配置源故障转移，请参阅 Amazon CloudFront 开发者指南中的创建源组。

[CloudFront.5] CloudFront 发行版应启用日志记录

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-accesslogs-enabled`

计划类型：已触发变更

参数：无

此控件检查 CloudFront 发行版上是否启用了服务器访问日志记录。如果未为分配启用访问日志记录，则控制失败。

CloudFront 访问日志提供有关 CloudFront 收到的每个用户请求的详细信息。每个日志都包含诸如收到请求的日期和时间、发出请求的查看器的 IP 地址、请求的来源以及查看器请求的端口号等信息。

这些日志对于安全和访问审计、取证调查等应用很有用。有关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。

修复

要为 CloudFront 分配配置访问日志，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 发行版应启用 WAF

相关要求：NIST.800-53.r5 AC-4(21)

类别：保护 > 防护服务

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-associated-with-waf`

计划类型：已触发变更

参数：无

此控件检查 CloudFront 分布是否与 AWS WAF 经典 ACL 或 AWS WAF Web ACL 相关联。如果分配未与 Web ACL 关联，则控制失败。

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 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，即 Web ACL），基于可自定义的 Web 安全规则以及您定义的条件，允许、阻止或统计 Web 请求。确保您的 CloudFront 发行版与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。

修复

要将 AWS WAF 网页 ACL 与 CloudFront 分配相关联，请参阅 Amazon CloudFront 开发者指南中的使用 AWS WAF 来控制对内容的访问权限。

[CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-custom-ssl-certificate`

计划类型：已触发变更

参数：无

此控件检查 CloudFront 发行版是否使用默认的 SSL/TLS 证书提供的信息。 CloudFront 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，则此控制失败。

自定义 SSL/TLS 允许用户使用备用域名访问内容。您可以将自定义证书存储在 AWS Certificate Manager （推荐）中，也可以存储在 IAM 中。

修复

要使用自定义 SSL/TLS 证书为 CloudFront 分配添加备用域名，请参阅亚马逊 CloudFront 开发者指南中的添加备用域名。

[CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-sni-enabled`

计划类型：已触发变更

参数：无

此控件检查亚马逊 CloudFront 分发是否使用自定义 SSL/TLS 证书，以及是否配置为使用 SNI 来处理 HTTPS 请求。如果关联了自定义 SSL/TLS 证书，但 SSL/TLS 支持方法是专用 IP 地址，则此控件将失败。

服务器名称指示 (SNI) 是对 TLS 协议的扩展，2010 年以后发布的浏览器和客户端均支持。如果您配置 CloudFront 为使用 SNI 处理 HTTPS 请求，请 CloudFront 将您的备用域名与每个边缘站点的 IP 地址相关联。当查看器提交针对内容的 HTTPS 请求时，DNS 将该请求传送到正确边缘站点的 IP 地址。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。

修复

要将 CloudFront 分配配置为使用 SNI 处理 HTTPS 请求，请参阅《 CloudFront 开发者指南》中的使用 SNI 处理 HTTPS 请求（适用于大多数客户端）。

[CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-traffic-to-origin-encrypted`

计划类型：已触发变更

参数：无

此控件可检查 Amazon CloudFront 分配是否正在加密流向自定义来源的流量。对于源协议策略允许“仅限 http”的 CloudFront 分发，此控制失败。如果分配的源协议策略为“match-viewer”，而查看器协议策略为“allow-all”，则此控制也会失败。

HTTPS (TLS) 可用于帮助防止侦听或操纵网络流量。只能允许通过 HTTPS (TLS) 进行加密连接。

修复

要更新源协议策略以要求对 CloudFront 连接进行加密，请参阅《亚马逊 CloudFront 开发者指南》中的要求 CloudFront 与您的自定义源之间的通信需要 HTTPS。

[CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-no-deprecated-ssl-protocols`

计划类型：已触发变更

参数：无

此控件可检查 Amazon CloudFront 分配是否使用已弃用的 SSL 协议进行 CloudFront 边缘站点和您的自定义源站之间的 HTTPS 通信。如果 CloudFront 分配`OriginSslProtocols`包含 where includes，则`CustomOriginConfig`此控件将失败`SSLv3`。

2015 年，国际互联网工程任务组 (IETF) 正式宣布，由于该协议不够安全，应弃用 SSL 3.0。建议您使用 TLSv1.2 或更高版本与自定义源进行 HTTPS 通信。

修复

要更新 CloudFront 分配的 Origin SSL 协议，请参阅 Amazon CloudFront 开发者指南中的要求 HTTPS 才能 CloudFront 与您的自定义源进行通信。

[CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

相关要求：NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

类别：识别 > 资源配置

严重性：高

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-s3-origin-non-existent-bucket`

计划类型：定期

参数：无

此控件可检查亚马逊 CloudFront 分发是否指向不存在的 Amazon S3 来源。如果源配置为指向不存在的存储桶，则 CloudFront 分配的控制将失败。此控件仅适用于没有静态网站托管的 S3 存储桶是 S3 来源的 CloudFront 分配。

当您账户中的 CloudFront 分配配置为指向不存在的存储桶时，恶意第三方可以创建引用的存储桶，并通过您的分配提供自己的内容。无论路由行为如何，我们都建议您检查所有源，以确保分布指向适当的源。

修复

要修改 CloudFront 分配以指向新的来源，请参阅《Amazon CloudFront 开发者指南》中的更新分配。

[CloudFront.13] CloudFront 发行版应使用源站访问控制

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：中

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则：`cloudfront-s3-origin-access-control-enabled`

计划类型：已触发变更

参数：无

此控件检查源为 Amazon S3 的亚马逊 CloudFront 分发是否配置了源站访问控制 (OAC)。如果没有为 CloudFront 分发配置 OAC，则控制失败。

使用 S3 存储桶作为 CloudFront 分配的源时，您可以启用 OAC。这仅允许通过指定的 CloudFront 分配访问存储桶中的内容，并禁止直接从存储桶或其他分配进行访问。尽管 CloudFront 支持原始访问身份 (OAI)，但 OAC 提供了其他功能，使用 OAI 的发行版可以迁移到 OAC。尽管 OAI 提供了一种安全的方式来访问 S3 源，但它也有一些局限性，例如缺乏对精细策略配置的支持，以及不支持使用需要 AWS 签名版本 4 (SigV4) 的 POST 方法的 HTTP/HTTPS 请求。 AWS 区域 OAI 也不支持使用进行加密。 AWS Key Management Service OAC 基于使用 IAM 服务主体向 S3 源进行身份验证 AWS 的最佳实践。

修复

要为具有 S3 来源的 CloudFront 分配配置 OAC，请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amazon S3 来源的访问权限。

[CloudFront.14] 应该给 CloudFront 发行版加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CloudFront::Distribution`

AWS Config 规则:`tagged-cloudfront-distribution`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件会检查 Amazon CloudFront 分配是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果分配没有任何标签密钥或者没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果分配未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 CloudFront 分配添加标签，请参阅《亚马逊 CloudFront 开发者指南》中的 “为亚马逊 CloudFront 分配添加标签”。

AWS CloudTrail 控件

这些控制措施与 CloudTrail 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪

相关要求：独联体 AWS 基金会基准 v1.2.0/2.1、CIS 基金会基准 v1.4.0/3.1、CIS 基金会基准 v3.0.0/3.1、nist.800-53.r5 AC-2 (4)、nist.800-53.r5 AC-4 (26)、nist.800-53.r5 AC-6 (9)、nist.800-53.r5 AU-10、nist.800-53.r5、nist.800-53.r5 AC-4 (26)、nist.800-53.r5 AC-6 (9)、nist.800-53.r5、nist.800-53.r5、nist.r5 AU-12、nist.800-53.r5 AU-2、nist.800-53.r5 AU-3、nist.800-53.r5 AU-6 (3)、nist.800-53.r5 AU-6 (4)、nist.800-53.r5 AU-14 (1)、nist.800-53.r5 C AWS A-7、nist.800-53.r5 CA-7、nist.800-53.r5 (1)、nist.800-53.r5 CA-7、nist.800-53.r5 CA-7、nist.800-53.r5 5 SC-7 (9)、nist.800-53.r5 SI-3 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-7 (8)、nist.800-53.r5 SA-8 (22) AWS

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`multi-region-cloudtrail-enabled`

计划类型：定期

参数：

- `readWriteType`：`ALL`（不可自定义）

  `includeManagementEvents`：`true`（不可自定义）

此控件检查是否至少有一个捕获读写管理事件的多区域 AWS CloudTrail 跟踪。如果 CloudTrail 禁用或没有至少一条 CloudTrail 跟踪可以捕获读写管理事件，则控件将失败。

AWS CloudTrail 记录您的账户 AWS 的 API 调用并将日志文件发送给您。记录的信息包括以下信息：

- 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
- 返回的响应元素 AWS 服务

CloudTrail 提供账户 AWS 的 API 调用历史记录，包括通过、软件开发工具 AWS 包 AWS 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的 API 调用，AWS 服务 例如。 AWS CloudFormation

生成的 AWS API 调用历史记录 CloudTrail 支持安全分析、资源变更跟踪和合规性审计。多区域跟踪还提供以下好处。

- 多区域跟踪有助于检测在其他本不应使用的区域中发生的意外活动。
- 多区域跟踪可确保默认情况下为跟踪启用全局服务事件日志记录。全球服务事件日志记录记录 AWS 全球服务生成的事件。
- 对于多区域跟踪，所有读取和写入操作的管理事件可确保 CloudTrail 记录中所有资源的管理操作。AWS 账户

默认情况下，使用创建的 CloudTrail 跟踪 AWS Management Console 是多区域跟踪。

修复

要在中创建新的多区域跟踪 CloudTrail，请参阅AWS CloudTrail 用户指南中的创建跟踪。使用以下值：

Field	Value
其他设置，日志文件验证	已启用
选择日志事件、管理事件、API 活动	读和写。清除排除项的复选框。

要更新现有跟踪，请参阅 AWS CloudTrail 用户指南中的更新跟踪。在管理事件中，对于 API 活动，选择读取和写入。

[CloudTrail.2] CloudTrail 应该启用静态加密

相关要求：PCI DSS v3.2.1/3.4、CIS 基金会基准 v1.2.0/2.7、CIS 基金会基准 v1.4.0/3.7、CIS AWS 基金会基准 v3.0.0/3.5、nist.800-53.r5 AU-9、nist.800-53.r5 C AWS A-9 (1)、nist.800-53.r5 C AWS M-3 (6)、nist.800-53.r5 SC-13，nist.800-53.r5 SC-28、nist.800-53.r5 SC-28 (1)、nist.800-53.r5 SC-7 (10)、nist.800-53.r5 SI-7 (10)、nist.800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：`cloud-trail-encryption-enabled`

计划类型：定期

参数：无

此控件检查 CloudTrail 是否配置为使用服务器端加密 (SSE) AWS KMS key 加密。如果 `KmsKeyId` 未定义，则控制失败。

为了增加敏感 CloudTrail 日志文件的安全性，您应该使用服务器端加密和 AWS KMS keys (SSE-KMS) 对 CloudTrail 日志文件进行静态加密。请注意，默认情况下，传送 CloudTrail 到您的存储桶的日志文件由亚马逊服务器端加密，使用 Amazon S3 托管的加密密钥 (SSE-S3) 进行加密。

修复

要为 CloudTrail 日志文件启用 SSE-KMS 加密，请参阅AWS CloudTrail 用户指南中的更新跟踪以使用 KMS 密钥。

[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪

相关要求：PCI DSS v3.2.1/10.1、PCI DSS v3.2.1/10.2.1、PCI DSS v3.2.1/10.2.2、PCI DSS v3.2.1/10.2.3、PCI DSS v3.2.1/10.2.4、PCI DSS v3.2.1/10.2.5、PCI DSS v3.2.1/10.2.6、PCI DSS v3.2.1/10.2.7、PCI DSS v3.2.1/10.3.1、PCI DSS v3.2.1/10.3.2、PCI DSS v3.2.1/10.3.3、PCI DSS v3.2.1/10.3.4、PCI DSS v3.2.1/10.3.5、PCI DSS v3.2.1/10.3.6。

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`cloudtrail-enabled`

计划类型：定期

参数：无

此控件可检查您的中是否启用了 AWS CloudTrail 跟踪 AWS 账户。如果您的账户未启用至少一条 CloudTrail 跟踪，则控制失败。

但是，某些 AWS 服务不允许记录所有 API 和事件。除了 “CloudTrail 支持的 CloudTrail 服务和集成” 中每项服务的文档之外，您还应实施任何其他审计跟踪。

修复

要开始使用 CloudTrail 和创建跟踪，请参阅《AWS CloudTrail 用户指南》中的入门 AWS CloudTrail 教程。

[CloudTrail.4] 应启用 CloudTrail 日志文件验证

相关要求：PCI DSS v3.2.1/10.5.2、PCI DSS v3.2.1/10.5.5、CIS 基金会基准 v1.2.0/2.2、CIS 基金会基准 v1.4.0/3.2、CIS AWS 基金会基准 v3.0.0/3.2、nist.800-53.r5 AU-9、nist.800-53.r5 SI AWS -4、nist.800-53.r5 SI-7 (1)，st.800-53.r5 SI AWS -7 (3)、nist.800-53.r5 SI-7 (7)

类别：数据保护 > 数据完整性

严重性：低

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：`cloud-trail-log-file-validation-enabled`

计划类型：定期

参数：无

此控件检查是否在 CloudTrail跟踪上启用了日志文件完整性验证。

CloudTrail 日志文件验证会创建一个经过数字签名的摘要文件，其中包含 CloudTrail 写入 Amazon S3 的每个日志的哈希值。您可以使用这些摘要文件来确定日志文件在 CloudTrail 传送日志后是更改、删除还是未更改。

Security Hub 建议您对所有跟踪启用文件验证。日志文件验证可对 CloudTrail 日志进行额外的完整性检查。

修复

要启用 CloudTrail 日志文件验证，请参阅AWS CloudTrail 用户指南 CloudTrail中的启用日志文件完整性验证。

[CloudTrail.5] 应将 CloudTrail 跟踪与 Amazon CloudWatch 日志集成

相关要求：PCI DSS v3.2.1/10.5.3、CIS 基金会基准 v1.2.0/2.4、CIS AWS 基金会基准 v1.4.0/3.4、nist.800-53.r5 AC-2 (4)、nist.800-53.r5 AC-4 (26)、nist.800-53.r5 AC-6 (9)、nist.800-53.r5 AU-10、nist.800-53.r5、nist.800-53.r5 AC-6 (9)、nist.800-53.r5、nist.800-800-800-800-800-53.r5 AU-12、nist.800-53.r5 AU-2、nist.800-53.r5

AU-3、nist.800-53.r5 AU-6 (1)、nist.800-53.r5 AU-6 (3)、nist.800-53.r5 AU-6 (4)、nist.800-53.r5 AU-6 (5)、nist.800-53.r5 AU-6 (5)，st.800-53.r5 AU-7 (1)、nist.800-53.r5 CA-7、nist.800-53.r5 SC-7 (9)、nist.800-53.r5 SI-20、nist.800-53.r5 SI-3 (8)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 SI-4 (20)、nist.800-53.r5 (20)、nist.800-53.r5 SI-4 (20) SI-4 (AWS 5)、nist.800-53.r5 SI-7 (8)

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：`cloud-trail-cloud-watch-logs-enabled`

计划类型：定期

参数：无

此控件检查 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 AWS API 调用。记录的信息包括以下内容：

- API 调用者的身份
- API 调用时间间
- API 调用方的源 IP 地址
- 请求参数
- 返回的响应元素 AWS 服务

CloudTrail 使用 Amazon S3 进行日志文件存储和传输。您可以捕获指定 S3 存储桶中的 CloudTrail 日志以进行长期分析。要执行实时分析，您可以配置为将日志发送 CloudTrail 到 CloudWatch 日志。

对于在账户中所有区域启用的跟踪， CloudTrail 会将所有这些区域的日志文件发送到 CloudWatch 日志日志组。

Security Hub 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、监视账户活动并适当发出警报。你可以使用 CloudWatch Logs 来设置你的 AWS 服务。此建议并不排除使用不同的解决方案。

将 CloudTrail 日志发送到 CloudWatch 日志便于根据用户、API、资源和 IP 地址进行实时和历史活动记录。您可以使用此方法为异常或敏感账户活动建立警报和通知。

修复

要 CloudTrail 与 CloudWatch 日志集成，请参阅AWS CloudTrail 用户指南中的向 CloudWatch 日志发送事件。

[CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问

相关要求：独联体 AWS 基金会基准 v1.2.0/2.3、CIS 基金会基准 v1.4.0/3.3 AWS

类别：识别 > 日志记录

严重性：严重

资源类型：`AWS::S3::Bucket`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期计划和触发变更

参数：无

CloudTrail 记录在您的账户中进行的每个 API 调用。这些日志文件存储在 S3 存储桶中。CIS 建议将 S3 存储桶策略或访问控制列表 (ACL) 应用于 CloudTrail 记录的 S3 存储桶，以防止公众访问 CloudTrail 日志。允许公众访问 CloudTrail 日志内容可能有助于对手识别受影响账户使用或配置中的弱点。

要运行此检查，Security Hub 首先使用自定义逻辑来查找存储 CloudTrail 日志的 S3 存储桶。然后，它使用 AWS Config 托管规则来检查存储桶是否可公开访问。

如果您将日志聚合到单个集中式 S3 存储桶中，则 Security Hub 仅针对集中式 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，控件状态为无数据。

如果存储桶可公开访问，则检查会生成失败的调查发现。

修复

要阻止公众访问您的 CloudTrail S3 存储桶，请参阅《A mazon 简单存储服务用户指南》中的 “为您的 S3 存储桶配置阻止公开访问设置”。选择所有四个 Amazon S3 屏蔽公共访问权限。

[CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录

相关要求：独联体 AWS 基金会基准 v1.2.0/2.6、独联体基金会基准 v1.4.0/3.6、独联体 AWS 基金会基准 v3.0.0/3.4 AWS

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

S3 存储桶访问日志记录会生成一个日志，其中包含对 S3 存储桶发出的每个请求的访问记录。访问日志记录包含与请求有关的详细信息，如请求类型、处理过的请求中指定的资源和请求的处理时间和日期。

CIS 建议您在 S3 存储桶上启用存储 CloudTrail 桶访问日志记录。

通过在目标 S3 存储桶上启用 S3 存储桶日志记录，您可以捕获可能影响目标存储桶中对象的所有事件。将日志配置为存放在单独的存储桶中可实现对日志信息的访问，这在安全和事故响应工作流程中非常有用。

要运行此检查，Security Hub 首先使用自定义逻辑查找存储 CloudTrail 日志的存储桶，然后使用 AWS Config 托管规则检查是否启用了日志记录。

如果 AWS 账户 将多个日志文件 CloudTrail 传送到单个目标 Amazon S3 存储桶，则 Security Hub 仅针对其所在地区的目标存储桶评估此控制权。这简化了结果。但是，您应该 CloudTrail 在所有将日志传送到目标存储桶的账户中开启。对于除持有目标存储桶的账户以外的所有账户，控件状态均为无数据。

如果存储桶可公开访问，则检查会生成失败的调查发现。

修复

要为 CloudTrail S3 存储桶启用服务器访问日志记录，请参阅《亚马逊简单存储服务用户指南》中的“启用 Amazon S3 服务器访问日志”。

[CloudTrail.9] CloudTrail 路径应加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CloudTrail::Trail`

AWS Config 规则：`tagged-cloudtrail-trail`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS CloudTrail 跟踪是否具有参数中定义的特定键的标签`requiredTagKeys`。如果跟踪没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果跟踪未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 CloudTrail 跟踪添加标签，请参阅 AWS CloudTrail API 参考AddTags中的。

亚马逊 CloudWatch 控制

这些控制措施与 CloudWatch 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CloudWatch.1] “root” 用户应有日志指标筛选器和警报

相关要求：PCI DSS v3.2.1/7.2.1、独联体基金会基准 v1.2.0/1.1、独联体基金会基准 v1.2.0/3.3、独联体 AWS 基金会基准 v1.4.0/1.7、独联体基金会基准 v1.4.0/1.7、CIS AWS 基金会基准 v1.4.0/4.3 AWS AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

根用户可以不受限制地访问 AWS 账户中的所有服务和资源。我们强烈建议您避免使用根用户执行日常任务。最大限度地减少根用户的使用并采用最低权限原则进行访问管理，可以降低意外更改和意外泄露高权限凭证的风险。

作为最佳实践，仅在需要执行账户和服务管理任务时才使用根用户凭证。将 AWS Identity and Access Management (IAM) 策略直接应用于群组和角色，但不适用于用户。有关如何设置管理员以供日常使用的教程，请参阅 IAM 用户指南中的创建第一个 IAM 管理员用户和组

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v1.4.0 中为控制 1. 7 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。

- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查控件状态为 NO_DATA 的结果：

- 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
- 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发现。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 ListSubscriptionsByTopic 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 WARNING 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT

Field	Value
	`EXISTS && $.eventType !="AwsServiceEvent"}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.1

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您创建指标筛选条件并对未经授权的 API 调用发出警报。监控未经授权的 API 调用有助于发现应用程序错误，并可能减少检测恶意活动所花费的时间。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。
>
> 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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.2

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您创建不受 MFA 保护的指标筛选条件和警报控制台登录。监控单因素控制台登录可提高不受 MFA 保护的账户的可见性。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security

Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
指标命名空间	**`LogMetrics`**
指标值	**`1`**

Field	Value
默认值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.4、CIS 基金会基准 v1.4.0/4.4 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

此控件通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报来检查您是否实时监控 API 调用。

CIS 建议您为 IAM policy 的更改创建指标筛选条件和警报。监控此类更改有助于确保身份验证和授权控制保持不变。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。
>
> 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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

> **Note**
>
> 我们在这些补救步骤中推荐的筛选条件模式与 CIS 指南中的筛选条件模式不同。我们推荐的筛选条件仅针对来自 IAM API 调用的事件。

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
指标命名空间	**`LogMetrics`**

Field	Value
指标值	**1**
默认值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.5、CIS 基金会基准 v1.4.0/4.5 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为 CloudTrail配置设置的更改创建指标筛选器和警报。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 CIS AWS 基金会基准 v1. 4.0 中为控制 4.5 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。
>
> 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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。

3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.6、CIS 基金会基准 v1.4.0/4.6 AWS

类别：检测 > 检测服务

严重性：低

资源类
型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为失败的控制台身份验证尝试创建指标筛选条件和警报。监控失败的控制台登录可能会缩短检测暴力破解凭证尝试的准备时间，这可能会提供可供您在其他事件相关性分析中使用的指标，例如源 IP。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v1. 4.0 中为控制 4.6 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 FAILED 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 NO_DATA 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
>   我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.7、CIS 基金会基准 v1.4.0/4.7 AWS

类别：检测 > 检测服务

严重性：低

资源类
型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为已将状态更改为禁用或计划删除的客户管理密钥创建指标筛选条件和警报。您无法再访问使用已禁用或已删除的密钥加密的数据。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v1. 4.0 中为控制 4.7 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。如果 `ExcludeManagementEventSources` 包含 `kms.amazonaws.com`，则控制也会失败。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。

在以下情况下，检查的 FAILED 结果是不确定的：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查控件状态为 NO_DATA 的结果：

- 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
- 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发现。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 ListSubscriptionsByTopic 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 WARNING 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
指标命名空间	**LogMetrics**
指标值	**1**
默认值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.8、CIS 基金会基准 v1.4.0/4.8 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为 S3 存储桶策略更改创建指标筛选条件和警告。监控此类更改可能会缩短检测和纠正敏感 S3 存储桶的宽松策略的时间。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v1. 4.0 中为控制 4.8 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

Note

当 Security Hub 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。多区域跟踪也可能位于不同区域。
在以下情况下，检查的 `FAILED` 结果是不确定的：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查控件状态为 `NO_DATA` 的结果：

- 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
- 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发现。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.9、CIS 基金会基准 v1.4.0/4.9 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。

CIS 建议您为对 AWS Config 配置设置的更改创建指标筛选条件和警告。监控此类更改有助于确保账户中配置项的持续可见性。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v1. 4.0 中为控制 4.9 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。
>
> 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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。

3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.10、CIS 基金会基准 v1.4.0/4.10 AWS

类别：检测 > 检测服务

严重性：低

资源类
型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。安全组是有状态的数据包筛选器，可用于控制 VPC 的传入和传出流量。

CIS 建议您为安全组更改创建指标筛选条件和警告。监控此类更改有助于确保不会意外公开 资源和服务。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v 1.4.0 中为控制 4.10 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 FAILED 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 NO_DATA 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
>   我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**

Field	Value
默认值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.11、CIS 基金会基准 v1.4.0/4.11 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。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 建议您为 NACL 更改创建指标筛选条件和警告。监控这些更改有助于确保 AWS 资源和服务不会被无意中暴露。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS 基金会基准 v 1.4.0 中为控制 4.11 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
> 我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。
>
> 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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 CloudWatch 日志日志组的名称。您将在下一步中为该日志组创建指标筛选条件。

3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
指标命名空间	**LogMetrics**
指标值	**1**
默认值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.12、CIS 基金会基准 v1.4.0/4.12 AWS

类别：检测 > 检测服务

严重性：低

资源类
型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。需要网络网关才能向位于 VPC 以外的目标发送流量或从其接收流量。

CIS 建议您为网络网关更改创建指标筛选条件和警告。监控此类更改有助于确保所有传入和传出流量都通过受控路径穿过 VPC 边界。

为了运行此检查，Security Hub 使用自定义逻辑来执行 CIS AWS Foundations Benchmark v 1.2 中为控制 4.12 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。
> - 当前区域内由当前账户拥有的可用追踪没有满足控制要求。
>
> 在以下情况下，检查控件状态为 `NO_DATA` 的结果：
>
> - 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
> - 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发现。
>
>   我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 `NO_DATA`。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 Log CloudWatch s 日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.13、CIS 基金会基准 v1.4.0/4.13 AWS

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

此控件通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报来检查您是否实时监控 API 调用。路由表在子网和网络网关之间路由网络流量。

CIS 建议您为路由表更改创建指标筛选条件和警告。监控此类更改有助于确保所有 VPC 流量都流经预期路径。

> **Note**
>
> 当 Security Hub 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。多区域跟踪也可能位于不同区域。
> 在以下情况下，检查的 `FAILED` 结果是不确定的：
>
> - 没有配置跟踪。

- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查控件状态为 NO_DATA 的结果：

- 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
- 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发现。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 ListSubscriptionsByTopic 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 WARNING 结果。

修复

> **Note**
>
> 我们在这些补救步骤中推荐的筛选条件模式与 CIS 指南中的筛选条件模式不同。我们推荐的筛选条件仅针对来自 Amazon Elastic Compute Cloud (EC2) API 调用的事件。

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 Log CloudWatch s 日志组的名称。您将在下一步中为该日志组创建指标筛选条件。

3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
指标命名空间	**LogMetrics**
指标值	**1**
默认值	**0**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*your-metric-name* 是...	大于/等于
比...	**1**

[CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

相关要求：独联体 AWS 基金会基准 v1.2.0/3.14、CIS 基金会基准 v1.4.0/4.14 AWS

类别：检测 > 检测服务

严重性：低

资源类
型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

您可以通过将 CloudTrail 日志定向到 CloudWatch 日志并建立相应的指标筛选器和警报，对 API 调用进行实时监控。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 更改创建指标筛选条件和警告。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 CIS AWS 基金会基准 v 1.4.0 中为控制 4.14 规定的确切审计步骤。如果不使用 CIS 规定的确切度量筛选条件，则此控制将会失败。不能向指标筛选条件中添加附加其他字段或搜索词。

Note

当 Security Hub 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。多区域跟踪也可能位于不同区域。
在以下情况下，检查的 FAILED 结果是不确定的：

- 没有配置跟踪。
- 当前区域内由当前账户拥有的可用追踪没有满足控制要求。

在以下情况下，检查控件状态为 NO_DATA 的结果：

- 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
- 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发现。

  我们建议使用组织跟踪来记录组织中许多账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户

中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

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 `ListSubscriptionsByTopic` 访问 Amazon SNS 主题。否则，Security Hub 会生成控件的 `WARNING` 结果。

修复

要通过此控制，请按照以下步骤为指标筛选器创建 Amazon SNS 主题、 AWS CloudTrail 跟踪、指标筛选条件和警报。

1. 创建 Amazon SNS 主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。创建一个接收所有 CIS 警报的主题，并至少创建一个该主题的订阅。
2. 创建一条适用于所有人的 CloudTrail 跟踪 AWS 区域。有关说明，请参阅 AWS CloudTrail 用户指南中的创建跟踪。

   记下与 CloudTrail 跟踪关联的 Log CloudWatch s 日志组的名称。您将在下一步中为该日志组创建指标筛选条件。
3. 创建指标筛选条件。有关说明，请参阅 Amazon CloudWatch 用户指南中的为日志组创建指标筛选条件。使用以下值：

Field	Value
定义模式，筛选条件模式	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicL`

Field	Value
	`inkVpc) || ($.eventName=Detac hClassicLinkVpc) \|\| ($.eventN ame=DisableVpcClassicLink) || ($.eventName=EnableVpcClass icLink)}`
指标命名空间	**`LogMetrics`**
指标值	**`1`**
默认值	**`0`**

4. 基于筛选条件创建警报 有关说明，请参阅 A mazon CloudWatch 用户指南中的基于日志组指标筛选条件创建 CloudWatch 警报。使用以下值：

Field	Value
条件，阈值类型	静态
什么时候*`your-metric-name`* 是...	大于/等于
比...	**`1`**

[CloudWatch.15] CloudWatch 警报应配置指定操作

类别：检测 > 检测服务

相关要求：NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 IR-4(1)、NIST.800-53.r5 IR-4(5)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)。

严重性：高

资源类型：`AWS::CloudWatch::Alarm`

AWS Config 规则：**`cloudwatch-alarm-action-check`**

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
alarmActionRequired	如果将参数设置为 true 并且警报状态变更为 ALARM 时警报会执行操作，则控件会生成 PASSED 调查发现。	布尔值	不可自定义	true
insufficientDataActionRequired	如果将参数设置为 true 并且警报状态变更为 INSUFFICIENT_DATA 时警报会执行操作，则控件会生成PASSED 调查发现。	布尔值	true 或者 false	false
okActionRequired	如果将参数设置为 true 并且警报状态变更为 OK 时警报会执行操作，则控件会生成PASSED 调查发现。	布尔值	true 或者 false	false

此控件检查 Amazon CloudWatch 警报是否为该ALARM状态配置了至少一个操作。如果警报没有为 ALARM 状态配置操作，则控制失败。或者，您可以包含自定义参数值，以便也要求对 INSUFFICIENT_DATA 或 OK 状态执行警报操作。

> **Note**
>
> Security Hub 根据 CloudWatch 指标警报评估此控件。指标警报可能是配置了指定操作的复合警报的一部分。在以下情况下，该控件会生成FAILED调查结果：
>
> - 未为指标警报配置指定的操作。
> - 指标警报是配置了指定操作的复合警报的一部分。

此控件侧重于 CloudWatch 警报是否配置了警报操作，而 CloudWatch.17 侧重于 CloudWatch 警报操作的激活状态。

我们建议采取 CloudWatch 警报措施，以便在监控的指标超出定义的阈值时自动提醒您。当警报进入特定状态时，监控警报可帮助您识别异常活动并快速响应安全和操作问题。最常见的警报操作类型是通过向 Amazon Simple Notification Service (Amazon SNS) 主题发送消息来通知一个或多个用户。

修复

有关 CloudWatch 警报支持的操作的信息，请参阅 Amazon CloudWatch 用户指南中的警报操作。

[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留

类别：识别 > 日志记录

相关要求：NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-11、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-12。

严重性：中

资源类型：`AWS::Logs::LogGroup`

AWS Config 规则：**`cw-loggroup-retention-period-check`**

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`minRetentionTime`	CloudWatch 日志组的最小保留期（以天为单位）	枚举	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

此控件检查 Amazon CloudWatch 日志组的保留期是否至少为指定的天数。如果保留期少于指定天数，则控制失败。除非您为保留期提供自定义参数值，否则 Security Hub 将使用默认值即 365 天。

CloudWatch 日志将来自所有系统、应用程序的日志集中到一个高度可扩展的服务 AWS 服务中。您可以使用 CloudWatch 日志来监控、存储和访问来自亚马逊弹性计算云 (EC2) 实例 AWS

CloudTrail、Amazon Route 53 和其他来源的日志文件。将日志保留至少 1 年可以帮助您遵守日志保留标准。

修复

要配置日志保留设置，请参阅《Amazon CloudWatch 用户指南》中的 “ CloudWatch 日志” 中的 “更改日志数据保留期”。

[CloudWatch.17] 应激 CloudWatch 活警报动作

类别：检测 > 检测服务

相关要求：NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-4(12)。

严重性：高

资源类型：`AWS::CloudWatch::Alarm`

AWS Config 规则：**`cloudwatch-alarm-action-enabled-check`**

计划类型：已触发变更

参数：无

此控件检查 CloudWatch 警报操作是否已激活（`ActionEnabled`应设置为 true）。如果警报的警报动作被停用， CloudWatch 则控制失败。

> **Note**
>
> Security Hub 根据 CloudWatch 指标警报评估此控件。指标警报可能是已激活警报操作的复合警报的一部分。在以下情况下，该控件会生成`FAILED`调查结果：
>
> - 未为指标警报配置指定的操作。
> - 指标警报是已激活警报操作的复合警报的一部分。

此控件侧重于 CloudWatch 警报操作的激活状态，而 CloudWatch.15 侧重于 CloudWatch 警报中是否配置了任何`ALARM`操作。

当监控的指标超出定义的阈值时，警报操作会自动向您发出警报。如果警报操作被停用，则警报状态变更时不会运行任何操作，也不会提醒您注意监控指标的变化。我们建议您激活 CloudWatch 警报操作，以帮助您快速应对安全和操作问题。

修复

激活 CloudWatch 警报操作（控制台）

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中的警报下，选择所有警报。
3. 选择要激活操作的警报。
4. 在操作中，选择警报操作-新建，然后选择启用。

有关激活 CloudWatch 警报操作的更多信息，请参阅 Amazon CloudWatch 用户指南中的警报操作。

AWS CodeArtifact 控件

这些控制措施与 CodeArtifact 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CodeArtifact.1] 应标记CodeArtifact 存储库

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::CodeArtifact::Repository`

AWS Config 规则：`tagged-codeartifact-repository`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS CodeArtifact 存储库是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果存储库没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如

果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果存储库未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 CodeArtifact 仓库添加标签，请参阅《AWS CodeArtifact 用户指南》 CodeArtifact中的为仓库添加标签。

AWS CodeBuild 控件

这些控制措施与 CodeBuild 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证

相关要求：PCI DSS v3.2.1/8.2.1、NIST.800-53.r5 SA-3。

类别：保护 > 安全开发

严重性：严重

资源类型：AWS::CodeBuild::Project

AWS Config 规则：codebuild-project-source-repo-url-check

计划类型：已触发变更

参数：无

此控件检查 AWS CodeBuild 项目 Bitbucket 源存储库 URL 是否包含个人访问令牌或用户名和密码。如果 Bitbucket 源存储库 URL 包含个人访问令牌或用户名和密码，则控制失败。

> **Note**
>
> 此控件会评估 CodeBuild 构建项目的主要来源和次要来源。有关项目源的更多信息，请参阅《AWS CodeBuild 用户指南》中的多个输入源和输出构件示例。

登录凭据不应以明文形式存储或传输，也不得出现在源存储库 URL 中。您不应该使用个人访问令牌或登录凭证，而是访问您的源代码提供商 CodeBuild，并将源存储库 URL 更改为仅包含 Bitbucket 存储库位置的路径。使用个人访问令牌或登录凭证可能会导致意外的数据泄露或未经授权的访问。

修复

您可以更新您的 CodeBuild 项目以使用 OAuth。

从 CodeBuild 项目源中移除基本身份验证/(GitHub) 个人访问令牌

1. 打开 CodeBuild 控制台，网址为 https://console.aws.amazon.com/codebuild/。
2. 选择包含个人访问令牌或用户名和密码的构建项目。
3. 从 Edit（编辑）中，选择 Source（源）。
4. 从 GitHub /Bitbucket 中选择断开连接。
5. 选择 “使用 OAuth 连接”，然后选择 “连接到 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《AWS CodeBuild 用户指南》中基于CodeBuild 用例的示例。

[CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证

相关要求：PCI DSS v3.2.1/8.2.1、NIST.800-53.r5 IA-5(7)、NIST.800-53.r5 SA-3。

类别：保护 > 安全开发

严重性：严重

资源类型：AWS::CodeBuild::Project

AWS Config 规则：codebuild-project-envvar-awscred-check

计划类型：已触发变更

参数：无

该控制检查项目是否包含环境变量 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。

身份验证凭证 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY 决不能以明文方式存储，因为这可能会导致意外的数据暴露和未经授权的访问。

修复

要从 CodeBuild 项目中移除环境变量，请参阅AWS CodeBuild 用户指南 AWS CodeBuild中的更改构建项目的设置。确保没有为环境变量选择任何内容。

您可以将带有敏感值的环境变量存储在 P AWS Systems Manager arameter Store 中 AWS Secrets Manager ，也可以从构建规范中检索它们。有关说明，请参阅 AWS CodeBuild 用户指南中“环境”部分中标有重要的方框。

[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：低

资源类型：AWS::CodeBuild::Project

AWS Config 规则：codebuild-project-s3-logs-encrypted

计划类型：已触发变更

参数：无

此控件可检查 AWS CodeBuild 项目的 Amazon S3 日志是否已加密。如果对 CodeBuild 项目的 S3 日志停用加密，则控制失败。

建议对静态数据进行加密，以在数据周围添加一层访问管理。对静态日志进行加密可以降低未经身份验证的 AWS 用户访问存储在磁盘上的数据的风险。它添加了另一组访问控制来限制未经授权的用户访问数据的能力。

修复

要更改 CodeBuild 项目 S3 日志的加密设置，请参阅AWS CodeBuild 用户指南 AWS CodeBuild中的更改构建项目的设置。

[CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

相关要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::CodeBuild::Project`

AWS Config 规则：`codebuild-project-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查 CodeBuild 项目环境是否至少有一个日志选项，要么是 S3 日志选项，要么是启用了 CloudWatch 日志。如果 CodeBuild 项目环境没有启用至少一个日志选项，则此控件将失败。

从安全角度来看，日志记录是一项重要功能，可以在发生任何安全事件时为将来的取证工作提供支持。将 CodeBuild 项目中的异常与威胁检测关联起来，可以增强人们对这些威胁检测准确性的信心。

修复

有关如何配置 CodeBuild 项目日志设置的更多信息，请参阅《 CodeBuild 用户指南》中的创建构建项目（控制台）。

[CodeBuild.5] CodeBuild 项目环境不应启用特权模式

> **Important**
>
> Security Hub 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::CodeBuild::Project`

AWS Config 规则：`codebuild-project-environment-privileged-check`

计划类型：已触发变更

参数：无

此控件检查 AWS CodeBuild 项目环境是启用还是禁用了特权模式。如果 CodeBuild 项目环境启用了特权模式，则控制失败。

默认情况下，Docker 容器不允许访问任何设备。特权模式将授予构建项目的 Docker 容器访问所有设备的权限。使用 `true` 值进行设置 `privilegedMode` 允许 Docker 进程守护程序在 Docker 容器内运行。Docker 进程守护程序侦听 Docker API 请求并管理 Docker 对象，例如映像、容器、网络和卷。仅当构建项目用于构建 Docker 映像时，才应将此参数设置为 true。否则，应禁用此设置以防止意外访问 Docker API 以及容器的底层硬件。`privilegedMode` 设置为 `false` 有助于保护关键资源免遭篡改和删除。

修复

要配置 CodeBuild 项目环境设置，请参阅《CodeBuild 用户指南》中的创建构建项目（控制台）。在环境部分中，不要选择特权设置。

AWS Config 控件

这些控制措施与 AWS Config 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录

相关要求：独联体 AWS 基金会基准 v1.2.0/2.5、CIS 基金会基准 v1.4.0/3.5、CIS AWS 基金会基准 v3.0.0/3.3、nist.800-53.r5 CM-3、nist.800-53.r5 CM-6 (1)、nist.800-53.r5 CM-8 (2)、PCI AWS DSS v3.2.r5 (2) 1/10.5.2，PCI DSS v3.2.1/11.5

类别：识别 > 清单

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：无（自定义 Security Hub 规则）

计划类型：定期

参数：无

此控件检查您的账户当前 AWS Config 是否已启用 AWS 区域，记录与当前区域中启用的控件对应的所有资源，并使用服务相关 AWS Config 角色。如果您不使用服务相关角色，则控制将失败，因为其他角色可能不具备准确记录您的资源的必要权限。 AWS Config

该 AWS Config 服务对您的账户中支持的 AWS 资源执行配置管理，并向您提供日志文件。记录的信息包括配置项目（AWS 资源）、配置项目之间的关系以及资源中的任何配置更改。全球资源是指任何地区都可用的资源。

该控件的评估方式如下：

- 如果将当前区域设置为聚合区域，则只有在记录 AWS Identity and Access Management (IAM) 全球资源时（如果您启用了需要这些资源的控件），控件才会生成`PASSED`调查结果。
- 如果将当前区域设置为关联区域，则该控件不会评估是否记录了 IAM 全球资源。
- 如果当前区域不在您的聚合器中，或者您的账户中未设置跨区域聚合，则该控件仅在记录 IAM 全球资源时才会生成`PASSED`调查结果（如果您启用了需要这些资源的控件）。

控制结果不受您选择每天还是连续记录资源状态变化的影响 AWS Config。但是，如果您配置了自动启用新控件或具有自动启用新控件的中央配置策略，则在发布新控件时，此控件的结果可能会发生变化。在这些情况下，如果您不记录所有资源，则必须为与新控件关联的资源配置录制才能收到`PASSED`调查结果。

Security Hub 安全检查只有 AWS Config 在所有区域中启用并针对需要它的控件配置资源记录时，才能按预期运行。

> **Note**
>
> Config.1 要求 AWS 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，因此对该控件执行的检查仅评估账户的当前区域。
> 要允许对某个区域中的 IAM 全球资源进行安全检查，您必须记录该区域的 IAM 全球资源。未记录 IAM 全球资源的地区将收到用于检查 IAM 全球资源的控制的默认PASSED结果。由于 IAM 全球资源各不相同 AWS 区域，因此我们建议您仅在本地区记录 IAM 全球资源（如果您的账户中启用了跨区域聚合）。IAM 资源将仅记录在已开启全球资源记录的区域。
> AWS Config 支持的 IAM 全球记录资源类型包括 IAM 用户、群组、角色和客户托管策略。您可以考虑在关闭全局资源记录的区域禁用用于检查这些资源类型的 Security Hub 控件。有关更多信息，请参阅 您可能想要禁用的 Security Hub 控件。

修复

有关必须为每个控件记录哪些资源的列表，请参阅AWS Config 生成控制结果所需的资源。

在主区域和不属于聚合器的区域中，记录当前区域中启用的控件所需的所有资源，包括 IAM 全球资源（如果您启用了需要 IAM 全球资源的控件）。

在关联的区域中，只要您 AWS Config 录制的是与当前区域中启用的控件相对应的所有资源，您就可以使用任何录制模式。在关联区域中，如果您启用了需要记录 IAM 全球资源的控件，则不会收到FAILED调查结果（您记录的其他资源就足够了）。

要启用 AWS Config 和配置它以记录资源，请参阅《AWS Config 开发者指南》中的控制台设置 AWS Config。您也可以使用 AWS CloudFormation 模板来自动执行此过程。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的AWS CloudFormation StackSets 示例模板。

亚马逊 Data Firehose 控件

这些控制措施与 Amazon Data Firehose 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DataFirehose.1] Firehose 传输流应在静态状态下进行加密

相关要求：nist.800-53.r5 AC-3、nist.800-53.r5 AU-3、nist.800-53.r5 SC-12、nist.800-53.r5 SC-13、nist.800-53.r5 SC-28

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::KinesisFirehose::DeliveryStream`

AWS Config 规则：`kinesis-firehose-delivery-stream-encrypted`

计划类型：定期

参数：无

此控件检查 Amazon Data Firehose 传送流是否使用服务器端加密进行静态加密。如果 Firehose 传送流未使用服务器端加密进行静态加密，则此控件将失败。

服务器端加密是 Amazon Data Firehose 交付流中的一项功能，它使用在 () 中创建 AWS Key Management Service 的密钥在数据静止之前自动对其进行加密。AWS KMS数据在写入 Data Firehose 流存储层之前先进行加密，从存储中检索出来后再进行解密。这使您能够遵守监管要求并增强数据的安全性。

修复

要在 Firehose 传输流上启用服务器端加密，请参阅亚马逊数据 Firehose 开发者指南中的亚马逊数据 Firehose 中的数据保护。

亚马逊 Detective 控件

这些控件与 Detective 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Detective.1] 应标记侦探行为图

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Detective::Graph`

AWS Config 规则：`tagged-detective-graph`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon Detective 行为图是否包含参数中定义的特定键的标签`requiredTagKeys`。如果行为图没有任何标签键或者没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果行为图未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向侦探行为图添加标签，请参阅《Amazon Detective 管理指南》中的向行为图添加标签。

AWS Database Migration Service 控件

这些控制措施与 AWS DMS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DMS.1] Database Migration Service 复制实例不应公开

相关要求：PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则：`dms-replication-not-public`

计划类型：定期

参数：无

此控件检查 AWS DMS 复制实例是否为公共实例。为此，它会检查 `PubliclyAccessible` 字段的值。

私有复制实例具有私有 IP 地址，您无法在复制网络外部访问该地址。当源数据库和目标数据库位于同一网络时，复制实例应具有私有 IP 地址。还必须使用 VPN 或 VPC 对等连接将网络连接到复制实例的 VPC。 AWS Direct Connect要了解有关公有和私有复制实例的更多信息，请参阅 AWS Database Migration Service 用户指南中的公有和私有复制实例。

您还应确保只有经过授权的用户才能访问您的 AWS DMS 实例配置。为此，请限制用户修改 AWS DMS 设置和资源的 IAM 权限。

修复

创建 DMS 复制实例后，您无法变更其公共访问设置。要变更公共访问设置，请删除您当前的实例，然后重新创建实例。不要选择公开访问选项。

[DMS.2] 应标记 DMS 证书

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::DMS::Certificate

AWS Config 规则：tagged-dms-certificate（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 AWS DMS 证书是否具有参数中定义的特定密钥的标签requiredTagKeys。如果证书没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果证书未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 证书添加标签，请参阅《AWS Database Migration Service 用户指南》 AWS Database Migration Service中的为资源添加标签。

[DMS.3] 应标记 DMS 活动订阅

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::EventSubscription`

AWS Config 规则：`tagged-dms-eventsubscription`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS DMS 事件订阅是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果事件订阅没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果事件订阅未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 事件订阅添加标签，请参阅AWS Database Migration Service 用户指南 AWS Database Migration Service中的标记资源。

[DMS.4] 应标记 DMS 复制实例

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则：`tagged-dms-replicationinstance`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS DMS 复制实例是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果复制实例没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果复制实例未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 复制实例添加标签，请参阅AWS Database Migration Service 用户指南AWS Database Migration Service中的标记资源。

[DMS.5] 应标记 DMS 复制子网组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DMS::ReplicationSubnetGroup`

AWS Config 规则：`tagged-dms-replicationsubnetgroup`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS DMS 复制子网组是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果复制子网组没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果复制子网组未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DMS 复制子网组添加标签，请参阅AWS Database Migration Service 用户指南 AWS Database Migration Service中的标记资源。

[DMS.6] DMS 复制实例应启用自动次要版本升级

相关要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::DMS::ReplicationInstance`

AWS Config 规则：`dms-auto-minor-version-upgrade-check`

计划类型：已触发变更

参数：无

此控件检查是否为 AWS DMS 复制实例启用了自动次要版本升级。如果未为 DMS 复制实例启用自动次要版本升级，则控制失败。

DMS 为每个支持的复制引擎提供自动次要版本升级，以便您可以保留复制实例 up-to-date。次要版本可以引入新的软件功能、错误修复、安全补丁和性能改进。通过在 DMS 复制实例上启用自动次要版本升级，可以在维护时段内自动应用次要升级，或者如果选择了“立即应用变更”选项，则会立即应用次要升级。

修复

要在 DMS 复制实例上启用自动次要版本升级，请参阅 AWS Database Migration Service 用户指南中的修改复制实例。

[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::DMS::ReplicationTask`

AWS Config 规则：`dms-replication-task-targetdb-logging`

计划类型：已触发变更

参数：无

此控件检查是否启用了日志记录，并且 DMS 复制任务 `TARGET_APPLY` 和 `TARGET_LOAD` 的最低严重级别为 `LOGGER_SEVERITY_DEFAULT`。如果未为这些任务启用日志记录，或者最低严重性级别低于 `LOGGER_SEVERITY_DEFAULT`，则控制失败。

在迁移过程中，DMS 使用 Amazon CloudWatch 来记录信息。使用日志记录任务设置，您可以指定记录哪些组件活动以及记录多少信息。您应该为以下任务指定日志记录：

- `TARGET_APPLY`——数据和数据定义语言 (DDL) 语句应用于目标数据库。
- `TARGET_LOAD`——数据将加载到目标数据库中。

日志记录通过启用监控、故障排除、审核、性能分析、错误检测和恢复以及历史分析和报告，在 DMS 复制任务中发挥着关键作用。日志记录有助于确保数据库之间数据的成功复制，同时保持数据完整性并符合法规要求。在故障排除期间，这些组件很少需要除了 `DEFAULT` 以外的其他日志级别。除非特别要求由 AWS Support变更这些组件的日志级别，否则我们建议保留这些组件的日志级别 `DEFAULT`。最低日志级别为 `DEFAULT` 可确保将信息性消息、警告和错误消息写入日志。此控件检查上述复制任务的日志记录级别是否至少为以下级别之一：`LOGGER_SEVERITY_DEFAULT`、`LOGGER_SEVERITY_DEBUG` 或 `LOGGER_SEVERITY_DETAILED_DEBUG`。

修复

要启用目标数据库 DMS 复制任务的日志记录，请参阅《AWS Database Migration Service 用户指南》中的查看和管理 AWS DMS 任务日志。

[DMS.8] 源数据库的 DMS 复制任务应启用日志记录

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::DMS::ReplicationTask`

AWS Config 规则：`dms-replication-task-sourcedb-logging`

计划类型：已触发变更

参数：无

此控件检查是否启用了日志记录，并且 DMS 复制任务 SOURCE_CAPTURE 和 SOURCE_UNLOAD 的最低严重级别为 LOGGER_SEVERITY_DEFAULT。如果未为这些任务启用日志记录，或者最低严重性级别低于 LOGGER_SEVERITY_DEFAULT，则控制失败。

在迁移过程中，DMS 使用 Amazon CloudWatch 来记录信息。使用日志记录任务设置，您可以指定记录哪些组件活动以及记录多少信息。您应该为以下任务指定日志记录：

- SOURCE_CAPTURE——正在进行的复制或变更数据捕获 (CDC) 数据从源数据库或服务中捕获，并传递到 SORTER 服务组件。
- SOURCE_UNLOAD——数据在满负荷期间从源数据库或服务中卸载。

日志记录通过启用监控、故障排除、审核、性能分析、错误检测和恢复以及历史分析和报告，在 DMS 复制任务中发挥着关键作用。日志记录有助于确保数据库之间数据的成功复制，同时保持数据完整性并符合法规要求。在故障排除期间，这些组件很少需要除了 DEFAULT 以外的其他日志级别。除非特别要求由 AWS Support变更这些组件的日志级别，否则我们建议保留这些组件的日志级别 DEFAULT。最低日志级别为 DEFAULT 可确保将信息性消息、警告和错误消息写入日志。此控件检查上述复制任务的日

志记录级别是否至少为以下级别之一：LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG 或 LOGGER_SEVERITY_DETAILED_DEBUG。

修复

要启用源数据库 DMS 复制任务的日志记录，请参阅《AWS Database Migration Service 用户指南》中的查看和管理 AWS DMS 任务日志。

[DMS.9] DMS 端点应使用 SSL

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：AWS::DMS::Endpoint

AWS Config 规则：dms-endpoint-ssl-configured

计划类型：已触发变更

参数：无

此控件检查 AWS DMS 端点是否使用 SSL 连接。如果端点不使用 SSL，则控制失败。

SSL/TLS 连接通过加密 DMS 复制实例与数据库之间的连接来提供一层安全性。使用证书通过验证是否与预期数据库建立连接来提供额外的安全保护。它通过检查自动安装在您预置的所有数据库实例上的服务器证书来实现这一点。通过在 DMS 端点上启用 SSL 连接，您可以在迁移过程中保护数据的机密性。

修复

要向新的或现有的 DMS 端点添加 SSL 连接，请参阅 AWS Database Migration Service 用户指南中的将 SSL 与 AWS Database Migration Service配合使用。

[DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权

相关要求：nist.800-53.r5 AC-2、nist.800-53.r5 AC-3、nist.800-53.r5 AC-6、nist.800-53.r5 AC-17、nist.800-53.r5 IA-2、nist.800-53.r5 IA-5

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：AWS::DMS::Endpoint

AWS Config 规则：dms-neptune-iam-authorization-enabled

计划类型：已触发变更

参数：无

此控件检查 Amazon Neptune 数据库的 AWS DMS 终端节点是否配置了 IAM 授权。如果 DMS 终端节点未启用 IAM 授权，则控制失败。

AWS Identity and Access Management (IAM) 在各个方面提供精细的访问控制。 AWS通过 IAM，您可以指定谁可以在哪些条件下访问哪些服务和资源。借助 IAM 策略，您可以管理员工和系统的权限，以确保权限最低。通过在 Neptune 数据库的 AWS DMS 终端节点上启用 IAM 授权，您可以使用参数指定的服务角色向 IAM 用户授予授权权限。ServiceAccessRoleARN

修复

要在海王星数据库的 DMS 终端节点上启用 IAM 授权，请参阅用户指南中的使用亚马逊 Neptune 作为目标 AWS Database Migration Service。AWS Database Migration Service

[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

相关要求：nist.800-53.r5 AC-3、nist.800-53.r5 AC-6、nist.800-53.r5 IA-2、nist.800-53.r5 IA-2、nist.800-53.r5 IA-5

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：AWS::DMS::Endpoint

AWS Config 规则：dms-mongo-db-authentication-enabled

计划类型：已触发变更

参数：无

此控件检查 MongoDB 的 AWS DMS 端点是否配置了身份验证机制。如果未为端点设置身份验证类型，则控制失败。

AWS Database Migration Service 支持 MongoDB 的两种身份验证方法：MongoDB 版本 2.x 的 MONGODB-CR 和 MongoDB 版本 3.x 或更高版本的 SCRAM-SHA-1。如果用户想使用密码访问数据库，则使用这些身份验证方法对MongoDB密码进行身份验证和加密。 AWS DMS 端点身份验证可确保只有经过授权的用户才能访问和修改数据库之间迁移的数据。如果没有适当的身份验证，未经授权的用户可能能够在迁移过程中访问敏感数据。这可能导致数据泄露、数据丢失或其他安全事件。

修复

要在 DMS 端点上为 MongoDB 启用身份验证机制，请参阅《用户指南》中的 “使用 MongoDB 作为来源”。 AWS DMSAWS Database Migration Service

[DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS

相关要求：nist.800-53.r5 SC-8、nist.800-53.r5 SC-13

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::DMS::Endpoint`

AWS Config 规则：`dms-redis-tls-enabled`

计划类型：已触发变更

参数：无

此控件检查 Redis 的 AWS DMS 终端节点是否配置了 TLS 连接。如果端点未启用 TLS，则控制失败。

当数据通过互联网在应用程序或数据库之间发送时，TLS 可提供 end-to-end 安全性。当您为 DMS 终端节点配置 SSL 加密时，它会在迁移过程中启用源数据库和目标数据库之间的加密通信。这有助于防止恶意行为者窃听和拦截敏感数据。如果没有 SSL 加密，可能会访问敏感数据，从而导致数据泄露、数据丢失或其他安全事件。

修复

要在 Redis 的 DMS 终端节点上启用 TLS 连接，请参阅用户指南 AWS Database Migration Service中的使用 Redis 作为目标。AWS Database Migration Service

Amazon DocumentDB 控件

这些控制与 Amazon DocumentDB 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`docdb-cluster-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 集群是否进行静态加密。如果 Amazon DocumentDB 集群未进行静态加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。Amazon DocumentDB 集群中的数据应进行静态加密，以增加安全性。Amazon DocumentDB 使用 256 位高级加密标准 (AES-256)，使用 AWS Key Management Service (AWS KMS) 中存储的加密密钥来加密您的数据。

修复

您可以在创建 Amazon DocumentDB 集群时启用静态加密。创建集群后，您将无法变更加密设置。有关更多信息，请参阅 Amazon DocumentDB 开发人员指南中的为 Amazon DocumentDB 集群启用静态加密。

[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期

相关要求：NIST.800-53.r5 SI-12。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：AWS::RDS::DBCluster

AWS Config 规则：docdb-cluster-backup-retention-check

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
minimumBackupRetentionPeriod	最小备份保留期（以天为单位）	整数	7 到 35	7	

此控件检查 Amazon DocumentDB 集群的备份保留期是否大于或等于指定时间范围。如果备份保留期小于指定时间范围，则控制失败。除非您为备份保留期提供自定义参数值，否则 Security Hub 将使用默认值即 7 天。

备份可帮助您更快地从安全事件中恢复并增强系统的故障恢复能力。通过自动备份 Amazon DocumentDB 集群，您将能够将系统恢复到某个时间点并最大限度地减少停机时间和数据丢失。在 Amazon DocumentDB 中，集群的默认备份保留期为 1 天。必须将其增加到 7 到 35 天之间的值才能通过此控件。

修复

要变更 Amazon DocumentDB 集群的备份保留期，请参阅 Amazon DocumentDB 开发人员指南中的修改 Amazon DocumentDB 集群。对于备份，选择备份保留期。

[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5

SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::RDS::DBClusterSnapshot`、`AWS::RDS:DBSnapshot`

AWS Config 规则：`docdb-cluster-snapshot-public-prohibited`

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 手动集群快照是否是公开的。如果手动集群快照是公共的，则控制失败。

除非有意图，否则 Amazon DocumentDB 手动集群快照不应公开。如果您将未加密的手动快照公开共享，则该快照可供所有 AWS 账户使用。公开快照可能会导致意外的数据泄露。

> **Note**
>
> 此控件评估手动集群快照。您无法共享 Amazon DocumentDB 自动集群快照。但是，您可以通过复制自动快照来创建手动快照，然后共享该副本。

修复

要移除对 Amazon DocumentDB 手动集群快照的公开访问权限，请参阅 Amazon DocumentDB 开发人员指南中的共享快照。通过编程方式，您可以使用 Amazon DocumentDB `modify-db-snapshot-attribute` 操作。将 `attribute-name` 设置为 `restore`，并将 `values-to-remove` 设置为 `all`。

[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`docdb-cluster-audit-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 集群是否将审核日志发布到亚马逊 CloudWatch 日志。如果集群不向日志发布审核日 CloudWatch 志，则控制失败。

Amazon DocumentDB（与 MongoDB 兼容）允许您审核在集群中执行的事件。记录的事件的示例包括成功和失败的身份验证尝试、删除数据库中的集合或创建索引。默认情况下，审计在 Amazon DocumentDB 中处于禁用状态，需要您采取措施才能启用审计。

修复

要将 Amazon DocumentDB 审计日志发布到 CloudWatch 日志，请参阅亚马逊 DocumentDB 开发者指南中的启用审计。

[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)。

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`docdb-cluster-deletion-protection-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon DocumentDB 集群是否已启用删除保护。如果集群未启用删除保护，则控制失败。

启用集群删除保护可提供额外保护，防止数据库意外删除或未经授权的用户删除。在启用删除保护时，无法删除 Amazon DocumentDB 集群。您必须先禁用删除保护，删除请求才能成功。当您在 Amazon DocumentDB 控制台中创建集群时，删除保护默认启用。

修复

要为现有 Amazon DocumentDB 集群启用删除保护，请参阅 Amazon DocumentDB 开发人员指南中的修改 Amazon DocumentDB 集群。在修改集群部分中，为删除保护选择启用。

Amazon DynamoDB 控件

这些控制与 DynamoDB 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[DynamoDB.1] DynamoDB 表应根据需求自动扩展容量

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：`dynamodb-autoscaling-enabled`

计划类型：定期

参数：

参数	描述	类型	有效的自定义值	Security Hub 默认值
`minProvisionedReadCapacity`	DynamoDB 自动扩缩的预置读取容量单位的最小数量	整数	`1` 到 `40000`	无默认值
`targetReadUtilization`	读取容量的目标使用率百分比	整数	`20` 到 `90`	无默认值

参数	描述	类型	有效的自定义值	Security Hub 默认值
`minProvisionedWriteCapacity`	DynamoDB 自动扩缩的预置写入容量单位的最小数量	整数	`1` 到 `40000`	无默认值
`targetWriteUtilization`	写入容量的目标使用率百分比	整数	`20` 到 `90`	无默认值

此控件检查 Amazon DynamoDB 表是否可以根据需要扩展其读取和写入容量。如果表不使用按需容量模式或配置了自动扩缩的预置模式，则控制失败。默认情况下，此控件只需要配置其中一种模式，而不考虑特定的读取或写入容量级别。或者，您可以提供自定义参数值，以便要求特定的读取和写入容量级别或目标利用率。

按需扩展容量可以避免节流异常，这有助于保持应用程序的可用性。按需容量模式下的 DynamoDB 表仅受 DynamoDB 吞吐量默认表配额的限制。要提高这些配额，您可以在预配置模式下向 AWS Support.dynamoDB 表提交支持票证，并自动缩放，根据流量模式动态调整预配置的吞吐容量。有关 DynamoDB 请求节流的更多信息，请参阅《Amazon DynamoDB 开发人员指南》中的请求节流和容量暴增。

修复

要在容量模式下对现有表启用 DynamoDB 自动扩缩，请参阅 Amazon DynamoDB 开发人员指南中的在现有表上启用 DynamoDB 自动扩缩。

[DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：dynamodb-pitr-enabled

计划类型：已触发变更

参数：无

此控件检查是否为亚马逊 DynamoDB 表启用了 point-in-time 恢复 (PITR)。

备份可以帮助您更快地从安全事件中恢复。它们还增强了系统的故障恢复能力。DynamoDB 恢复功能可 point-in-time 自动对 DynamoDB 表进行备份。它可以缩短从意外删除或写入操作中恢复的时间。启用 PITR 的 DynamoDB 表可以恢复到过去 35 天内的任何时间点。

修复

要将 DynamoDB 表恢复到某个时间点，请参阅 Amazon DynamoDB 开发人员指南中的将 DynamoDB 表恢复到某个时间点。

[DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：AWS::DAX::Cluster

AWS Config 规则：dax-encryption-enabled

计划类型：定期

参数：无

此控件检查亚马逊 DynamoDB 加速器 (DAX) 集群是否处于静态加密状态。如果 DAX 集群未进行静态加密，则控制失败。

对静态数据进行加密可降低存储在磁盘上的数据被未经身份验证的用户访问的风险。 AWS加密添加了另一组访问控制，以限制未经授权的用户访问数据的能力。例如，需要 API 权限才能解密数据，然后才能读取数据。

修复

创建集群后，您无法启用或禁用静态加密。您必须重新创建集群才能启用静态加密。有关如何创建启用静态加密的 DAX 集群的详细说明，请参阅 Amazon DynamoDB 开发人员指南中的使用 AWS Management Console启用静态加密。

[DynamoDB.4] 备份计划中应有 DynamoDB 表

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：**`dynamodb-resources-protected-by-backup-plan`**

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`backupVaultLockCheck`	如果将参数设置为，`true`并且资源使用 AWS Backup 文件库锁定，则控件会生成PASSED结果。	布尔值	`true` 或者 `false`	无默认值

此控件评估备份计划是否涵盖了处于 `ACTIVE` 状态的 Amazon DynamoDB 表。如果备份计划不涵盖 DynamoDB 表，则控制失败。如果将`backupVaultLockCheck`参数设置为`true`，则只有在锁定的文件库中备份 DynamoDB 表时，控制才会通过。 AWS Backup

AWS Backup 是一项完全托管的备份服务，可帮助您集中和自动备份数据 AWS 服务。使用 AWS Backup，您可以创建定义备份要求的备份计划，例如备份数据的频率以及保留这些备份的时间。将 DynamoDB 表纳入备份计划可帮助您保护数据免遭意外丢失或删除。

修复

要将 DynamoDB 表添加到 AWS Backup 备份计划，请参阅开发人员指南中的AWS Backup 为备份计划分配资源。

[DynamodB.5] 应标记 DynamoDB 表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：`tagged-dynamodb-table`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件会检查 Amazon DynamoDB 表是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果表没有任何标签键或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签键是否存在，如果表未使用任何键标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 DynamoDB 表添加标签，请参阅亚马逊 DynamoDB 开发者指南中的在 DynamoDB 中为资源添加标签。

[DynamodB.6] DynamoDB 表应启用删除保护

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)。

类别：保护 > 数据保护 > 数据删除保护

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：**`dynamodb-table-deletion-protection-enabled`**

计划类型：已触发变更

参数：无

此控件检查 Amazon DynamoDB 表是否已启用删除保护。如果 DynamoDB 表未启用删除保护，则控制失败。

您可以使用删除保护属性保护 DynamoDB 表免遭意外删除。为表启用此属性有助于确保在管理员执行常规表管理操作期间不会意外删除表。这有助于防止您的常规业务运营受到干扰。

修复

要为 DynamoDB 表启用删除保护，请参阅《Amazon DynamoDB 开发者指南》中的使用删除保护。

[DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密

相关要求：nist.800-53.r5 AC-17、nist.800-53.r5 SC-8、nist.800-53.r5 SC-13、nist.800-53.r5、nist.800-53.r5 SC-23

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::DynamoDB::Table`

AWS Config 规则：**`dax-tls-endpoint-encryption`**

计划类型：定期

参数：无

此控件检查亚马逊 DynamoDB 加速器 (DAX) 集群在传输过程中是否经过加密，终端节点加密类型设置为 TLS。如果 DAX 集群在传输过程中未加密，则控制失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击来窃听或操纵网络流量。您应该只允许通过 TLS 的加密连接访问 DAX 集群。但是，加密传输中的数据可能会影响性能。您应该在开启加密的情况下测试您的应用程序，以了解 TLS 的性能概况和 TLS 的影响。

修复

创建 DAX 集群后，您无法更改 TLS 加密设置。要加密现有 DAX 集群，请创建一个启用传输中加密功能的新集群，将应用程序的流量转移到该集群，然后删除旧集群。有关更多信息，请参阅《Amazon DynamoDB 开发人员指南》中的使用删除保护。

Amazon Elastic Container Registry 控件

这些控件与 Amazon ECR 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ECR.1] ECR 私有存储库应配置图像扫描

相关要求：NIST.800-53.r5 RA-5。

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::ECR::Repository`

AWS Config 规则：`ecr-private-image-scanning-enabled`

计划类型：定期

参数：无

此控件检查私有 Amazon ECR 存储库是否配置了图像扫描。如果未将私有 ECR 存储库配置为推送时扫描或连续扫描，则控制失败。

ECR 映像扫描有助于识别容器映像中的软件漏洞。在 ECR 存储库上配置图像扫描为所存储图像的完整性和安全性添加了一层验证。

修复

要为 ECR 存储库配置图像扫描，请参阅 Amazon Elastic Container Registry 用户指南中的图像扫描。

[ECR.2] ECR 私有存储库应配置标签不可变性

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-8(1)。

类别：识别 > 清单 > 标记

严重性：中

资源类型：`AWS::ECR::Repository`

AWS Config 规则：`ecr-private-tag-immutability-enabled`

计划类型：已触发变更

参数：无

此控件检查私有 ECR 存储库是否启用了标签不可变性。如果私有 ECR 存储库禁用了标签不可变性，则此控制失败。如果启用了标签不可变性并且具有值 `IMMUTABLE`，则此规则通过。

Amazon ECR 标签不变性使客户能够依靠图像的描述性标签作为跟踪和唯一识别图像的可靠机制。不可变标签是静态的，这意味着每个标签都引用一个唯一的图像。这提高了可靠性和可扩展性，因为使用静态标签总是会导致部署相同的映像。配置后，标签不变性可防止标签被覆盖，从而减少攻击面。

修复

要创建配置了不可变标签的存储库或更新现有存储库的图像标签可变性设置，请参阅 Amazon Elastic Container Registry 用户指南中的图像标签可变性。

[ECR.3] ECR 存储库应至少配置一个生命周期策略

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::ECR::Repository`

AWS Config 规则：`ecr-private-lifecycle-policy-configured`

计划类型：已触发变更

参数：无

此控件检查 Amazon ECR 存储库是否至少配置了一个生命定期策略。如果 ECR 存储库未配置任何生命定期策略，则此控制失败。

Amazon ECR 生命周期策略使您能够指定存储库中镜像的生命周期管理。通过配置生命周期策略，您可以根据年龄或数量自动清理未使用的映像以及到期的映像。自动执行这些任务可以帮助您避免无意中使用存储库中过时的映像。

修复

要配置生命周期策略，请参阅 Amazon Elastic Container Registry 用户指南中的创建生命周期策略预览。

[ECR.4] 应标记 ECR 公共存储库

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECR::PublicRepository`

AWS Config 规则：`tagged-ecr-publicrepository`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon ECR 公共存储库是否具有参数requiredTagKeys中定义的特定密钥的标签。如果公共存储库没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果公共存储库未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECR 公共存储库添加标签，请参阅《亚马逊弹性容器注册表用户指南》中的 “为 Ama zon ECR 公共存储库添加标签”。

Amazon ECS 控件

这些控制与 Amazon ECS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config 规则：`ecs-task-definition-user-for-host-mode-check`

计划类型：已触发变更

参数：

- `SkipInactiveTaskDefinitions`：`true`（不可自定义）

此控件检查主机联网模式下的活动 Amazon ECS 任务定义是否具有 `privileged` 或 `user` 容器定义。对于具有主机网络模式和容器定义为 `privileged=false`、空或 `user=root` 的任务定义，控制失败。

此控件仅评估 Amazon ECS 任务定义的最新活动版本。

此控件的目的是确保在运行使用主机网络模式的任务时有意定义访问。如果任务定义具有更高的权限，那是因为您选择了该配置。当任务定义启用了主机网络并且您未选择更高的权限时，此控件会检查意外的权限升级。

修复

有关如何更新任务定义的信息，请参阅 Amazon Elastic Container Service 开发人员指南 中的更新任务定义。

当您更新任务定义时，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，您必须使用新任务定义重新部署该任务。

[ECS.2] ECS 服务不应自动分配公有 IP 地址

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5

SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::ECS::Service`

AWS Config规则：`ecs-service-assign-public-ip-disabled`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

- `exemptEcsServiceArns`（不可自定义）。Security Hub 不会填充此参数。不受此规则约束的 Amazon ECS 服务的 ARN 的逗号分隔列表。

  如果 Amazon ECS 服务已设置 `AssignPublicIP` 为 `ENABLED` 并在此参数列表中指定，则此规则即为 `COMPLIANT`。

  如果 Amazon ECS 服务已设置 `AssignPublicIP` 为 `ENABLED` 并未在此参数列表中指定，则此规则即为 `NON_COMPLIANT`。

此控件检查 Amazon ECS 服务是否配置为自动分配公有 IP 地址。如果 `AssignPublicIP` 是 `ENABLED`，则控制失败。如果 `AssignPublicIP` 是 `DISABLED`，则此控件通过。

公有 IP 地址是指可通过 Internet 访问的 IP 地址。如果您使用公有 IP 地址启动 Amazon ECS 实例，则可以通过 Internet 访问 Amazon ECS 实例。Amazon ECS 服务不应公开访问，因为这可能会允许对容器应用程序服务器进行意外访问。

修复

要禁用自动公有 IP 分配，请参阅 Amazon Elastic Container Service 开发人员指南 中的为服务配置 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

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：高

资源类型：AWS::ECS::TaskDefinition

AWS Config规则：ecs-task-definition-pid-模式检查

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义是否配置为与其容器共享主机的进程命名空间。如果任务定义与其上运行的容器共享主机的进程命名空间，则控制失败。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

进程 ID (PID) 命名空间提供了进程之间的分离。它防止系统进程可见，并允许重复使用 PID，包括 PID 1。如果主机的 PID 命名空间与容器共享，则容器可以看到主机系统上的所有进程。这降低了主机和容器之间进程级分离的好处。这些情况可能导致未经授权访问主机本身的进程，包括操纵和终止这些进程的能力。客户不应与其上运行的容器共享主机的进程命名空间。

修复

要对任务定义进行配置，请参阅 pidMode Amazon Elastic Container Service 开发人员指南中的任务定义参数。

[ECS.4] ECS 容器应以非特权身份运行

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 >根用户访问限制

严重性：高

资源类型：AWS::ECS::TaskDefinition

AWS Config规则：ecs-containers-nonprivileged

计划类型：已触发变更

参数：无

此控件检查 Amazon ECS 任务定义的容器定义中的 `privileged` 参数是否设置为 `true`。如果此参数等于，则控制失败`true`。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

我们建议您从 ECS 任务定义中删除提升权限。当权限参数为 `true` 时，容器被赋予对宿主容器实例的提升权限（类似于根用户）。

修复

要配置任务定义的 `privileged` 参数，请参阅 Amazon Elastic Container Service 开发人员指南中的高级容器定义参数。

[ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config规则：ecs-containers-readonly-access

计划类型：已触发变更

参数：无

此控件检查 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 `readonlyRootFilesystem` 参数设置为 `false` 或任务定义中的容器定义中不存在该参数，则控制失败。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

启用此选项可以减少安全攻击向量，因为除非容器实例对其文件系统文件夹和目录具有明确的读写权限，否则容器实例的文件系统无法被篡改或写入。这种控制还遵循最低权限原则。

修复

将容器定义限制为对根文件系统的只读访问

1. 打开 Amazon ECS 经典控制台：https://console.aws.amazon.com/ecs/。
2. 在左侧导航窗格中，选择 Task definitions（任务定义）。

3. 选择包含需要更新的容器定义的任务定义。请完成以下各个步骤：

   - 从下拉列表中选择使用 JSON 创建新修订版。
   - 添加 `readonlyRootFilesystem` 参数，并在任务定义的容器定义中将其设置为 `true`。
   - 选择创建。

[ECS.8] 密钥不应作为容器环境变量传递

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全开发 > 凭证未硬编码

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config规则：ecs-no-environment-secrets

计划类型：已触发变更

参数：

- SecretKeys = `AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA`（不可自定义）

此控件检查容器定义 `environment` 参数中任何变量的键值是否包括 `AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY` 或 `ECS_ENGINE_AUTH_DATA`。如果任何容器定义中的单个环境变量等于 `AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY` 或 `ECS_ENGINE_AUTH_DATA`，则此控制失败。此控件不包括从其他位置（例如 Amazon S3）传入的环境变量。此控件仅评估 Amazon ECS 任务定义的最新活动版本。

AWS Systems Manager Parameter Store 可以帮助您改善组织的安全状况。我们建议使用 Parameter Store 存储密钥和凭证，而不是直接将其传递到容器实例或将其硬编码到代码中。

修复

要使用 SSM 创建参数，请参阅 AWS Systems Manager 用户指南中的创建 Systems Manager 参数。有关创建指定密钥的任务定义的更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的使用 Secrets Manager 指定敏感数据。

[ECS.9] ECS 任务定义应具有日志配置

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::ECS::TaskDefinition`

AWS Config规则：ecs-task-definition-log-配置

计划类型：已触发变更

参数：无

此控件检查最新的活动的 Amazon ECS 任务定义是否指定了日志配置。如果任务定义未定义 `logConfiguration` 属性，或者至少有一个容器定义中的 `logDriver` 值为空，则控制失败。

日志记录可帮助您保持 Amazon ECS 的可靠性、可用性和性能。从任务定义中收集数据可提供可见性，这可以帮助您调试流程并找到错误的根本原因。如果您使用的日志记录解决方案不必在 ECS 任务定义中定义（例如第三方日志解决方案），则可以在确保正确捕获和传送日志后禁用此控件。

修复

要为 Amazon ECS 任务定义定义日志配置，请参阅 Amazon Elastic Container Service 开发人员指南中的在任务定义中指定日志配置。

[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行

相关要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::ECS::Service`

AWS Config规则：`ecs-fargate-latest-platform-version`

计划类型：已触发变更

参数：

- `latestLinuxVersion: 1.4.0`（不可自定义）
- `latestWindowsVersion: 1.0.0`（不可自定义）

此控件检查 Amazon ECS Fargate 服务是否正在运行最新的 Fargate 平台版本。如果平台版本不是最新版本，则此控制失败。

AWS Fargate 平台版本是指 Fargate 任务基础架构的特定运行时环境，它是内核和容器运行时版本的组合。随着运行时系统环境的发展，将不断发布新的平台版本。例如，可能会发布新版本以进行内核或操作系统更新、新功能、错误修复或安全更新。 Fargate 任务的安全更新和补丁将自动部署。如果发现影响平台版本的安全问题，请 AWS 修补平台版本。

修复

要更新现有服务，包括其平台版本，请参阅 Amazon Elastic Container Service 开发人员指南中的更新服务。

[ECS.12] ECS 集群应该使用容器详情

相关要求：NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ECS::Cluster`

AWS Config规则：`ecs-container-insights-enabled`

计划类型：已触发变更

参数：无

此控件检查 ECS 集群是否使用容器见解。如果未为集群设置 Container Insights，则此控制失败。

监控是维护 Amazon ECS 集群的可靠性、可用性和性能的重要组成部分。使用 CloudWatch Container Insights 收集、汇总和汇总来自容器化应用程序和微服务的指标和日志。 CloudWatch 自动收集许多资

源的指标，例如 CPU、内存、磁盘和网络。Container Insights 还提供诊断信息（如容器重新启动失败），以帮助您查明问题并快速解决问题。您还可以对容器洞察收集的指标设置 CloudWatch 警报。

修复

要使用容器见解，请参阅 Amazon CloudWatch 用户指南中的更新服务。

[ECS.13] 应标记 ECS 服务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECS::Service`

AWS Config规则：`tagged-ecs-service`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon ECS 服务是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果服务没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果服务未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托

人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECS 服务添加标签，请参阅亚马逊弹性容器服务开发人员指南中的为你的 Amazon ECS 资源添加标签。

[ECS.14] 应标记 ECS 群集

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECS::Cluster`

AWS Config规则：`tagged-ecs-cluster`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon ECS 集群是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果集群没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果集群未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECS 集群添加标签，请参阅亚马逊弹性容器服务开发人员指南中的为你的 Amazon ECS 资源添加标签。

[ECS.15] 应标记 ECS 任务定义

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::ECS::TaskDefinition`

AWS Config规则：`tagged-ecs-taskdefinition`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon ECS 任务定义是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果任务定义没有任何标签密钥或者没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果任务定义未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 ECS 任务定义添加标签，请参阅亚马逊弹性容器服务开发人员指南中的标记您的 Amazon ECS 资源。

Amazon Elastic Compute Cloud 控件

这些控制与 Amazon EC2 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EC2.1] Amazon EBS 快照不应公开恢复

相关要求：PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`ebs-snapshot-public-restorable-check`

计划类型：定期

参数：无

此控件检查 Amazon Elastic Block Store 快照是否非公开。如果任何人都可以恢复 Amazon EBS 快照，则控制失败。

EBS 快照用于将 EBS 卷上的数据在特定时间点备份到 Amazon S3。您可以使用快照还原 EBS 卷的先前状态。与公众共享快照几乎是不允许的。通常，公开共享快照的决定要么是决策错误，要么是没有完全理解其含义。此检查有助于确保所有此类共享都是完全经过规划并且是有意进行的。

要将公有 EBS 快照设为私有，请参阅 Amazon EC2 用户指南中的共享快照。在操作、修改权限中，选择私有。

[EC2.2] VPC 默认安全组不应允许入站或出站流量

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/2.1、CIS 基金会基准 v1.2.0/4.3、CIS 基金会基准 v1.4.0/5.3、CIS AWS 基金会基准 v3.0.0/5.4、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-4 (21) -53.r5 SC AWS -7、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC AWS -7 (16)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-7 (5)

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`vpc-default-security-group-closed`

计划类型：已触发变更

参数：无

此控件检查 VPC 的默认安全组是否允许入站或出站流量。如果安全组允许入站或出站流量，则控制失败。

默认安全组的规则允许来自分配给相同安全组的网络接口（及其关联实例）的所有出站和入站流量。我们建议您不要使用默认安全组。由于无法删除默认安全组，因此您应更改默认安全组规则设置以限制入站和出站流量。如果意外为 EC2 实例等资源配置了默认安全组，这可以防止意外的流量。

修复

要修复此问题，请先创建新的最低权限安全组。有关说明，请参阅 Amazon VPC 用户指南中的创建安全组。然后，将新的安全组分配给 EC2 实例。有关说明，请参阅 Amazon EC2 用户指南中的更改实例的安全组。

将新安全组分配给资源后，从默认安全组中删除所有入站和出站规则。有关说明，请参阅 Amazon VPC 用户指南中的删除安全组规则。

[EC2.3] 挂载的 Amazon EBS 卷应进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::EC2::Volume`

AWS Config 规则：`encrypted-volumes`

计划类型：已触发变更

参数：无

该控制检查处于连接状态的 EBS 卷是否已加密。要通过此检查，EBS 卷必须处于使用中并加密。如果 EBS 卷未挂载，则不需要接受此检查。

为了增加 EBS 卷中敏感数据的安全性，您应该启用静态 EBS 加密。Amazon EBS 加密提供了直接用于 EBS 资源的加密解决方案，无需您构建、维护和保护自己的密钥管理基础设施。它在创建加密卷和快照时使用 KMS 密钥。

要了解有关亚马逊 EBS 加密的更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EBS 加密。

修复

没有直接对现有未加密卷或快照进行加密的方法。您只能在新的卷或快照创建时对其进行加密。

如果您启用了默认加密，Amazon EBS 使用您用于 Amazon EBS 加密的默认密钥对生成的新卷或快照实施加密。即使您未启用默认加密，也可以在创建单个卷或快照时启用加密。在这两种情况下，您都可以覆盖 Amazon EBS 加密的默认密钥并选择对称的客户管理密钥。

有关更多信息，请参阅 Amazon EC2 用户指南中的创建 Amazon EBS 卷和复制 Amazon EBS 快照。

[EC2.4] 停止的 EC2 实例应在指定时间段后删除

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 清单

严重性：中

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-stopped-instance`

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`AllowedDays`	在生成失败的调查发现之前，允许 EC2 实例处于停止状态的天数。	整数	1 到 365	30

此控件检查 Amazon EC2 实例是否已停止超过允许的天数。如果 EC2 实例的停止时间超过允许的最大时间段，则控制失败。除非您为允许的最大时间段提供自定义参数值，否则 Security Hub 将使用默认值即 30 天。

当 EC2 实例在很长一段时间内没有运行时，会造成安全风险，因为该实例没有得到积极维护（分析、修补、更新）。如果稍后启动，则由于缺乏适当的维护，可能会导致您的 AWS 环境出现意外问题。要安全地将 EC2 实例长期保持不活动状态，请定期启动已对其进行维护，然后在维护后将其停止。理想情况下，这应是一个自动化的过程。

修复

要终止非活动的 EC2 实例，请参阅 Amazon EC2 用户指南中的终止实例。

[EC2.6] 应在所有 VPC 中启用 VPC 流日志记录

相关要求：独联体 AWS 基金会基准 v1.2.0/2.9、CIS 基金会基准 v1.4.0/3.9、CIS AWS 基金会基准 v3.0.0/3.7、PCI DSS v3.2.1/10.3.3、PCI DSS v3.2.1/10.3.4、PCI DSS v3.2.1/10.3.6、nist.800-53.r5 AC-4 (26)、nist.800-800-800-53.r5 AU-12、nist.800-53.r5 AU-2、nist.800-53.r5 AU-3、nist.800-53.r5 AU-6 (3)、nist.800-53.r5 AU-6 (4)、nist.800-53.r5 CA-7、nist.800-53.r5 SI-7 (8) AWS

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::EC2::VPC`

AWS Config 规则：`vpc-flow-logs-enabled`

计划类型：定期

参数：

- `trafficType`：`REJECT`（不可自定义）

此控件检查是否找到并为 VPC 启用 Amazon VPC 流日志。流量类型设置为 `Reject`。

通过 VPC 流日志功能，您可以捕获有关进出 VPC 中网络接口的 IP 地址流量的信息。创建流日志后，可以在 CloudWatch 日志中查看和检索其数据。为了降低成本，您还可以将流日志发送到 Amazon S3。

Security Hub 建议您为 VPC 的数据包拒绝启用流日志记录。流日志提供了对穿过 VPC 的网络流量的可见性，并且可以检测异常流量或在安全工作流程期间提供见解。

默认情况下，记录包括 IP 地址流的不同组件的值，包括源、目标和协议。有关日志字段的更多信息和描述，请参阅 Amazon VPC 用户指南中的 VPC 流日志。

修复

要创建 VPC 流日志，请参阅 Amazon VPC 用户指南中的创建流日志。打开 Amazon VPC 控制台后，选择您的 VPC。对于筛选条件，选择拒绝或全部。

[EC2.7] 应启用 EBS 默认加密

相关要求：独联体 AWS 基金会基准 v1.4.0/2.2.1、CIS 基金会基准 v3.0.0/2.2.1、nist.800-53.r5 C AWS A-9 (1)、nist.800-53.r5 CM-3 (6)、nist.800-53.r5 SC-13、nist.800-53.r5 SC-28、nist.800-53.r5

SC-28 (1)、nist.800-53.r5 (1)、nist.800-53.r5、nist.800-53.r5、nist.800-53.r5 (1)、nist.800-53.r5 (1)、nist.-53.r5 SC-7 (10)、nist.800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`ec2-ebs-encryption-by-default`

计划类型：定期

参数：无

此控件检查在默认情况下，Amazon Elastic Block Store (Amazon EBS) 是否启用账户级加密。如果未启用账户级别加密，则控制失败。

为账户启用加密后，Amazon EBS 卷和快照副本将进行静态加密。这为数据增加了一层额外的保护。有关更多信息，请参阅 Amazon EC2 用户指南中的默认加密。

请注意，以下实例类型不支持加密：R1、C1 和 M1。

修复

要为 Amazon EBS 卷配置默认加密，请参阅 Amazon EC2 用户指南中的默认加密。

[EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)

相关要求：CIS AWS 基金会基准 v3.0.0/5.6、nist.800-53.r5 AC-3、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (7)、nist.800-53.r5 AC-6 (7)、nist.800-53.r5 AC-6

类别：保护 > 网络安全

严重性：高

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-imdsv2-check`

计划类型：已触发变更

参数：无

此控件检查 EC2 实例元数据版本是否配置了实例元数据服务版本 2 (IMDSv2)。如果将 `HttpTokens` 设置为对 imdsv2 是“必需”，则控制通过。如果设置为，`HttpTokens`则控制失败`optional`。

您可以使用实例元数据来配置或管理正在运行的实例。IMDS 提供对临时的、经常轮换的凭证的访问权限。这些凭证消除了手动或以编程方式对实例进行硬编码或分发敏感凭证的需要。IMDS 在本地连接到每个 EC2 实例。它在特殊的“链路本地地址”IP 地址 169.254.169.254。该 IP 地址只能由实例上运行的软件访问。

IMDS 版本 2 为以下类型的漏洞添加了新的保护。这些漏洞可用于尝试访问 IMDS。

- 打开网站应用程序防火墙
- 打开反向代理
- 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。

修复

要使用 imdsv2 配置 EC2 实例，请参阅 Amazon EC2 用户指南中的推荐要求 imdsv2 的路径。

[EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-instance-no-public-ip`

计划类型：已触发变更

参数：无

此控件检查 EC2 实例是否具有公有 IP 地址。如果EC2实例配置项中存在 `publicIp` 字段，则控制失败。此控件仅适用于 IPv4 地址。

公共 IPv4 地址是可从 Internet 访问的 IP 地址。如果您使用公共 IP 地址启动实例，则可以通过 Internet 访问 EC2 实例。私有 IPv4 地址是无法从 Internet 访问的 IP 地址。您可以使用私有 IPv4 地址在同一 VPC 或连接的私有网络中的 EC2 实例之间进行通信。

IPv6 地址是全球唯一的，因此可以通过 Internet 访问。但是，默认情况下，所有子网的 IPv6 寻址属性都设置为 false。有关 IPv6 的更多信息，请参阅 Amazon VPC 用户指南中的 VPC 中的 IP 地址。

如果您有合法的用例来维护带有公有 IP 地址的 EC2 实例，则可以隐藏此控件的调查发现。有关前端架构选项的更多信息，请参阅 AWS 架构博客或这就是我的架构系列。

修复

使用非默认 VPC，以便实例默认情况下不会分配公有 IP 地址。

当您在默认 VPC 中启动 EC2 实例时，系统会为其分配一个公共 IP 地址。当您在非默认 VPC 中启动 EC2 实例时，子网配置决定其是否接收公有 IP 地址。子网具有一个属性，用于确定子网中的新 EC2 实例是否从公共 IPv4 地址池接收公共 IP 地址。

您无法手动将自动分配的公共 IP 地址与 EC2 实例关联或取消关联。要控制 EC2 实例是否接收公共 IP 地址，请执行以下操作之一：

- 修改子网的公共 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 地址分配功能。这将覆盖子网的公有 IP 寻址属性。有关更多信息，请参阅 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《Amazon EC2 用户指南》中的公有 IPv4 地址和外部 DNS 主机名。

如果 EC2 实例与弹性 IP 地址关联，则可以通过 Internet 访问 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。要取消关联弹性 IP 地址，请参阅 Amazon EC2 用户指南中的取消关联弹性 IP 地址。

[EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5

SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)。

类别：保护 > 安全网络配置 > API 私有访问

严重性：中

资源类型：`AWS::EC2::VPC`

AWS Config 规则：`service-vpc-endpoint-enabled`

计划类型：定期

参数：

- `serviceName`：`ec2`（不可自定义）

此控件检查是否为每个 VPC 创建了 Amazon EC2 的服务端点。如果 VPC 没有为 Amazon EC2 服务创建 VPC 端点，则控制失败。

此控件评估单个账户中的资源。它不能描述账户之外的资源。由于而 AWS Config 且 Security Hub 不进行跨账户检查，因此您将看到跨账户共享的 VPC 的`FAILED`调查结果。Security Hub 建议您隐瞒这些 `FAILED` 结果。

要改善 VPC 的安全状况，您可以将 Amazon EC2 配置为使用接口 VPC 端点。接口终端节点由一项技术提供支持 AWS PrivateLink，该技术使您能够私下访问 Amazon EC2 API 操作。它将 VPC 和 Amazon EC2 之间的所有网络流量限制为 Amazon 网络。由于端点仅在同一区域内受支持，因此您无法在 VPC 和不同区域中的服务之间创建端点。这样可以防止对其他区域进行意外的 Amazon EC2 API 调用。

要了解有关为亚马逊 EC2 创建 VPC 终端节点的更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 和接口 VPC 终端节点。

修复

要从 Amazon VPC 控制台创建到 Amazon EC2 的接口端点，请参阅 AWS PrivateLink 指南中的创建 VPC 端点。对于服务名称，选择 com.amazonaws.***region***.ec2。

您还可以创建端点策略并将其附加到 VPC 端点以控制对 Amazon EC2 API 的访问。有关创建 VPC 终端节点策略的说明，请参阅 Amazon EC2 用户指南中的创建终端节点策略。

[EC2.12] 应删除未使用的 Amazon EC2 EIP

相关要求：PCI DSS v3.2.1/2.4、NIST.800-53.r5 CM-8(1)。

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::EC2::EIP`

AWS Config 规则：`eip-attached`

计划类型：已触发变更

参数：无

此控件检查分配给 VPC 的弹性 IP (EIP) 地址是否附加到 EC2 实例或正在使用的弹性网络接口 (ENI)。

失败的调查发现表示，您可能具有未使用的 EC2 EIP。

这将帮助您在持卡人数据环境 (CDE) 中维护准确的 EIP 资产清单。

要释放未使用的 EIP，请参阅 Amazon EC2 用户指南中的释放弹性 IP 地址。

[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量

相关要求：CIS AWS 基金会基准 v1.2.0/4.1、PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/2.2、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 CM-7、nist.800-53.r5 CM-7、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 CM-7、nist.800-53.r5 5 SC-7、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (16)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-7 (5)

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`restricted-ssh`

计划类型：已触发变更

参数：无

该控件检查 Amazon EC2 安全组是否允许从 0.0.0.0/0 或 ::/0 进入端口 22。如果安全组允许从 0.0.0.0/0 或 ::/0 进入端口 22，则控制失败。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。我们建议不要让任何安全组允许对端口 22 进行不受限制的传入访问。删除与 SSH 等远程控制台服务的自由连接可减少服务器暴露的风险。

修复

要禁止进入端口 22，请移除允许与 VPC 关联的每个安全组进行此类访问的规则。有关说明，请参阅 Amazon EC2 用户指南中的更新安全组规则。在 Amazon EC2 控制台中选择安全组后，选择操作、编辑入站规则。删除允许访问端口 22 的规则。

[EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量

相关要求：独联体 AWS 基金会基准 v1.2.0/4.2

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则:**`restricted-common-ports`**（创建的规则是`restricted-rdp`）

计划类型：已触发变更

参数：无

该控件检查 Amazon EC2 安全组是否允许从 0.0.0.0/0 或 ::/0 进入端口 3389。如果安全组允许从 0.0.0.0/0 或 ::/0 进入端口 3389，则控制失败。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。我们建议不要让任何安全组允许对端口 3389 进行不受限制的传入访问。删除与 RDP 等远程控制台服务的自由连接可减少服务器暴露的风险。

修复

要禁止进入端口 3389，请移除允许与 VPC 关联的每个安全组进行此类访问的规则。有关说明，请参阅 Amazon VPC 用户指南中的更新安全组规则。在 Amazon VPC 控制台中选择安全组后，选择操作、编辑入站规则。删除允许访问端口 3389 的规则。

[EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::EC2::Subnet`

AWS Config 规则：`subnet-auto-assign-public-ip-disabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon Virtual Private Cloud (Amazon VPC) 子网中的公有 IP 分配是否已设置 `MapPublicIpOnLaunch` 为 `FALSE`。如果将该标志设置为 `FALSE`，则控制通过。

所有子网都有一个属性，用于确定在子网中创建的网络接口是否自动接收公共 IPv4 地址。启动到启用了此属性的子网中的实例会为其主网络接口分配一个公共 IP 地址。

修复

要将子网配置为不分配公有 IP 地址，请参阅 Amazon VPC 用户指南中的修改子网的公有 IPv4 寻址属性。清除启用自动分配公有 IPv4 地址复选框。

[EC2.16] 应删除未使用的网络访问控制列表

相关要求：NIST.800-53.r5 CM-8(1)。

类别：保护 > 网络安全

严重性：低

资源类型：`AWS::EC2::NetworkAcl`

AWS Config 规则：`vpc-network-acl-unused-check`

计划类型：已触发变更

参数：无

此控件检查您的虚拟私有云 (VPC) 中是否存在任何未使用的网络访问控制列表（网络 ACL）。如果网络 ACL 未与子网关联，则控制失败。该控件不会生成未使用的默认网络 ACL 的调查结果。

此控件检查资源 `AWS::EC2::NetworkAcl` 的项目配置并确定网络 ACL 的关系。

如果唯一的关系是网络 ACL 的 VPC，则控制失败。

如果列出了其他关系，则控件通过。

修复

有关删除未使用的网络 ACL 的说明，请参阅 Amazon VPC 用户指南中的删除网络 ACL。您无法删除默认网络 ACL 或与子网相关联的 ACL。

[EC2.17] Amazon EC2 实例不应使用多个 ENI

相关要求：NIST.800-53.r5 AC-4(21)

类别：保护 > 网络安全

严重性：低

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`ec2-instance-multiple-eni-check`

计划类型：已触发变更

参数：

- `Adapterids` - 附加到 EC2 实例的网络接口 ID 列表（不可定制）

此控件检查 EC2 实例是否使用多个弹性网络接口 (ENI) 或 Elastic Fabric Adapters (EFAs)。如果使用单个网络适配器，则此控制通过。该控件包括一个可选参数列表，用于标识允许的 ENI。如果属于 Amazon EKS 集群的 EC2 实例使用多个 ENI，则此控制也会失败。如果 EC2 实例需要将多个 ENI 作为 Amazon EKS 集群的一部分，则可以隐藏这些控件调查发现。

多个 ENI 可能导致双主机实例，即具有多个子网的实例。这会增加网络安全的复杂性并引入意外的网络路径和访问。

修复

要将网络接口与 EC2 实例分离，请参阅 A mazon EC2 用户指南中的将网络接口与实例分离。

[EC2.18] 安全组应只允许授权端口不受限制的传入流量

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)。

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`vpc-sg-open-only-to-authorized-ports`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`authorizedTcpPorts`	授权的 TCP 端口列表	IntegerList（最多 32 个项目）	1 到 65535	`[80,443]`
`authorizedUdpPorts`	授权的 UDP 端口列表	IntegerList（最多 32 个项目）	1 到 65535	无默认值

此控件检查 Amazon EC2 安全组是否允许从未经授权的端口传入不受限制的流量。控制状态如下所示确定：

- 如果您使用 `authorizedTcpPorts` 的默认值，则当安全组允许从端口 80 和 443 以外的任何端口传入无限制流量时，则控制失败。
- 如果您为 `authorizedTcpPorts` 或 `authorizedUdpPorts` 提供自定义值，则当安全组允许从任何未列出的端口传入无限制流量时，则控制失败。

- 如果不使用任何参数，则对于任何具有不受限制入站流量规则的安全组，则控制失败。

安全组提供对 AWS的传入和传出网络流量的状态筛选。安全组规则应遵循最低权限访问的原则。不受限制的访问（带有 /0 后缀的 IP 地址）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。除非明确允许某个端口，否则该端口应拒绝不受限制的访问。

修复

要修改安全组，请参阅《Amazon VPC 用户指南》中的使用安全组。

[EC2.19] 安全组不应允许不受限制地访问高风险端口

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)。

类别：保护 > 受限网络访问

严重性：严重

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则:**`restricted-common-ports`**（创建的规则是`vpc-sg-restricted-common-ports`）

计划类型：已触发变更

参数：`"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560`可自定义）

此控件检查高风险的指定端口是否可以访问 Amazon EC2 安全组的不受限制的传入流量。如果安全组中的任何规则允许从“0.0.0.0/0”或“::/0”传入这些端口的流量，则控制失败。

安全组为 AWS 资源提供传入和传出网络流量的有状态筛选。不受限制的访问 (0.0.0.0/0) 增加了恶意活动的机会，例如黑客 denial-of-service 攻击、攻击和数据丢失。任何安全组都不应允许对以下端口进行不受限制的入口访问：

- 20、21 (FTP)
- 22 (SSH)

- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000（Go、Node.js 和 Ruby Web 开发框架）
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000（Python 网络开发框架）
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601（仪表板）OpenSearch
- 8080（代理）
- 8088（传统的 HTTP 端口）
- 8888（备用 HTTP 端口）
- 9200 或 9300 () OpenSearch

修复

要从安全组中删除规则，请参阅 Amazon EC2 用户指南中的从安全组中删除规则。

[EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::EC2::VPNConnection`

AWS Config 规则：vpc-vpn-2-tunnels-up

计划类型：已触发变更

参数：无

VPN 隧道是一种加密链路，数据可以在其中从客户网络传输到站点到站点 VPN 连接或从 AWS 站点到站点 VPN 连接 AWS 内传输。每个 VPN 连接均包括两条 VPN 隧道，可以同时使用这两条隧道来实现高可用性。确保两个 VPN 隧道都已开通 VPN 连接对于确认 VP AWS C 和远程网络之间的安全且高度可用的连接非常重要。

此控件检查 AWS 站点到站点 VPN 提供的两个 VPN 隧道是否都处于 UP 状态。如果一条或两条隧道都处于关闭状态，则控制失败。

修复

要修改 VPN 隧道选项，请参阅站点到站点 VPN 用户指南中的修改站点到站点 VPN 隧道选项。 AWS

[EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389

相关要求：独联体 AWS 基金会基准 v1.4.0/5.1、CIS 基金会基准 v3.0.0/5.1、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 C AWS A-9 (1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-7、nist.800-53.r5 CM-7、nist.800-53.r5 SC-7、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (5)

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::EC2::NetworkAcl

AWS Config 规则：nacl-no-unrestricted-ssh-rdp

计划类型：已触发变更

参数：无

此控件检查网络访问控制列表（网络 ACL）是否允许 SSH/RDP 入口流量不受限制地访问默认 TCP 端口。如果网络 ACL 入站条目允许 TCP 端口 22 或 3389 的源 CIDR 块为 '0.0.0.0/0' 或 ':: /0'，则控制失败。该控件不会生成默认网络 ACL 的调查结果。

对远程服务器管理端口（例如端口 22 (SSH) 和端口 3389 (RDP)）的访问不应公开访问，因为这可能会允许对 VPC 内的资源进行意外访问。

修复

要编辑网络 ACL 流量规则，请参阅 Amazon VPC 用户指南中的使用网络 ACL。

[EC2.22] 应删除未使用的 Amazon EC2 安全组

> **Important**
>
> 退出特定标准 — Security Hub 于 2023 年 9 月 20 日从《 AWS 基础安全最佳实践》标准和 NIST SP 800-53 Rev. 5 中删除了此控件。此控件仍然是服务管理标准的一部分: AWS Control Tower. 如果安全组连接到 EC2 实例或弹性网络接口，此 控件会生成一个通过的调查发现。但是，对于某些用例，未附加的安全组不会构成安全风险。您可以使用其他 EC2 控件（例如 EC2.2、EC2.13、EC2.14、EC2.18 和 EC2.19）来监控您的安全组。

类别：识别 > 清单

严重性：中

资源类型：`AWS::EC2::NetworkInterface`、`AWS::EC2::SecurityGroup`

AWS Config 规则：`ec2-security-group-attached-to-eni-periodic`

计划类型：定期

参数：无

此控件检查安全组是连接到亚马逊弹性计算云 (Amazon EC2) 实例还是连接到弹性网络接口。如果安全组未与 Amazon EC2 实例或弹性网络接口关联，则控制失败。

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] Amazon EC2 中转网关不应自动接受 VPC 附件请求

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2。

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EC2::TransitGateway`

AWS Config 规则：ec2-transit-gateway-auto-vpc-attach-disabled

计划类型：已触发变更

参数：无

此控件检查 EC2 中转网关是否自动接受共享 VPC 附件。对于自动接受共享 VPC 附件请求的中转网关，此控制失败。

开启后，中转网关将 AutoAcceptSharedAttachments 配置为自动接受任何跨账户 VPC 附件请求，无需验证请求或源自哪个账户。为了遵循授权和身份验证的最佳实践，我们建议关闭此功能，以确保仅接受经过授权的 VPC 附件请求。

修复

要修改中转网关，请参阅 Amazon VPC 开发人员指南中的修改中转网关。

[EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

相关要求：NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：AWS::EC2::Instance

AWS Config 规则：ec2-paravirtual-instance-check

计划类型：已触发变更

参数：无

此控件检查 EC2 实例的虚拟化类型是否为半虚拟化。如果 EC2 实例的 virtualizationType 设置为 paravirtual，则控制失败。

Linux 亚马逊机器映像（AMI）使用两种虚拟化类型之一：半虚拟 (PV) 或硬件虚拟机 (HVM)。半虚拟化和 HVM AMI 之间的主要区别在于它们的启动方式，以及它们能否使用特定硬件扩展 (CPU、网络和存储) 实现更好的性能。

以往，半虚拟化来宾在许多情况下的性能优于 HVM 来宾，但是由于硬件虚拟机虚拟化的功能增强以及 HVM AMI 可使用半虚拟化驱动程序，情况发生了改变。有关更多信息，请参阅 Amazon EC2 用户指南中的 Linux AMI 虚拟化类型。

修复

要将 EC2 实例更新为新的实例类型，请参阅 Amazon EC2 用户指南中的更改实例类型。

[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EC2::LaunchTemplate`

AWS Config 规则：`ec2-launch-template-public-ip-disabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon EC2 启动模板是否配置为在启动时将公共 IP 地址分配给网络接口。如果 EC2 启动模板配置为向网络接口分配公共 IP 地址，或者至少有一个网络接口具有公共 IP 地址，则则控制失败。

公共 IP 地址是可通过 Internet 访问的地址。如果您使用公共 IP 地址配置网络接口，则可以通过 Internet 访问与这些网络接口关联的资源。EC2 资源不应公开访问，因为这可能会导致对工作负载的意外访问。

修复

要更新 EC2 启动模板，请参阅 Amazon EC2 Auto Scaling 用户指南中的变更默认网络接口设置。

[EC2.28] 备份计划应涵盖 EBS 卷

类别：恢复 > 弹性 > 启用备份

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

严重性：低

资源类型：AWS::EC2::Volume

AWS Config 规则：**ebs-resources-protected-by-backup-plan**

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
backupVaultLockCheck	如果将参数设置为，true并且资源使用 AWS Backup 文件库锁定，则控件会生成PASSED结果。	布尔值	true 或者 false	无默认值

此控件评估备份计划是否涵盖处于 in-use 状态的 Amazon EBS 卷。如果备份计划不涵盖某个 EBS 卷，则控制失败。如果将backupVaultLockCheck参数设置为true，则仅当 EBS 卷备份到 AWS Backup 锁定的存储库中时，控制才会通过。

备份可帮助您更快地从安全事件中恢复。它们还增强了系统的故障恢复能力。将 Amazon EBS 卷包含在备份计划中可帮助您保护数据免遭意外丢失或删除。

修复

要将 Amazon EBS 卷添加到 AWS Backup 备份计划中，请参阅AWS Backup 开发人员指南中的为备份计划分配资源。

[EC2.33] 应标记 EC2 传输网关附件

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::TransitGatewayAttachment

AWS Config 规则：tagged-ec2-transitgatewayattachment（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 传输网关附件是否具有参数中定义的特定密钥的标签requiredTagKeys。如果公交网关附件没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果没有使用任何密钥标记公交网关附件，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 传输网关附件添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.34] 应标记 EC2 传输网关路由表

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::TransitGatewayRouteTable

AWS Config 规则：`tagged-ec2-transitgatewayroutetable`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 传输网关路由表是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果公交网关路由表没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果公交网关路由表未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 传输网关路由表添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.35] 应标记 EC2 网络接口

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::NetworkInterface`

AWS Config 规则：`tagged-ec2-networkinterface`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 网络接口是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果网络接口没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果网络接口未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 网络接口添加标签，请参阅亚马逊 EC2 用户指南中的为亚马逊 EC2 资源添加标签。

[EC2.36] 应标记 EC2 客户网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::CustomerGateway

AWS Config 规则：tagged-ec2-customergateway（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 客户网关是否具有参数中定义的特定密钥的标签requiredTagKeys。如果客户网关没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果客户网关未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 客户网关添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.37] 应标记 EC2 弹性 IP 地址

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::EIP`

AWS Config 规则：`tagged-ec2-eip`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 弹性 IP 地址是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果弹性 IP 地址没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果弹性 IP 地址未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 弹性 IP 地址添加标签，请参阅亚马逊 EC2 用户指南中的为亚马逊 EC2 资源添加标签。

[EC2.38] 应标记 EC2 实例

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::Instance`

AWS Config 规则：`tagged-ec2-instance`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 实例是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果实例没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如

果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果实例未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 实例添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.39] 应标记 EC2 互联网网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::InternetGateway

AWS Config 规则：tagged-ec2-internetgateway（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 互联网网关是否具有参数中定义的特定密钥的标签requiredTagKeys。如果 Internet 网关没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果未使用任何密钥标记 Internet 网关，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 互联网网关添加标签，请参阅亚马逊 EC2 用户指南中的为亚马逊 EC2 资源添加标签。

[EC2.40] 应标记 EC2 NAT 网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::NatGateway

AWS Config 规则：`tagged-ec2-natgateway`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 网络地址转换 (NAT) 网关是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果 NAT 网关没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果 NAT 网关未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 NAT 网关添加标签，请参阅亚马逊 EC2 用户指南中的为亚马逊 EC2 资源添加标签。

[EC2.41] 应标记 EC2 网络 ACL

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::NetworkAcl`

AWS Config 规则：`tagged-ec2-networkacl`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 网络访问控制列表 (网络 ACL) 是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果网络 ACL 没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果网络 ACL 未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 网络 ACL 添加标签，请参阅亚马逊 EC2 用户指南中的为亚马逊 EC2 资源添加标签。

[EC2.42] 应标记 EC2 路由表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::RouteTable`

AWS Config 规则：`tagged-ec2-routetable`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 路由表是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果路由表没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果路由表未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 路由表添加标签，请参阅亚马逊 EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.43] 应标记 EC2 安全组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::SecurityGroup`

AWS Config 规则：`tagged-ec2-securitygroup`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 安全组是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果安全组没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如

果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果安全组未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 安全组添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.44] 应标记 EC2 子网

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::Subnet

AWS Config 规则：tagged-ec2-subnet（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 子网是否具有参数中定义的特定密钥的标签requiredTagKeys。如果子网没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果子网未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 子网添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.45] 应标记 EC2 卷

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::EC2::Volume

AWS Config 规则：`tagged-ec2-subnet`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 卷是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果卷没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果卷未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 卷添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.46] 应给亚马逊 VPC 加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPC`

AWS Config 规则：`tagged-ec2-vpc`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查亚马逊虚拟私有云（Amazon VPC）是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果 Amazon VPC 没有任何标签密钥或参数中没有指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果 Amazon VPC 未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 VPC 添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.47] 应标记 Amazon VPC 终端节点服务

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPCEndpointService`

AWS Config 规则：`tagged-ec2-vpcendpointservice`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon VPC 终端节点服务是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果终端节点服务没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果终端节点服务未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Amazon VPC 终端节点服务添加标签，请参阅AWS PrivateLink 指南配置终端节点服务部分中的管理标签。

[EC2.48] 应标记 Amazon VPC 流日志

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::FlowLog`

AWS Config 规则：`tagged-ec2-flowlog`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon VPC 流日志是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果流日志没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果流日志未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Amazon VPC 流日志添加标签，请参阅 A mazon VPC 用户指南中的为流日志添加标签。

[EC2.49] 应标记 Amazon VPC 对等连接进行标记

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPCPeeringConnection`

AWS Config 规则：`tagged-ec2-vpcpeeringconnection`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon VPC 对等连接是否具有参数requiredTagKeys中定义的特定密钥的标签。如果对等连接没有任何标签密钥或者没有参数requiredTagKeys中指定的所有密钥，则控件将失败。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果对等连接未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Amazon VPC 对等连接添加标签，请参阅亚马逊 EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.50] 应标记 EC2 VPN 网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::VPNGateway`

AWS Config 规则：`tagged-ec2-vpngateway`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 VPN 网关是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果 VPN 网关没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果 VPN 网关未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 VPN 网关添加标签，请参阅亚马逊 EC2 用户指南中的为亚马逊 EC2 资源添加标签。

[EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录

相关要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：低

资源类型：`AWS::EC2::ClientVpnEndpoint`

AWS Config 规则：**`ec2-client-vpn-connection-log-enabled`**

计划类型：已触发变更

参数：无

此控件检查 AWS Client VPN 端点是否启用了客户端连接日志记录。如果端点未启用客户端连接日志记录，则控制失败。

客户端 VPN 端点允许远程客户端安全地连接到 AWS中虚拟私有云（VPC）中的资源。连接日志允许您跟踪 VPN 端点上的用户活动并提供可见性。启用连接日志记录时，可以在日志组中指定日志流的名称。如果未指定日志流，Client VPN 服务会为您创建一个日志流。

修复

要启用连接日志记录，请参阅《AWS Client VPN 管理员指南》中的为现有 Client VPN 端点启用连接日志记录。

[EC2.52] 应标记 EC2 传输网关

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EC2::TransitGateway`

AWS Config 规则：`tagged-ec2-transitgateway`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 Amazon EC2 传输网关是否具有参数中定义的特定密钥的标签requiredTagKeys。如果公交网关没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果传输网关未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EC2 传输网关添加标签，请参阅 Amazon EC2 用户指南中的标记您的 Amazon EC2 资源。

[EC2.53] EC2 安全组不应允许从 0.0.0.0/0 进入远程服务器管理端口

相关要求：独联体 AWS 基金会基准 v3.0.0/5.2

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：AWS::EC2::SecurityGroup

AWS Config 规则：vpc-sg-port-restriction-check

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
ipType	IP 版本	String	不可自定义	IPv4
restrictPorts	应拒绝入口流量的端口列表	IntegerList	不可自定义	22,3389

此控件检查 Amazon EC2 安全组是否允许从 0.0.0.0/0 进入远程服务器管理端口（端口 22 和 3389）。如果安全组允许从 0.0.0.0/0 到端口 22 或 3389 的入口，则控制失败。

安全组对流向资源的入口和出口网络流量提供状态过滤。 AWS 我们建议任何安全组都不允许使用 TDP (6)、UDP (17) 或 ALL (-1) 协议不受限制地访问远程服务器管理端口，例如 SSH 到端口 22，RDP 到端口 3389。允许公众访问这些端口会增加资源攻击面和资源泄露的风险。

修复

要更新 EC2 安全组规则以禁止进入指定端口的流量，请参阅 Amazon EC2 用户指南中的更新安全组规则。在 Amazon EC2 控制台中选择安全组后，选择操作、编辑入站规则。删除允许访问端口 22 或端口 3389 的规则。

[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口

相关要求：独联体 AWS 基金会基准 v3.0.0/5.3

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：AWS::EC2::SecurityGroup

AWS Config 规则：vpc-sg-port-restriction-check

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`ipType`	IP 版本	String	不可自定义	`IPv6`
`restrictPorts`	应拒绝入口流量的端口列表	IntegerList	不可自定义	`22,3389`

此控件检查 Amazon EC2 安全组是否允许从:: /0 进入远程服务器管理端口（端口 22 和 3389）。如果安全组允许从:: /0 进入端口 22 或 3389，则控制失败。

安全组对流向资源的入口和出口网络流量提供状态过滤。 AWS 我们建议任何安全组都不允许使用 TDP (6)、UDP (17) 或 ALL (-1) 协议不受限制地访问远程服务器管理端口，例如 SSH 到端口 22，RDP 到端口 3389。允许公众访问这些端口会增加资源攻击面和资源泄露的风险。

修复

要更新 EC2 安全组规则以禁止进入指定端口的流量，请参阅 Amazon EC2 用户指南中的更新安全组规则。在 Amazon EC2 控制台中选择安全组后，选择操作、编辑入站规则。删除允许访问端口 22 或端口 3389 的规则。

Amazon EC2 Auto Scaling 控件

这些控件与 Amazon EC2 Auto Scaling 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查

相关要求：PCI DSS v3.2.1/2.2、NIST.800-53.r5 CA-7、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 SI-2。

类别：识别 > 清单

严重性：低

资源类型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 规则：autoscaling-group-elb-healthcheck-required

计划类型：已触发变更

参数：无

此控件检查与负载均衡器关联的 Amazon EC2 Auto Scaling 组是否使用弹性负载平衡 (ELB) 运行状况检查。如果 Auto Scaling 组不使用 ELB 运行状况检查，则控制失败。

ELB 运行状况检查有助于确保 Auto Scaling 组能够根据负载均衡器提供的其他测试来确定实例的运行状况。使用 Elastic Load Balancing 运行状况检查还有助于支持使用 EC2 Auto Scaling 组的应用程序的可用性。

修复

要添加弹性负载均衡运行状况检查，请参阅 Amazon EC2 Auto Scaling 用户指南中的添加弹性负载均衡运行状况检查。

[AutoScaling.2] Amazon EC2 Auto Scaling 组应覆盖多个可用区

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::AutoScaling::AutoScalingGroup

AWS Config 规则：autoscaling-multiple-az

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
minAvailabilityZones	可用区的最小数量	枚举	2, 3, 4, 5, 6	2	

该控件检查 Amazon EC2 Auto Scaling 组是否至少跨越指定数量的可用区（AZ）。如果自动扩缩组未跨越至少指定数量的可用区，则控制失败。除非您为可用区的最小数量提供自定义参数值，否则 Security Hub 将使用默认值即两个可用区。

如果配置的单个可用区不可用，不跨多个可用区的自动扩缩组无法在另一个可用区中启动实例来进行补偿。但在某些使用案例中，例如批处理作业，或需要将可用区间传输成本保持在最低时，首选具有单个可用区的自动扩缩组。在这种情况下，您可以禁用此控件或隐藏其调查发现。

修复

要向现有自动扩缩组添加可用区，请参阅《Amazon EC2 Auto Scaling 用户指南》中的添加和删除可用区。

[AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)

相关要求：NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2。

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 规则：`autoscaling-launchconfig-requires-imdsv2`

计划类型：已触发变更

参数：无

此控件检查是否在 Amazon EC2 自动扩缩组启动的所有实例上启用了 IMDSv2。如果启动配置中未包含实例元数据服务（IMDS）版本，或者同时启用 IMDSv1 和 IMDSv2，则控制失败。

IMDS 提供有关实例的数据，您可以使用这些数据来配置或管理正在运行的实例。

IMDS 第 2 版添加了 IMDSv1 中没有的新保护措施，以进一步保护 EC2 实例。

修复

自动扩缩组一次与一个启动配置关联。在创建启动配置后，您将无法对其进行修改。要更改自动扩缩组的启动配置，请使用现有启动配置作为启用 IMDSv2 的新启动配置的基础。有关更多信息，请参阅 Amazon EC2 用户指南中的为新实例配置实例元数据选项。

[AutoScaling.4] Auto Scaling 组启动配置的元数据响应跳跃限制不应大于 1

> **Important**
>
> Security Hub 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 规则：`autoscaling-launch-config-hop-limit`

计划类型：已触发变更

参数：无

此控件检查元数据令牌可以传输的网络跃点数。如果元数据响应跳数限制大于 1，则控制失败。

实例元数据服务（IMDS）提供有关 Amazon EC2 实例的元数据信息，对于应用程序配置非常有用。将元数据服务的 HTTP PUT 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) 字段每个跳点上减少一个。这种减少可用于确保数据包不会在 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。在 IMDSv2 中，由于默认的元数据响应跃点限制设置为 1，因此包含密钥令牌的 PUT 响应无法传送到实例之外。但是，如果该值大于 1，则令牌可以离开 EC2 实例。

修复

要修改现有启动配置的元数据响应跳跃限制，请参阅 Amazon EC2 用户指南中的修改现有实例的实例元数据选项。

[Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5

SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 规则：`autoscaling-launch-config-public-ip-disabled`

计划类型：已触发变更

参数：无

此控件检查自动扩缩组的关联启动配置是否为该组的实例分配了公有 IP 地址。如果关联的启动配置分配了公有 IP 地址，则控制失败。

自动扩缩组启动配置中的 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，而不能直接暴露在 Internet 上。

修复

自动扩缩组一次与一个启动配置关联。在创建启动配置后，您将无法对其进行修改。要更改 Auto Scaling 组的启动配置，请将现有的启动配置作为新启动配置的基础。然后，更新 Auto Scaling 组以使用新的启动配置。有关 step-by-step 说明，请参阅 Amazon EC2 Auto Scaling 用户指南中的更改 Auto Scaling 组的启动配置。创建新的启动配置时，在其他配置下，在高级详细信息、IP 地址类型下，选择不要为任何实例分配公有 IP 地址。

变更启动配置后，自动扩缩会使用新的配置选项启动新实例。现有实例不受影响。要更新现有实例，我们建议您刷新实例，或者根据终止策略启用自动扩缩，以逐步使用较新实例替换较旧实例。有关更新自动扩缩实例的更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的更新自动扩缩实例。

[AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 规则：autoscaling-multiple-instance-types

计划类型：已触发变更

参数：无

此控件检查 Amazon EC2 自动扩缩组是否使用多种实例类型。如果自动扩缩组仅定义了一个实例类型，则控制失败。

您可以跨多个可用区中运行的多个实例类型部署应用程序以提高可用性。Security Hub 建议使用多种实例类型，以便自动扩缩组在您选择的可用区中实例容量不足时可以启动另一种实例类型。

修复

要创建具有多个实例类型的自动扩缩组，请参阅 Amazon EC2 Auto Scaling 用户指南中的具有多个实例类型和购买选项的自动扩缩组。

[AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 资源配置

严重性：中

资源类型：AWS::AutoScaling::AutoScalingGroup

AWS Config 规则：autoscaling-launch-template

计划类型：已触发变更

参数：无

此控件检查 Amazon EC2 自动扩缩组是否是基于 EC2 启动模板创建的。如果未使用启动模板创建 Amazon EC2 自动扩缩组，或者混合实例策略中未指定启动模板，则此控制失败。

可以从 EC2 启动模板或启动配置创建 EC2 自动扩缩组。但是，使用启动模板创建自动扩缩组可确保您能够访问最新功能和改进。

修复

要使用 EC2 启动模板创建自动扩缩组，请参阅 Amazon EC2 Auto Scaling 用户指南 中的使用启动模板创建自动扩缩组。有关如何用启动模板替换启动配置的信息，请参阅 Amazon EC2 用户指南中的将启动配置替换为启动模板。

[AutoScaling.10] 应标记 EC2 Auto Scaling 群组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 规则：`tagged-autoscaling-autoscalinggroup`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EC2 Auto Scaling 组是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果 Auto Scaling 组没有任何标签密钥或者该组没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果 Auto Scaling 组未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Auto Scaling 组添加标签，请参阅 Amazon EC2 Auto Scaling 用户指南中的为 Auto Scaling 组和实例添加标签。

Amazon EC2 Systems Manager 控件

这些控制与由管理的 Amazon EC2 实例相关 AWS Systems Manager。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

相关要求：PCI DSS v3.2.1/2.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(2)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SA-15(2)、NIST.800-53.r5 SA-15(8)、NIST.800-53.r5 SA-3、NIST.800-53.r5 SI-2(3)。

类别：识别 > 清单

严重性：中

评估的资源：`AWS::EC2::Instance`

所需的 AWS Config 录制资源：`AWS::EC2::Instance`，`AWS::SSM::ManagedInstanceInventory`

AWS Config 规则：`ec2-instance-managed-by-systems-manager`

计划类型：已触发变更

参数：无

此控件检查您账户中已停止和正在运行的 EC2 实例是否由管理 AWS Systems Manager。您可以使用 S AWS 服务 ystems Manager 来查看和控制您的 AWS 基础架构。

为了帮助您维护安全性和合规性，Systems Manager 会扫描已停止和正在运行的托管实例。托管实例是配置为与 Systems Manager 一起使用的机器。然后，Systems Manager 会报告其检测到的任何策略违规行为或采取纠正措施。Systems Manager 还可以帮助您配置和维护托管实例。

要了解有关更多信息，请参阅 AWS Systems Manager 用户指南。

修复

要使用 Systems Manager 管理 EC2 实例，请参阅 AWS Systems Manager 用户指南中的 Amazon EC2 主机管理。在配置选项部分，您可以保留默认选项或根据需要对其进行变更，以满足首选配置。

[SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

相关要求：PCI DSS v3.2.1/6.2、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(3)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::SSM::PatchCompliance`

AWS Config 规则：`ec2-managedinstance-patch-compliance-status-check`

计划类型：已触发变更

参数：无

该控件在实例上安装补丁后检查 Systems Manager 补丁合规性的合规状态是否为 `COMPLIANT` 或 `NON_COMPLIANT`。如果合规性状态为 `NON_COMPLIANT`，则控制失败。该控件仅检查 Systems Manager Patch Manager 管理的实例。

根据您的组织的要求修补 EC2 实例可以减少 AWS 账户的攻击面。

修复

Systems Manager 建议使用补丁策略为您的托管实例配置补丁。您也可以使用 Systems Manager 文档（如以下过程所述）来修补实例。

修复不合规的补丁

1. 打开 AWS Systems Manager 控制台，网址为 https://console.aws.amazon.com/systems-manager/。
2. 对于节点管理，选择运行命令，然后选择运行命令。
3. 选择 AWS- 的选项RunPatchBaseline。
4. 将 Operation (操作) 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. 选择运行。
7. 命令完成后，要监控已修补实例的新合规性状态，请在导航窗格中选择合规性。

[SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT

相关要求：PCI DSS v3.2.1/2.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2(3)。

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::SSM::AssociationCompliance`

AWS Config 规则：`ec2-managedinstance-association-compliance-status-check`

计划类型：已触发变更

参数：无

此控件检查 AWS Systems Manager 关联合规性的状态是`COMPLIANT`还是关联在实例上运行`NON_COMPLIANT`之后。如果关联合规性状态为 `NON_COMPLIANT`，则控制失败。

状态管理器关联是分配给托管实例的配置。该配置定义要在实例上保持的状态。例如，关联可以指定必须在实例上安装并运行防病毒软件，或者必须关闭某些端口。

创建一个或多个状态管理器关联后，您可以立即获得合规状态信息。您可以在控制台中查看合规性状态，也可以在响应 AWS CLI 命令或相应的 Systems Manager API 操作时查看合规性状态。对于关

联，配置合规性显示合规性状态（Compliant 或 Non-compliant）。它还显示分配给关联的严重性级别，例如 Critical 或 Medium。

要了解有关 State Manager 关联合规性的更多信息，请参阅 AWS Systems Manager 用户指南中的关于 State Manager 关联合规性。

修复

失败的关联可能与不同的事物相关，包括目标和 SSM 文档名称。要修复此问题，您必须首先通过查看关联历史记录来识别和调查关联。有关查看关联历史记录的说明，请参阅 AWS Systems Manager 用户指南中的查看关联历史记录。

调查完成后，您可以编辑关联以更正已结果的问题。您可以编辑关联以指定新名称、计划、严重级别或目标。编辑关联后， AWS Systems Manager 创建新版本。有关编辑关联的说明，请参阅 AWS Systems Manager 用户指南中的编辑和创建关联的新版本。

[SSM.4] SSM 文档不应公开

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：AWS::SSM::Document

AWS Config 规则：ssm-document-not-public

计划类型：定期

参数：无

此控件检查账户拥有的 AWS Systems Manager 文档是否公开。如果所有者 Self 的 SSM 文档是公开的，则此控制失败。

公开的 SSM 文档可能会允许文档被意外访问。公共 SSM 文档可以公开有关账户、资源和内部流程的有价值的信息。

除非使用案例要求公开共享，否则我们建议您阻止对 Self 所有的 Systems Manager 文档进行公开共享设置。

修复

要阻止 SSM 文档的公开共享，请参阅 AWS Systems Manager 用户指南中的屏蔽 SSM 文档的公开共享。

Amazon Elastic File System 控件

这些控件与 Amazon EFS 资源相关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS

相关要求：CIS AWS 基金会基准 v3.0.0/2.4.1、nist.800-53.r5 CA-9 (1)、nist.800-53.r5 CM-3 (6)、nist.800-53.r5 SC-13、nist.800-53.r5 SC-28、nist.800-53.r5 SC-28 (1)、nist.800-53.r5 SC-7 (10))，nist.800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：`efs-encrypted-check`

计划类型：定期

参数：无

此控件检查 Amazon Elastic File System 是否配置为使用加密文件数据 AWS KMS。在以下情况下，检查失败。

- 在 `DescribeFileSystems` 响应中 `Encrypted` 设置为 `false`。
- `DescribeFileSystems` 响应中的 `KmsKeyId` 密钥与 `efs-encrypted-check` 的 `KmsKeyId` 参数不匹配。

请注意，此控件不使用 `efs-encrypted-check` 的 `KmsKeyId` 参数。它只检查 `Encrypted` 的值。

为了为 Amazon EFS 中的敏感数据增加一层安全保护，您应该创建加密文件系统。Amazon EFS 支持静态文件系统加密。您可以在创建 Amazon EFS 文件系统时启用静态数据加密。要了解有关 Amazon

EFS 加密的更多信息，请参阅 Amazon Elastic File System 用户指南中的 Amazon EFS 中的数据加密。

修复

有关如何加密新的 Amazon EFS 文件系统的详细信息，请参阅 Amazon Elastic File System 用户指南中的加密静态数据。

[EFS.2] Amazon EFS 卷应包含在备份计划中

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

分类：恢复 > 弹性 > 备份

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：`efs-in-backup-plan`

计划类型：定期

参数：无

此控件检查 Amazon Elastic File System (Amazon EFS) 文件系统是否已添加到 AWS Backup中的备份计划中。如果 Amazon EFS 文件系统未包含在备份计划中，控制失败。

在备份计划中包括 EFS 文件系统可帮助您保护数据免遭删除和数据丢失。

修复

要为现有 Amazon EFS 文件系统启用自动备份，请参阅 AWS Backup 开发人员指南中的入门 4：创建 Amazon EFS 自动备份。

[EFS.3] EFS 接入点应强制使用根目录

相关要求：NIST.800-53.r5 AC-6(10)

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::EFS::AccessPoint

AWS Config 规则：efs-access-point-enforce-root-directory

计划类型：已触发变更

参数：无

此控件检查 Amazon EFS 接入点是否配置为强制使用根目录。如果的 Path 值设置为 /（文件系统的默认根目录），则控制失败。

在强制执行根目录时，使用访问点的 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。强制接入点使用根目录可确保接入点的用户只能访问指定子目录的文件，从而有助于限制数据访问。

修复

有关如何为 Amazon EFS 接入点强制使用根目录的说明，请参阅 Amazon Elastic File System 用户指南中的使用接入点强制使用根目录。

[EFS.4] EFS 接入点应强制使用用户身份

相关要求：NIST.800-53.r5 AC-6(2)。

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::EFS::AccessPoint

AWS Config 规则：efs-access-point-enforce-user-identity

计划类型：已触发变更

参数：无

此控件检查 Amazon EFS 接入点是否配置为强制执行用户身份。如果在创建 EFS 接入点时未定义 POSIX 用户身份，则此控制失败。

Amazon EFS 接入点是 EFS 文件系统中特定于应用程序的入口点，便于轻松地管理应用程序对共享数据集的访问。接入点可以为通过接入点发出的所有文件系统请求强制执行用户身份（包括用户的 POSIX 组）。接入点还可以为文件系统强制执行不同的根目录，以便客户端只能访问指定目录或其子目录中的数据。

修复

要强制执行 Amazon EFS 接入点的用户身份，请参阅 Amazon Elastic File System 用户指南中的使用接入点强制使用用户身份。

[EFS.5] 应标记 EFS 接入点

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EFS::AccessPoint`

AWS Config规则：`tagged-efs-accesspoint`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EFS 接入点是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果接入点没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果接入点未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EFS 接入点添加标签，请参阅亚马逊 Elastic F ile System 用户指南中的为 Amazon EFS 资源添加标签。

[EFS.6] EFS 挂载目标不应与公有子网关联

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：中

资源类型：`AWS::EFS::FileSystem`

AWS Config 规则：`efs-mount-target-public-accessible`

计划类型：定期

参数：无

此控件检查 Amazon EFS 挂载目标是否与私有子网关联。如果挂载目标与公有子网关联，则控制失败。

默认情况下，只能从创建文件系统的虚拟私有云 (VPC) 访问该文件系统。我们建议在无法从 Internet 访问的私有子网中创建 EFS 挂载目标。这有助于确保只有经过授权的用户才能访问您的文件系统，并且不会受到未经授权的访问或攻击。

修复

创建挂载目标后，您无法更改 EFS 挂载目标和子网之间的关联。要将现有装载目标与其他子网关联，您必须在私有子网中创建一个新的挂载目标，然后移除旧的挂载目标。有关管理挂载目标的信息，请参阅 Amazon Elastic File System 用户指南中的创建和管理挂载目标和安全组。

Amazon Elastic Kubernetes Service 控件

这些控件与 Amazon EKS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EKS.1] EKS 集群端点不应公开访问

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：高

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：`eks-endpoint-no-public-access`

计划类型：定期

参数：无

此控件检查 Amazon EKS 集群端点是否公开访问。如果 EKS 集群具有公开访问的端点，则控制失败。

当您创建新集群时，Amazon EKS 会为您用来与集群通信的托管 Kubernetes API 服务器创建一个端点。默认情况下，此 API 服务器端点可在 Internet 上公开使用。使用 (IAM) 和原生 Kubernetes 基于角色的访问控制 AWS Identity and Access Management (RBAC) 的组合来保护对 API 服务器的访问。通过移除对端点的公共访问权限，您可以避免意外暴露和访问集群。

修复

要修改现有 EKS 集群的端点访问权限，请参阅 Amazon EKS 用户指南中的修改集群端点访问权限。您可以在创建新 EKS 集群时为其设置端点访问权限。有关创建新 Amazon EKS 集群的说明，请参阅 Amazon EKS 用户指南中的创建 Amazon EKS 集群。

[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：`eks-cluster-supported-version`

计划类型：已触发变更

参数：

- `oldestVersionSupported`：`1.26`（不可自定义）

此控件检查 Amazon Elastic Kubernetes Service（Amazon EKS）集群是否在支持的 Kubernetes 版本上运行。如果 EKS 集群在不支持的版本上运行，则控制失败。

如果您的应用程序不需要特定版本的 Kubernetes，我们建议您为集群使用 EKS 支持的最新可用 Kubernetes 版本。有关更多信息，请参阅 Amazon EKS 用户指南中的 AAmazon EKS Kubernetes 发布日历和 Amazon EKS 版本支持以及常见问题解答。

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。

[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

相关要求：nist.800-53.r5 SC-8、nist.800-53.r5 SC-12、nist.800-53.r5 SC-13、nist.800-53.r5 SI-28

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：`eks-secrets-encrypted`

计划类型：定期

参数：无

此控件检查 Amazon EKS 集群是否使用加密的 Kubernetes 密钥。如果集群的 Kubernetes 密钥未加密，则控制失败。

加密密钥时，可以使用 AWS Key Management Service (AWS KMS) 密钥为集群提供存储在 etcd 中的 Kubernetes 密钥的信封加密。这种加密是对 EBS 卷加密的补充，默认情况下，EBS 卷加密对作为 EKS 集群的一部分存储在 etcd 中的所有数据（包括机密）启用。对您的 EKS 集群使用密钥加密允许

您使用您定义和管理的 KMS 密钥对 Kubernetes 密钥进行加密，从而为 Kubernetes 应用程序部署深度防御策略。

修复

要在 EKS 集群上启用密钥加密，请参阅 Amazon EKS 用户指南中的在现有集群上启用秘密加密。

[EKS.6] 应标记 EKS 集群

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EKS::Cluster`

AWS Config规则：`tagged-eks-cluster`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EKS 集群是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果集群没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果集群未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EKS 集群添加标签，请参阅 Amazon EKS 用户指南中的为你的 Amazon EKS 资源添加标签。

[EKS.7] 应标记 EKS 身份提供商配置

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::EKS::IdentityProviderConfig`

AWS Config规则：`tagged-eks-identityproviderconfig`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EKS 身份提供商配置是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果配置没有任何标签密钥或参数中没有指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果配置未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EKS 身份提供商配置添加标签，请参阅 Amazon EKS 用户指南中的为你的 Amazon EKS 资源添加标签。

[EKS.8] EKS 集群应启用审核日志记录

相关要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::EKS::Cluster`

AWS Config 规则：`eks-cluster-logging-enabled`

计划类型：定期

参数：无

此控件检查 Amazon EKS 集群是否启用了审核日志记录。如果没有为集群启用审核日志记录，则控制失败。

EKS 控制平面日志将审计和诊断日志直接从 EKS 控制平面提供给您账户中的 Amazon CloudWatch Logs。您可以选择所需的日志类型，日志将作为日志流发送到中每个 EKS 集群的群组 CloudWatch。通过日志记录，可以了解 EKS 集群的访问情况和性能。通过将 EKS 集群的 EKS 控制平面 CloudWatch 日志发送到日志，您可以在中心位置记录用于审计和诊断目的的操作。

修复

要为您的 EKS 集群启用审核日志，请参阅《Amazon EKS 用户指南》中的启用和禁用控制面板日志。

亚马逊 ElastiCache 控制

这些控制措施与 ElastiCache 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ElastiCache.1] ElastiCache Redis 集群应启用自动备份

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 启用备份

严重性：高

资源类型：`AWS::ElastiCache::CacheCluster`

AWS Config 规则：**`elasticache-redis-cluster-automatic-backup-check`**

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`snapshotRetentionPeriod`	最短快照保留期（以天为单位）	整数	1 到 35	1

此控件 ElastiCache 用于评估 Amazon for Redis 集群是否已计划自动备份。如果 Redis 集群的 `SnapshotRetentionLimit` 小于指定时间段，则控制失败。除非您为快照保留期提供自定义参数值，否则 Security Hub 将使用默认值即 1 天。

Amazon ElastiCache for Redis 集群可以备份其数据。可以使用备份还原集群或为新集群做种。备份包含集群的元数据以及集群中的所有数据。所有备份都会写入 Amazon Simple Storage Service (Amazon S3)，该服务提供持久存储。您可以通过创建新的 Redis 集群并使用备份中的数据填充该集群来恢复数据。您可以使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 和 ElastiCache API 管理备份。

修复

要在 for Redis 集群上 ElastiCache 安排自动备份，请参阅 Amazon ElastiCache 用户指南中的安排自动备份。

[ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级

相关要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::ElastiCache::CacheCluster`

AWS Config 规则：`elasticache-auto-minor-version-upgrade-check`

计划类型：定期

参数：无

此控件 ElastiCache 用于评估 Redis 是否自动对缓存集群应用次要版本升级。如果 ElastiCache Redis 缓存集群没有自动应用次要版本升级，则此控件将失败。

`AutoMinorVersionUpgrade`是您可以为 Redis 开启的一项功能， ElastiCache 以便在新的次要缓存引擎版本可用时自动升级您的缓存集群。这些升级可能包括安全补丁和错误修复。继续 up-to-date 安装补丁是保护系统的重要一步。

修复

要对现有 ElastiCache 的 Redis 缓存集群应用自动次要版本升级，请参阅 Amazon ElastiCache 用户指南中的升级引擎版本。

[ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 规则：`elasticache-repl-grp-auto-failover-enabled`

计划类型：定期

参数：无

此控件检查 Red ElastiCache is 复制组是否启用了自动故障转移。如果未为 Redis 复制组启用自动失效转移，则此控制失败。

为复制组启用自动失效转移后，主节点的角色将自动将失效转移到其中一个只读副本。此失效转移和副本升级可确保您可以在升级完成后恢复写入新的主数据库，从而减少发生故障时的总体停机时间。

修复

要 ElastiCache 为现有的 Redis 复制组启用自动故障转移，请参阅 Amazon ElastiCache 用户指南中的修改 ElastiCache 集群。如果您使用 ElastiCache 控制台，请将自动故障转移设置为启用。

[ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 规则：`elasticache-repl-grp-encrypted-at-rest`

计划类型：定期

参数：无

此控件检查 Red ElastiCache is 复制组是否处于静态加密状态。如果未 ElastiCache 对适用于 Redis 的复制组进行静态加密，则此控件将失败。

对静态数据进行加密可降低未经身份验证的用户访问存储在磁盘上的数据的风险。 ElastiCache 对于 Redis，为了增加安全性，应对复制组进行静态加密。

修复

要在 For Redis 复制组上配置静态加密，请参阅 A ma ElastiCache zon 用户指南中的启用静态加密。 ElastiCache

[ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 规则：`elasticache-repl-grp-encrypted-in-transit`

计划类型：定期

参数：无

此控件 ElastiCache 用于检查 Redis 复制组在传输过程中是否已加密。如果 For Redis ElastiCache 的复制组在传输过程中未加密，则此控件将失败。

对传输中数据进行加密可降低未经授权的用户侦听网络流量的风险。在 for Redis 复制组上启用传输中的加密可在数据从一个位置移动到另一个位置时对其进行加密，例如在集群中的节点之间或集群与应用程序之间。 ElastiCache

修复

要在 for Redis 复制组上配置传输中加密，请参阅 A ma ElastiCache zon 用户指南中的启用传输中加密。 ElastiCache

[ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 规则：`elasticache-repl-grp-redis-auth-enabled`

计划类型：定期

参数：无

此控件 ElastiCache 用于检查 Redis 复制组是否启用了 Redis 身份验证。如果适用于 Redis ElastiCache 的复制组节点的 Redis 版本低于 6.0 且`AuthToken`未在使用中，则该控件将失败。

当您使用 Redis 身份验证令牌或密码时，Redis 在允许客户端运行命令之前需要密码，这提高了数据安全性。对于Redis 6.0及更高版本，我们建议使用基于角色的访问控制（RBAC）。由于 6.0 之前的 Redis 版本不支持 RBAC，因此此控件仅评估无法使用 RBAC 功能的版本。

修复

要在 ElastiCache 适用于 Redis 的复制组上使用 Redis 身份验证，请参阅亚马逊用户指南中的修改现有 ElastiCache 适用于 Redis 的集群上的身份验证令牌。 ElastiCache

[ElastiCache.7] ElastiCache 群集不应使用默认子网组

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)。

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::ElastiCache::CacheCluster`

AWS Config 规则：elasticache-subnet-group-check

计划类型：定期

参数：无

此控件检查 ElastiCache 集群是否配置了自定义子网组。如果CacheSubnetGroupName具有该值，则 ElastiCache 集群的控件将失败default。

启动 ElastiCache 集群时，如果尚不存在默认子网组，则会创建一个默认子网组。默认组使用来自默认虚拟私有云（VPC）的子网。我们建议使用对集群所在子网以及集群从子网继承的网络进行更严格的限制的自定义子网组。

修复

要为 ElastiCache 集群创建新的子网组，请参阅 Amazon ElastiCache 用户指南中的创建子网组。

AWS Elastic Beanstalk 控件

这些控件与 Elastic Beanstalk 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：AWS::ElasticBeanstalk::Environment

AWS Config 规则：beanstalk-enhanced-health-reporting-enabled

计划类型：已触发变更

参数：无

此控件可检查 AWS Elastic Beanstalk 环境是否启用了增强型运行状况报告。

Elastic Beanstalk 增强型运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。

Elastic Beanstalk 增强版运行状况报告提供了状态描述符，用于衡量已结果问题的严重性并确定可能的调查原因。支持的亚马逊机器映像（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 AWS Elastic Beanstalk 开发人员指南中的增强型运行状况报告和监控。

修复

有关如何启用增强型运行状况报告的说明，请参阅 AWS Elastic Beanstalk 开发人员指南中的使用 Elastic Beanstalk 控制台启用增强型运行状况报告。

[ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新

相关要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::ElasticBeanstalk::Environment`

AWS Config 规则：`elastic-beanstalk-managed-updates-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`UpdateLevel`	版本更新级别	枚举	`minor`, `patch`	无默认值

此控件检查是否为 Elastic Beanstalk 环境启用了托管平台更新。如果未启用托管平台更新，则控制失败。默认情况下，如果启用了任何类型的平台更新，则控制才会通过。或者，您可以提供自定义参数值以要求特定的更新级别。

启用托管平台更新可确保为环境安装最新的可用平台修补程序、更新和功能。及时安装补丁程序是保护系统安全的重要一步。

修复

要启用托管平台更新，请参阅《AWS Elastic Beanstalk 开发人员指南》中的在托管平台更新下配置托管平台更新。

[ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch

类别：识别 > 日志记录

严重性：高

资源类型：`AWS::ElasticBeanstalk::Environment`

AWS Config 规则：`elastic-beanstalk-logs-to-cloudwatch`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`RetentionInDays`	日志事件在到期前保留的天数	枚举	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 , 400, 545, 731, 1827, 3653	无默认值

此控件检查 Elastic Beanstalk 环境是否配置为向日志发送日志。 CloudWatch 如果 Elastic Beanstalk 环境未配置为向日志发送日志，则控制失败。 CloudWatch 或者，如果您希望仅当日志在到期前保留指定天数时控制才通过，则可以为 `RetentionInDays` 参数提供自定义值。

CloudWatch 帮助您收集和监控应用程序和基础设施资源的各种指标。您还可以使用 CloudWatch 根据特定指标配置警报操作。我们建议将 Elastic Beanstalk 与集成，以提高您的 Ela CloudWatch stic Beanstalk 环境的可见性。Elastic Beanstalk 日志包括 eb-activity.log、来自环境 nginx 或 Apache 代理服务器的访问日志以及特定于环境的日志。

修复

要将 Elastic B CloudWatch eanstalk 与日志集成，请参阅开发者指南中的将实例日志流式传输到 CloudWatch 日志。AWS Elastic Beanstalk

弹性负载均衡控件

这些控件与弹性负载均衡资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

相关要求：PCI DSS v3.2.1/2.3、PCI DSS v3.2.1/4.1、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：检测 > 检测服务

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：`alb-http-to-https-redirection-check`

计划类型：定期

参数：无

此控件检查是否在应用程序负载均衡器的所有 HTTP 侦听器上配置了 HTTP 到 HTTPS 重定向。如果应用程序负载均衡器的任何 HTTP 侦听器未配置 HTTP 到 HTTPS 重定向，则控制失败。

在开始使用应用程序负载均衡器之前，必须添加一个或多个侦听器。侦听器是使用配置的协议和端口检查连接请求的进程。侦听器支持 HTTP 和 HTTPS 协议。您可以使用 HTTPS 侦听器将加密和解密工作卸载到负载均衡器。要强制传输过程中的加密，您应该使用应用程序负载均衡器的重定向操作，将客户端 HTTP 请求重定向到端口 443 上的 HTTPS 请求。

要了解更多信息，请参阅应用程序负载均衡器用户指南中的应用程序负载均衡器的侦听器。

修复

要将 HTTP 请求重定向到 HTTPS，您必须添加应用程序负载均衡器侦听器规则或编辑现有规则。

有关添加新规则的说明，请参阅 应用程序负载均衡器用户指南中的添加规则。对于协议：端口，选择 HTTP，然后输入 **80**。对于添加操作，选择重定向到，选择 HTTPS，然后输入 **443**。

有关编辑现有规则的说明，请参阅应用程序负载均衡器用户指南中的编辑规则。对于协议：端口，选择 HTTP，然后输入 **80**。对于添加操作，选择重定向到，选择 HTTPS，然后输入 **443**。

[ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(5)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：`elb-acm-certificate-required`

计划类型：已触发变更

参数：无

此控件检查经典负载均衡器是否使用 AWS Certificate Manager (ACM) 提供的 HTTPS/SSL 证书。如果配置了 HTTPS/SSL 侦听器的经典负载均衡器不使用 ACM 提供的证书，则控制失败。

要创建证书，您可以使用 ACM 或支持 SSL 和 TLS 协议的工具（例如 OpenSSL）。Security Hub 建议您使用 ACM 为负载均衡器创建或导入证书。

ACM 与经典负载均衡器集成，以便您可以在负载均衡器上部署证书。您还应该自动续订这些证书。

修复

有关如何将 ACM SSL/TLS 证书与经典负载均衡器关联的信息，请参阅 AWS 知识中心文章如何将 ACM SSL/TLS 证书与经典负载均衡器、应用程序或网络负载均衡器相关联？

[ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5

SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：`elb-tls-https-listeners-only`

计划类型：已触发变更

参数：无

此控件检查经典负载均衡器侦听器是使用 HTTPS 还是 TLS 协议配置以进行前端（客户端到负载均衡器）连接。如果经典负载均衡器有侦听器，则该控件适用。如果经典负载均衡器没有配置侦听器，则该控件不会报告任何结果。

如果经典负载均衡器侦听器为前端连接配置了 TLS 或 HTTPS，则控制通过。

如果侦听器没有为前端连接配置 TLS 或 HTTPS，则控制失败。

在开始使用负载均衡器之前，必须添加一个或多个侦听器。侦听器是使用配置的协议和端口检查连接请求的进程。侦听器可以支持 HTTP 和 HTTPS/TLS 协议。您应始终使用 HTTPS 或 TLS 侦听器，以便负载均衡器在传输过程中完成加密和解密工作。

修复

要修复此问题，请更新侦听器以使用 TLS 或 HTTPS 协议。

将所有不合规的侦听器变更为 TLS/HTTPS 侦听器

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的负载平衡下，选择负载均衡器。
3. 选择您的经典负载均衡器。
4. 在 Listeners 选项卡上，选择 Edit。
5. 对于所有未将负载均衡器协议设置为 HTTPS 或 SSL 的侦听器，将设置变更为 HTTPS 或 SSL。
6. 对于所有修改过的侦听器，在证书选项卡上，选择变更默认值。
7. 对于 ACM 和 IAM 证书，选择一个证书。

8. 选择另存为默认值。
9. 更新所有侦听器后，选择保存。

[ELB.4] 应将应用程序负载均衡器配置为删除 http 标头

相关要求：NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(2))。

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：`alb-http-drop-invalid-header-enabled`

计划类型：已触发变更

参数：无

此控件评估 AWS 应用程序负载均衡器，以确保它们配置为丢弃无效的 HTTP 标头。如果 `false` 的值设置为 `routing.http.drop_invalid_header_fields.enabled`，则控制失败。

默认情况下，应用程序负载均衡器未配置为删除无效的 HTTP 标头值。删除这些标头值可以防止 HTTP 不同步攻击。

请注意，如果启用 ELB.12，则可以禁用此控件。

修复

要修复此问题，将负载均衡器配置为删除无效标头字段。

配置负载均衡器以删除无效标头字段

1. 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. 选择应用程序负载均衡器。
4. 在操作中，选择编辑属性。
5. 在删除无效标题字段下，选择启用。
6. 选择保存。

[ELB.5] 应启用应用程序和经典负载均衡器日志记录

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`、`AWS::ElasticLoadBalancingV2::LoadBal`

AWS Config 规则：`elb-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查应用程序负载均衡器和传统负载均衡器是否启用了日志记录。如果 `access_logs.s3.enabled` 是 `false`，则控制失败。

Elastic Load Balancing 提供了访问日志，该访问日志可捕获有关发送到负载均衡器的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。您可以使用这些访问日志分析流量模式并解决问题。

要了解更多信息，请参阅 经典负载均衡器用户指南中的经典负载均衡器的访问日志。

修复

要启用访问日志，请参阅 应用程序负载均衡器用户指南中的步骤 3：配置访问日志。

[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：elb-deletion-protection-enabled

计划类型：已触发变更

参数：无

此控件检查应用程序、网关或 Network Load Balancer 是否启用了删除保护。如果禁用了删除保护，则控件将失败。

启用删除保护以保护您的应用程序、网关或 Network Load Balancer 不被删除。

修复

为了防止您的负载均衡器被意外删除，您可以启用删除保护。默认情况下，已为负载均衡器禁用删除保护。

如果您为负载均衡器启用删除保护，则必须先禁用删除保护，然后才能删除负载均衡器。

要为 Application Load Balancer 启用删除保护，请参阅应用程序负载均衡器用户指南中的删除保护。要为 Gateway Load Balancer 启用删除保护，请参阅网关负载均衡器用户指南中的删除保护。要为 Network Load Balancer 启用删除保护，请参阅网络负载均衡器用户指南中的删除保护。

[ELB.7] 经典负载均衡器应启用连接耗尽功能

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：恢复 > 弹性

严重性：中

资源类型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config规则：elb-connection-draining-enabled（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查经典负载均衡器是否已启用连接耗尽功能。

在经典负载均衡器上启用连接耗尽可确保负载均衡器停止向正在取消注册或运行状况不佳的实例发送请求。它使现有连接保持打开状态。这对于自动扩缩组中的实例特别有用，可确保连接不会突然断开。

修复

要在经典负载均衡器上启用连接耗尽，请参阅经典负载均衡器用户指南中的为经典负载均衡器配置连接耗尽。

[ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：`elb-predefined-security-policy-ssl-check`

计划类型：已触发变更

参数：

- `predefinedPolicyName`：`ELBSecurityPolicy-TLS-1-2-2017-01`（不可自定义）

此控件会检查经典负载均衡器 HTTPS/SSL 侦听器是否使用预定义的策略 `ELBSecurityPolicy-TLS-1-2-2017-01`。如果经典负载均衡器HTTPS/SSL 侦听器不使用 `ELBSecurityPolicy-TLS-1-2-2017-01`，则控制失败。

安全策略是 SSL 协议、密码和服务器顺序首选项选项的组合。预定义策略控制客户端和负载均衡器之间的 SSL 协商期间支持的密码、协议和优先顺序。

使用 `ELBSecurityPolicy-TLS-1-2-2017-01` 可以帮助您满足要求您禁用特定版本的 SSL 和 TLS 的合规性和安全标准。有关更多信息，请参阅经典负载均衡器用户指南中的经典负载均衡器的预定义 SSL 安全策略。

修复

有关如何在经典负载均衡器上使用预定义安全策略 `ELBSecurityPolicy-TLS-1-2-2017-01` 的信息，请参阅 经典负载均衡器用户指南中的配置安全设置。

[ELB.9] 经典负载均衡器应启用跨区域负载均衡器

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：`elb-cross-zone-load-balancing-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为经典负载均衡器 (CLB) 启用了跨区域负载平衡。如果负载均衡未启用跨区负载均衡，则控制失败。

负载均衡器节点仅在其可用区中的注册目标之间分配流量。禁用了跨区域负载均衡后，每个负载均衡器节点会仅在其可用区中的已注册目标之间分配流量。如果可用区中注册的目标数量不同，流量将不会均匀分布，并且与另一区域中的实例相比，一个区域中的实例可能最终会被过度利用。启用跨区域负载均衡后，经典负载均衡器的每个负载均衡器节点都会在所有已启用的可用区中的注册实例之间均匀分配请求。有关详细信息，请参阅弹性负载均衡用户指南中的跨可用区负载均衡。

修复

要在经典负载均衡器中启用跨区域负载均衡，请参阅经典负载均衡器用户指南中的启用跨区域负载均衡。

[ELB.10] 经典负载均衡器应跨越多个可用区

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：clb-multiple-az

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
minAvailabilityZones	可用区的最小数量	枚举	2, 3, 4, 5, 6	2

此控件检查经典负载均衡器是否已配置为跨越至少指定数量的可用区（AZ）。如果经典负载均衡器未跨越至少指定数量的可用区，则控制失败。除非您为可用区的最小数量提供自定义参数值，否则 Security Hub 将使用默认值即两个可用区。

可以将经典负载均衡器设置为跨单个可用区或多个可用区中的 Amazon EC2 实例分发传入请求。如果唯一配置的可用区不可用，则不跨多个可用区的经典负载均衡器无法将流量重定向到另一个可用区中的目标。

修复

要向经典负载均衡器添加可用区，请参阅《经典负载均衡器用户指南》中的为您的经典负载均衡器添加或删除子网。

[ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2。

类别：保护 > 数据保护 > 数据完整性

严重性：中

资源类型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 规则：alb-desync-mode-check

计划类型：已触发变更

参数：

- `desyncMode`：`defensive, strictest`（不可自定义）

此控件检查应用程序负载均衡器配置了防御模式还是最严格的异步缓解模式。如果应用程序负载均衡器未配置防御或最严格的异步缓解模式，则控制失败。

HTTP Desync 问题可能导致请求走私，并使应用程序容易受到请求队列或缓存中毒的影响。反过来，这些漏洞可能导致凭证填充或执行未经授权的命令。配置了防御性或最严格的异步缓解模式的应用程序负载均衡器可保护应用程序免受 HTTP Desync 可能导致的安全问题的影响。

修复

要更新应用程序负载均衡器的异步缓解模式，请参阅应用程序负载均衡器用户指南中的异步缓解模式。

[ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：`elbv2-multiple-az`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`minAvailabilityZones`	可用区的最小数量	枚举	`2, 3, 4, 5, 6`	2

此控件检查 Elastic Load Balancer V2（应用程序、网络或网关负载均衡器）是否注册了来自指定数量的可用区（AZ）的实例。如果 Elastic Load Balancer V2 没有注册来自指定数量或更多的可用区的实

例，则控制失败。除非您为可用区的最小数量提供自定义参数值，否则 Security Hub 将使用默认值即两个可用区。

弹性负载均衡 在一个或多个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。弹性负载均衡 根据传入流量随时间的变化对负载均衡器进行扩展。建议至少配置两个可用区，以保证服务的可用性，因为当一个可用区不可用时，弹性负载均衡器可以将流量引导到另一个可用区。配置多个可用区将有助于消除应用程序的单点故障。

修复

要向应用程序负载均衡器添加可用区，请参阅应用程序负载均衡器用户指南中的应用程序负载均衡器的可用区。要向网络负载均衡器添加可用区，请参阅网络负载均衡器用户指南中的网络负载均衡器。要向网关负载均衡器添加可用区，请参阅网关负载均衡器用户指南中的创建网关负载均衡器。

[ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2。

类别：保护 > 数据保护 > 数据完整性

严重性：中

资源类型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 规则：`clb-desync-mode-check`

计划类型：已触发变更

参数：

- `desyncMode`：`defensive, strictest`（不可自定义）

此控件检查经典负载均衡器是配置了防御模式还是最严格的异步缓解模式。如果经典负载均衡器未配置防御或最严格的异步缓解模式，则控制失败。

HTTP Desync 问题可能导致请求走私，并使应用程序容易受到请求队列或缓存中毒的影响。反过来，这些漏洞可能导致凭证劫持或执行未经授权的命令。配置了防御性或最严格的异步缓解模式的经典负载均衡器可保护应用程序免受 HTTP Desync 可能导致的安全问题的影响。

修复

要更新经典负载均衡器上的异步缓解模式，请参阅经典负载均衡器用户指南中的修改异步缓解模式。

[ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF

相关要求：NIST.800-53.r5 AC-4(21)

类别：保护 > 防护服务

严重性：中

资源类型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 规则：`alb-waf-enabled`

计划类型：已触发变更

参数：无

此控件检查 Application Load Balancer 是与 AWS WAF 经典访问控制列表 (AWS WAF Web ACL) 关联还是与 Web 访问控制列表 (Web ACL) 关联。如果 AWS WAF 配置的 `Enabled` 字段设置为 `false`，则控制失败。

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 API 免受攻击。使用 AWS WAF，您可以配置 Web ACL，这是一组基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求的规则。我们建议将应用程序负载均衡器与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。

修复

要将 Application Load Balancer 与 Web ACL 关联，请参阅开发者指南中的将网页 ACL 与 AWS 资源关联或取消关联。AWS WAF

Amazon EMR 控件

这些控件与 Amazon EMR 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址

相关要求：PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5

SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置

严重性：高

资源类型：`AWS::EMR::Cluster`

AWS Config 规则：`emr-master-no-public-ip`

计划类型：定期

参数：无

此控件检查 Amazon EMR 集群上的主节点是否具有公有 IP 地址。如果公有 IP 地址与任何主节点实例相关联，则控制失败。

公有 IP 地址是在实例的 `NetworkInterfaces` 配置 `PublicIp` 字段中指定的。此控件仅检查处于 `RUNNING` 或 `WAITING` 状态的 Amazon EMR 集群。

修复

在启动期间，您可以控制是否为默认子网或非默认子网中的实例分配公有 IPv4 地址。默认情况下，默认子网的此属性设置为 `true`。除非由 Amazon EC2 启动实例向导创建，否则 IPv4 公有寻址属性设置为 `false`。在这种情况下，会将属性设置为 `true`。

启动后，您无法手动取消公有 IPv4 地址与实例的关联。

要修复失败的调查发现，您必须在私有子网的 VPC 中启动一个新集群，该子网的 IPv4 公有寻址属性设置为 `false`。有关说明，请参阅 Amazon EMR 管理指南中的在 VPC 中启动集群。

[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`emr-block-public-access`

计划类型：定期

参数：无

此控件会检查您的账户是否配置了 Amazon EMR 屏蔽公共访问权限。如果未启用屏蔽公共访问权限设置或允许除端口 22 之外的任何端口，则控制失败。

如果集群的安全配置允许来自公有 IP 地址的入站流量通过某个端口，Amazon EMR 屏蔽公共访问权限会阻止您在公有子网中启动该集群。当来自您的 AWS 账户 的用户启动集群时，Amazon EMR 会检查该集群的安全组中的端口规则，并将其与您的入站流量规则进行比较。如果安全组具有向公有 IP 地址 IPv4 0.0.0.0/0 或 IPv6 ::/0 开放端口的入站规则，且这些端口并未指定为您账户的例外，则 Amazon EMR 不允许用户创建集群。

> **Note**
>
> 默认情况下，阻止公有访问处于启用状态。为了增强账户保护，我们建议您将其保持启用状态。

修复

要为 Amazon EMR 配置屏蔽公共访问权限，请参阅《亚马逊 EMR 管理指南》中的使用 Amazon EMR 阻止公有访问。

Elasticsearch 控件

这些控件与 Elasticsearch 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ES.1] Elasticsearch 域应启用静态加密

相关要求：PCI DSS v3.2.1/3.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-encrypted-at-rest`

计划类型：定期

参数：无

此控件检查 Elasticsearch 域是否启用静态加密配置。如果未启用静态加密，检查将失败。

为了在中为您的敏感数据增加一层安全性 OpenSearch，您应将您的数据配置 OpenSearch 为静态加密。Elasticsearch 域提供静态数据加密。该功能 AWS KMS 用于存储和管理您的加密密钥。为执行加密，它使用具有 256 位密钥 (AES-256) 的高级加密标准算法。

要了解有关静 OpenSearch 态加密的更多信息，请参阅《亚马逊服务开发者指南》中的亚马逊 OpenSearch 服务静态数据加密。 OpenSearch

某些实例类型，例如 `t.small` 和 `t.medium`，不支持静态数据加密。有关详细信息，请参阅《Amazon OpenSearch 服务开发者指南》中的支持的实例类型。

修复

要为新的和现有的 Elasticsearch 域启用静态加密，请参阅《亚马逊 OpenSearch 服务开发者指南》中的启用静态数据加密。

[ES.2] Elasticsearch 域名不可供公共访问

相关要求：PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：严重

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-in-vpc-only`

计划类型：定期

参数：无

此控件检查 Elasticsearch 域是否位于 VPC 中。它不会评估 VPC 子网路由配置来确定公共访问。您应确保 Elasticsearch 域未附加到公共子网。请参阅《Amazon OpenSearch 服务开发者指南》中的基于资源的政策。您还应该确保根据建议的最佳实践配置了 VPC。请参阅 Amazon VPC 用户指南中的 VPC 安全最佳实践。

部署在 VPC 内的 Elasticsearch 域可以通过私有 AWS 网络与 VPC 资源通信，无需穿越公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。VPC 提供了许多网络控制来保护对 Elasticsearch 域的访问，包括网络 ACL 和安全组。Security Hub 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端点的域，则以后无法将其放置在 VPC 中。您必须创建一个新的域，然后迁移数据。反之亦然。如果在 VPC 中创建一个域，则该域不能具有公有端点。您必须创建另一个域或禁用该控制。

请参阅亚马逊 OpenSearch 服务开发者指南中的在 VPC 内启动您的亚马逊 OpenSearch 服务域。

[ES.3] Elasticsearch 域应加密节点之间发送的数据

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-node-to-node-encryption-check`

计划类型：已触发变更

参数：无

此控件用于检查 Elasticsearch 域名是否启用了 node-to-node 加密。如果 Elasticsearch 域未启用 node-to-node 加密，则控制失败。如果 Elasticsearch 版本不支持 node-to-node 加密检查，则该控件还会生成失败的结果。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击窃听或操纵网络流量。只允许通过 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。

此配置可能会降低性能。在启用此选项之前，您应该了解并测试性能权衡。

修复

有关在新域和现有域上启用 node-to-node 加密的信息，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用 node-to-node加密。

[ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 – 日志记录

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-logs-to-cloudwatch`

计划类型：已触发变更

参数：

- `logtype = 'error'`（不可自定义）

此控件检查 Elasticsearch 域是否配置为向日志发送错误日志。 CloudWatch

您应该为 Elasticsearch 域启用错误日志，并将这些日志发送到 CloudWatch 日志以进行保留和响应。域错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

修复

有关如何启用日志发布的信息，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用日志发布（控制台）。

[ES.5] Elasticsearch 域名应该启用审核日志

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-audit-logging-enabled`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

- `cloudWatchLogsLogGroupArnList`（不可自定义）。Security Hub 不会填充此参数。应为审核日志配置的 CloudWatch 日志组列表，以逗号分隔。

  此规则适用于`NON_COMPLIANT`未在此参数列表中指定 Elasticsearch 域的 CloudWatch 日志组的情况。

此控件用于检查 Elasticsearch 域名是否启用了审核日志。如果 Elasticsearch 域未启用审核日志，则此控制失败。

审核日志是高度可定制的。它们允许您跟踪 Elasticsearch 集群上的用户活动，包括身份验证成功和失败、对身份验证的请求 OpenSearch、索引更改以及传入的搜索查询。

修复

有关启用审计日志的详细说明，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用审计日志。

[ES.6] Elasticsearch 域应拥有至少三个数据节点

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-data-node-fault-tolerance`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件会检查 Elasticsearch 域是否配置了至少三个数据节点，并且 `zoneAwarenessEnabled` 是 `true`。

一个 Elasticsearch 域至少需要三个数据节点才能实现高可用性和容错能力。部署至少具有三个数据节点的 Elasticsearch 域可以确保在节点发生故障时集群正常运行。

修复

修改 Elasticsearch 域中的数据节点数量

1. 打开亚马逊 OpenSearch 服务控制台，网址为 https://console.aws.amazon.com/aos/。
2. 在域下，选择要编辑的域的名称。
3. 选择 Edit domain (编辑域)。
4. 在数据节点下，将节点数设置为大于或等于 3 的数字。

   对于三个可用区部署，请设置为三的倍数，以确保可用区间的分布均等。
5. 选择提交。

[ES.7] 应将 Elasticsearch 域配置为至少三个专用的主节点

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config规则：`elasticsearch-primary-node-fault-tolerance`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查 Elasticsearch 域是否配置了至少三个专用的主节点。如果域不使用专用主节点，则此控制失败。如果 Elasticsearch 域有五个专用的主节点，则此控制权通过。但是，为了降低可用性风险，可能没有必要使用三个以上的主节点，并且会导致额外的成本。

一个 Elasticsearch 域至少需要三个专用的主节点才能实现高可用性和容错能力。在数据节点蓝/绿部署期间，专用的主节点资源可能会紧张，因为还有其他节点需要管理。部署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/aos/。
2. 在域下，选择要编辑的域的名称。
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或大于三个。
6. 选择提交。

[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`elasticsearch-https-required`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

它控制检查 Elasticsearch 域端点是否已配置为使用最新的 TLS 安全策略。如果 Elasticsearch 域终端节点未配置为使用最新的支持策略或未启用 HTTP，则控制失败。当前最新支持的 TLS 安全策略是`Policy-Min-TLS-1-2-PFS-2023-10`。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle或类似的攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试应用程序，以了解性能概况和 TLS 的影响。与先前版本的 TLS 相比，TLS 1.2 提供了多项安全增强功能。

修复

要启用 TLS 加密，请使用 UpdateDomainConfigAPI 操作配置DomainEndpointOptions对象。这设置了`TLSSecurityPolicy`.

[ES.9] 应标记 Elasticsearch 域名

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Elasticsearch::Domain`

AWS Config 规则：`tagged-elasticsearch-domain`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Elasticsearch 域名是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果域名没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如

果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果该域未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Elasticsearch 域添加标签，请参阅亚马逊 OpenSearch 服务开发者指南中的使用标签。

亚马逊 EventBridge 控制

这些控制措施与 EventBridge 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[EventBridge.2] 应标记 EventBridge 活动总线

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::Events::EventBus

AWS Config 规则:tagged-events-eventbus（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon EventBridge 事件总线是否具有参数中定义的特定密钥的标签requiredTagKeys。如果事件总线没有任何标签键或者没有参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则控件仅检查标签键是否存在，如果事件总线未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 EventBridge 事件总线添加标签，请参阅《亚马逊 EventBridge 用户指南》中的 Amazon EventBridge 标签。

[EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略

相关要求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)。

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：低

资源类型：`AWS::Events::EventBus`

AWS Config 规则：`custom-schema-registry-policy-attached`

计划类型：已触发变更

参数：无

此控件会检查 Amazon EventBridge 自定义事件总线是否附加了基于资源的策略。如果自定义事件总线没有基于资源的策略，则此控制失败。

默认情况下， EventBridge 自定义事件总线不附加基于资源的策略。这允许账户中的主体访问事件总线。通过将基于资源的策略附加到事件总线，您可以将对事件总线的访问权限限制为指定账户，也可以有意向另一个账户中的实体授予访问权限。

修复

要将基于资源的策略附加到 EventBridge 自定义事件总线，请参阅 Amazon EventBridge 用户指南中的管理事件总线权限。

[EventBridge.4] EventBridge 全局端点应启用事件复制

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Events::Endpoint`

AWS Config 规则：`global-endpoint-event-replication-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon EventBridge 全局终端节点启用了事件复制。如果未为全局端点启用事件复制，则控制失败。

全球端点有助于使应用程序具有区域容错能力。首先，您为端点分配一个 Amazon Route 53 运行状况检查。启动失效转移时，运行状况检查会报告“不正常”状态。在失效转移启动后的几分钟内，所有自定义事件都将路由到辅助区域的事件总线，并由该事件总线进行处理。使用全局端点时，可以启用事件复制。事件复制使用托管规则将所有自定义事件发送到主区域和次要区域的事件总线。我们建议在设置全局端点时启用事件复制。事件复制可帮助您验证全局端点配置是否正确。需要事件复制才能从失效转移事件中自动恢复。如果您未启用事件复制，则必须手动将 Route 53 运行状况检查重置为“正常”，然后才能将事件重新路由回主区域。

> **Note**
>
> 如果您使用的是自定义事件总线，则需要在每个区域中使用同一个名称和相同账户的自定义偶数总线，这样失效转移才能正常运行。启用事件复制可能会增加月度成本。有关定价的信息，请参阅 Amazon EventBridge 定价。

修复

要为 EventBridge 全局终端节点启用事件复制，请参阅 Amazon EventBridge 用户指南中的创建全局终端节点。对于事件复制，请选择启用事件复制。

Amazon FSx 控件

这些控件与 Amazon FSx 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：`fsx-openzfs-copy-tags-enabled`

计划类型：已触发变更

参数：无

此控件检查适用于 OpenZFS 的 Amazon FSX 文件系统是否配置为将标签复制到备份和卷。如果 OpenZFS 文件系统未配置为将标签复制到备份和卷，则控制失败。

IT 资产的识别和清点是治理和安全的一个重要方面。标签可帮助您以不同的方式对 AWS 资源进行分类，例如按用途、所有者或环境进行分类。这在您具有很多类型相同的资源时会很有用，因为您可以根据分配给特定资源的标签快速识别该资源。

修复

要将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷，请参阅《Amazon FSX OpenZF S 用户指南》中的更新文件系统。

[fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份

相关要求：nist.800-53.r5 CP-9、nist.800-53.r5 CM-8

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::FSx::FileSystem`

AWS Config 规则：`fsx-lustre-copy-tags-to-backups`

计划类型：已触发变更

参数：无

此控件可检查 Amazon FSx for Lustre 文件系统是否配置为将标签复制到备份和卷。如果 Lustre 文件系统未配置为将标签复制到备份和卷，则控制失败。

IT 资产的识别和清点是治理和安全的一个重要方面。标签可帮助您以不同的方式对 AWS 资源进行分类，例如按用途、所有者或环境进行分类。这在您具有很多类型相同的资源时会很有用，因为您可以根据分配给特定资源的标签快速识别该资源。

修复

要将 FSX for Lustre 文件系统配置为将标签复制到备份，请参阅 Amazon FSX OpenZFS 用户指南中的更新文件系统。

AWS Global Accelerator 控件

这些控件与全球加速器资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[GlobalAccelerator.1] 应标记全球加速器加速器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GlobalAccelerator::Accelerator`

AWS Config 规则：`tagged-globalaccelerator-accelerator`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Global Accelerator 加速器是否具有参数中定义的特定键的标签`requiredTagKeys`。如果加速器没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果加速器未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托

人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向全球加速器全球加速器添加标签，请参阅AWS Global Accelerator 开发者指南 AWS Global Accelerator中的标记。

AWS Glue 控件

这些控制措施与 AWS Glue 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Glue.1] 应该给 AWS Glue 工作加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Glue::Job`

AWS Config 规则:`tagged-glue-job`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Glue 作业是否具有参数中定义的特定键的标签`requiredTagKeys`。如果作业没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果未使用任何密钥标记作业，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS Glue 作业添加标签，请参阅《AWS Glue 用户指南》AWS Glue中的AWS 标签。

亚马逊 GuardDuty 控制

这些控制措施与 GuardDuty 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[GuardDuty.1] GuardDuty 应该启用

相关要求：PCI DSS v3.2.1/11.4、NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 RA-3(4)、NIST.800-53.r5 SA-11(1)、NIST.800-53.r5 SA-11(6)、NIST.800-53.r5 SA-15(2)、NIST.800-53.r5 SA-15(8)、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SA-8(21)、NIST.800-53.r5 SA-8(25)、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-5(1)、NIST.800-53.r5 SC-5(3)、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(1)、NIST.800-53.r5 SI-4(13)、NIST.800-53.r5

SI-4(2)、NIST.800-53.r5 SI-4(22)、NIST.800-53.r5 SI-4(25)、NIST.800-53.r5 SI-4(4)、NIST.800-53.r5 SI-4(5)。

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`guardduty-enabled-centralized`

计划类型：定期

参数：无

此控件会检查您的 GuardDuty 账户和地区 GuardDuty 是否启用了 Amazon。

强烈建议您在所有支持的 AWS 区域 GuardDuty 中启用。这样 GuardDuty 做可以生成有关未经授权或异常活动的调查结果，即使在您不经常使用的地区也是如此。这还 GuardDuty 允许监控全球 CloudTrail 事件， AWS 服务 例如 IAM。

修复

要修复此问题，请启用 GuardDuty。

有关如何启用 GuardDuty（包括 AWS Organizations 如何使用管理多个账户）的详细信息，请参阅 Amazon GuardDuty 用户指南 GuardDuty中的入门指南。

[GuardDuty.2] 应该给 GuardDuty 过滤器加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GuardDuty::Filter`

AWS Config 规则：`tagged-guardduty-filter`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件会检查 Amazon GuardDuty 筛选条件是否具有参数中定义的特定密钥的标签requiredTagKeys。如果过滤器没有任何标签键或者没有在参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果过滤器未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 GuardDuty 筛选条件添加标签，请参阅 Amazon GuardDuty API 参考TagResource中的。

[GuardDuty.3] 应 GuardDuty 标记 IP 集

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GuardDuty::IPSet`

AWS Config 规则：`tagged-guardduty-ipset`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon GuardDuty IPset 是否具有参数`requiredTagKeys`中定义的特定密钥的标签。如果 IPSet 没有任何标签密钥或参数`requiredTagKeys`中没有指定的所有密钥，则控件将失败。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果未使用任何密钥标记 IPSet，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 GuardDuty IPset 添加标签，请参阅亚马逊 GuardDuty API 参考TagResource中的。

[GuardDuty.4] 应 GuardDuty 标记探测器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::GuardDuty::Detector`

AWS Config 规则：`tagged-guardduty-detector`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon GuardDuty 探测器是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果探测器没有任何标签键或者没有在参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则控件仅检查标签密钥是否存在，如果检测器未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 GuardDuty 探测器添加标签，请参阅 Amazon GuardDuty API 参考TagResource中的。

AWS Identity and Access Management 控件

这些控制与 IAM 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[IAM.1] IAM policy 不应允许完整的“*”管理权限

相关要求：PCI DSS v3.2.1/7.2.1、CIS 基金会基准 v1.2.0/1.22、CIS AWS 基金会基准 v1.4.0/1.16、nist.800-53.r5 AC-2、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15) r5 AC-3 (7)、nist.800-53.r5 AC-5、nist.800-53.r5 AC-6、nist.800-53.r5 AC-6 (10)、nist.800-53.r5 AC-6 (2)、nist.800-53.r5 AC-6 (3) AWS

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::IAM::Policy`

AWS Config 规则：`iam-policy-no-statements-with-admin-access`

计划类型：已触发变更

参数：

- `excludePermissionBoundaryPolicy: true`（不可自定义）

此控件检查 IAM policy 的默认版本（也称为客户管理型策略）是否具有管理员访问权限，方法是包含一个在 `"Resource": "*"` 上对 `"Effect": "Allow"` 和 `"Action": "*"` 的声明。如果您有带有此类声明的 IAM policy，则控制失败。

该控制仅检查您创建的客户托管策略。它不检查内联策略和 AWS 托管策略。

IAM policy 定义一组授予用户、组或角色的权限。按照标准的安全建议， AWS 建议您授予最低权限，即仅授予执行任务所需的权限。当您提供完全管理权限而不是用户所需的最低权限集时，您会将资源暴给可能有害的操作。

首先确定用户需要执行的任务，然后拟定仅限用户执行这些任务的策略，而不是允许完全管理权限。最开始只授予最低权限，然后根据需要授予其他权限，则样会更加安全。请不要一开始就授予过于宽松的权限而后再尝试收紧权限。

您应该移除包含在 `"Resource": "*"` 上对 `"Effect": "Allow"` 和 `"Action": "*"` 的声明的 IAM policy。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要修改 IAM policy 使其不允许完全的 "*" 管理权限，请参阅 IAM 用户指南中的编辑 IAM policy。

[IAM.2] IAM 用户不应附加 IAM policy

相关要求：PCI DSS v3.2.1/7.2.1、CIS 基金会基准 v3.0.0/1.15、CIS AWS 基金会基准 v1.2.0/1.16、nist.800-53.r5 AC-2、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15) r5 AC-3 (7)、nist.800-53.r5 AC-6、nist.800-53.r5 AC-6 (3) AWS

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::IAM::User`

AWS Config 规则：`iam-user-no-policies-check`

计划类型：已触发变更

参数：无

此控件检查 IAM 用户是否附加了策略。如果 IAM 用户附加了策略，则控制失败。相反，IAM 用户必须继承 IAM 组的权限或承担角色。

默认情况下，IAM 用户、群组和角色无权访问 AWS 资源。IAM policy 向用户、组或角色授予权限。我们建议您将 IAM policy 直接应用于组和角色，而不是用户。随着用户数量的增长，在组或角色级别分

配权限可降低访问管理的复杂性。降低访问管理的复杂性有助于减少委托人意外收到或保留过多权限的机会。

> **Note**
>
> Amazon Simple Email Service 创建的 IAM 用户是使用内联策略自动创建的。Security Hub 会自动将这些用户排除在此控制范围之外。
> AWS 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，请创建一个 IAM 群组，并将该策略附加到该群组。然后，将用户添加到组中。策略将应用于组中的每一位用户。要删除直接附加到用户的策略，请参阅 IAM 用户指南中的添加和删除 IAM 身份权限。

[IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次

相关要求：独联体 AWS 基金会基准 v3.0.0/1.14、独联体基金会基准 v1.4.0/1.14、独联体 AWS 基金会基准 v1.2.0/1.4、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-2 (3)、nist.800-53.r5 AC-3 (15) AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`access-keys-rotated`

计划类型：定期

参数：

- `maxAccessKeyAge`：`90`（不可自定义）

该控制检查是否在 90 天内轮换了活动访问密钥。

我们强烈建议您不要在账户中生成和删除所有访问密钥。相反，推荐的最佳做法是创建一个或多个 IAM 角色或通过使用联合 AWS IAM Identity Center。您可以使用这些方法来允许您的用户访问 AWS Management Console 和 AWS CLI。

每种方法都有其使用案例。对于拥有现有中心目录或计划需要超过当前 IAM 用户限制的企业来说，联合身份验证通常更好。在 AWS 环境之外运行的应用程序需要访问密钥才能以编程方式访问 AWS 资源。

但是，如果需要编程访问权限的资源在内部运行 AWS，则最佳做法是使用 IAM 角色。通过角色，您可以授予资源访问权限，而无需在配置中硬编码访问密钥 ID 和私有访问密钥。

要了解有关保护访问密钥和帐户的更多信息，请参阅中的管理 AWS 访问密钥的最佳实践AWS 一般参考。另请参阅博客文章《使用编程访问权限 AWS 账户 时保护您的指南》。

如果您已有访问密钥，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用账户或已终止账户关联的访问密钥的风险。这还可以确保无法使用可能已丢失、遭破解或被盗用的旧密钥访问数据。轮换访问密钥后，始终更新您的应用程序。

访问密钥包含一个访问密钥 ID 和一个私有访问密钥。它们用于签署您向 AWS发出的编程请求。用户需要自己的访问密钥才能 AWS 从适用于 Windows 的工具 AWS CLI、 AWS 软件开发工具包进行编程调用 PowerShell，或者使用个人 AWS 服务的 API 操作进行直接 HTTP 调用。

如果您的组织使用 AWS IAM Identity Center （ IAM 身份中心 ），则您的用户可以登录 Active Directory、内置的 IAM 身份中心目录或其他连接到 IAM 身份中心的身份提供商 (IdP)。然后可以将它们映射到一个 IAM 角色，使他们无需访问密钥即可运行 AWS CLI 命令或调用 AWS API 操作。要了解更多信息，请参阅AWS Command Line Interface 用户指南 AWS IAM Identity Center中的配置 AWS CLI 以使用。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要轮换超过 90 天的访问密钥，请参阅 IAM 用户指南中的轮换访问密钥。对于任何访问密钥有效期超过 90 天的用户，请按照说明进行操作。

[IAM.4] 不应存在 IAM 根用户访问密钥

相关要求：独联体 AWS 基金会基准 v3.0.0/1.4、CIS 基金会基准 v1.4.0/1.4、CIS AWS 基金会基准 v1.2.0/1.12、PCI DSS v3.2.1/2.1、PCI DSS v3.2.1/2.2、PCI DSS v3.2.1/7.2.1、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5

AC-3 (15)、nist.800-53.r5 AC-3 (15)、n800-53.r5 AC-3 (7)、nist.800-53.r5 AC-6、nist.800-53.r5 AC-6 (10)、nist.800-53.r5 AC-6 (10)、nist.800-53.r5 AC-6 (2) AWS

类别：保护 > 安全访问管理

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`iam-root-access-key-check`

计划类型：定期

参数：无

此控件检查根用户访问密钥是否存在。

root 用户是中权限最高的用户 AWS 账户。 AWS 访问密钥提供对给定账户的编程访问权限。

Security Hub 建议您删除与根用户关联的所有访问密钥。这限制了可用于危害您的账户的向量。它还鼓励创建和使用最小权限的基于角色的账户。

修复

要删除根用户访问密钥，请参阅 IAM 用户指南中的删除根用户的访问密钥。要从中删除 root 用户访问密钥 AWS GovCloud (US)，请参阅用户指南 AWS 账户 中的删除我的 AWS GovCloud (US) 账户 root AWS GovCloud (US) 用户访问密钥。

[IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA

相关要求：独联体 AWS 基金会基准 v3.0.0/1.10、CIS 基金会基准 v1.4.0/1.10、CIS AWS 基金会基准 v1.2.0/1.2、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 IA-2 (2)、nist.800-53.r5 IA-2 (2)、st.800-53.r5 IA-2 (6)、nist.800-53.r5 IA-2 (8) AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`mfa-enabled-for-iam-console-access`

计划类型：定期

参数：无

此控件检查是否为所有使用控制台密码的 IAM 用户启用了 AWS 多重身份验证 (MFA)。

多重身份验证 (MFA) 在用户名和密码之上增加了一层额外的防护。启用 MFA 后，当用户登录 AWS 网站时，系统会提示他们输入用户名和密码。此外，系统还会提示他们从 AWS MFA 设备输入身份验证码。

我们建议为拥有控制台密码的所有账户启用 MFA。MFA 旨在为控制台访问提供更高的安全性。身份验证委托人必须拥有发放具有时效性的密钥的设备，并且必须知道凭证。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要为 IAM 用户添加 MFA，请参阅 IAM 用户指南 中的在 AWS上使用多重身份验证（MFA）。

我们为符合条件的客户提供免费的 MFA 安全密钥。查看您是否符合资格，然后订购免费密钥。

[IAM.6] 应该为根用户启用硬件 MFA

相关要求：独联体 AWS 基金会基准 v3.0.0/1.6、CIS 基金会基准 v1.4.0/1.6、CIS AWS 基金会基准 v1.2.0/1.14、PCI DSS v3.2.1/8.3.1、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 IA-2 (1) r5 IA-2 (2)、nist.800-53.r5 IA-2 (6)、nist.800-53.r5 IA-2 (8) AWS

类别：保护 > 安全访问管理

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`root-account-hardware-mfa-enabled`

计划类型：定期

参数：无

此控件会检查您 AWS 账户 是否允许使用硬件多因素身份验证 (MFA) 设备使用根用户凭据登录。如果未启用 MFA 或者允许任何虚拟 MFA 设备使用根用户凭证登录，则控制失败。

虚拟 MFA 无法提供与硬件 MFA 设备相同的安全水平。我们建议您仅在等待硬件购买批准或等待硬件到达时使用虚拟 MFA 设备。要了解更多信息，请参阅 IAM 用户指南中的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 Universal 2nd Factor (U2F) 令牌都可以作为硬件 MFA 选项。

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 AWS 账户 根用户启用硬件 MFA 设备（控制台）。

我们为符合条件的客户提供免费的 MFA 安全密钥。查看您是否符合资格，然后订购免费密钥。

[IAM.7] IAM 用户的密码策略应具有可靠的配置

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-5(1)。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`RequireUppercaseCharacters`	密码中要求至少包含一个大写字符	布尔值	`true` 或者 `false`	`true`
`RequireLowercaseCharacters`	密码中要求至少包含一个小写字符	布尔值	`true` 或者 `false`	`true`

参数	描述	类型	允许的自定义值	Security Hub 默认值
RequireSymbols	密码中要求至少包含一个符号	布尔值	true 或者 false	true
RequireNumbers	密码中要求至少包含一个数字	布尔值	true 或者 false	true
MinimumPasswordLength	密码中的最少字符数	整数	8 到 128	8
PasswordReusePrevention	在可以重复使用旧密码之前的密码轮换次数	整数	12 到 24	无默认值
MaxPasswordAge	密码到期前的天数	整数	1 到 90	无默认值

此控件检查 IAM 用户的账户密码策略是否使用可靠的配置。如果密码策略未使用可靠配置，则控制失败。除非您提供自定义参数值，否则 Security Hub 将使用上表中提到的默认值。PasswordReusePrevention 和 MaxPasswordAge 参数没有默认值，因此，如果排除这些参数，Security Hub 在评估此控件时会忽略密码轮换次数和密码使用期限。

要访问 AWS 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身份验证，而不是创建 IAM 用户。联合身份验证允许用户使用其现有的公司凭证登录 AWS Management Console。使用 AWS IAM Identity Center（IAM 身份中心）创建用户或联合用户，然后在账户中担任 IAM 角色。

要了解有关身份提供商和联合身份验证的更多信息，请参阅 IAM 用户指南中的身份提供程序和联合身份验证。要了解有关 IAM Identity Center 的更多信息，请参阅 AWS IAM Identity Center 用户指南。

如果您需要使用 IAM 用户，Security Hub 建议您强制创建强用户密码。您可以对您的设置密码策略，AWS 账户 以指定密码的复杂性要求和强制轮换周期。创建或更改密码策略时，大多数密码策略设置会在用户下次更改其密码时实施。某些设置会立即强制执行。

修复

要更新密码策略，请参阅《IAM 用户指南》中的为 IAM 用户设置账户密码策略。

[IAM.8] 应移除未使用的 IAM 用户凭证

相关要求：PCI DSS v3.2.1/8.1.4、CIS AWS 基金会基准 v1.2.0/1.3、nist.800-53.r5 AC-2、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-2 (3)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 AC-3 (15)、NIS800-53.r5 AC-3 (7)、nist.800-53.r5 AC-6

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`iam-user-unused-credentials-check`

计划类型：定期

参数：

- `maxCredentialUsageAge`：`90`（不可自定义）

此控件可检查您的 IAM 用户是否拥有 90 天未使用的密码或有效访问密钥。

IAM 用户可以使用不同类型的证书（例如密码或访问密钥）访问 AWS 资源。

Security Hub 建议您删除或停用 90 天或更长时间未使用的所有凭证。禁用或删除不必要的凭证可减少他人使用遭盗用账户或已弃用账户的关联凭证的风险。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

当您在 IAM 控制台中查看用户信息时，会有访问密钥年龄、密码使用期限和上次活动列。如果上述列中的任何一个中的值大于 90 天，请停用这些用户的凭证。

您还可以使用凭证报告来监控用户并识别那些连续 90 天或以上没有活动的用户。您可以从 IAM 控制台下载 `.csv` 格式的凭证报告。

确定非活动账户或未使用的凭证后，将其停用。有关说明，请参阅 IAM 用户指南中的创建、变更或删除 IAM 用户密码（控制台）。

[IAM.9] 应为根用户启用 MFA

相关要求：PCI DSS v3.2.1/8.3.1、CIS 基金会基准 v3.0.0/1.5、CIS 基金会基准 v1.4.0/1.5、CIS AWS 基金会基准 v1.2.0/1.13、nist.800-53.r5 AC-2 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 I AWS A-2 (1)、nist.800-53.r5 (1)、nist.800-53.r5 AC-3 (15)、nist.800-53.r5 IA-2 (1) r5 IA-2 (2)、nist.800-53.r5 IA-2 (6)、nist.800-53.r5 IA-2 (8) AWS

类别：保护 > 安全访问管理

严重性：严重

资源类型：`AWS::::Account`

AWS Config 规则：`root-account-mfa-enabled`

计划类型：定期

参数：无

根用户拥有对 AWS 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，当用户登录时 AWS Management Console，系统会提示他们输入用户名和密码以及从 MFA AWS 设备输入身份验证码。

当您为根用户使用虚拟 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。

修复

要为根用户启用 MFA，请参阅《AWS 账户管理参考指南》中的在 AWS 账户 根用户上激活 MFA。

[IAM.10] IAM 用户的密码策略应该有很长的持续时间 AWS Config

相关要求：PCI DSS v3.2.1/8.1.4、PCI DSS v3.2.1/8.2.3、PCI DSS v3.2.1/8.2.4、PCI DSS v3.2.1/8.2.5。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

此控件检查 IAM 用户的账户密码策略是否使用以下最低 PCI DSS 配置。

- `RequireUppercaseCharacters`——密码中要求至少包含一个大写字符。（默认值 = `true`）
- `RequireLowercaseCharacters`——密码中要求至少包含一个小写字符。（默认值 = `true`）
- `RequireNumbers`——密码中要求至少包含一个数字。（默认值 = `true`）
- `MinimumPasswordLength`——密码最小长度。（默认值 = 7 或更长）
- `PasswordReusePrevention`——允许重用前的密码数。（默认值 = 4）
- MaxPasswordAge — 密码到期前的天数。（默认值 = 90）

修复

要更新您的密码策略以使用推荐的配置，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。

[IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母

相关要求：独联体 AWS 基金会基准 v1.2.0/1.5

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。

CIS 建议密码策略至少需要一个大写字母。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个拉丁字母表中的大写字母 (A–Z)。

[IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母

相关要求：独联体 AWS 基金会基准 v1.2.0/1.6

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。CIS 建议密码策略要求包含至少一个小写字母。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个拉丁字母表中的小写字母 (A–Z)。

[IAM.13] 确保 IAM 密码策略要求包含至少一个符号

相关要求：独联体 AWS 基金会基准 v1.2.0/1.7

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::::Account

AWS Config 规则：iam-password-policy

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。

CIS 建议密码策略要求包含至少一个符号。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个非字母数字字符。

[IAM.14] 确保 IAM 密码策略要求包含至少一个数字

相关要求：独联体 AWS 基金会基准 v1.2.0/1.8

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::::Account

AWS Config 规则：iam-password-policy

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略可确保密码使用不同的字符集。

CIS 建议密码策略要求包含至少一个数字。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码强度，选择需要至少一个数字。

[IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14

相关要求：独联体 AWS 基金会基准 v3.0.0/1.8、独联体基金会基准 v1.4.0/1.8、CIS AWS 基金会基准 v1.2.0/1.9 AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

密码策略在某种程度上强制实施密码复杂性要求。使用 IAM 密码策略确保密码至少为给定长度。

CIS 建议密码策略要求最短密码长度为 14 个字符。设置密码复杂性策略可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于密码最小长度，请输入 **14** 或更大的数字。

[IAM.16] 确保 IAM 密码策略阻止重复使用密码

相关要求：独联体 AWS 基金会基准 v3.0.0/1.9、独联体基金会基准 v1.4.0/1.9、独联体 AWS 基金会基准 v1.2.0/1.10 AWS

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

此控件检查要记住的密码数量是否设置为 24。如果该值不是 24，则控制失败。

IAM 密码策略可以阻止同一用户重复使用给定密码。

CIS 建议密码策略阻止重复使用密码。阻止重复使用密码可提高账户抵抗暴力登录尝试的弹性。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。在防止密码重复使用中，输入 **24**。

[IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效

相关要求：独联体 AWS 基金会基准 v1.2.0/1.11

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::::Account`

AWS Config 规则：`iam-password-policy`

计划类型：定期

参数：无

IAM 密码策略可以要求在给定天数后轮换密码或使密码失效。

CIS 建议密码策略在 90 天或更短时间后使密码失效。缩短密码生存期可提高账户抵抗暴力登录尝试的弹性。在以下情况下，要求定期更改密码也是非常有用的：

- 密码可能会在您不知情的情况下被窃取或泄露。系统遭受攻击、软件漏洞或内部威胁都可能导致发生这种情况。
- 某些公司和政府的 Web 筛选条件或代理服务器能够拦截和记录流量（即使流量已加密）。
- 很多用户对于许多系统（例如工作系统、电子邮件和个人系统）都使用相同的密码。
- 遭受攻击的最终用户工作站可能存在击键记录器。

修复

要变更密码策略，请参阅 IAM 用户指南中的为 IAM 用户设置账户密码策略。对于开启密码到期，请输入 **90** 或一个较小的数字。

[IAM.18] 确保已创建支持角色来管理事件 AWS Support

相关要求：独联体 AWS 基金会基准 v3.0.0/1.17、独联体基金会基准 v1.4.0/1.17、独联体 AWS 基金会基准 v1.2.0/1.20 AWS

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::::Account`

AWS Config 规则：`iam-policy-in-use`

计划类型：定期

参数：

- `policyARN`：`arn:partition:iam::aws:policy/AWSSupportAccess`（不可自定义）
- `policyUsageType`：`ANY`（不可自定义）

AWS 提供了一个支持中心，可用于事件通知和响应，以及技术支持和客户服务。

创建一个 IAM 角色以允许授权用户管理与 AWS Support 相关的事件。通过实施访问控制的最低权限，IAM 角色将需要相应的 IAM 策略来允许访问支持中心，以便管理事件 AWS Support。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要纠正此问题，请创建一个角色以允许授权用户管理 AWS Support 事件。

创建用于 AWS Support 访问的角色

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在 IAM 导航窗格中，选择角色，然后选择创建角色。

3. 对于角色类型，选择其他 AWS 账户。
4. 在账户 AWS 账户 ID 中，输入您要 AWS 账户 向其授予资源访问权限的 ID。

   如果将代入此角色的用户或组位于同一账户中，则输入本地账户号码。

   > **Note**
   >
   > 指定账户的管理员可向该账户中的任何用户授予代入该角色的权限。为此，管理员需要将策略附加到用户或组来授予 `sts:AssumeRole` 操作的权限。在该策略中，资源必须是角色 ARN。

5. 选择下一步: 权限。
6. 搜索托管策略 `AWSSupportAccess`。
7. 选中 `AWSSupportAccess` 托管策略的复选框。
8. 选择下一步：标签。
9. （可选）要将元数据添加到角色，将标签附加为键值对。

   有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南中的标记 IAM 用户和角色。
10. 选择 Next: Review (下一步：审核)。
11. 对于 Role name (角色名称)，为您的角色输入一个名称。

    角色名称在您的角色中必须是唯一的 AWS 账户。它们不区分大小写。
12. （可选）对于角色描述，输入新角色的描述。
13. 检查该角色，然后选择Create role (创建角色)。

[IAM.19] 应为所有 IAM 用户启用 MFA

相关要求：PCI DSS v3.2.1/8.3.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2(6)、NIST.800-53.r5 IA-2(8)。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：`iam-user-mfa-enabled`

计划类型：定期

参数：无

此控件检查 IAM 用户是否启用了多重身份验证（MFA）。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要为 IAM 用户添加 MFA，请参阅 IAM 用户指南中的为用户启用 AWS中 MFA 设备。

[IAM.20] 避免使用根用户

> **Important**
>
> Security Hub 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：独联体 AWS 基金会基准 v1.2.0/1.1

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::IAM::User`

AWS Config 规则：`use-of-root-account-test`（自定义 Security Hub 规则）

计划类型：定期

参数：无

此控件检查是否对 root 用户的使用有限制。 AWS 账户 该控件评估以下资源：

- Amazon Simple Notification Service（Amazon SNS）主题
- AWS CloudTrail 步道

- 与 CloudTrail 跟踪关联的指标筛选器
- 基于筛选条件的 Amazon CloudWatch 警报

如果以下一条或多条陈述为真，此检查将导致 FAILED 调查发现结果：

- 该账户中不存在任何 CloudTrail 跟踪。
- CloudTrail 跟踪已启用，但未配置至少一个包含读写管理事件的多区域跟踪。
- CloudTrail 跟踪已启用，但未与 CloudWatch 日志日志组关联。
- 没有使用 Center for Internet Security (CIS) 规定的确切指标筛选条件。规定的指标筛选条件是 `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`。
- 账户中不存在基于指标筛选条件的 CloudWatch 警报。
- CloudWatch 配置为向关联的 SNS 主题发送通知的警报不会根据警报条件触发。
- SNS 主题不符合向 SNS 主题发送消息的限制。
- SNS 主题没有至少一个订阅用户。

如果以下一条或多条陈述为真，则此检查的控件状态为 NO_DATA：

- 多区域跟踪基于不同区域。Security Hub 只能在跟踪所在的区域生成调查发现。
- 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发现。

如果以下一条或多条陈述为真，则此检查的控件状态为 WARNING：

- 当前账号不拥有 CloudWatch 警报中提及的 SNS 话题。
- 调用 `ListSubscriptionsByTopic` SNS API 时，当前账号无权访问 SNS 主题。

> **Note**
>
> 我们建议使用组织跟踪来记录来自组织中多个账户的事件。默认情况下，组织跟踪是多区域跟踪，只能由 AWS Organizations 管理账户或 CloudTrail 委派的管理员账户进行管理。使用组织跟踪会导致在组织成员账户中评估的控件的控件状态为 NO_DATA。在成员账户中，Security Hub 仅针对成员拥有的资源生成调查发现。与组织跟踪相关的调查发现在资源所有者的账户中生成。您可以使用跨区域聚合在 Security Hub 委托管理员账户中查看这些结果。

作为最佳实践，仅在需要执行账户和服务管理任务时才使用根用户凭证。将 IAM policy 直接应用于组和角色，但不应用于用户。有关设置日常使用管理员的说明，请参阅 IAM 用户指南中的创建第一个 IAM 管理员用户和组。

修复

修复此问题的步骤包括设置 Amazon SNS 主题、 CloudTrail跟踪、指标筛选条件和指标筛选器警报。

创建 Amazon SNS 主题

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 创建接收所有 CIS 警报的 Amazon SNS 主题。

   为该主题创建至少一个订阅者。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。

接下来，设置 CloudTrail 一个适用于所有地区的活动。为此，请按照the section called “[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪”中的修复步骤进行操作。

记下与 CloudTrail 跟踪关联的 Log CloudWatch s 日志组的名称。您为该日志组创建指标筛选条件。

最后，创建指标筛选条件和警报。

创建指标筛选条件和警报

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 日志组。
3. 选中与您创建的 CloudTrail 跟踪关联的 Logs CloudWatch 日志组对应的复选框。
4. 从操作中，选择创建指标筛选条件。
5. 在定义模式下，请执行以下操作：

   a. 复制以下模式，然后将其粘贴到 Filter Pattern (筛选条件模式) 字段中。

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. 选择下一步。
6. 在分配指标下，执行以下操作：

   a. 在筛选条件名称中，输入指标筛选条件的名称。

b. 对于指标命名空间，输入 **LogMetrics**。

如果您对所有 CIS 日志指标筛选条件使用相同的命名空间，则所有 CIS Benchmark 指标都会组合在一起。

c. 对于指标名称，为指标输入名称。记住指标的名称。在创建警报时，您将需要选择指标。

d. 对于 Metric value（指标值），输入 **1**。

e. 选择下一步。

7. 在查看并创建下，验证您为新指标筛选器提供的信息。选择创建指标筛选条件。
8. 在导航窗格中，选择日志组，然后选择您在指标筛选器下创建的筛选条件。
9. 选中筛选条件的复选框。选择创建警报。
10. 在指定指标和条件下，执行以下操作：

a. 在条件下，对于阈值，选择静态。

b. 对于定义警报条件，选择大于/等于。

c. 在定义阈值中输入 **1**。

d. 选择下一步。

11. 在配置操作下，执行以下操作：

a. 在警报状态触发下，选择在警报中。

b. 在 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. 对于发送通知至，输入您在上一过程中创建的 SNS 主题的名称。

d. 选择下一步。

12. 在添加名称和描述下，输入警报的名称和描述，例如 **CIS-1.1-RootAccountUsage**。然后选择下一步。
13. 在预览并创建下，查看警报配置。然后选择 Create alarm (创建警报)。

[IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作

相关要求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)、NIST.800-53.r5 AC-6(3)

类别：检测 > 安全访问管理

严重性：低

资源类型：AWS::IAM::Policy

AWS Config 规则：iam-policy-no-statements-with-full-access

计划类型：已触发变更

参数：

- excludePermissionBoundaryPolicy：True（不可自定义）

此控制检查您创建的 IAM 基于身份的策略是否具有使用 * 通配符的允许语句来授予对任何服务的所有操作的权限。如果任何策略声明包含 "Action": "Service:*" 的 "Effect": "Allow"，则控制失败。

例如，策略中的以下语句会导致失败的调查发现。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

如果 "Effect": "Allow" 与 "NotAction": "*service*:*" 配合使用，控制也会失败。在这种情况下，NotAction元素提供对中所有操作的访问权限 AWS 服务，中指定的操作除外NotAction。

此控制仅适用于客户托管的 IAM policy。它不适用于由 AWS管理的 IAM policy。

当您向分配权限时 AWS 服务，请务必在您的 IAM 策略中确定允许的 IAM 操作的范围。您应将 IAM 操作限制为仅需要的操作。这可以帮助您预置最低权限权限。如果策略附加到可能不需要权限的 IAM 主体，则过于宽松的策略可能会导致权限升级。

在某些情况下，您可能需要允许具有相似前缀的 IAM 操作，例如 DescribeFlowLogs 和 DescribeAvailabilityZones。在这些授权的情况下，您可以在通用前缀中添加带后缀的通配符。例如，ec2:Describe*。

如果您使用带有后缀通配符的带前缀的 IAM 操作，则此控制通过。例如，策略中的以下语句会形成通过的调查发现。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

以这种方式对相关的 IAM 操作进行分组时，还可以避免超出 IAM policy 的大小限制。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，可以在单个区域启用全局资源记录。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

要修复此问题，请更新 IAM policy，使其不允许完全的 "*" 管理权限。有关如何编辑 IAM policy 的详细信息，请参阅 IAM 用户指南中的编辑 IAM policy。

[IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证

相关要求：独联体 AWS 基金会基准 v3.0.0/1.12、CIS 基金会基准 v1.4.0/1.12 AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::IAM::User`

AWS Config 规则：**`iam-user-unused-credentials-check`**

计划类型：定期

参数：无

此控制检查 IAM 用户是否拥有 45 天或更长时间未使用的密码或活动访问密钥。为此，它会检查 AWS Config 规则的`maxCredentialUsageAge`参数是否等于 45 或更大。

用户可以使用不同类型的凭证（例如密码或访问密钥）访问 AWS 资源。

CIS 建议您删除或停用 45 天或更长时间未使用的所有凭证。禁用或删除不必要的凭证可减少他人使用遭盗用账户或已弃用账户的关联凭证的风险。

此控件的 AWS Config 规则使用`GetCredentialReport`和 `GenerateCredentialReport`API 操作，它们仅每四小时更新一次。对 IAM 用户的更改最多可能需要四小时才能对此控件显示。

> **Note**
>
> AWS Config 应在您使用 Security Hub 的所有区域中启用。但是，您可以启用在单个区域中记录全局资源。如果您仅在一个区域中记录全局资源，则可以在所有区域（记录全局资源的区域除外）中禁用此控件。

修复

当您在 IAM 控制台中查看用户信息时，会有访问密钥年龄、密码使用期限和上次活动列。如果上述列中的任何一个中的值大于 45 天，请停用这些用户的凭证。

您还可以使用凭证报告来监控用户并识别那些连续 45 天或以上没有活动的用户。您可以从 IAM 控制台下载 `.csv` 格式的凭证报告。

确定非活动账户或未使用的凭证后，将其停用。有关说明，请参阅 IAM 用户指南中的创建、变更或删除 IAM 用户密码（控制台）。

[IAM.23] 应标记 IAM 访问分析器分析器

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AccessAnalyzer::Analyzer`

AWS Config 规则:`tagged-accessanalyzer-analyzer`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查由 AWS Identity and Access Management Access Analyzer （ IAM Access Analyzer ）管理的分析器是否具有参数中定义的特定密钥的标签requiredTagKeys。如果分析器没有任何标签键或者没有在参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则控件仅检查标签密钥是否存在，如果分析器未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向分析器添加标签，请参阅 AWS IAM 访问分析器 API 参考TagResource中的。

[IAM.24] 应标记 IAM 角色

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IAM::Role`

AWS Config 规则:`tagged-iam-role`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Identity and Access Management (IAM) 角色是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果角色没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果该角色未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 IAM 角色添加标签，请参阅 IAM 用户指南中的标记 IAM 资源。

[IAM.25] 应标记 IAM 用户

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IAM::User`

AWS Config 规则:`tagged-iam-user`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Identity and Access Management (IAM) 用户是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果用户没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果用户未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 IAM 用户添加标签，请参阅 I AM 用户指南中的为 IAM 资源添加标签。

[IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书

相关要求：独联体 AWS 基金会基准 v3.0.0/1.19

类别：识别 > 合规

严重性：中

资源类型：`AWS::IAM::ServerCertificate`

AWS Config 规则：**`iam-server-certificate-expiration-check`**

计划类型：定期

参数：无

它控制检查在 IAM 中管理的有效 SSL/TLS 服务器证书是否已过期。如果未删除过期的 SSL/TLS 服务器证书，则控制失败。

要在中启用与您的网站或应用程序的 HTTPS 连接 AWS，您需要一个 SSL/TLS 服务器证书。您可以使用 IAM 或 AWS Certificate Manager (ACM) 来存储和部署服务器证书。只有在您必须支持 ACM 不支持的 HTTPS 连接时 AWS 区域 ，才使用 IAM 作为证书管理器。IAM 安全地加密您的私有密钥并将加密的版本存储在 IAM SSL 证书存储中。IAM 支持在所有区域部署服务器证书，但您必须从外部提供商处获取证书才能使用 AWS。您无法将 ACM 证书上传到 IAM。此外，您无法从 IAM 控制台管理您的证书。删除过期的 SSL/TLS 证书可以消除无效证书意外部署到资源的风险，这可能会损害底层应用程序或网站的可信度。

修复

要从 IAM 中删除服务器证书，请参阅 IAM 用户指南中的在 IAM 中管理服务器证书。

[IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess

相关要求：独联体 AWS 基金会基准 v3.0.0/1.22

类别：保护 > 安全访问管理 > 安全 IAM 策略

严重性：中

资源类型：`AWS::IAM::Role`、`AWS::IAM::User`、`AWS::IAM::Group`

AWS Config 规则：**`iam-policy-blacklisted-check`**

计划类型：已触发变更

参数：

- “policyarns”：“arn: aws: iam:: aws: policy/，arn: aws-cn: iam:: aws: policy/，arn:: iam:AWSCloudShellFullAccess: aws: policy/” AWSCloudShellFullAccess aws-us-gov AWSCloudShellFullAccess

此控件检查 IAM 身份（用户、角色或群组）是否`AWSCloudShellFullAccess`附加了 AWS 托管策略。如果 IAM 身份附加了`AWSCloudShellFullAccess`策略，则控制失败。

AWS CloudShell 提供了一种对运行 CLI 命令的便捷方法 AWS 服务。 AWS 托管策略`AWSCloudShellFullAccess`提供对的完全访问权限 CloudShell，允许用户在本地系统和 CloudShell 环境之间上传和下载文件。在 CloudShell 环境中，用户具有 sudo 权限，并且可以访问互联网。因此，将此托管策略附加到 IAM 身份后，他们就可以安装文件传输软件并将数据从外部互联网服务器移动 CloudShell 到外部 Internet 服务器。我们建议遵循最小权限原则，为你的 IAM 身份附加更窄的权限。

修复

要将`AWSCloudShellFullAccess`策略与 IAM 身份分离，请参阅 I AM 用户指南中的添加和删除 IAM 身份权限。

[IAM.28] 应启用 IAM 访问分析器外部访问分析器

相关要求：独联体 AWS 基金会基准 v3.0.0/1.20

类别：检测 > 检测服务 > 特权使用情况监控

严重性：高

资源类型：`AWS::AccessAnalyzer::Analzyer`

AWS Config 规则：**`iam-external-access-analyzer-enabled`**

计划类型：定期

参数：无

此控件检查是否启用 AWS 账户 了 IAM 访问分析器外部访问分析器。如果您当前选择的账户中未启用外部访问分析器，则控制失败 AWS 区域。

IAM Access Analyzer 外部访问分析器可帮助识别您的组织和账户中与外部实体共享的资源，例如亚马逊简单存储服务 (Amazon S3) 存储桶或 IAM 角色。这可以帮助您避免意外访问您的资源和数据。IAM 访问分析器是区域性的，必须在每个区域启用。为了识别与外部主体共享的资源，访问分析器使用基于逻辑的推理来分析环境中基于资源的策略。 AWS 启用外部访问分析器后，即为整个组织或账户创建一个分析器。

修复

要在特定区域启用外部访问分析器，请参阅 IAM 用户指南中的启用 IAM 访问分析器。您必须在要监控资源访问的每个区域启用分析器。

AWS IoT 控件

这些控制措施与 AWS IoT 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[IoT.1] 应 AWS IoT Core 标记安全配置文件

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::SecurityProfile`

AWS Config 规则：`tagged-iot-securityprofile`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 AWS IoT Core 安全配置文件是否具有参数中定义的特定密钥的标签requiredTagKeys。如果安全配置文件没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果安全配置文件未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 AWS IoT Core 安全配置文件添加标签，请参阅AWS IoT 开发人员指南中的为AWS IoT 资源添加标签。

[IoT.2] 应 AWS IoT Core 标记缓解措施

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::IoT::MitigationAction

AWS Config 规则：tagged-iot-mitigationaction（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 AWS IoT Core 缓解操作是否具有参数中定义的特定密钥的标签requiredTagKeys。如果缓解操作没有任何标签密钥或参数中未指定所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果缓解操作未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 缓解操作添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[IoT.3] 应为 AWS IoT Core 维度加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::Dimension`

AWS Config 规则：`tagged-iot-dimension`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS IoT Core 维度是否具有参数中定义的特定键的标签`requiredTagKeys`。如果维度没有任何标签键或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签键是否存在，如果该维度未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 维度添加标签，请参阅AWS IoT 开发者指南中的为AWS IoT 资源添加标签。

[IoT.4] 应给 AWS IoT Core 授权者加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::Authorizer`

AWS Config 规则：`tagged-iot-authorizer`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS IoT Core 授权方是否具有参数`requiredTagKeys`中定义的特定密钥的标签。如果授权者没有任何标签密钥或者没有参数`requiredTagKeys`中指定的所有密钥，则控件将失败。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果授权者未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 AWS IoT Core 授权方添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[Iot.5] 应标记 AWS IoT Core 角色别名

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::RoleAlias`

AWS Config 规则：`tagged-iot-rolealias`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS IoT Core 角色别名是否具有参数中定义的特定键的标签`requiredTagKeys`。如果角色别名没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果角色别名未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 角色别名添加标签，请参阅《AWS IoT 开发者指南》中的为AWS IoT 资源添加标签。

[IoT.6] AWS IoT Core 策略应该被标记

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::IoT::Policy`

AWS Config 规则：`tagged-iot-policy`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS IoT Core 策略是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果策略没有任何标签密钥或者没有在参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则控件仅检查标签密钥是否存在，如果策略未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为 AWS IoT Core 策略添加标签，请参阅AWS IoT 开发者指南中的为AWS IoT 资源添加标签。

Amazon Kinesis 控件

这些控制与 Kinesis 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Kinesis.1] Kinesis 直播应在静态状态下进行加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Kinesis::Stream`

AWS Config 规则：`kinesis-stream-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Kinesis Data Streams 是否使用服务器端加密进行静态加密。如果 Kinesis 流未使用服务器端加密进行静态加密，则此控制失败。

服务器端加密是 Amazon Kinesis Data Streams 中的一项功能，它使用 AWS KMS key在数据静止之前自动对其进行加密。数据在写入 Kinesis 流存储层之前进行加密，并在从存储中检索后进行解密。因此，在 Amazon Kinesis Data Streams 服务中对数据进行静态加密。

修复

有关启用 Kinesis 流的服务器端加密的信息，请参阅 Amazon Kinesis 开发人员指南中的“如何开始使用服务器端加密？”。

[Kinesis.2] Kinesis 直播应该被标记

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Kinesis::Stream`

AWS Config规则：`tagged-kinesis-stream`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon Kinesis 数据流是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果数据流没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果数据流未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Kinesis 数据流添加标签，请参阅《亚马逊 Kinesis 开发者指南》中的在 Amazon Kinesis 数据流中为直播添加标签。

AWS Key Management Service 控件

这些控制措施与 AWS KMS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作

相关要求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)。

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::IAM::Policy

AWS Config 规则：iam-customer-policy-blocked-kms-actions

计划类型：已触发变更

参数：

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt（不可自定义）
- excludePermissionBoundaryPolicy：True（不可自定义）

检查 IAM 客户托管策略的默认版本是否允许委托人对所有资源使用 AWS KMS 解密操作。如果策略足够开放，可以允许对所有 KMS 密钥执行 kms:Decrypt 或 kms:ReEncryptFrom 操作，则控制失败。

该控件仅检查 Resource 元素中的 KMS 密钥，而不考虑策略的 Condition 元素中的任何条件。此外，该控件还会评估附加和独立的客户管理型策略。它不检查内联策略或 AWS 托管策略。

使用 AWS KMS，您可以控制谁可以使用您的 KMS 密钥并访问您的加密数据。IAM policy 定义了一个身份（用户、组或角色）可以对哪些资源执行哪些操作。遵循安全最佳实践，AWS 建议您允许最低权限。换句话说，您应仅授予身份 kms:Decrypt 或 kms:ReEncryptFrom 权限，并仅授予执行任务所需的密钥。否则，用户可能会使用不适合数据的密钥。

不要授予所有密钥的权限，而是确定用户访问加密数据所需的最小密钥集。然后设计允许用户仅使用这些密钥的策略。例如，不要允许对所有 KMS 密钥的 kms:Decrypt 权限。取而代之的是，仅允许 kms:Decrypt 使用特定区域中您账户的密钥。通过采用最低权限原则，您可以降低数据意外泄露的风险。

修复

要修改 IAM 客户托管策略，请参阅 IAM 用户指南中的编辑客户管理型策略。编辑策略时，在 Resource 字段中提供您要允许执行解密操作的一个或多个密钥的 Amazon 资源名称（ARN）。

[KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

相关要求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)。

类别：保护 > 安全访问管理

严重性：中

资源类型：

- AWS::IAM::Group
- AWS::IAM::Role
- AWS::IAM::User

AWS Config 规则：iam-inline-policy-blocked-kms-actions

计划类型：已触发变更

参数：

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt（不可自定义）

此控件检查嵌入在您的 IAM 身份（角色、用户或群组）中的内联策略是否允许对所有 KMS AWS KMS 密钥执行解密和重新加密操作。如果策略足够开放，可以允许对所有 KMS 密钥执行 kms:Decrypt 或 kms:ReEncryptFrom 操作，则控制失败。

该控件仅检查 Resource 元素中的 KMS 密钥，而不考虑策略的 Condition 元素中的任何条件。

使用 AWS KMS，您可以控制谁可以使用您的 KMS 密钥并访问您的加密数据。IAM policy 定义了一个身份（用户、组或角色）可以对哪些资源执行哪些操作。遵循安全最佳实践， AWS 建议您允许最低权限。换句话说，您应该仅向身份授予他们所需的权限，并且仅授予执行任务所需的密钥。否则，用户可能会使用不适合数据的密钥。

不要授予所有密钥的权限，而是确定用户访问加密数据所需的最小密钥集。然后设计允许用户仅使用这些密钥的策略。例如，不要允许对所有 KMS 密钥的 kms:Decrypt 权限。相反，请仅允许对账户特定区域中的特定密钥授予权限。通过采用最低权限原则，您可以降低数据意外泄露的风险。

修复

要修改 IAM 内联策略，请参阅 IAM 用户指南中的编辑内联策略。编辑策略时，在 Resource 字段中提供您要允许执行解密操作的一个或多个密钥的 Amazon 资源名称（ARN）。

AWS KMS keys 不应无意中删除 [KMS.3]

相关要求：NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)。

类别：保护 > 数据保护 > 数据删除保护

严重性：严重

资源类型：`AWS::KMS::Key`

AWS Config 规则：`kms-cmk-not-scheduled-for-deletion-2`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查是否计划删除 KMS 密钥。如果计划删除 KMS 密钥，则控制失败。

KMS 密钥一经删除就无法恢复。如果删除 KMS 密钥，则使用 KMS 密钥加密的数据也将永久无法恢复。如果在计划删除的 KMS 密钥下加密了有意义的数据，请考虑使用新的 KMS 密钥对数据进行解密或重新加密数据，除非您故意执行加密擦除。

当计划删除 KMS 密钥时，如果计划错误，则会强制执行强制等待期，以便有时间撤消删除。默认等待期为 30 天，但当计划删除 KMS 密钥时，等待期可缩短至短至 7 天。在等待期限内，可以取消预定删除，KMS 密钥不会被删除。

有关删除 KMS 密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的删除 KMS 密钥。

修复

要取消预定的 KMS 密钥删除，请参阅 AWS Key Management Service 开发人员指南中的计划和取消密钥删除（控制台）下的取消密钥删除。

[KMS.4] 应启用 AWS KMS 密钥轮换

相关要求：PCI DSS v3.2.1/3.6.4、CIS 基金会基准 v3.0.0/3.6、CIS 基金会基准 v1.4.0/3.8、CIS AWS 基金会基准 v1.2.0/2.8、nist.800-53.r5 SC-12、nist.800-53.r5 SC-12 (2)、nist.800 AWS -53.r5 SC-28 (3) AWS

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::KMS::Key`

AWS Config 规则：`cmk-backing-key-rotation-enabled`

计划类型：定期

参数：无

AWS KMS 允许客户轮换备用密钥，后备密钥是存储在 KMS 密钥中的 AWS KMS 密钥材料，与 KMS 密钥的密钥 ID 相关联。备用密钥被用于执行加密操作，例如加密和解密。目前，自动密钥轮换会保留所有之前的备用密钥，以便解密已加密数据的操作可以不被察觉地进行。

CIS 建议您启用 KMS 密钥轮换。轮换加密密钥有助于减少遭盗用密钥的潜在影响，因为使用可能已泄露的先前密钥无法访问使用新密钥加密的数据。

修复

要启用 KMS 密钥轮换，请参阅AWS Key Management Service 开发人员指南中的如何启用和禁用自动密钥轮换。

AWS Lambda 控件

这些控制与 Lambda 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Lambda.1] Lambda 函数策略应禁止公共访问

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::Lambda::Function`

AWS Config 规则：`lambda-function-public-access-prohibited`

计划类型：已触发变更

参数：无

此控件检查 Lambda 函数基于资源的策略是否禁止您账户之外的公开访问。如果允许公共访问，则控制失败。如果从 Amazon S3 调用 Lambda 函数，并且该策略不包含限制公共访问的条件，则控制也会失败，例如 `AWS:SourceAccount`。我们建议在存储桶策略中使用 `AWS:SourceAccount` 与其他 S3 条件以获得更精细的访问权限。

Lambda 函数不应公开访问，因为这可能会导致意外访问函数代码。

修复

要修复此问题，您必须更新函数的基于资源的策略以移除权限或添加 `AWS:SourceAccount` 条件。您只能通过 Lambda API 或更新基于资源的策略。 AWS CLI

首先，请在 Lambda 控制台上查看基于资源的策略。确定具有公开策略的 `Principal` 字段值的策略声明，例如 `"*"` 或 `{ "AWS": "*" }`。

您无法从控制台编辑策略。要移除函数的权限，请从 AWS CLI中运行 `remove-permission` 命令。

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

<function-name> 替换为 Lambda 函数的名称，*<statement-id>* 替换为要删除的语句的语句 ID (`Sid`)。

[Lambda.2] Lambda 函数应使用受支持的运行时系统

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：保护 > 安全开发

严重性：中

资源类型：`AWS::Lambda::Function`

AWS Config 规则：`lambda-function-settings-check`

计划类型：已触发变更

参数：

- `runtime`：`dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2`（不可自定义）

此控件检查 AWS Lambda 函数运行时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。如果 Lambda 函数不使用支持的运行时，控制就会失败，如前面在参数下所述。Security Hub 会忽略包类型为的`Image`函数。

Lambda 运行时系统是围绕操作系统、编程语言和需要维护和安全更新的软件库的组合构建的。护和安全更新的操作系统、编程语言和软件库的组合构建的。当安全更新不再支持某个运行时组件时，Lambda 将弃用该运行时系统。尽管您无法创建使用已弃用运行时的函数，但该函数仍可用于处理调用事件。我们建议确保您的 Lambda 函数是最新的，并且不要使用已弃用的运行时环境。有关支持的运行时列表，请参阅《开发人员指南》中的 Lambda 运行时。AWS Lambda

修复

有关支持的运行时和弃用计划的更多信息，请参阅AWS Lambda 开发人员指南中的运行时系统弃用策略。将运行时迁移到最新版本时，请遵循语言发布者的语法和指导。我们还建议应用运行时更新，以帮助降低在运行时版本不兼容的罕见情况下影响工作负载的风险。

[Lambda.3] Lambda 函数应位于 VPC 中

相关要求：PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::Lambda::Function`

AWS Config 规则：**`lambda-inside-vpc`**

计划类型：已触发变更

参数：无

此控件检查 Lambda 函数是否部署在虚拟私有云 (VPC) 中。如果 Lambda 函数未部署在 VPC 中，则控制失败。Security Hub 不会评估 VPC 子网路由配置来确定公共可达性。您可能会看到 Lambda @Edge 资源的失败的调查发现。

在 VPC 中部署资源可增强安全性和对网络配置的控制。此类部署还提供了跨多个可用区域的可扩展性和高容错能力。您可以自定义 VPC 部署以满足不同的应用程序要求。

修复

要将现有函数配置为连接到您的 VPC 中的私有子网，请参阅 AWS Lambda 开发人员指南中的配置 VPC 访问权限。我们建议至少选择两个私有子网以实现高可用性，并至少选择一个满足功能连接要求的安全组。

[Lambda.5] VPC Lambda 函数应在多个可用区内运行

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::Lambda::Function`

AWS Config 规则：`lambda-vpc-multi-az-check`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`availabilityZones`	可用区的最小数量	枚举	`2, 3, 4, 5, 6`	2

此控件检查连接到虚拟私有云 (VPC) 的 AWS Lambda 功能是否至少在指定数量的可用区 (AZ) 中运行。如果该功能未在指定数量或更多的可用区中运行，则控制失败。除非您为可用区的最小数量提供自定义参数值，否则 Security Hub 将使用默认值即两个可用区。

跨多个可用区部署资源是确保架构内高可用性 AWS 的最佳实践。可用性是机密性、完整性和可用性三合一安全模型的核心支柱。连接到 VPC 的所有 Lambda 函数都应具有多可用区部署，以确保单个区域的故障不会导致操作完全中断。

修复

如果您将函数配置为连接到您账户中的 VPC，请指定多个可用区中的子网以确保高可用性。有关说明，请参阅 AWS Lambda 开发人员指南》中的配置 VPC 访问权限。

Lambda 自动在多个可用区中运行其他功能，以确保在单个可用区发生服务中断时可以处理事件。

[Lambda.6] 应标记 Lambda 函数

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Lambda::Function`

AWS Config 规则：`tagged-lambda-function`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Lambda 函数是否具有参数中定义的特定键的标签`requiredTagKeys`。如果函数没有任何标签键或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签键是否存在，如果该函数未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为

您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Lambda 函数添加标签，请参阅开发人员指南中的在 Lambda 函数上使用标签。AWS Lambda

Amazon Macie 控件

这些控件与 Macie 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Macie.1] 应该启用亚马逊 Macie

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

类别：检测 > 检测服务

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：`macie-status-check`

计划类型：定期

该控件检查是否为账户启用了 Amazon Macie。如果没有为该账户启用 Macie，则控制失败。

Amazon Macie 使用机器学习和模式匹配来发现敏感数据，提供对数据安全风险的可见性，并实现针对这些风险的自动防护。Macie 会自动持续评估您的 Amazon Simple Storage Service（Amazon S3）存储桶的安全性和访问控制，并生成调查发现以通知您有关 Amazon S3 数据的安全性或隐私的潜在问题。Macie 还会自动发现和报告个人身份信息（PII）等敏感数据，，让您更好地了解在 Amazon S3 中存储的数据。要了解更多信息，请参阅《Amazon Macie 用户指南》。

修复

要启用 Macie，请参阅《Amazon Macie 》中的启用 Macie。

[Macie.2] 应启用 Macie 自动发现敏感数据

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

类别：检测 > 检测服务

严重性：高

资源类型：`AWS::::Account`

AWS Config 规则：`macie-auto-sensitive-data-discovery-check`

计划类型：定期

此控件用于检查 Amazon Macie 管理员账户是否启用了自动敏感数据发现功能。如果未为 Macie 管理员帐户启用自动发现敏感数据，则控制失败。此控件仅适用于管理员帐户。

Macie 可以自动发现和报告亚马逊简单存储服务 (Amazon S3) 存储桶中的敏感数据，例如个人身份信息 (PII)。通过自动发现敏感数据，Macie 可以持续评估您的存储桶清单，并使用采样技术从您的存储桶中识别和选择具有代表性的 S3 对象。然后，Macie 会分析所选对象，检查它们是否有敏感数据。随着分析的进行，Macie 会更新统计数据、清单数据以及它提供的有关您的 S3 数据的其他信息。Macie 还会生成调查结果以报告其发现的敏感数据。

修复

要创建和配置自动敏感数据发现任务以分析 S3 存储桶中的对象，请参阅 A mazon Macie 用户指南中的为您的账户配置自动敏感数据发现。

Amazon MSK 控件

这些控件与 Amazon Managed Streaming for Apache Kafka (Amazon MSK) 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[MSK.1] MSK 集群应在代理节点之间传输时进行加密

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::MSK::Cluster`

AWS Config 规则：`msk-in-cluster-node-require-tls`

计划类型：已触发变更

参数：无

它控制检查 Amazon MSK 集群在传输过程中是否在集群的代理节点之间使用 HTTPS (TLS) 进行加密。如果为集群代理节点连接启用了纯文本通信，则控制失败。

HTTPS 提供了额外的安全层，因为它使用 TLS 来移动数据，可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击来窃听或操纵网络流量。默认情况下，Amazon MSK 使用 TLS 对传输中数据进行加密。但是，您可以在创建集群时覆盖此默认值。对于代理节点连接，我们建议使用通过 HTTPS (TLS) 的加密连接。

修复

要更新 MSK 集群的加密设置，请参阅 适用于 Apache Kafka 的 Amazon Managed Streaming 开发人员指南中的更新集群的安全设置。

[MSK.2] MSK 集群应配置增强型监控

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::MSK::Cluster`

AWS Config 规则：`msk-enhanced-monitoring-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon MSK 集群是否配置了增强型监控，且监控级别至少指定为 `PER_TOPIC_PER_BROKER`。如果集群的监控级别设置为 `DEFAULT` 或 `PER_BROKER`，则控制失败。

PER_TOPIC_PER_BROKER 监控级别可以帮助您更精细地了解 MSK 集群的性能，还提供与资源利用率相关的指标，例如 CPU 和内存使用情况。这可以帮助您确定各个主题和代理的性能瓶颈和资源利用率模式。反过来，这种可见性可以优化 Kafka 代理的性能。

修复

要为 MSK 集群配置增强型监控，请完成以下步骤：

1. 打开 Amazon MSK 控制台，网址为：https://console.aws.amazon.com/msk/home?region=us-east-1#/home/。
2. 在导航窗格中，选择集群。然后选择一个集群。
3. 在操作中，选择编辑监控。
4. 选择增强主题级别监控选项。
5. 选择保存更改。

有关监控级别的更多信息，请参阅《Amazon Managed Streaming for Apache Kafka 开发人员指南》中的更新集群的安全设置。

Amazon MQ 控件

这些控件与 Amazon MQ 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch

相关要求：nist.800-53.r5 AU-2、nist.800-53.r5 AU-3、nist.800-53.r5 AU-12、nist.800-53.r5、nist.800-53.r5 SI-4

类别：识别 > 日志记录

严重性：中

资源类型：AWS::AmazonMQ::Broker

AWS Config 规则：mq-cloudwatch-audit-log-enabled

计划类型：已触发变更

参数：无

此控件可检查 Amazon MQ ActiveMQ 代理是否将审计日志流式传输到亚马逊日志。 CloudWatch 如果代理不将审核日志流式传输到日 CloudWatch 志，则控制失败。

通过将 ActiveMQ 代理日志发布 CloudWatch 到日志，您可以 CloudWatch 创建警报和指标，以提高安全相关信息的可见性。

修复

要将 ActiveMQ 代理日志流式传输 CloudWatch 到日志，请参阅亚马逊 MQ 开发者指南中的为 Amazon MQ 日志配置 Amazon MQ。

[MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级

相关要求：nist.800-53.r5 CM-3、nist.800-53.r5 SI-2

类别：识别 > 漏洞、补丁和版本管理

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`mq-auto-minor-version-upgrade-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon MQ 代理是否启用了自动次要版本升级。如果代理未启用自动次要版本升级，则控制失败。

由于 Amazon MQ 发布并支持新的代理引擎版本，因此这些更改与现有应用程序向后兼容，不会弃用现有功能。自动代理引擎版本更新可保护您免受安全风险，帮助修复错误并改进功能。

> **Note**
>
> 当与自动次要版本升级关联的代理已安装最新补丁且不再受支持时，您必须采取手动操作进行升级。

修复

要为 MQ 代理启用自动次要版本升级，请参阅 Amazon M Q 开发者指南中的自动升级次要引擎版本。

[MQ.4] 应给亚马逊 MQ 经纪商加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`tagged-amazonmq-broker`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon MQ 代理是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果代理没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果代理未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要为亚马逊 MQ 代理添加标签，请参阅亚马逊 MQ 开发者指南中的标记资源。

[MQ.5] ActiveMQ 代理应使用主动/备用部署模式

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`mq-active-deployment-mode`

计划类型：已触发变更

参数：无

此控件检查 Amazon MQ ActiveMQ 代理的部署模式是否设置为主动/备用。如果将单实例代理（默认启用）设置为部署模式，则控制失败。

主动/备用部署为 AWS 区域中的 Amazon MQ ActiveMQ 代理提供高可用性。主动/备用部署模式包括两个不同可用区中的两个代理实例，以冗余对配置。这些代理与应用程序同步通信，这可以减少发生故障时的停机时间和数据丢失。

修复

要创建具有主动/备用部署模式的新 ActiveMQ 代理，请参阅 Amazon MQ 开发人员指南中的创建和配置 ActiveMQ 代理。对于部署模式，选择主动/备用代理。您无法变更现有代理的部署模式。相反，您必须创建一个新的代理并复制旧代理的设置。

[MQ.6] RabbitMQ 代理应该使用集群部署模式

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：低

资源类型：`AWS::AmazonMQ::Broker`

AWS Config 规则：`mq-rabbit-deployment-mode`

计划类型：已触发变更

参数：无

此控件检查 Amazon MQ RabbitMQ 代理的部署模式是否设置为集群部署。如果将单实例代理（默认启用）设置为部署模式，则控制失败。

集群部署为 AWS 区域中的 Amazon MQ RabbitMQ 代理提供了高可用性。集群部署是三个 RabbitMQ 代理节点的逻辑分组，每个节点都有自己的 Amazon Elastic Block Store (Amazon EBS) 卷和共享状态。集群部署确保数据被复制到集群中的所有节点，这可以减少故障时的停机时间和数据丢失。

修复

要创建具有集群部署模式的新 RabbitMQ 代理，请参阅 Amazon MQ 开发人员指南中的创建和连接 RabbitMQ 代理。对于部署模式，选择集群部署。您无法变更现有代理的部署模式。相反，您必须创建一个新的代理并复制旧代理的设置。

Amazon Neptune 控件

这些控制与 Neptune 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Neptune.1] 应对 Neptune 数据库集群进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否进行静态加密。如果 Neptune 数据库集群未在静态状态下加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。加密您的 Neptune 数据库集群可保护数据和元数据免遭未经授权的访问。它还满足了生产文件系统 data-at-rest 加密的合规性要求。

修复

您可以在创建 Neptune 数据库集群时启用静态加密。创建集群后，您将无法变更加密设置。有关更多信息，请参阅 Neptune 用户指南中的加密 Neptune 静态资源。

[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 AU-7(1)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-4(5)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-cloudwatch-log-export-enabled`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否将审核日志发布到 Ama CloudWatch zon 日志。如果 Neptune 数据库集群不向 CloudWatch 日志发布审核日志，则控制失败。 `EnableCloudWatchLogsExport`应设置为`Audit`。

Amazon Neptune 和亚马逊 CloudWatch 集成在一起，因此您可以收集和分析绩效指标。Neptune 会自动向警报发送指标 CloudWatch ，还支持 CloudWatch 警报。审核日志是高度可定制的。审计数据库时，可以监视对数据的每个操作并将其记录到审计跟踪记录中，包括有关访问哪个数据库集群以及如何访问的信息。我们建议将这些日志发送到， CloudWatch 以帮助您监控 Neptune 数据库集群。

修复

要将 Neptune 审核日志发布到日 CloudWatch 志，请参阅《Neptune 用户指南》 CloudWatch 中的 “将 Neptune 日志发布到亚马逊日志”。在日志导出部分中，选择审计。

[Neptune.3] Neptune 数据库集群快照不应公开

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::RDS::DBClusterSnapshot`

AWS Config 规则：`neptune-cluster-snapshot-public-prohibited`

计划类型：已触发变更

参数：无

此控件检查 Neptune 手动数据库集群快照是否公开。如果 Neptune 手动数据库集群快照是公开的，则控制失败。

除非有意图，否则 Neptune 数据库集群手动快照不应公开。如果您将未加密的手动快照公开共享，则该快照可供所有 AWS 账户使用。公开快照可能会导致意外的数据泄露。

修复

要移除 Neptune 手动数据库集群快照的公共访问权限，请参阅 Neptune 用户指南中的共享数据库集群快照。

[Neptune.4] Neptune 数据库集群应启用删除保护

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)。

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：neptune-cluster-deletion-protection-enabled

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否启用了删除保护。如果 Neptune 数据库集群未启用删除保护，则控制失败。

启用集群删除保护可提供额外保护，防止数据库意外删除或未经授权的用户删除。启用删除保护时，无法删除 Neptune 数据库集群。您必须先禁用删除保护，删除请求才能成功。

修复

要为现有 Neptune 数据库集群启用删除保护，请参阅 Amazon Aurora 用户指南中的使用控制台、CLI 和 API 修改数据库集群。

[Neptune.5] Neptune 数据库集群应启用自动备份

相关要求：NIST.800-53.r5 SI-12。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：neptune-cluster-backup-retention-check

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`minimumBackupRetentionPeriod`	最小备份保留期（以天为单位）	整数	7 到 35	7	

此控件检查 Neptune 数据库集群是否启用了自动备份，以及备份保留期是否大于或等于指定时间范围。如果没有为 Neptune 数据库集群启用备份，或者保留期小于指定时间范围，则控制失败。除非您为备份保留期提供自定义参数值，否则 Security Hub 将使用默认值即 7 天。

备份可帮助您更快地从安全事件中恢复并增强系统的故障恢复能力。通过自动备份 Neptune 数据库集群，您将能够将系统恢复到某个时间点，并最大限度地减少停机时间和数据丢失。

修复

要启用自动备份并为 Neptune 数据库集群设置保留期，请参阅《Amazon RDS 用户指南》中的启用自动备份。对于备份保留期，请选择大于或等于 7 的值。

[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(18)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBClusterSnapshot`

AWS Config 规则：`neptune-cluster-snapshot-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群快照是否处于静态加密状态。如果 Neptune 数据库集群未在静态状态下加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。为了增加安全性，Neptune 数据库集群快照中的数据应进行静态加密。

修复

您无法加密现有的 Neptune 数据库集群快照。相反，您必须将快照还原到新的数据库集群并在集群上启用加密。您可以从加密集群创建加密快照。有关说明，请参阅 Neptune 用户指南中的从数据库集群快照恢复和在 Neptune 中创建数据库集群快照。

[Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-iam-database-authentication`

计划类型：已触发变更

参数：无

此控件检查 Neptune 数据库集群是否启用了 IAM 数据库身份验证。如果未为 Neptune 数据库集群启用 IAM 数据库身份验证，则控制失败。

Amazon Neptune 数据库集群的 IAM 数据库身份验证无需在数据库配置中存储用户凭证，因为身份验证是使用 IAM 在外部管理的。启用 IAM 数据库身份验证后，每个请求都需要使用签 AWS 名版本 4 进行签名。

修复

默认情况下，创建 Neptune 数据库集群时禁用 IAM 数据库身份验证。要启用它，请参阅 Neptune 用户指南中的在 Neptune 中启用 IAM 数据库身份验证。

[Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-copy-tags-to-snapshot-enabled`

计划类型：已触发变更

参数：无

此控制会检查 Neptune 数据库集群是否配置为在创建快照时将所有标签复制到快照。如果 Neptune 数据库集群未配置为将标签复制到快照，则控制失败。

IT 资产的识别和清点是治理和安全的一个重要方面。您应使用与其父级 Amazon RDS 数据库集群相同的方式为快照添加标签。复制标签可确保数据库快照的元数据与父数据库集群的元数据匹配，并且数据库快照的访问策略也与父数据库实例的访问策略匹配。

修复

要将标签复制到 Neptune 数据库集群的快照，请参阅 Neptune 用户指南中的在 Neptune 中复制标签。

[Neptune.9] Neptune 数据库集群应跨多个可用区部署

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`neptune-cluster-multi-az-enabled`

计划类型：已触发变更

参数：无

此控件会检查 Amazon Neptune 数据库集群在多个可用区（AZ）中是否有只读副本实例。如果集群仅部署在一个可用区中，则控制失败。

如果可用区不可用且处于定期维护事件期间，只读副本将用作主实例的失效转移目标。也就是说，如果主实例失败，Neptune 将只读副本实例提升为主实例。相比之下，如果您的数据库集群不包含任何只读副本实例，则当主实例出现故障时，您的数据库集群将保持不可用状态，直到重新创建该实例。与提升只读副本相比，重新创建主实例所需的时间要长得多。为确保高可用性，我们建议您创建一个或多个只读副本实例，这些实例的数据库实例类与主实例相同，并且与主实例位于不同的可用区。

修复

要在多个可用区中部署 Neptune 数据库集群，请参阅《Neptune 用户指南》中的 Neptune 数据库集群中的只读副本数据库实例。

AWS Network Firewall 控件

这些控制与 Network Firewall 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则：`netfw-multi-az-enabled`

计划类型：已触发变更

参数：无

此控件评估通过管理的防火墙 AWS Network Firewall 是否部署在多个可用区 (AZ) 上。如果防火墙仅部署在一个可用区中，则控制失败。

AWS 全球基础设施包括多个 AWS 区域。每个区域内的可用区位置在物理上是相互独立、相互隔离的，通过低延迟、高吞吐量且高冗余性的网络连接在一起。通过跨多个可用区部署 Network Firewall 防火墙，您可以在可用区之间平衡和转移流量，这可以帮助您设计高度可用的解决方案。

修复

跨多个可用区部署 Network Firewall 防火墙

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在导航窗格中的网络防火墙 下，选择防火墙。
3. 在防火墙页面上，选择要编辑的防火墙。
4. 在防火墙详细信息页面上，选择防火墙详细信息选项卡。
5. 在关联策略和 VPC 部分中，选择编辑
6. 要添加新的可用区，请选择添加新子网。请选择您要使用的可用区和子网。确保您至少选择两个可用区。

7. 选择保存。

[NetworkFirewall.2] 应启用 Network Firewall 日志记录

相关要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::NetworkFirewall::LoggingConfiguration`

AWS Config 规则：`netfw-logging-enabled`

计划类型：定期

参数：无

此控件检查是否已为 AWS Network Firewall 防火墙启用日志记录。如果没有为至少一种日志类型启用日志记录或者日志记录目标不存在，则控制失败。

日志记录可帮助您保持防火墙的可靠性、可用性和性能。在 Network Firewall 中，日志记录为您提供有关网络流量的详细信息，包括有状态引擎接收数据包流的时间、有关数据包流的详细信息以及针对数据包流采取的任何有状态规则操作。

修复

要启用防火墙日志记录，请参阅《AWS Network Firewall 开发人员指南》中的更新防火墙的日志记录配置。

[NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 规则：netfw-policy-rule-group-associated

计划类型：已触发变更

参数：无

此控件检查 Network Firewall 策略是否关联了任何状态或无状态规则组。如果未分配无状态或有状态规则组，则控制失败。

防火墙策略定义防火墙如何监控和处理 Amazon Virtual Private Cloud（Amazon VPC）中的流量。配置无状态和有状态规则组有助于筛选数据包和流量，并定义默认流量处理。

修复

要向 Network Firewall 策略添加规则组，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙策略。有关创建和管理规则组的信息，请参阅 AWS Network Firewall中的规则组。

[NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 规则：netfw-policy-default-action-full-packets

计划类型：已触发变更

参数：

- statelessDefaultActions: aws:drop,aws:forward_to_sfe（不可自定义）

此控件检查 Network Firewall 策略中对完整数据包的默认无状态操作是丢弃还是转发。如果选择了 Drop 或 Forward，则控制通过，如果选择 Pass 则控制失败。

防火墙策略定义防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来筛选数据包和流量。默认为 Pass 可能会允许意外流量。

修复

要变更您的防火墙策略，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙策略。对于无状态默认操作，请选择编辑。然后，选择丢弃或转发到有状态的规则组作为操作。

[NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::NetworkFirewall::FirewallPolicy`

AWS Config 规则：`netfw-policy-default-action-fragment-packets`

计划类型：已触发变更

参数：

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`（不可自定义）

此控件检查 Network Firewall 策略中对碎片数据包的默认无状态操作是丢弃还是转发。如果选择了 `Drop` 或 `Forward`，则控制通过，如果选择 `Pass` 则控制失败。

防火墙策略定义防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来筛选数据包和流量。默认为 `Pass` 可能会允许意外流量。

修复

要变更您的防火墙策略，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙策略。对于无状态默认操作，请选择编辑。然后，选择丢弃或转发到有状态的规则组作为操作。

[NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(5)。

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::NetworkFirewall::RuleGroup`

AWS Config 规则：`netfw-stateless-rule-group-not-empty`

计划类型：已触发变更

参数：无

此控件检查中的无状态规则组是否 AWS Network Firewall 包含规则。如果规则组中没有规则，则控制失败。

规则组包含的规则定义防火墙如何处理您的 VPC 中的流量。当防火墙策略中存在空的无状态规则组时，可能会给人一种规则组将处理流量的印象。但是，当无状态规则组为空时，它不处理流量。

修复

要将规则添加到 Network Firewall 规则组，请参阅 AWS Network Firewall 开发人员指南中的更新有状态规则组。在防火墙详细信息页面上，对于无状态规则组，选择编辑以添加规则。

[NetworkFirewall.7] 应标记 Network Firewall 防火墙

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则：`tagged-networkfirewall-firewall`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Network Firewall 防火墙是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果防火墙没有任何标签密钥或者没有在参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果防火墙未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Network Firewall 防火墙添加标签，请参阅《AWS Network Firewall 开发者指南》中的标记 AWS Network Firewall 资源。

[NetworkFirewall.8] 应标记 Network Firewall 防火墙策略

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::NetworkFirewall::FirewallPolicy`

AWS Config 规则：`tagged-networkfirewall-firewallpolicy`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Network Firewall 防火墙策略是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果防火墙策略没有任何标签密钥或参数中没有指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果防火墙策略未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Network Firewall 策略添加标签，请参阅AWS Network Firewall 开发者指南中的标记 AWS Network Firewall 资源。

[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)。

类别：保护 > 网络安全

严重性：中

资源类型：`AWS::NetworkFirewall::Firewall`

AWS Config 规则：`netfw-deletion-protection-enabled`

计划类型：已触发变更

参数：无

此控件检查 AWS Network Firewall 防火墙是否启用了删除保护。如果未为防火墙启用删除保护，则控制失败。

AWS Network Firewall 是一项有状态的托管网络防火墙和入侵检测服务，可让您检查和过滤进出虚拟私有云 (VPC) 或虚拟私有云 (VPC) 之间的流量。删除保护设置可防止意外删除防火墙。

修复

要在现有 Network Firewall 防火墙上启用删除保护，请参阅 AWS Network Firewall 开发人员指南中的更新防火墙。对于变更保护，选择启用。您也可以通过调用 UpdateFirewallDeleteProtectionAPI 并将该`DeleteProtection`字段设置为来`true`启用删除保护。

亚马逊 OpenSearch 服务控制

这些控制与 OpenSearch 服务资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Opensearch.1] OpenSearch 域名应启用静态加密

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-encrypted-at-rest`

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域名是否启用了 encryption-at-rest 配置。如果未启用静态加密，检查将失败。

为了增加敏感数据的安全性，您应将 OpenSearch 服务域配置为静态加密。配置静态数据加密时，会 AWS KMS 存储和管理您的加密密钥。要执行加密，请 AWS KMS 使用带有 256 位密钥的高级加密标准算法 (AES-256)。

要了解有关静态 OpenSearch 服务加密的更多信息，请参阅《亚马逊服务开发者指南》中的亚马逊 OpenSearch 服务静态数据加密。 OpenSearch

修复

要为新域和现有 OpenSearch 域名启用静态加密，请参阅 Amazon S OpenSearch ervice 开发者指南中的启用静态数据加密。

[Opensearch.2] OpenSearch 域名不应向公众开放

相关要求：PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：严重

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-in-vpc-only`

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域是否在 VPC 中。它不会评估 VPC 子网路由配置来确定公共访问。

您应确保 OpenSearch 域名未连接到公有子网。请参阅《Amazon OpenSearch 服务开发者指南》中的基于资源的政策。您还应该确保根据建议的最佳实践配置了 VPC。请参阅 Amazon VPC 用户指南中的 VPC 安全最佳实践。

OpenSearch 部署在 VPC 中的域可以通过私有 AWS 网络与 VPC 资源通信，无需穿越公共互联网。此配置通过限制对传输中数据的访问来提高安全状况。VPC 提供了许多网络控制来保护对 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 以利用这些控制措施。

修复

如果您创建一个具有公有端点的域，则以后无法将其放置在 VPC 中。您必须创建一个新的域，然后迁移数据。反之亦然。如果在 VPC 中创建一个域，则该域不能具有公有端点。您必须创建另一个域或禁用该控制。

有关说明，请参阅《亚马逊 OpenSearch 服务开发者指南》中的在 VPC 内启动您的亚马逊 OpenSearch 服务域。

[Opensearch.3] OpenSearch 域应加密节点之间发送的数据

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-node-to-node-encryption-check`

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域名是否启用了 node-to-node 加密。如果在域上禁用了 node-to-node 加密，则此控件将失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。为 OpenSearch 域启用 node-to-node 加密可确保集群内部通信在传输过程中得到加密。

此配置可能会降低性能。在启用此选项之前，您应该了解并测试性能权衡。

修复

要在 OpenSearch 域上启用 node-to-node 加密，请参阅《亚马逊 OpenSearch 服务开发者指南》中的启用 node-to-node 加密。

[Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-logs-to-cloudwatch`

计划类型：已触发变更

参数：

- `logtype = 'error'`（不可自定义）

此控件检查 OpenSearch 域是否配置为向日志发送错误 CloudWatch 日志。如果未为域启用错误记录功能， CloudWatch 则此控件将失败。

您应该为 OpenSearch 域启用错误日志，并将这些日志发送到 CloudWatch 日志以进行保留和响应。域错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

修复

要启用日志发布，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用日志发布（控制台）。

[Opensearch.5] OpenSearch 域应启用审核日志

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-audit-logging-enabled`

计划类型：已触发变更

参数：

- `cloudWatchLogsLogGroupArnList`（不可自定义）- Security Hub 不会填充此参数。应为审核日志配置的 CloudWatch 日志组列表，以逗号分隔。

`NON_COMPLIANT`如果未在此参数列表中指定 OpenSearch域的 CloudWatch 日志日志组，则此规则适用。

此控件检查 OpenSearch 域名是否启用了审核日志。如果 OpenSearch 域未启用审核日志，则此控件将失败。

审核日志是高度可定制的。它们允许您跟踪OpenSearch 集群上的用户活动，包括身份验证成功和失败、对身份验证的请求OpenSearch、索引更改以及传入的搜索查询。

修复

有关启用审计日志的说明，请参阅《Amazon S OpenSearch ervice 开发者指南》中的启用审计日志。

[Opensearch.6] OpenSearch 域名应至少有三个数据节点

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：opensearch-data-node-fault-tolerance

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域是否配置了至少三个数据节点，并且zoneAwarenessEnabled是true。如果 OpenSearch 域小于 3 或小instanceCount于 3，zoneAwarenessEnabled则此控制失败false。

一个 OpenSearch 域至少需要三个数据节点才能实现高可用性和容错能力。部署具有至少三个数据节点的 OpenSearch 域可确保在节点出现故障时集群运行。

修复

修改 OpenSearch 域中数据节点的数量

1. 登录 AWS 主机并打开亚马逊 OpenSearch 服务控制台，网址为 https://console.aws.amazon.com/aos/。
2. 在我的域名下，选择要编辑的域名，然后选择编辑。
3. 在数据节点下，将节点数设置为大于 3 的数字。如果您要部署到三个可用区，将该数字设置为三的倍数，以确保可用区间的分布均等。
4. 选择提交。

[Opensearch.7] OpenSearch 域名应启用精细的访问控制

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 > 敏感的 API 操作受限

严重性：高

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：opensearch-access-control-enabled

计划类型：已触发变更

参数：无

此控件检查 OpenSearch 域名是否启用了细粒度访问控制。如果未启用精细访问控制，则控制失败。细粒度的访问控制需要`advanced-security-options`在 OpenSearch 参数中启`update-domain-config`用。

精细的访问控制提供了更多控制您在 Ama OpenSearch zon Service 上数据的访问权限的方法。

修复

要启用精细访问控制，请参阅亚马逊服务开发者指南中的亚马逊 OpenSearch 服务中的精细访问控制。 OpenSearch

[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密

相关要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-https-required`

计划类型：已触发变更

参数：

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`（不可自定义）

此控制检查是否将 Amazon S OpenSearch ervice 域终端节点配置为使用最新的 TLS 安全策略。如果未将 OpenSearch 域终端节点配置为使用最新的支持策略或未启用 HTTP，则控制失败。

HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。加密传输中数据可能会影响性能。您应该使用此功

能测试应用程序，以了解性能概况和 TLS 的影响。与先前版本的 TLS 相比，TLS 1.2 提供了多项安全增强功能。

修复

要启用 TLS 加密，请使用 UpdateDomainConfigAPI 操作。配置DomainEndpointOptions字段以指定其值TLSSecurityPolicy。有关更多信息，请参阅《亚马逊 OpenSearch 服务开发者指南》中的 Node-to-node 加密。

[Opensearch.9] 应该给 OpenSearch 域名加标签

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::OpenSearch::Domain

AWS Config 规则：tagged-opensearch-domain（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 Amazon S OpenSearch ervice 域名是否具有参数中定义的特定密钥的标签requiredTagKeys。如果域名没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果该域未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 OpenSearch 服务域添加标签，请参阅《亚马逊 OpenSearch 服务开发者指南》中的使用标签。

[Opensearch.10] OpenSearch 域名应安装最新的软件更新

相关要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：低

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-update-check`

计划类型：已触发变更

参数：无

此控件用于检查 Amazon S OpenSearch ervice 域是否安装了最新的软件更新。如果已有可用软件更新但没有为该域安装，则控制失败。

OpenSearch 服务软件更新提供适用于该环境的最新平台修复、更新和功能。继续 up-to-date 安装补丁有助于维护域的安全性和可用性。如果没有对必需更新采取任何操作，将自动更新服务软件（通常在 2 周后）。我们建议在域流量较低的时段安排更新，以最大限度地减少服务中断。

修复

要为 OpenSearch 域安装软件更新，请参阅《亚马逊 OpenSearch 服务开发者指南》中的启动更新。

[Opensearch.11] OpenSearch 域名应至少有三个专用的主节点

相关要求：nist.800-53.r5 CP-10、nist.800-53.r5 CP-2、nist.800-53.r5 SC-5、nist.800-53.r5 SC-36、nist.800-53.r5、nist.800-53.r5 SI-13

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::OpenSearch::Domain`

AWS Config 规则：`opensearch-primary-node-fault-tolerance`

计划类型：已触发变更

参数：无

此控件会检查 Amazon S OpenSearch ervice 域是否配置了至少三个专用主节点。如果域的专用主节点少于三个，则控制失败。

OpenSearch 服务使用专用的主节点来提高集群稳定性。专用主节点执行集群管理任务，但不保存数据或响应数据上传请求。我们建议您使用带备用空间的多可用区，这会向每个生产 OpenSearch 域添加三个专用的主节点。

修复

要更改 OpenSearch 域的主节点数量，请参阅《亚马逊 OpenSearch 服务开发者指南》中的创建和管理亚马逊 OpenSearch 服务域名。

AWS Private Certificate Authority 控件

这些控制措施与 AWS Private CA 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[PCA.1] 应禁用 AWS Private CA 根证书颁发机构

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::ACMPCA::CertificateAuthority`

AWS Config 规则：`acm-pca-root-ca-disabled`

计划类型：定期

参数：无

此控件检查根证书颁发机构 (CA) 是否 AWS Private CA 已禁用。如果启用了根 CA，则控制失败。

使用 AWS Private CA，您可以创建包含根 CA 和从属 CA 的 CA 层次结构。您应该尽量减少在日常任务中使用根 CA，尤其是在生产环境中。根 CA 应仅用于为中间 CA 颁发证书。这样，在中间 CA 执行颁发终端实体证书的日常任务时，根 CA 可以不受损害地存储。

修复

要禁用根 CA，请参阅《AWS Private Certificate Authority 用户指南》中的更新 CA 状态。

Amazon Relational Database Service 控件

这些控件与 Amazon RDS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[RDS.1] RDS 快照应为私有

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::RDS::DBClusterSnapshot`、`AWS::RDS::DBSnapshot`

AWS Config 规则：`rds-snapshots-public-prohibited`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 快照是否公有。如果 RDS 快照是公开的，则控制失败。此控件评估 RDS 实例、Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群。

RDS 快照用于备份 RDS 实例上在特定时间点的数据。它们可用于将 RDS 实例还原到之前的状态。

除非有意这样做，否则 RDS 快照不得为公有快照。如果您将未加密的手动快照作为公有快照进行共享，这会使所有 AWS 账户均可获得此快照。这可能会导致 RDS 实例意外的数据泄露。

请注意，如果将配置更改为允许公共访问，则该 AWS Config 规则可能在长达 12 小时内无法检测到更改。在 AWS Config 规则检测到更改之前，即使配置违反了规则，检查也会通过。

要了解有关共享数据库快照的更多信息，请参阅 Amazon RDS 用户指南中的共享数据库快照。

修复

要从 RDS 快照中删除公共访问权限，请参阅 Amazon RDS 用户指南中的共享快照。对于数据库快照可见性，我们选择私有。

[RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config

相关要求：CIS AWS 基金会基准 v3.0.0/2.3.3、PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4、nist.dss v3.2.1/1.3.6 800-53.r5 AC-4 (21)、nist.800-53.r5 SC-7、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (16)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-7 (4) 53.r5 SC-7 (5)

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-public-access-check`

计划类型：已触发变更

参数：无

该控制通过评估实例配置项中的 `PubliclyAccessible` 字段，以检查是否可以公开访问 Amazon RDS 实例。

Neptune 数据库实例和 Amazon DocumentDB 集群没有 `PubliclyAccessible` 标志，因此无法进行评估。但是，这种控件仍然可以为这些资源生成调查发现。您可以隐瞒这些结果。

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。

除非您希望 RDS 实例可公开访问，否则不应将 RDS 实例配置为 `PubliclyAccessible` 值。这样做可能会给数据库实例带来不必要的流量。

修复

要移除 RDS 数据库实例的公有访问权限，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。对于公有访问权限，选择否。

[RDS.3] RDS 数据库实例应启用静态加密

相关要求：独联体 AWS 基金会基准 v3.0.0/2.3.1、CIS 基金会基准 v1.4.0/2.3.1、nist.800-53.r5 C AWS A-9 (1)、nist.800-53.r5 CM-3 (6)、nist.800-53.r5 SC-13、nist.800-53.r5 SC-28、nist.800-53.r5 SC-28 (1)、nist.800-53.r5 (1)、nist.800-53.r5、nist.800-53.r5、nist.800-53.r5 (1)、nist.800-53.r5 (1)、nist.-53.r5 SC-7 (10)、nist.800-53.r5 SI-7 (6)

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-storage-encrypted`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库实例是否启用了存储加密。

此控件适用于 RDS 数据库实例。但是，它也可以生成 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的调查发现。如果这些结果没有用，那么您可以隐瞒它们。

为了增加 RDS 数据库实例中敏感数据的安全性，您应将 RDS 数据库实例配置为静态加密。要静态加密 RDS DB 数据库实例和快照，请启用 RDS 数据库实例的加密选项。静态加密的数据包括数据库实例的底层存储、自动备份、只读副本和快照。

RDS 加密的数据库实例使用开放的标准 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] RDS 集群快照和数据库快照应进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBClusterSnapshot`、 `AWS::RDS::DBSnapshot`

AWS Config 规则：`rds-snapshot-encrypted`

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库快照是否已加密。如果 RDS 数据库快照未加密，则控制失败。

此控件适用于 RDS 数据库实例。但是，它也可以生成 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的快照的调查发现。如果这些结果没有用，那么您可以隐瞒它们。

对静态数据进行加密可降低未经身份验证的用户访问存储在磁盘上的数据的风险。为了增加安全性，RDS 快照中的数据应进行静态加密。

修复

要加密 RDS 快照，请参阅 Amazon RDS 用户指南中的加密 Amazon RDS 资源。加密 RDS 数据库实例时，加密的数据包括实例的底层存储、其自动备份、只读副本和快照。

您只能在创建 RDS 数据库实例时而不是创建该数据库实例之后加密该数据库实例。不过，由于您可以加密未加密快照的副本，因此，您可以高效地为未加密的数据库实例添加加密。也就是说，您可以创建数据库实例快照，然后创建该快照的加密副本。然后，您可以从加密快照还原数据库实例，从而获得原始数据库实例的加密副本。

[RDS.5] RDS 数据库实例应配置多个可用区

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-multi-az-support`

计划类型：已触发变更

参数：无

此控件检查是否为 RDS 数据库实例启用了高可用性。

RDS 数据库实例应配置为多个可用区 (AZ)。这样可以确保所存储数据的可用性。多可用区部署允许在可用区可用性出现问题和定期 RDS 维护期间进行自动失效转移。

修复

要在多个可用区中部署数据库实例，请参阅 Amazon RDS 用户指南中的将数据库实例修改为多可用区数据库实例部署。

[RDS.6] 应为 RDS 数据库实例配置增强监控

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

类别：检测 > 检测服务

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-enhanced-monitoring-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`monitoringInterval`	监控指标收集间隔之间的秒数	枚举	`1`, `5`, `10`, `15`, `30`, `60`	无默认值	

该控件检查是否为 Amazon Relational Database Service（Amazon RDS）数据库实例启用了增强监控。如果没有为实例启用增强监控，则控制失败。如果您为 `monitoringInterval` 参数提供自定义值，则仅当在按指定间隔收集实例的增强监控指标时，控制才会通过。

在 Amazon RDS 中，增强型监控可以更快地响应底层基础设施的性能变化。这些性能变化可能会导致数据可用性不足。增强监控提供 RDS 数据库实例运行的操作系统的实时指标。实例上安装了代理。与从虚拟机管理程序层相比，代理可以更准确地获取指标。

若您想了解数据库实例上不同进程或线程对 CPU 的使用差异，增强监测指标非常有用。有关更多信息，请参阅《Amazon RDS 用户指南》中的增强监控。

修复

有关为数据库实例启用增强监控的详细说明，请参阅 Amazon RDS 用户指南中的设置和启用增强监控。

[RDS.7] RDS 集群应启用删除保护

相关要求：NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)。

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-deletion-protection-enabled`

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库集群是否已启用删除保护。如果 RDS 数据库集群未启用删除保护，则控制失败。

此控件适用于 RDS 数据库实例。但是，它也可以生成 Aurora 数据库实例、Neptune 数据库实例和 Amazon DocumentDB 集群的调查发现。如果这些结果没有用，那么您可以隐瞒它们。

启用集群删除保护是针对意外数据库删除或未经授权实体删除的额外保护层。

启用删除保护后，RDS 集群将无法被删除。在删除请求成功之前，必须禁用删除保护。

修复

要为 RDS 数据库集群启用删除保护，请参阅 Amazon RDS 用户指南中的使用控制台、CLI 和 API 修改数据库集群。对于删除保护，选择启用删除保护。

[RDS.8] RDS 数据库实例应启用删除保护

相关要求：NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-deletion-protection-enabled`

计划类型：已触发变更

参数：

- `databaseEngines`：`mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web`（不可自定义）

此控件会检查使用所列数据库引擎之一的 RDS 数据库实例是否启用了删除保护。如果 RDS 数据库实例未启用删除保护，则控制失败。

启用实例删除保护是针对意外数据库删除或未经授权实体删除的额外保护层。

启用删除保护后，RDS 数据库实例无法删除。在删除请求成功之前，必须禁用删除保护。

修复

要对 RDS 数据库实例启用删除保护，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。对于删除保护，选择启用删除保护。

[RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库实例是否配置为将以下日志发布到 Amazon L CloudWatch ogs。如果实例未配置为将以下日志发布到 CloudWatch 日志，则控制失败：

- Oracle:（警报、审计、跟踪、侦听器）

- PostgreSQL:（Postgresql，升级）
- MySQL:（审计、错误、常规、 SlowQuery）
- MariaDB:（审计、错误、常规、 ）SlowQuery
- SQL 服务器：（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。数据库日志可以协助安全和访问审计，并可以帮助诊断可用性问题。

修复

要将 RDS 数据库日志发布到 CloudWatch 日志，请参阅 Amazon RDS 用户指南中的指定要发布到 CloudWatch 日志的日志。

[RDS.10] 应为 RDS 实例配置 IAM 身份验证

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-iam-authentication-enabled`

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库实例是否启用了 IAM 数据库身份验证。如果未为 RDS 数据库实例配置 IAM 身份验证，则控制失败。此控件仅评估具有以下引擎类型的 RDS 实例：`mysql`、`postgres`、`aurora`、`aurora-mysql`、`aurora-postgresql` 和 `mariadb`。RDS 实例还必须处于以下状态之一才能生成调查发现：`available`、`backing-up`、`storage-optimization` 或 `storage-full`。

IAM 数据库身份验证允许使用身份验证令牌而不是密码对数据库实例进行身份验证。进出数据库的网络流量使用 SSL 加密。有关更多信息，请参阅《Amazon Aurora 用户指南》中的 IAM 数据库身份验证。

修复

要在 RDS 数据库实例上激活 IAM 数据库身份验证，请参阅 Amazon RDS 用户指南中的启用和禁用 IAM 数据库身份验证。

[RDS.11] RDS 实例应启用自动备份

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`db-instance-backup-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`backupRetentionMinimum`	最小备份保留期（以天为单位）	整数	7 到 35	7	
`checkReadReplicas`	检查 RDS 数据库实例是否已针对只读副本启用备份。	布尔值	不可自定义	`false`	

此控件检查 Amazon Relational Database Service 实例是否启用了自动备份以及备份保留期是否大于或等于指定时间范围。只读副本不在评估范围内。如果没有为实例启用备份或保留期小于指定时间范围，则控制失败。除非您为备份保留期提供自定义参数值，否则 Security Hub 将使用默认值即 7 天。

备份可帮助您更快地从安全事件中恢复并增强系统的故障恢复能力。Amazon RDS 使您能够配置每日完整实例卷快照。有关 Amazon RDS 自动备份的更多信息，请参阅《Amazon RDS 用户指南》中的处理备份。

修复

要在 RDS 数据库实例上启用自动备份，请参阅 Amazon RDS 用户指南中的启用自动备份。

[RDS.12] 应为 RDS 集群配置 IAM 身份验证

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 > 无密码身份验证

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-iam-authentication-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库集群是否启用了 IAM 数据库身份验证。

IAM 数据库身份验证允许对数据库实例进行免密码身份验证。身份验证使用身份验证令牌。进出数据库的网络流量使用 SSL 加密。有关更多信息，请参阅《Amazon Aurora 用户指南》中的 IAM 数据库身份验证。

修复

要为数据库集群启用 IAM 身份验证，请参阅 Amazon Aurora 用户指南中的启用和禁用 IAM 数据库身份验证。

[RDS.13] 应启用 RDS 自动次要版本升级

相关要求：CIS AWS 基金会基准 v3.0.0/2.3.2、nist.800-53.r5 SI-2、nist.800-53.r5 SI-2 (2)、nist.800-53.r5 SI-2 (4)、nist.800-53.r5 SI-2 (5)

类别：识别 > 漏洞、补丁和版本管理

严重性：高

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-automatic-minor-version-upgrade-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 RDS 数据库实例启用了自动次要版本升级。

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。及时安装补丁程序是保护系统安全的重要一步。

修复

要为现有数据库实例启用自动次要版本升级，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。对于自动次要版本升级，请选择是。

[RDS.14] Amazon Aurora 集群应启用回溯功能

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`aurora-mysql-backtracking-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`BacktrackWindowInHours`	回溯 Aurora MySQL 集群所需的小时数	Double	`0.1` 到 `72`	无默认值	

此控件检查 Amazon Aurora 集群是否启用了回溯。如果集群未启用回溯，则控制失败。如果您为 `BacktrackWindowInHours` 参数提供自定义值，则仅当集群在指定的时间长度内被回溯时，控制才会通过。

备份可以帮助您更快地从安全事件中恢复。它们还可以增强系统的弹性。Aurora 回溯可将数据库还原到某个时间点的时间。这样做不需要数据库恢复。

修复

要启用 Aurora 回溯，请参阅《Amazon Aurora 用户指南》中的配置回溯。

请注意，您无法在现有集群上启用回溯功能。相反，您可创建启用回溯功能的克隆。有关 Aurora 回溯限制的更多信息，请参阅回溯概述中的限制列表。

[RDS.15] 应为多个可用区配置 RDS 数据库集群

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-multi-az-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 RDS 数据库集群启用了高可用性。如果 RDS 数据库集群未部署在多个可用区 (AZ) 中，则控制失败。

应为多个可用区配置 RDS 数据库集群，以确保存储数据的可用性。部署到多个可用区允许在出现可用区可用性问题和定期 RDS 维护事件期间进行自动失效转移。

修复

要在多个可用区中部署数据库集群，请参阅 Amazon RDS 用户指南中的将数据库实例修改为多可用区数据库实例部署。

Aurora 全球数据库的修复步骤有所不同。要为 Aurora 全球数据库配置多个可用区，请选择数据库集群。然后，选择操作和添加读取器，并指定多个 AZ。有关更多信息，请参阅 Amazon Aurora 用户指南中的将 Aurora 副本添加到数据库集群。

[RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 清单

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-copy-tags-to-snapshots-enabled`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控制检查 RDS 数据库集群是否配置为在创建快照时将所有标签复制到快照。

IT 资产的识别和清点是治理和安全的一个重要方面。您需要了解所有 RDS 数据库集群的可见性，以便评测其安全状况并对潜在的薄弱环节采取行动。快照的标记方式应与其父级 RDS 数据库集群相同。启用此设置可确保快照继承其父级数据库集群的标签。

修复

要自动将标签复制到 RDS 数据库集群的快照，请参阅 Amazon Aurora 用户指南中的使用控制台、CLI 和 API 修改数据库集群。选择将标签复制到快照。

[RDS.17] 应将 RDS 数据库实例配置为将标签复制到快照

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)。

类别：识别 > 清单

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-copy-tags-to-snapshots-enabled`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控制检查 RDS 数据库实例是否配置为在创建快照时将所有标签复制到快照。

IT 资产的识别和清点是治理和安全的一个重要方面。您需要了解所有 RDS 数据库实例，以便评测其安全状况并对潜在的薄弱环节采取行动。快照的标记方式应与其父 RDS 数据库实例相同。启用此设置可确保快照继承其父级数据库实例的标签。

修复

要自动将标签复制到 RDS 数据库实例的快照，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。选择将标签复制到快照。

[RDS.18] RDS 实例应部署在 VPC 中

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：高

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-deployed-in-vpc`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查是否在 EC2-VPC 上部署了 Amazon RDS 实例。

VPC 提供了许多网络控制来保护对 RDS 资源的访问。这些控制包括 VPC 端点、网络 ACL 和安全组。要利用这些控制，我们建议您在 EC2-VPC 上创建 RDS 实例。

修复

有关将 RDS 实例移至 VPC 的说明，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现有 RDS 事件通知订阅

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则：`rds-cluster-event-notifications-configured`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查数据库集群的现有 Amazon RDS 事件订阅是否为以下源类型和事件类别键值对启用了通知：

```
DBCluster: ["maintenance","failure"]
```

如果账户中没有现有活动订阅，则控件通过。

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 集群事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
源类型	集群
要包括的集群	所有集群

Field	Value
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则：`rds-instance-event-notifications-configured`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查数据库实例的现有 Amazon RDS 事件订阅是否为以下源类型和事件类别键值对启用了通知：

```
DBInstance: ["maintenance","configuration change","failure"]
```

如果账户中没有现有活动订阅，则控件通过。

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 实例事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
源类型	实例

Field	Value
要包括的实例	所有实例
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.21] 应为关键数据库参数组事件配置 RDS 事件通知订阅

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则：`rds-pg-event-notifications-configured`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查是否存在针对以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。如果账户中没有现有活动订阅，则控件通过。

```
DBParameterGroup: ["configuration change"]
```

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 数据库参数组事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
源类型	参数组
要包括的参数组	所有参数组

Field	Value
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.22] 应为关键数据库安全组事件配置 RDS 事件通知订阅

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2。

分类：检测 > 检测服务 > 应用程序监控

严重性：低

资源类型：`AWS::RDS::EventSubscription`

AWS Config 规则：`rds-sg-event-notifications-configured`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查是否存在针对以下源类型、事件类别键值对启用通知的 Amazon RDS 事件订阅。如果账户中没有现有活动订阅，则控件通过。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 事件通知使用 Amazon SNS 来通知 RDS 资源的可用性或配置的变化。这些通知允许快速响应。有关 RDS 事件通知的更多信息，请参阅 Amazon RDS 用户指南中的使用 Amazon RDS 事件通知。

修复

要订阅 RDS 实例事件通知，请参阅 Amazon RDS 用户指南中的订阅 Amazon RDS 事件通知。使用以下值：

Field	Value
源类型	安全组
要包括的安全组	所有安全组
要包括的事件类别	选择特定事件类别或所有事件类别

[RDS.23] RDS 实例不应使用数据库引擎的默认端口

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)。

类别：保护 > 安全网络配置

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-no-default-ports`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查 RDS 集群或实例是否使用数据库引擎默认端口以外的端口。如果 RDS 集群或实例使用默认端口，则控制失败。

如果您使用已知端口部署 RDS 集群或实例，攻击者可以猜测有关集群或实例的信息。攻击者可以将此信息与其他信息结合使用来连接到 RDS 集群或实例，或者获取有关应用程序的其他信息。

变更端口时，还必须更新用于连接到旧端口的现有连接字符串。您还应检查数据库实例的安全组，确保其包含允许在新端口上进行连接的入口规则。

修复

要修改现有 RDS 数据库实例的默认端口，请参阅 Amazon RDS 用户指南中的修改 Amazon RDS 数据库实例。要修改现有 RDS 数据库集群的默认端口，请参阅 Amazon Aurora 用户指南中的使用控制台、CLI 和 API 修改数据库集群。对于数据库端口，将端口值变更为非默认值。

[RDS.24] RDS 数据库集群应使用自定义管理员用户名

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：`rds-cluster-default-admin-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon RDS 数据库集群是否已将管理员用户名从其默认值变更为其他值。该控件不适用于 Neptune (Neptune 数据库) 或 docdb (DocumentDB) 类型的引擎。如果管理员用户名设置为默认值，则此规则将失败。

创建 Amazon RDS 数据库时，应将默认管理员用户名变更为唯一值。默认用户名是众所周知的，应在创建 RDS 数据库期间进行变更。变更默认用户名可以降低意外访问的风险。

修复

要变更与 Amazon RDS 数据库集群关联的管理员用户名，请在创建数据库时创建一个新的 RDS 数据库集群并变更默认管理员用户名。

[RDS.25] RDS 数据库实例应使用自定义管理员用户名

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：`rds-instance-default-admin-check`

计划类型：已触发变更

参数：无

此控件检查您是否变更了 Amazon Relational Database Service (Amazon RDS) 数据库实例的管理用户名，而不是默认值。该控件不适用于 Neptune (Neptune 数据库) 或 docdb (DocumentDB) 类型的引擎。如果将管理用户名设置为默认值，则控制失败。

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变更为唯一值，以降低意外访问的风险。

修复

要变更与 RDS 数据库实例关联的管理用户名，请先创建一个新的 RDS 数据库实例。在创建数据库时变更默认的管理用户名。

[RDS.26] RDS 数据库实例应受备份计划保护

类别：恢复 > 弹性 > 启用备份

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

严重性：中

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则：**`rds-resources-protected-by-backup-plan`**

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`backupVaultLockCheck`	如果参数设置为 true 且资源使用 AWS Backup 文件库锁定，则控件会生成PASSED查找结果。	布尔值	`true` 或者 `false`	无默认值	

此控件用于评估备份计划是否涵盖 Amazon RDS 数据库实例。如果备份计划未涵盖 RDS 数据库实例，则控制失败。如果将`backupVaultLockCheck`参数设置为`true`，则仅当实例备份到 AWS Backup 锁定的文件库中时，控制才会通过。

AWS Backup 是一项完全托管的备份服务，可集中和自动备份数据。 AWS 服务使用 AWS Backup，您可以创建名为备份计划的备份策略。您可以使用这些计划来定义备份要求，例如数据的备份频率以及这些备份的保留时间。将 RDS 数据库实例纳入备份计划可帮助您保护数据免遭意外丢失或删除。

修复

要将 RDS 数据库实例添加到 AWS Backup 备份计划，请参阅AWS Backup 开发人员指南中的为备份计划分配资源。

[RDS.27] 应对 RDS 数据库集群进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：**`rds-cluster-encrypted-at-rest`**

计划类型：已触发变更

参数：无

此控件检查 RDS 数据库集群是否进行静态加密。如果 RDS 数据库集群未进行静态加密，则控制失败。

静态数据指的是存储在持久、非易失性存储介质中的任何数据，无论存储时长如何。加密可帮助您保护此类数据的机密性，降低未经授权的用户访问这些数据的风险。加密 RDS 数据库集群可保护数据和元数据免遭未经授权的访问。它还满足了生产文件系统 data-at-rest 加密的合规性要求。

修复

您可以在创建 RDS 数据库集群时启用静态加密。创建集群后，您将无法变更加密设置。有关更多信息，请参阅 Amazon Aurora 用户指南中的加密 Amazon Aurora 数据库集群。

[RDS.28] 应标记 RDS 数据库集群

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则:`tagged-rds-dbcluster`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon RDS 数据库集群是否具有参数中定义的特定密钥的标签requiredTagKeys。如果数据库集群没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果数据库集群未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库集群添加标签，请参阅 Amazon RDS 用户指南中的为 Amazon RDS 资源添加标签。

[RDS.29] 应标记 RDS 数据库集群快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::RDS::DBClusterSnapshot

AWS Config 规则:`tagged-rds-dbclustersnapshot`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon RDS 数据库集群快照是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果数据库集群快照没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果数据库集群快照未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库集群快照添加标签，请参阅 Amazon RDS 用户指南中的为 Amazon RDS 资源添加标签。

[RDS.30] 应标记 RDS 数据库实例

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBInstance`

AWS Config 规则:`tagged-rds-dbinstance`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon RDS 数据库实例是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果数据库实例没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果数据库实例未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库实例添加标签，请参阅 Amazon RDS 用户指南中的为 Amazon RDS 资源添加标签。

[RDS.31] 应标记 RDS 数据库安全组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBSecurityGroup`

AWS Config 规则:`tagged-rds-dbsecuritygroup`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon RDS 数据库安全组是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果数据库安全组没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果数据库安全组未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库安全组添加标签，请参阅 Amazon RDS 用户指南中的为 Amazon RDS 资源添加标签。

[RDS.32] 应标记 RDS 数据库快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBSnapshot`

AWS Config 规则:`tagged-rds-dbsnapshot`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon RDS 数据库快照是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果数据库快照没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果数据库快照未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负

责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库快照添加标签，请参阅 Amazon RDS 用户指南中的为 Amazon RDS 资源添加标签。

[RDS.33] 应标记 RDS 数据库子网组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::RDS::DBSubnetGroup`

AWS Config 规则:`tagged-rds-dbsubnetgroups`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon RDS 数据库子网组是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果数据库子网组没有任何标签密钥或者没有参数中指定的所有密钥，则控制失

败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果数据库子网组未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 RDS 数据库子网组添加标签，请参阅 Amazon RDS 用户指南中的为 Amazon RDS 资源添加标签。

[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：AWS::RDS::DBCluster

AWS Config 规则：**rds-aurora-mysql-audit-logging-enabled**

计划类型：已触发变更

参数：无

此控件检查是否将 Amazon Aurora MySQL 数据库集群配置为向亚马逊日志发布审核 CloudWatch 日志。如果集群未配置为向日志发布审核日志，则控制失败。 CloudWatch 该控件不会为 Aurora Serverless v1 数据库集群生成调查结果。

审核日志记录捕获数据库活动的记录，包括登录尝试、数据修改、架构变更和其他可以出于安全性和合规性目的进行审计的事件。当您将 Aurora MySQL 数据库集群配置为向 Amazon CloudWatch 日志中的日志组发布审计日志时，您可以对日志数据进行实时分析。 CloudWatch 日志将日志保留在高度耐用的存储空间中。您还可以在中创建警报和查看指标 CloudWatch。

> **Note**
>
> 将审计日志发布到 CloudWatch 日志的另一种方法是启用高级审计，并将集群级别的数据库参数`server_audit_logs_upload`设置为。`1server_audit_logs_upload parameter` 的默认值为 `0`。但是，我们建议您改用以下补救说明来传递此控件。

修复

要将 Aurora MySQL 数据库集群审计日志发布到 CloudWatch 日志，请参阅亚马逊 Aurora 用户指南中的将 Amazon Aurora MySQL CloudWatch 日志发布到亚马逊日志。

[RDS.35] RDS 数据库集群应启用自动次要版本升级

相关要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::RDS::DBCluster`

AWS Config 规则：**`rds-cluster-auto-minor-version-upgrade-enable`**

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon RDS 多可用区数据库集群启用了自动次要版本升级。如果未为多可用区数据库集群启用自动次要版本升级，则控制失败。

RDS 提供自动次要版本升级，因此您可以使多可用区数据库集群保持最新状态。次要版本可以引入新的软件功能、错误修复、安全补丁和性能改进。通过在 RDS 数据库集群上启用自动次要版本升级，当有新版本可用时，集群以及集群中的实例将收到次要版本的自动更新。更新会在维护时段自动应用。

修复

要在多可用区数据库集群上启用自动次要版本升级，请参阅 A mazon RDS 用户指南中的修改多可用区数据库集群。

Amazon Redshift 控件

这些控件与 Amazon Redshift 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Redshift.1] Amazon Redshift 集群应禁止公共访问

相关要求：PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置 > 不公开访问的资源

严重性：严重

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-cluster-public-access-check`

计划类型：已触发变更

参数：无

此控件可检查 Amazon Redshift 集群是否公开访问。它会评估集群配置项目中的 `PubliclyAccessible` 字段。

Amazon Redshift 集群配置的 `PubliclyAccessible` 属性表示集群是否公开访问。当集群配置为 `PubliclyAccessible` 设置为 `true` 时，它是一个面向 Internet 的实例，具有可公开解析的 DNS 名称，可解析为公共 IP 地址。

当集群不可公开访问时，它是一个内部实例，其 DNS 名称可解析为私有 IP 地址。除非您希望集群可以公开访问，否则不应将集群配置为把 `PubliclyAccessible` 设置为 `true`。

修复

要更新 Amazon Redshift 集群以禁用公共访问，请参阅 Amazon Redshift 管理指南中的修改集群。将公开访问设置为否。

[Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)。

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::Redshift::ClusterAWS::Redshift::ClusterParameterGroup`

AWS Config 规则：`redshift-require-tls-ssl`

计划类型：已触发变更

参数：无

此控件检查是否需要连接到 Amazon Redshift 集群才能在传输中使用加密。如果 Amazon Redshift 集群参数 `require_SSL` 未设置为 `True`，则检查将失败。

TLS 可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击来窃听或操纵网络流量。只应允许通过 TLS 进行加密连接。加密传输中数据可能会影响性能。您应该使用此功能测试应用程序，以了解性能概况和 TLS 的影响。

修复

要将 Amazon Redshift 参数组更新为要求加密，请参阅 Amazon Redshift 管理指南中的修改参数组。将 `require_ssl` 设置为 True。

[Redshift.3] Amazon Redshift 集群应启用自动快照

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-13(5)。

类别：恢复 > 弹性 > 启用备份

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-backup-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值	
`MinRetentionPeriod`	最短快照保留期（以天为单位）	整数	7 到 35	7	

此控件检查 Amazon Redshift 集群是否启用了自动快照，以及保留期是否大于或等于指定的时间范围。如果没有为集群启用自动快照，或者保留期小于指定的时间范围，则控制失败。除非您为快照保留期提供自定义参数值，否则 Security Hub 将使用默认值即 7 天。

备份可以帮助您更快地从安全事件中恢复。它们增强了系统的弹性。默认情况下，Amazon Redshift 会定期拍摄快照。此控件检查是否已启用自动快照并将其保留至少七天。有关 Amazon Redshift 自动快照的更多详情，请参阅 Amazon Redshift 管理指南中的自动快照。

修复

要更新 Amazon Redshift 集群的快照保留期，请参阅 Amazon Redshift 管理指南中的修改集群。对于备份，将快照保留期设置为 7 或更大。

[Redshift.4] Amazon Redshift 集群应启用审核日志记录

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-cluster-audit-logging-enabled`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

- `loggingEnabled = true`（不可自定义）

此控件用于检查 Amazon Redshift 集群是否启用了审核日志。

Amazon Redshift 审核日志记录提供有关集群中的连接和用户活动的其他信息。这些数据可以存储在 Amazon S3 中并加以保护，有助于安全审计和调查。有关更多信息，请参阅 Amazon Redshift 管理指南中的数据库审核日志记录。

修复

要为 Amazon Redshift 集群配置审核日志记录，请参阅 Amazon Redshift 管理指南中的使用控制台配置审计。

[Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)。

类别：识别 > 漏洞、补丁和版本管理

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-cluster-maintenancesettings-check`

计划类型：已触发变更

参数：

- `allowVersionUpgrade = true`（不可自定义）

此控件检查是否为 Amazon Redshift 集群启用了自动主要版本升级。

启用自动主要版本升级可确保在维护时段内安装 Amazon Redshift 集群的最新主要版本更新。这些更新可能包括安全补丁和错误修复。及时安装补丁程序是保护系统安全的重要一步。

修复

要从中修复此问题 AWS CLI，请使用 Amazon `modify-cluster` Redshift 命令设置`--allow-version-upgrade`属性。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

其中，*`clustername`* 是 Amazon Redshift 集群名称的位置。

[Redshift.7] Redshift 集群应使用增强型 VPC 路由

相关要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > API 私有访问

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-enhanced-vpc-routing-enabled`

计划类型：已触发变更

参数：无

此控件会检查 Amazon Redshift 集群是否已启用 `EnhancedVpcRouting`。

增强型 VPC 路由强制集群和数据存储库之间的所有 `COPY` 和 `UNLOAD` 流量通过 VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能来保护网络流量。您还可以使用 VPC Flow 日志监控网络流量。

修复

有关详细的补救说明，请参阅 Amazon Redshift 管理指南中的启用增强型 VPC 路由。

[Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-default-admin-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon Redshift 集群是否已将管理员用户名从其默认值变更为其他值。如果 Redshift 集群的管理员用户名设置为 `awsuser`，则此控制失败。

创建 Redshift 集群时，应将默认管理员用户名变更为唯一值。默认用户名是众所周知的，应在配置时进行变更。变更默认用户名可以降低意外访问的风险。

修复

创建 Amazon Redshift 集群后，您无法更改其管理员用户名。要创建新集群，请按照此处的说明进行操作。

[Redshift.9] Redshift 集群不应使用默认的数据库名称

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：识别 > 资源配置

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-default-db-name-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon Redshift 集群是否已将数据库名称从其默认值变更为其他名称。如果 Redshift 集群的数据库名称设置为 dev，则控制失败。

创建 Redshift 集群时，应将默认数据库名称变更为唯一值。默认名称是众所周知的，应在配置时进行变更。例如，如果在 IAM policy 条件中使用众所周知的名称，则可能会导致意外访问。

修复

创建 Amazon Redshift 集群后，您无法更改其数据库名称。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。

[Redshift.10] Redshift 集群应在静态状态下进行加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-cluster-kms-enabled`

计划类型：已触发变更

参数：无

此控件会检查 Amazon Redshift 集群是否处于静态加密状态。如果 Redshift 集群未静态加密或者加密密钥与规则参数中提供的密钥不同，则则控制失败。

在 Amazon Redshift 中，您可以为集群开启数据库加密，以帮助保护静态数据。为集群开启加密时，会对集群及其快照的数据块和系统元数据进行加密。静态数据加密是推荐的最佳实践，因为它为数据添加了一层访问管理。对静态 Redshift 集群进行加密可降低未经授权的用户访问磁盘上存储的数据的风险。

修复

要将 Redshift 集群修改为使用 KMS 加密，请参阅 Amazon Redshift 管理指南中的变更集群加密。

[Redshift.11] 应该标记 Redshift 集群

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`tagged-redshift-cluster`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon Redshift 集群是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果集群没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果集群未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 集群添加标签，请参阅亚马逊 Redshift 管理指南中的在亚马逊 Redshift 中为资源添加标签。

[Redshift.12] 应标记 Redshift 事件通知订阅

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::EventSubscription`

AWS Config 规则：`tagged-redshift-eventsubscription`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon Redshift 集群快照是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果集群快照没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果集群快照未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 事件通知订阅添加标签，请参阅亚马逊 Redshift 管理指南中的在亚马逊 Redshift 中为资源添加标签。

[Redshift.13] 应标记 Redshift 集群快照

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::ClusterSnapshot`

AWS Config 规则：`tagged-redshift-clustersnapshot`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon Redshift 集群快照是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果集群快照没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果集群快照未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 集群快照添加标签，请参阅亚马逊 Redshift 管理指南中的在亚马逊 Redshift 中为资源添加标签。

[Redshift.14] 应标记 Redshift 集群子网组

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Redshift::ClusterSubnetGroup`

AWS Config 规则：`tagged-redshift-clustersubnetgroup`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon Redshift 集群子网组是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果集群子网组没有任何标签密钥或者没有参数中指定的所有密钥，则控制失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果集群子网组未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Redshift 集群子网组添加标签，请参阅亚马逊 Redshift 管理指南中的在 Amazon Redshift 中为资源添加标签。

[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口

类别：保护 > 安全网络配置 > 安全组配置

严重性：高

资源类型：`AWS::Redshift::Cluster`

AWS Config 规则：`redshift-unrestricted-port-access`

计划类型：定期

参数：无

此控件检查与 Amazon Redshift 集群关联的安全组是否具有允许从互联网访问集群端口的入口规则（0.0.0.0/0 或:: /0）。如果安全组入口规则允许从 Internet 访问集群端口，则控制失败。

允许对 Redshift 集群端口（带有 /0 后缀的 IP 地址）进行不受限制的入站访问可能会导致未经授权的访问或安全事件。我们建议在创建安全组和配置入站规则时应用最低权限访问原则。

修复

要将 Redshift 集群端口的入口限制为受限来源，请参阅 Amazon VPC 用户指南中的使用安全组规则。更新规则，其中端口范围与 Redshift 集群端口相匹配，IP 端口范围为 0.0.0.0/0。

Amazon Route 53 控制

这些控制与 Route 53 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Route53.1] 应标记 Route53 运行状况检查

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Route53::HealthCheck`

AWS Config 规则:`tagged-route53-healthcheck`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon Route 53 运行状况检查是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果运行状况检查没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥

是否存在，如果运行状况检查未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Route 53 运行状况检查添加标签，请参阅 Amazon Route 53 开发者指南中的命名和标记运行状况检查。

[Route53.2] Route 53 公有托管区域应记录 DNS 查询

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::Route53::HostedZone`

AWS Config 规则：`route53-query-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon Route 53 公共托管区域启用了 DNS 查询日志记录。如果未为 Route 53 公共托管区域启用 DNS 查询日志记录，控制将会失败。

记录 Route 53 托管区域的 DNS 查询可满足 DNS 安全性和合规性要求并授予可见性。日志包含诸如查询的域或子域、查询的日期和时间、DNS 记录类型（例如 A 或 AAAA）以及 DNS 响应代码（例如 `NoError` 或 `ServFail`）等信息。启用 DNS 查询日志记录后，Route 53 会将日志文件发布到 Amazon CloudWatch 日志。

修复

要记录 Route 53 公共托管区域的 DNS 查询，请参阅 Amazon Route 53 开发人员指南中的 DNS 查询配置日志记录。

Amazon Simple Storage Service 控制

这些控件与 Amazon S3 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[S3.1] S3 通用存储桶应启用阻止公共访问设置

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：CIS AWS 基金会基准 v3.0.0/2.1.4、CIS 基金会基准 v1.4.0/2.1.5、PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、nist.800-53.r5 AC-21、nist.800-53.r5、nist.800-53.5-53 3.r5 AC-3、nist.800-53.r5 AC-3 (7)、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-6、nist.800-53.r5 SC AWS -7、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (11) 800-53.r5 SC-7 (16)、nist.800-53.r5 SC-7 (20)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (3)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-7 (9))

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：s3-account-level-public-access-blocks-periodic

计划类型：定期

参数：

- ignorePublicAcls：true（不可自定义）
- blockPublicPolicy：true（不可自定义）
- blockPublicAcls：true（不可自定义）
- restrictPublicBuckets：true（不可自定义）

此控件检查前面的 Amazon S3 阻止公开访问设置是否是在账户级别为 S3 通用存储桶配置的。如果将一个或多个屏蔽公共访问设置设置设置为，则控制失败false。

如果将任何设置设置为 false，或者未配置任何设置，则控制失败。

Amazon S3 公有访问区块旨在提供对整个 S3 存储桶 AWS 账户 或单个 S3 存储桶级别的控制，以确保对象永远无法公开访问。通过访问控制列表 (ACL) 和/或存储桶策略向存储桶和对象授予公有访问权限。

除非您打算让 S3 存储桶可公开访问，否则您应该配置账户级别 Amazon S3 屏蔽公共访问权限功能。

要了解更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 屏蔽公共访问权限。

修复

要为您启用 Amazon S3 阻止公共访问 AWS 账户，请参阅《亚马逊简单存储服务用户指南》中的为您的账户配置阻止公开访问设置。

[S3.2] S3 通用存储桶应阻止公共读取权限

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5

AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-bucket-public-read-prohibited`

计划类型：定期计划和触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否允许公共读取权限。它会对阻止公有访问设置、存储桶策略和存储桶访问控制列表 (ACL) 进行评估。如果存储桶允许公共读取权限，则控制失败。

有些使用案例可能要求 Internet 上的每个人都能够从 S3 存储桶中读取数据。然而，这种情况很少见。为确保数据的完整性和安全性，您的 S3 存储桶不应可公开读取。

修复

要阻止对您的 Amazon S3 存储桶的公共读取权限，请参阅 Amazon 简单存储服务用户指南中的为 S3 存储桶配置阻止公开访问设置。

[S3.3] S3 通用存储桶应阻止公共写入权限

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5

SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置

严重性：严重

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-bucket-public-write-prohibited`

计划类型：定期计划和触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否允许公共写入权限。它会对阻止公有访问设置、存储桶策略和存储桶访问控制列表 (ACL) 进行评估。如果存储桶允许公共写入权限，则控制失败。

有些使用案例要求互联网上的每个人都能写入您的 S3 存储桶。然而，这种情况很少见。为确保数据的完整性和安全性，您的 S3 存储桶不应可公开写入。

修复

要阻止对您的 Amazon S3 存储桶的公共写入权限，请参阅 Amazon 简单存储服务用户指南中的为 S3 存储桶配置阻止公开访问设置。

[S3.5] S3 通用存储桶应要求请求使用 SSL

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：独联体 AWS 基金会基准 v3.0.0/2.1.1、CIS 基金会基准 v1.4.0/2.1.2、PCI DSS v3.2.1/4.1、nist.800-53.r5 AC-17 (2)、nist.800-53.r5 AC-4、nist.800-53.r5 IA-5 (1)、nist.800-53.r5 SC-12 (3)、nist.800-53.r5 (3)、nist.800-53.r5 (3)、nist.800-800-800-800-53.r5 SC-13、nist.800-53.r5 SC-23、nist.800-53.r5 SC-23 (3)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-8、nist.800-53.r5 SC-8 (1)、nist.800-53.r5 SC-8 (2)、nist.800-53.r5 SC-8 (2)、nist.800-53.r5 (2) 800-53.r5 SI-7 (6) AWS

类别：保护 > 安全访问管理

严重性：中

资源类型：AWS::S3::Bucket

AWS Config 规则：s3-bucket-ssl-requests-only

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否有要求请求使用 SSL 的策略。如果存储桶策略不要求请求使用 SSL，则控制失败。

S3 存储桶的策略应要求所有请求 (Action: S3:*) 在 S3 资源策略中仅接受通过 HTTPS 传输的数据，由条件密钥 aws:SecureTransport 表示。

修复

要更新 Amazon S3 存储桶策略以拒绝不安全的传输，请参阅亚马逊简单存储服务用户指南中的使用 Amazon S3 控制台添加存储桶策略。

添加与以下策略中的策略语句相似的策略语句。将 DOC-EXAMPLE-BUCKET 替换为您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:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
```

```
    ]
}
```

有关更多信息，请参阅我应该使用哪个 S3 存储桶策略来遵守 AWS Config 规则 s3-bucket-ssl-requests-only？ 在AWS 官方知识中心。

[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全访问管理 > 敏感的 API 操作操作受限

严重性：高

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-bucket-blacklisted-actions-prohibited`

计划类型：已触发变更

参数：

- `blacklistedactionpatterns`：`s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl`（不可自定义）

此控件检查 Amazon S3 通用存储桶策略是否 AWS 账户 阻止其他人的委托人对 S3 存储桶中的资源执行被拒绝的操作。如果存储桶策略允许另一位委托人执行上述一项或多项操作，则控制失败 AWS 账户。

实施最低权限访问对于降低安全风险以及错误或恶意意图的影响至关重要。如果 S3 存储桶策略允许从外部账户进行访问，则可能会导致内部威胁或攻击者泄露数据。

`blacklistedactionpatterns` 参数允许成功评估 S3 存储桶的规则。该参数授予对未包含在 `blacklistedactionpatterns` 列表中的操作模式的外部账户访问权限。

修复

要更新 Amazon S3 存储桶策略以删除权限，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 控制台添加存储桶策略。

在编辑存储桶策略页面的策略编辑文本框中，执行以下操作之一：

- 删除授予其他 AWS 账户 访问被拒绝操作的权限的语句。
- 从语句中删除允许的拒绝操作。

[S3.7] S3 通用存储桶应使用跨区域复制

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：PCI DSS v3.2.1/2.2、NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-36(2)、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：保护 > 安全访问管理

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：**`s3-bucket-cross-region-replication-enabled`**

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否启用了跨区域复制。如果存储桶未启用跨区域复制，则控制失败。

复制是指在相同或不同的 AWS 区域存储桶之间自动异步复制对象。复制操作会将源存储桶中新创建的对象和对象更新复制到目标存储桶。 AWS 最佳实践建议对由同一 AWS 账户拥有的源存储桶和目标存储桶进行复制。除了可用性以外，您还应该考虑其他系统强化设置。

修复

要在 S3 存储桶上启用跨区域复制，请参阅 Amazon Simple Storage Service 用户指南中的为同一账户拥有的源存储桶和目标存储桶配置复制。对于源存储桶，选择应用到存储桶中的所有对象。

[S3.8] S3 通用存储桶应阻止公共访问

相关要求：独联体 AWS 基金会基准 v3.0.0/2.1.4、CIS 基金会基准 v1.4.0/2.1.5、nist.800-53.r5 AC-21、nist.800-53.r5 AC-3、nist.800-53.r5 AC-3 (7)、nist.800-53.r5 AC-4、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-4 (21)、nist.800-53.r5 AC-4 (21) 53.r5 AC-6、nist.800-53.r5 SC AWS -7、nist.800-53.r5 SC-7 (11)、nist.800-53.r5 SC-7 (16)、nist.800-53.r5 SC-7 (20)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (21)、nist.800-53.r5 SC-7 (21) -7 (3)、nist.800-53.r5 SC-7 (4)、nist.800-53.r5 SC-7 (9)

类别：保护 > 安全访问管理 > 访问控制

严重性：高

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-bucket-level-public-access-prohibited`

计划类型：已触发变更

参数：

- `excludedPublicBuckets`（不可自定义）- 已知允许的公共 S3 存储桶名称的逗号分隔列表

此控件检查 Amazon S3 通用存储桶是否在存储桶级别阻止公开访问。如果将以下任一设置设置为，则控件将失败`false`：

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

S3 存储桶级别的阻止公共访问提供了控制，以确保对象永远不会具有公共访问权限。通过访问控制列表 (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 S3 存储桶，否则您应该配置存储桶级别 Amazon S3 屏蔽公共访问权限功能。

修复

有关如何在存储桶级别删除公开访问权限的信息，请参阅 Amazon S3 用户指南中的阻止公众访问 Amazon S3 存储。

[S3.9] S3 通用存储桶应启用服务器访问日志记录

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-bucket-logging-enabled`

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon S3 通用存储桶启用了服务器访问日志功能。如果未启用服务器访问日志记录，则控件将失败。启用日志记录后，Amazon S3 将源存储桶的访问日志传送到选定的目标存储桶。目标存储桶必须与源存储桶位于同一 AWS 区域 存储桶中，并且不得配置默认保留期。目标日志存储桶不需要启用服务器访问日志记录，您应该隐藏该存储桶的调查发现。

服务器访问日志记录提供对存储桶发出的请求的详细记录。服务器访问日志可以帮助进行安全和访问审核。有关更多信息，请参阅 Amazon S3 的安全最佳实践：启用 Amazon S3 服务器访问日志记录。

修复

要启用 Amazon S3 服务器访问日志，请参阅 Amazon S3 用户指南中的启用 Amazon S3 服务器访问日志。

[S3.10] 启用版本控制的 S3 通用存储桶应具有生命周期配置

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。Security Hub于2024年4月从 AWS 基础安全最佳实践标准中取消了该控件，但它仍包含在NIST SP 800-53 Rev. 53标准中。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-version-lifecycle-policy-check`

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用版本存储桶是否具有生命周期配置。如果存储桶没有生命周期配置，则控制失败。

我们建议您为 S3 存储桶创建生命周期配置，以帮助您定义希望 Amazon S3 在对象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，请参阅在存储桶上设置生命周期配置和管理存储生命周期。

[S3.11] S3 通用存储桶应启用事件通知

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。Security Hub 于 2024 年 4 月从 AWS 基础安全最佳实践标准中取消了该控件，但它仍包含在 NIST SP 800-53 Rev. 5 标准中：。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(4)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-event-notifications-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`eventTypes`	首选 S3 事件类型列表	EnumList（最多 28 个项目）	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:LifecycleTransition`, `s3:ObjectAcl:Put`, `s3:Object`	无默认值

参数	描述	类型	允许的自定义值	Security Hub 默认值
			Created:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed,	

参数	描述	类型	允许的自定义值	Security Hub 默认值
			s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:Ope	

参数	描述	类型	允许的自定义值	Security Hub 默认值
			`rationNotTracked`, `s3:ReplicationOperationReplicatedAfterThreshold`, `s3:TestEvent`	

此控件检查是否在 Amazon S3 通用存储桶上启用 S3 事件通知。如果存储桶上未启用 S3 事件通知，则控制失败。如果您为`eventTypes`参数提供自定义值，则只有在为指定类型的事件启用事件通知时，控件才会通过。

启用 S3 事件通知后，当发生影响您的 S3 存储桶的特定事件时，您会收到警报。例如，您可以收到有关对象创建、对象移除和对象恢复的通知。这些通知可以提醒相关团队注意可能导致未经授权的数据访问的意外或故意修改。

修复

有关检测 S3 存储桶和对象变更的信息，请参阅 Amazon S3 用户指南中的 Amazon S3 事件通知。

[S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6。

类别：保护 > 安全访问管理 > 访问控制

严重性：中

资源类型：AWS::S3::Bucket

AWS Config 规则：s3-bucket-acl-prohibited

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否为用户提供访问控制列表 (ACL) 权限。如果配置了 ACL 来管理用户对存储桶的访问权限，则控制失败。

ACL 是早于 IAM 的传统访问控制机制。我们建议不要使用 ACL，而是使用 S3 存储桶策略或 AWS Identity and Access Management (IAM) 策略来管理对 S3 存储桶的访问权限。

修复

要通过此控制，您应该为 S3 存储桶禁用 ACL。有关说明，请参阅 Amazon Simple Storage Service 用户指南中的控制对象所有权和禁用存储桶的 ACL。

要创建 S3 存储桶策略，请参阅使用 Amazon S3 控制台添加存储桶策略。要在 S3 存储桶上创建 IAM 用户策略，请参阅使用用户策略控制对存储桶的访问权限。

[S3.13] S3 通用存储桶应具有生命周期配置

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)。

类别：保护 > 数据保护

严重性：低

资源类型：AWS::S3::Bucket

AWS Config 规则：s3-lifecycle-policy-check

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`targetTransitionDays`	对象创建后转换到指定存储类的天数。	整数	1 到 36500	无默认值
`targetExpirationDays`	对象创建后到被删除为止的天数。	整数	1 到 36500	无默认值
`targetTransitionStorageClass`	目标 S3 存储类类型	枚举	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	无默认值

此控件检查 Amazon S3 通用存储桶是否具有生命周期配置。如果存储桶没有生命周期配置，则控制失败。如果您为前面的一个或多个参数提供自定义值，则仅当策略包含指定的存储类、删除时间或转换时间时，控制才会通过。

为您的 S3 存储桶创建生命周期配置定义了您希望 Amazon S3 在对象生命周期内执行的操作。例如，您可以创建一个生命定期策略，该策略将对象转换为另一个存储类别，存档对象，或在指定时间段后将其删除。

修复

有关在 Amazon S3 存储桶上配置生命周期策略的信息，请参阅在存储桶上设置生命周期配置，并参阅 Amazon S3 用户指南中的管理存储生命周期。

[S3.14] S3 通用存储桶应启用版本控制

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

类别：保护 > 数据保护 > 数据删除保护

相关要求：NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)。

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：`s3-bucket-versioning-enabled`

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否启用了版本控制。如果存储桶的版本控制已暂停，则控制将失败。

版本控制将对象的多个变体保留在同一个 S3 存储桶中。您可以使用版本控制来保留、检索和恢复 S3 存储桶中存储的对象的早期版本。版本控制可帮助您从意外的用户操作和应用程序故障中恢复。

> **Tip**
>
> 随着版本控制导致存储桶中对象数量的增加，您可以设置生命周期配置，以根据规则自动存档或删除受版本控制的对象。有关更多信息，请参阅受版本控制的对象的 Amazon S3 生命周期管理。

修复

要在 S3 存储桶上使用版本控制，请参阅 Amazon S3 用户指南中的在存储桶上启用版本控制。

[S3.15] S3 通用存储桶应启用对象锁定

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

类别：保护 > 数据保护 > 数据删除保护

相关要求：NIST.800-53.r5 CP-6(2)。

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：**`s3-bucket-default-lock-enabled`**

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`mode`	S3 对象锁定保留模式	枚举	`GOVERNANCE`，`COMPLIANCE`	无默认值

此控件检查 Amazon S3 通用存储桶是否启用了对象锁定。如果未为存储桶启用对象锁定，则控制失败。如果您为 `mode` 参数提供自定义值，则仅当 S3 对象锁定使用指定的保留模式时，控制才会通过。

您可以使用 S3 对象锁定通过 write-once-read-many (WORM) 模型存储对象。对象锁定可以帮助防止 S3 存储桶中的对象在固定时间内或无限期地被删除或覆盖。您可以使用 S3 对象锁定满足需要 WORM 存储的法规要求，或添加一个额外的保护层来防止对象被更改和删除。

修复

要为新的和现有 S3 存储桶配置对象锁定，请参阅《Amazon S3 用户指南》中的配置 S3 对象锁定。

[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys

> **Important**
>
> 2024 年 3 月 12 日，此控件的标题更改为显示的标题。有关更多信息，请参阅 Security Hub 控件的更改日志。

类别：保护 > 数据保护 > 加密 data-at-rest

相关要求：NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 SI-7(6)、NIST.800-53.r5 AU-9。

严重性：中

资源类型：`AWS::S3::Bucket`

AWS Config 规则：**`s3-default-encryption-kms`**

计划类型：已触发变更

参数：无

此控件检查 Amazon S3 通用存储桶是否使用 AWS KMS key （SSE-KMS 或 DSSE-KMS）进行加密。如果存储桶使用默认加密 (SSE-S3) 进行加密，则控制失败。

服务器端加密（SSE）是接收数据的应用程序或服务在数据目的地对其进行加密。密是指由接收数据的应用程序或服务在目标位置对数据进行加密。除非您另行指定，否则 S3 存储桶默认使用 Amazon S3 托管密钥 (SSE-S3) 进行服务器端加密。但是，为了增加控制力，您可以选择将存储桶配置为改用服务器端加密 AWS KMS keys （SSE-KMS 或 DSSE-KMS）。当您的数据写入数据中心的磁盘时，Amazon S3 会在对象级别对其进行加密，并在您访问 AWS 数据时为您解密。

修复

要使用 SSE-KMS 加密 S3 存储桶，请参阅 Amazon S3 用户指南中的使用 AWS KMS (SSE-KMS) 指定服务器端加密。要使用 DSSE-KMS 加密 S3 存储桶，请参阅 Amazon S3 用户指南中的使用 AWS KMS keys (DSSE-KMS) 指定双层服务器端加密。

[S3.19] S3 接入点已启用屏蔽公共访问权限设置

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全访问管理 > 资源不公开访问

严重性：严重

资源类型：`AWS::S3::AccessPoint`

AWS Config 规则：**`s3-access-point-public-access-blocks`**

计划类型：已触发变更

参数：无

该控件检查 Amazon S3 接入点是否启用了屏蔽公共访问权限设置。如果没有为接入点启用屏蔽公共访问权限设置，则控制失败。

Amazon S3 屏蔽公共访问权限功能可帮助您在 3 个级别上管理对 S3 资源的访问权限：账户、存储桶和接入点级别。可以独立配置每个级别的设置，从而允许您对数据设置不同级别的公共访问权限限制。接入点设置不能单独覆盖更高级别的、限制性更高的设置（账户级别或分配给接入点的存储桶）。相反，接入点级别的设置是附加的，这意味着它们作为其他级别的设置的补充，并与之配合使用。除非您打算让 S3 接入点可供公共访问，否则应启用屏蔽公共访问权限设置。

修复

Amazon S3 当前不支持在创建接入点之后更改接入点的屏蔽公共访问权限设置。默认情况下，在创建新的接入点时，将启用所有屏蔽公共访问权限设置。除非您有特定的需求要禁用任何一个设置，建议您将所有设置保持为启用状态。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的管理接入点的公共访问权限。

[S3.20] S3 通用存储桶应启用 MFA 删除

相关要求：独联体 AWS 基金会基准 v3.0.0/2.1.2、CIS 基金会基准 v1.4.0/2.1.3、nist.800-53.r5 C AWS A-9 (1)、nist.800-53.r5 CM-2、nist.800-53.r5 CM-2 (2)、nist.800-53.r5 CM-3、nist.800-53.r5 SC-5 (2)

类别：保护 > 数据保护 > 数据删除保护

严重性：低

资源类型：`AWS::S3::Bucket`

AWS Config 规则：**`s3-bucket-mfa-delete-enabled`**

计划类型：已触发变更

参数：无

此控件检查是否在 Amazon S3 通用版本存储桶上启用了多重身份验证 (MFA) 删除。如果存储桶上未启用 MFA 删除，则控制失败。该控件不会为具有生命周期配置的存储桶生成调查结果。

在 Amazon S3 存储桶中使用 S3 版本控制时，您可以选择通过将存储桶配置为启用 MFA 删除来添加另一层安全保护。执行此操作时，存储桶拥有者必须在任何请求中包含两种形式的身份验证，以删除版本或更改存储桶的版本控制状态。如果安全凭证被泄露，则 MFA 删除可提供更高的安全性。MFA 删除要求启动删除操作的用户证明其实际拥有具有 MFA 代码的 MFA 设备，并为删除操作增加额外的摩擦和安全性，这样也有助于防止存储桶被意外删除。

> **Note**
>
> MFA 删除功能需要将存储桶版本控制作为依赖项。存储桶版本控制是在相同的存储桶中保留 S3 对象的多个变体的方法。此外，只有以根用户身份登录的存储桶拥有者才能启用 MFA 删除并对 S3 存储桶执行删除操作。

修复

要启用 S3 版本控制并在存储桶上配置 MFA 删除，请参阅《Amazon Simple Storage Service 用户指南》中的配置 MFA 删除。

[S3.22] S3 通用存储桶应记录对象级写入事件

相关要求：独联体 AWS 基金会基准 v3.0.0/3.8

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：**`cloudtrail-all-write-s3-data-event-check`**

计划类型：定期

参数：无

此控件检查是否至少 AWS 账户 有一个 AWS CloudTrail 多区域跟踪，用于记录 Amazon S3 存储桶的所有写入数据事件。如果该账户没有用于记录 S3 存储桶写入数据事件的多区域跟踪，则控制失败。

S3 对象级操作（例如`GetObject`、`DeleteObject`和`PutObject`）称为数据事件。默认情况下，CloudTrail 不记录数据事件，但您可以配置跟踪以记录 S3 存储桶的数据事件。当您为写入数据事件启用对象级日志记录时，您可以在 S3 存储桶中记录每个单独的对象（文件）访问权限。启用对象级日志记录可以帮助您满足数据合规性要求，执行全面的安全分析，监控您的特定用户行为模式 AWS 账户，并使用 Amazon Events 对 S3 存储桶中的对象级 API 活动采取措施。 CloudWatch 如果您配置了记录所有 S3 存储桶的只写或所有类型的数据事件的多区域跟踪，则此控件会生成`PASSED`结果。

修复

要为 S3 存储桶启用对象级日志记录，请参阅《Amaz on 简单存储服务用户指南》中的 “为 S3 存储桶和对象启用 CloudTrail 事件记录”。

[S3.23] S3 通用存储桶应记录对象级读取事件

相关要求：独联体 AWS 基金会基准 v3.0.0/3.9

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::::Account`

AWS Config 规则：**`cloudtrail-all-read-s3-data-event-check`**

计划类型：定期

参数：无

此控件检查是否至少 AWS 账户 有一个 AWS CloudTrail 多区域跟踪，用于记录 Amazon S3 存储桶的所有读取数据事件。如果该账户没有用于记录 S3 存储桶读取数据事件的多区域跟踪，则控制失败。

S3 对象级操作（例如GetObjectDeleteObjectPutObject、和）称为数据事件。默认情况下，CloudTrail 不记录数据事件，但您可以配置跟踪以记录 S3 存储桶的数据事件。当您为读取数据事件启用对象级日志记录时，您可以记录 S3 存储桶中每个单独的对象（文件）访问权限。启用对象级日志记录可以帮助您满足数据合规性要求，执行全面的安全分析，监控您的特定用户行为模式 AWS 账户，并使用 Amazon Events 对 S3 存储桶中的对象级 API 活动采取措施。 CloudWatch 如果您配置的多区域跟踪记录所有 S3 存储桶的只读或所有类型的数据事件，则此控件会生成PASSED结果。

修复

要为 S3 存储桶启用对象级日志记录，请参阅《Amaz on 简单存储服务用户指南》中的 “为 S3 存储桶和对象启用 CloudTrail 事件记录”。

亚马逊 SageMaker 控制

这些控制措施与 SageMaker 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网

相关要求：PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

类别：保护 > 安全网络配置

严重性：高

资源类型：AWS::SageMaker::NotebookInstance

AWS Config 规则：sagemaker-notebook-no-direct-internet-access

计划类型：定期

参数：无

此控件检查 SageMaker 笔记本实例是否禁用了直接互联网接入。如果为笔记本实例启用了该DirectInternetAccess字段，则控件将失败。

如果您在不使用 VPC 的情况下配置 SageMaker 实例，则默认情况下，您的实例将启用直接互联网访问。您应该使用 VPC 配置实例，并将默认设置变更为禁用——通过 VPC 访问 Internet。要使用笔记本电脑训练或托管模型，您需要访问 Internet。要启用互联网访问，您的 VPC 必须具有接口终端节点 (AWS PrivateLink) 或 NAT 网关，以及允许出站连接的安全组。要详细了解如何将笔记本实例连接到 VPC 中的资源，请参阅 Amazon SageMaker 开发者指南中的将笔记本实例连接到 VPC 中的资源。您还应确保只有经过授权的用户才能访问您的 SageMaker 配置。限制允许用户更改 SageMaker 设置和资源的 IAM 权限。

修复

在创建笔记本实例后，您无法变更 Internet 访问设置。相反，您可以停止、删除和重新创建 Internet 访问受阻的实例。要删除允许直接访问互联网的笔记本实例，请参阅 Amazon SageMaker 开发者指南中的使用笔记本实例构建模型：清理。要重新创建拒绝 Internet 访问的笔记本实例，请参阅创建笔记本实例。对于网络，直接访问Internet，选择禁用-通过 VPC 访问 Internet。

[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

相关要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)。

类别：保护 > 安全网络配置 > VPC 内的资源

严重性：高

资源类型：`AWS::SageMaker::NotebookInstance`

AWS Config 规则：`sagemaker-notebook-instance-inside-vpc`

计划类型：已触发变更

参数：无

此控件检查是否在自定义虚拟私有云 (VPC) 中启动了 Amazon SageMaker 笔记本实例。如果 SageMaker 笔记本实例未在自定义 VPC 内启动或在 SageMaker 服务 VPC 中启动，则此控制失败。

子网是 VPC 内的一系列 IP 地址。我们建议尽可能将资源保留在自定义 VPC 内，以确保为您的基础设施提供安全的网络保护。Amazon VPC 是专用于您的虚拟网络 AWS 账户。使用 Amazon VPC，您可以控制 SageMaker Studio 和笔记本实例的网络访问和互联网连接。

修复

在创建笔记本实例后，您无法变更 VPC 设置。相反，您可以停止、删除和重新创建实例。有关说明，请参阅 Amazon SageMaker 开发者指南中的使用笔记本实例构建模型：清理。

[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

类别：保护 > 安全访问管理 >根用户访问限制

严重性：高

资源类型：`AWS::SageMaker::NotebookInstance`

AWS Config 规则：`sagemaker-notebook-instance-root-access-check`

计划类型：已触发变更

参数：无

此控件检查是否为 Amazon SageMaker 笔记本实例开启了根访问权限。如果为 SageMaker 笔记本实例开启了根访问权限，则控制失败。

根据最低权限原则，建议的安全最佳实践是限制根用户对实例资源的访问权限，以避免无意中过度预置权限。

修复

要限制对 SageMaker 笔记本实例的根访问权限，请参阅 Amazon SageMaker 开发者指南中的控制 SageMaker 笔记本实例的根访问权限。

[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

相关要求：nist.800-53.r5 CP-10、nist.800-53.r5 SC-5、nist.800-53.r5 SC-36、nist.800-53.r5、nist.800-53.r5 SA-13

类别：恢复 > 弹性 > 高可用性

严重性：中

资源类型：`AWS::SageMaker::EndpointConfig`

AWS Config 规则：`sagemaker-endpoint-config-prod-instance-count`

计划类型：定期

参数：无

此控件会检查 Amazon SageMaker 终端节点的生产变体的初始实例数是否大于 1。如果端点的生产变体只有 1 个初始实例，则控制失败。

在实例数大于 1 的情况下运行的生产变体允许由SageMaker管理的多可用区实例冗余。跨多个可用区部署资源是在您的架构中提供高可用性 AWS 的最佳实践。高可用性可帮助您从安全事件中恢复。

> **Note**
>
> 此控件仅适用于基于实例的端点配置。

修复

有关终端节点配置参数的更多信息，请参阅 Amazon SageMaker 开发者指南中的创建终端节点配置。

AWS Secrets Manager 控件

这些控件与 Secrets Manager 资源相关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SecretsManager.1] Secrets Manager 密钥应启用自动轮换

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)。

类别：保护 > 安全开发

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-rotation-enabled-check`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`maximumAllowedRotationFrequency`	密钥轮换频率的最大允许天数（以天为单位）。	整数	1 到 365	无默认值

此控件检查存储在中的密钥 AWS Secrets Manager 是否配置了自动轮换。如果密钥未配置自动轮换，则控制失败。如果您为 `maximumAllowedRotationFrequency` 参数提供自定义值，则仅当密钥在指定的时间窗口内自动轮换时，控制才会通过。

Screts Manager 可帮助您改善组织的安全状况。密钥包括数据库凭证、密码和第三方 API 密钥。您可以使用 Secrets Manager 集中存储机密、自动加密机密、控制对机密的访问以及安全自动轮换机密。

Secrets Manager 可以轮换密钥。您可以使用轮换将长期密钥替换为短期机密。轮换密钥会限制未经授权的用户使用泄露密钥的时间。因此，您应该经常轮换机密。要了解有关轮换的更多信息，请参阅AWS Secrets Manager 用户指南中的轮换 AWS Secrets Manager 密钥。

修复

要启用 Secrets Manager 密钥的自动轮换，请参阅《AWS Secrets Manager 用户指南》中的使用控制台为 AWS Secrets Manager 密钥设置自动轮换。必须选择和配置轮换 AWS Lambda 函数。

[SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)。

类别：保护 > 安全开发

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-scheduled-rotation-success-check`

计划类型：已触发变更

参数：无

此控件根据轮换计划检查 AWS Secrets Manager 密钥是否成功轮换。如果 `RotationOccurringAsScheduled` 是 `false`，则控制失败。该控件只评估已开启轮换。

Screts Manager 可帮助您改善组织的安全状况。密钥包括数据库凭证、密码和第三方 API 密钥。您可以使用 Secrets Manager 集中存储机密、自动加密机密、控制对机密的访问以及安全自动轮换机密。

Secrets Manager 可以轮换密钥。您可以使用轮换将长期密钥替换为短期机密。轮换密钥会限制未经授权的用户使用泄露密钥的时间。因此，您应该经常轮换机密。

除了将机密配置为自动轮换之外，您还应确保这些机密根据轮换计划成功轮换。

要了解有关轮换的更多信息，请参阅 AWS Secrets Manager 用户指南中的轮换 AWS Secrets Manager 密钥。

修复

如果自动轮换失败，那么 Secrets Manager 可能遇到了配置错误。要在 Secrets Manager 中轮换密钥，您可以使用 Lambda 函数来定义如何与拥有该密钥的数据库或服务进行交互。

有关诊断和修复与密钥轮换相关的常见错误的帮助，请参阅AWS Secrets Manager 用户指南中的密钥 AWS Secrets Manager 轮换疑难解答。

[SecretsManager.3] 移除未使用的 Secrets Manager 密钥

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-secret-unused`

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`unusedForDays`	密钥可以保持未使用状态的最大天数	整数	1 到 365	90

此控件检查 AWS Secrets Manager 密钥是否在指定的时间范围内被访问。如果密钥在指定的时间范围之外未使用，则控制失败。除非您为访问期提供自定义参数值，否则 Security Hub 将使用默认值即 90 天。

删除未使用的机密与轮换机密一样重要。未使用的机密可能会被以前的用户滥用，他们不再需要访问这些机密。此外，随着越来越多的用户访问秘密，有人可能会处理不当并将其泄露给未经授权的实体，这增加了滥用的风险。删除未使用的密钥有助于撤销不再需要的用户的密钥访问权限。它还有助于降低 Secrets Manager 的使用 Secrets Manager 的成本。因此，必须定期删除未使用的密钥。

修复

要删除不活跃的 Sec rets Manager AWS Secrets Manager 密钥，请参阅AWS Secrets Manager 用户指南中的删除密钥。

[SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换

相关要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)。

类别：保护 > 安全访问管理

严重性：中

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`secretsmanager-secret-periodic-rotation`

计划类型：定期

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`maxDaysSinceRotation`	密钥可以保持不变的最大天数	整数	1 到 180	90

此控件检查 AWS Secrets Manager 密钥是否在指定的时间范围内至少轮换一次。如果密钥未达到该轮换频率，则控制失败。除非您为轮换期提供自定义参数值，否则 Security Hub 将使用默认值即 90 天。

轮换密钥可以帮助您降低未经授权在 AWS 账户中使用密钥的风险。示例包括数据库凭证、密码、第三方 API 密钥，甚至任意文本。如果您长时间不更改密钥，则密钥更有可能被泄露。

随着越来越多的用户访问密钥，有人处理不当并将其泄露给未经授权的实体的可能性就变得更大。密钥可能会通过日志和缓存数据泄露出去。密钥可能会共享用于调试目的，但在调试完成后未更改或撤销。出于所有这些原因，密钥应该频繁地轮换。

您可以在 AWS Secrets Manager中为密钥配置自动轮换。通过自动轮换，您可以用短期密钥替换长期密钥，从而显着降低泄露风险。我们建议您为 Secrets Manager 密钥配置自动轮换。有关更多信息，请参阅 AWS Secrets Manager 用户指南中的轮换 AWS Secrets Manager 密钥。

修复

要启用 Secrets Manager 密钥的自动轮换，请参阅《AWS Secrets Manager 用户指南》中的使用控制台为 AWS Secrets Manager 密钥设置自动轮换。必须选择和配置轮换 AWS Lambda 函数。

[SecretsManager.5] 应标记 Secrets Manager 机密

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SecretsManager::Secret`

AWS Config 规则：`tagged-secretsmanager-secret`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Secrets Manager 密钥是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果密钥没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果该密钥未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Secrets Manager 密钥添加标签，请参阅AWS Secrets Manager 用户指南中的标签 AWS Secrets Manager 密钥。

AWS Service Catalog 控件

这些控件与 Service Catalog 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享

相关要求：nist.800-53.r5 AC-3、nist.800-53.r5 AC-4、nist.800-53.r5 AC-6、nist.800-53.r5 CM-8、nist.800-53.r5 CM-8、nist.800-53.r5 SC-7

类别：保护 > 安全访问管理

严重性：高

资源类型：`AWS::ServiceCatalog::Portfolio`

AWS Config 规则：`servicecatalog-shared-within-organization`

计划类型：已触发变更

参数：无

此控件会检查启用与 AWS Organizations 集成后，组织内是否 AWS Service Catalog 共享投资组合。如果组织内部不共享产品组合，则控制失败。

仅在 Organizations 内部共享作品集有助于确保共享的作品集不会与不正确的人共享 AWS 账户。要与组织中的账户共享服务目录组合，Security Hub 建议使用`ORGANIZATION_MEMBER_ACCOUNT`代替`ACCOUNT`。这通过管理整个组织内授予账户的访问权限来简化管理。如果您有业务需要与外部账户共享 Service Catalog 产品组合，则可以自动隐藏或禁用此控件的结果。

修复

要启用与 Organizations 共享产品组合，请参阅《S ervice Catalog 管理员指南》 AWS Organizations中的 “共享给”

Amazon 简单电子邮件服务控件

这些控制与 Amazon SES 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SES.1] 应标记 SES 联系人列表

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SES::ContactList`

AWS Config规则：`tagged-ses-contactlist`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon SES 联系人列表中是否包含参数中定义的特定密钥的标签`requiredTagKeys`。如果联系人列表没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果联系人列表未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向亚马逊 SES 联系人列表添加标签，请参阅TagResource《亚马逊 SES API v2 参考》。

[SES.2] 应标记 SES 配置集

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SES::ConfigurationSet`

AWS Config规则：`tagged-ses-configurationset`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 Amazon SES 配置集是否具有参数中定义的特定密钥的标签`requiredTagKeys`。如果配置集没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果配置集未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Amazon SES 配置集添加标签，请参阅TagResource《亚马逊 SES API v2 参考》。

Amazon Simple Notification Service 控件

这些控件与 Amazon SNS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS

> **Important**
>
> Security Hub于2024年4月从 AWS 基础安全最佳实践标准中取消了该控件，但它仍包含在 NIST SP 800-53 Rev. 53标准中。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::SNS::Topic`

AWS Config 规则：`sns-encrypted-kms`

计划类型：已触发变更

参数：无

此控件检查是否使用在 AWS Key Management Service ()AWS KMS中管理的密钥对 Amazon SNS 主题进行静态加密。如果 SNS 主题不使用 KMS 密钥进行服务器端加密 (SSE)，则控制失败。默认情况下，SNS 使用磁盘加密存储消息和文件。要通过此控制，必须选择改用 KMS 密钥进行加密。这增加了额外的安全层，并提供了更大的访问控制灵活性。

对静态数据进行加密可降低存储在磁盘上的数据被未经身份验证的用户访问的风险。 AWS需要有 API 权限才能解密数据，然后才能读取数据。为了增加安全性，我们建议使用 KMS 密钥加密 SNS 主题。

修复

要为 SNS 主题启用 SSE，请参阅《亚马逊简单通知服务开发者指南》中的 “为亚马逊 SNS 启用服务器端加密 (SSE)” 主题。在使用 SSE 之前，还必须配置 AWS KMS key 策略以允许对主题进行加密以及对消息进行加密和解密。有关更多信息，请参阅《Amazon 简单通知服务开发者指南》中的配置 AWS KMS 权限。

[SNS.2] 应为发送到主题的通知消息启用传输状态记录

> **Important**
>
> Security Hub 于 2024 年 4 月取消了该控制权。有关更多信息，请参阅 Security Hub 控件的更改日志。

相关要求：NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::SNS::Topic`

AWS Config 规则：`sns-topic-message-delivery-notification-enabled`

计划类型：已触发变更

参数：无

此控件检查是否启用记录发送到端点的 Amazon SNS 主题的通知消息的传输状态。如果未启用邮件的传输状态通知，则此控件将失败。

日志记录是维护服务的可靠性、可用性和性能的重要组成部分。记录消息传送状态有助于提供操作见解，例如：

- 了解消息是否已传输到 Amazon SNS 端点。
- 识别从 Amazon SNS 端点发送到 Amazon SNS 的响应。
- 确定消息停留时间（发布时间戳和移交到 Amazon SNS 端点之间的时间）。

修复

要为主题配置传输状态日志，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 消息传输状态。

[SNS.3] 应标记 SNS 话题

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::SNS::Topic`

AWS Config 规则：`tagged-sns-topic`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 Amazon SNS 主题是否具有参数中定义的特定密钥的标签。`requiredTagKeys`如果主题没有任何标签密钥或者没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果主题未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 SNS 主题添加标签，请参阅亚马逊简单通知服务开发者指南中的配置 Amazon SNS 主题标签。

Amazon Simple Queue Service 控件

这些控件与 Amazon SQS 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[SQS.1] 应对 Amazon SQS 队列进行静态加密

相关要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)。

类别：保护 > 数据保护 > 加密 data-at-rest

严重性：中

资源类型：`AWS::SQS::Queue`

AWS Config 规则：`sqs-queue-encrypted`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：无

此控件检查是否对 Amazon SQS 队列进行了静态加密。如果队列未使用 SQS 托管密钥 (SSE-SQS) 或 () 密钥 (SSE-KMS) 加密， AWS Key Management Service 则控制失败。AWS KMS

对静态数据进行加密可降低未经身份验证的用户访问磁盘上存储的数据的风险。服务器端加密 (SSE) 使用 SQS 托管的加密密钥 (SSE-SQS) 或密钥 (SSE-KMS) 保护 SQS 队列中的消息内容。 AWS KMS

修复

要为 SQS 队列配置 SSE，请参阅《亚马逊简单队列服务开发者指南》中的为队列（控制台）配置服务器端加密 (SS E)。

[SQS.2] 应标记 SQS 队列

类别：识别 > 清单 > 标记

严重性：低

资源类型：AWS::SQS::Queue

AWS Config 规则：tagged-sqs-queue（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
requiredTagKeys	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	No default value

此控件检查 Amazon SQS 队列是否具有参数中定义的特定密钥的标签。requiredTagKeys如果队列没有任何标签密钥或者没有参数中指定的所有密钥，则控件将失败requiredTagKeys。如果requiredTagKeys未提供该参数，则该控件仅检查标签密钥是否存在，如果队列未使用任何密钥标记，则该控件将失败。系统标签会自动应用并以其开头aws:，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要使用 Amazon SQS 控制台向现有队列添加标签，请参阅《亚马逊简单队列服务开发者指南》中的为亚马逊 SQS 队列（控制台）配置成本分配标签。

AWS Step Functions 控件

这些控件与 Step Functions 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[StepFunctions.1] Step Functions 状态机应该开启日志功能

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::StepFunctions::StateMachine`

AWS Config 规则：`step-functions-state-machine-logging-enabled`

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`logLevel`	最低日志记录级别	枚举	`ALL`, `ERROR`, `FATAL`	无默认值

此控件检查 AWS Step Functions 状态机是否已开启日志记录。如果状态机没有开启日志记录，则控制失败。如果您为 `logLevel` 参数提供自定义值，则仅当状态机开启了指定的日志记录级别时，控制才会通过。

监控可帮助您保持 Step Functions 的可靠性、可用性和性能。您应从中收集尽可能多的监控数据 AWS 服务 ，以便可以更轻松地调试多点故障。为你的 Step Function CloudWatch s 状态机定义日志配置后，你就可以在 Amazon Logs 中跟踪执行历史和结果。或者，您只能跟踪错误或致命事件。

修复

要为 Step Functions 状态机开启日志记录，请参阅 AWS Step Functions 开发人员指南中的配置日志记录。

[StepFunctions.2] 应标记 Step Functions 活动

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::StepFunctions::Activity`

AWS Config 规则:`tagged-stepfunctions-activity`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	无默认值

此控件检查 AWS Step Functions 活动是否具有参数中定义的特定键的标签`requiredTagKeys`。如果 Activity 没有任何标签密钥或者没有在参数中指定的所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果活动未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

要向 Step Functions 活动添加标签，请参阅《AWS Step Functions 开发者指南》中的 “在 Step Functions 中添加标签”。

AWS Transfer Family 控件

这些控制与 Transfer Family 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[Transfer.1] 应标记 AWS Transfer Family 工作流程

类别：识别 > 清单 > 标记

严重性：低

资源类型：`AWS::Transfer::Workflow`

AWS Config 规则：`tagged-transfer-workflow`（自定义 Security Hub 规则）

计划类型：已触发变更

参数：

参数	描述	类型	允许的自定义值	Security Hub 默认值
`requiredTagKeys`	评估的资源必须包含的非系统标签密钥列表。标签键区分大小写。	StringList	符合AWS 要求的标签列表	`No default value`

此控件检查 AWS Transfer Family 工作流程是否具有参数中定义的特定键的标签`requiredTagKeys`。如果工作流程没有任何标签密钥或者没有在参数中指定所有密钥，则控件将失败`requiredTagKeys`。如果`requiredTagKeys`未提供该参数，则该控件仅检查标签密钥是否存在，如果工作流程未使用任何密钥进行标记，则该控件将失败。系统标签会自动应用并以其开头`aws:`，但会被忽略。

标签是您分配给 AWS 资源的标签，它由密钥和可选值组成。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。标签可以帮助您识别、组织、搜索和筛选资源。标记还可以帮助您跟踪负责任的资源所有者的操作和通知。使用标记时，可以实现基于属性的访问控制 (ABAC) 作为一种授权策

略，该策略根据标签定义权限。您可以向 IAM 实体（用户或角色）和 AWS 资源附加标签。您可以为您的 IAM 委托人创建单个 ABAC 策略或一组单独的策略。您可以将这些 ABAC 策略设计为允许在委托人的标签与资源标签匹配时进行操作。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

> **Note**
>
> 不要在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多人都可以访问标签 AWS 服务，包括 AWS Billing。有关更多标记最佳做法，请参阅中的为AWS 资源添加标签。AWS 一般参考

修复

向 Transfer Family 工作流程添加标签（控制台）

1. 打开控制 AWS Transfer Family 台。
2. 在导航窗格上，选择工作流程。然后，选择要标记的工作流程。
3. 选择管理标签，然后添加标签。

[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

相关要求：nist.800-53.r5 CM-7、nist.800-53.r5 IA-5、nist.800-53.r5 SC-8

类别：保护 > 数据保护 > 加密 data-in-transit

严重性：中

资源类型：`AWS::Transfer::Server`

AWS Config 规则：`transfer-family-server-no-ftp`

计划类型：定期

参数：无

此控件检查 AWS Transfer Family 服务器是否使用 FTP 以外的协议进行端点连接。如果服务器使用 FTP 协议让客户端连接到服务器的端点，则控制失败。

FTP（文件传输协议）通过未加密的通道建立端点连接，使得通过这些通道发送的数据容易被拦截。使用 SFTP（SSH 文件传输协议）、FTPS（安全文件传输协议）或 AS2（适用性声明 2）通过加密传输

中的数据来提供额外的安全层，并可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击来窃听或操纵网络流量。

修复

要修改 Transfer Family 服务器的协议，请参阅AWS Transfer Family 用户指南中的编辑文件传输协议。

AWS WAF 控件

这些控制措施与 AWS WAF 资源有关。

这些控件可能并非全部可用 AWS 区域。有关更多信息，请参阅 按地区划分的控件可用性。

[WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::WAF::WebACL`

AWS Config 规则：`waf-classic-logging-enabled`

计划类型：定期

参数：无

此控件检查是否为 AWS WAF 全局 Web ACL 启用了日志记录。如果未为 Web ACL 启用日志记录，则此控制失败。

日志记录是维护 AWS WAF 全球可靠性、可用性和性能的重要组成部分。这是许多组织中的业务和合规性要求，并允许您对应用程序行为进行故障排除。它还提供有关附加到 AWS WAF的 Web ACL 所分析的流量的详细信息。

修复

要启用 AWS WAF Web ACL 的日志记录，请参阅AWS WAF 开发人员指南中的记录 Web ACL 流量信息。

[WAF.2] AWS WAF 经典区域规则应至少有一个条件

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)。

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAFRegional::Rule`

AWS Config 规则：`waf-regional-rule-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 区域规则是否至少具有一个条件。如果规则中不存在任何条件，则控制失败。

WAF 区域规则可以包含多个条件。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何条件的情况下，流量未经检查就通过。没有任何条件但带有建议允许、阻止或计数的名称或标签的 WAF 区域规则可能会导致错误地假设其中一项操作正在发生。

修复

要向空规则添加条件，请参阅 AWS WAF 开发人员指南中的在规则中添加和删除条件。

[WAF.3] AWS WAF 经典区域规则组应至少有一条规则

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)。

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAFRegional::RuleGroup`

AWS Config 规则：`waf-regional-rulegroup-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 区域规则组是否至少有一条规则。如果规则组中不存在任何规则，则控制失败。

一个 WAF 区域规则组可以包含多个规则。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何规则的情况下，流量未经检查就通过。没有规则但具有建议允许、阻止或计数的名称或标签的 WAF 区域规则组可能会导致错误地假设其中一项操作正在发生。

修复

要向空规则组添加规则和规则条件，请参阅《AWS WAF 开发者指南》中的在 AWS WAF 经典规则组中添加和删除规则以及在规则中添加和删除条件。

[WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAFRegional::WebACL`

AWS Config 规则：`waf-regional-webacl-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF Classic Regional Web ACL 是否包含任何 WAF 规则或 WAF 规则组。如果 Web ACL 不包含任何 WAF 规则或规则组，则此控制失败。

WAF Regional Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，则根据默认操作，Web 流量可以在不被 WAF 检测到或处理的情况下通过。

修复

要向空的 AWS WAF 经典区域 Web ACL 添加规则或规则组，请参阅AWS WAF 开发人员指南中的编辑 Web ACL。

[WAF.6] AWS WAF 经典全局规则应至少有一个条件

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAF::Rule`

AWS Config 规则：`waf-global-rule-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 全局规则是否包含任何条件。如果规则中不存在任何条件，则控制失败。

一个 WAF 全局规则可以包含多个条件。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何条件的情况下，流量未经检查就通过。不带条件但带有建议允许、阻止或计数的名称或标签的 WAF 全局规则可能会导致错误地假设其中一项操作正在发生。

修复

有关创建规则和添加条件的说明，请参阅 AWS WAF 开发人员指南中的创建规则和添加条件。

[WAF.7] AWS WAF 经典全局规则组应至少有一条规则

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAF::RuleGroup`

AWS Config 规则：`waf-global-rulegroup-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 全局规则组是否至少有一条规则。如果规则组中不存在任何规则，则控制失败。

一个 WAF 全局规则组可以包含多个规则。规则的条件允许进行流量检查并采取定义的操作（允许、阻止或计数）。在没有任何规则的情况下，流量未经检查就通过。没有规则但具有建议允许、阻止或计数的名称或标签的 WAF 全局规则组可能会导致错误地假设其中一项操作正在发生。

修复

有关向规则组添加规则的说明，请参阅《AWS WAF 开发人员指南》中的创建 AWS WAF 经典规则组。

[WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

相关要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)。

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAF::WebACL`

AWS Config 规则：`waf-global-webacl-not-empty`

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 全局 Web ACL 是否包含至少一个 WAF 规则或 WAF 规则组。如果 Web ACL 不包含任何 WAF 规则或规则组，则控制失败。

WAF 全局 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，则根据默认操作，Web 流量可以在不被 WAF 检测到或处理的情况下通过。

修复

要向空的 AWS WAF 全局 Web ACL 添加规则或规则组，请参阅AWS WAF 开发人员指南中的编辑 Web ACL。对于 “筛选”，选择 “全局” (CloudFront)。

[WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组

相关要求：NIST.800-53.r5 CA-9(1)，NIST.800-53.r5 CM-2

类别：保护 > 安全网络配置

严重性：中

资源类型：`AWS::WAFv2::WebACL`

AWS Config 规则：wafv2-webacl-not-empty

计划类型：已触发变更

参数：无

此控件检查 AWS WAF V2 Web 访问控制列表 (Web ACL) 是否至少包含一个规则或规则组。如果 Web ACL 不包含任何规则或规则组，则控制失败。

Web ACL 可让您对受保护资源响应的所有 HTTP(S) Web 请求进行精细控制。Web ACL 应包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，则 AWS WAF 根据默认操作，Web 流量可以在不被检测或处理的情况下通过。

修复

要向空的 WAFV2 Web ACL 添加规则或规则组，请参阅 AWS WAF 开发人员指南中的编辑 Web ACL。

[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：低

资源类型：AWS::WAFv2::WebACL

AWS Config 规则：**wafv2-logging-enabled**

计划类型：定期

参数：无

此控件检查 AWS WAF V2 Web 访问控制列表 (Web ACL) 是否已激活日志记录。如果停用 Web ACL 的日志记录，则此控制失败。

日志记录可维护的可靠性、可用性和性能 AWS WAF。此外，在许多组织中，日志记录是一项业务和合规要求。通过记录由 Web ACL 分析的流量，您可以对应用程序行为进行故障排除。

修复

要激活 AWS WAF Web ACL 的日志记录，请参阅AWS WAF 开发人员指南中的管理 Web ACL 的日志记录。

[WAF.12] AWS WAF 规则应启用指标 CloudWatch

相关要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)。

类别：识别 > 日志记录

严重性：中

资源类型：`AWS::WAFv2::RuleGroup`

AWS Config 规则：**`wafv2-rulegroup-logging-enabled`**

计划类型：已触发变更

参数：无

此控件检查 AWS WAF 规则或规则组是否启用了 Amazon CloudWatch 指标。如果规则或规则组未启用 CloudWatch 指标，则控件将失败。

在 AWS WAF 规则和规则组上配置 CloudWatch 指标可提供对流量的可见性。您可以看到哪些 ACL 规则被触发，哪些请求被接受和阻止。这种可见性可以帮助您识别关联资源上的恶意活动。

修复

要在 AWS WAF 规则组上启用 CloudWatch 指标，请调用 UpdateRuleGroupAPI。要在 AWS WAF 规则上启用 CloudWatch 指标，请调用 UpdateWebACL API。将 `CloudWatchMetricsEnabled` 字段设置为 `true`。当您使用 AWS WAF 控制台创建规则或规则组时， CloudWatch 指标会自动启用。

查看和管理安全控件

控件是安全标准中的一种保护措施，可帮助组织保护其信息的机密性、完整性和可用性。在 Security Hub 中，控件与特定 AWS 资源相关。

整合控件视图

S ec urity Hub 控制台的 “控件” 页面显示当前版本中所有可用的控件 AWS 区域 （ 您可以通过访问 “安全标准” 页面并选择启用的标准来查看标准环境中的控件 ）。Security Hub 为控件分配了各类标准一致的安全控件 ID、标题和描述。控件 ID 包括相关的 AWS 服务 唯一数字（ 例如， CodeBuild.3 ）。

Security Hub 控制台的控制页面上提供了以下信息。

- 总体安全评分基于已通过的控件占已启用控件总数与包含数据的控件总数的比例
- 在所有已启用的控件中，安全检查失败的百分比
- 针对不同严重程度的控件通过和未通过的安全检查的数量
- 根据启用状态划分为不同选项卡的控件列表。不适用于任何已启用标准的可用控件将显示在已禁用列中。未处理的控件（ 例如您当前区域中不可用的控件 ）将显示在无数据列中。全部列中的控件数等于失败、未知、已通过、已禁用和无数据列中控件的总和。

在控件页面中，您可以选择一个控件来查看其详细信息并对该控件生成的调查发现采取行动。在此页面上，您还可以在当前 AWS 账户 和中启用或禁用安全控件 AWS 区域。控件页面中的启用和禁用操作适用于所有标准。有关更多信息，请参阅 在所有标准中启用和禁用控件。

对于管理员账户，控件页面反映了成员账户中的控件状态。如果至少有一个成员账户的控件检查失败，则该控件将显示在控件页面的失败选项卡中。如果您设置了聚合区域，则控件页面将反映所有关联区域中控件的状态。如果至少一个关联区域的控件检查失败，则该控件将显示在控件页面的失败选项卡中。

合并控件视图会导致对 AWS 安全调查结果格式 (ASFF) 中的控制查找字段进行更改，这可能会影响工作流程。有关更多信息，请参阅 整合的控件视图——ASFF 变更。

控件的总体安全评分

控件页面显示的总体安全评分介于 0-100% 之间。总体安全评分是根据通过的控件与启用的带有数据的控件总数的比例来计算的。

> **Note**
>
> 要查看控件的总体安全评分，您必须添加调用 **`BatchGetControlEvaluations`** 用于访问 Security Hub 的 IAM 角色的权限。查看特定标准的安全评分不需要此权限。

启用 Security Hub 后，Security Hub 会在您首次访问 Security Hub 控制台上的摘要页面或安全标准页面后 30 分钟内计算出初始安全分数。在中国地区和 AWS GovCloud (US) Region生成首次获得安全评

分最多需要 24 小时。仅针对您访问这些页面时启用的标准生成分数。要查看当前启用的标准列表，请使用 `GetEnabledStandards` API 操作。此外，必须配置 AWS Config 资源记录才能显示分数。总体安全评分是标准安全评分的平均值。

首次生成分数后，Security Hub 每 24 小时更新一次安全分数。Security Hub 显示时间戳以指示安全评分上次更新的时间。

如果您设置了聚合区域，则总体安全分数将反映关联区域的控件调查发现。

主题

控件类别

每个控件都被分配了一个类别。控件的类别反映了它应用于的安全功能。

类别值包含类别、类别内的子类别以及可选的子类别内的分类器。例如：

- 识别 > 清单
- 保护 > 数据保护 > 传输中数据加密

以下是对可用类别、子类别和分类器的描述。

识别

了解组织情况以管理系统、资产、数据和功能面临的网络安全风险。

清单

该服务是否实施了正确的资源标记策略？ 标记策略是否包含资源拥有者？

该服务使用哪些资源？ 该服务是否有权使用这些资源？

您是否知道批准的库存？ 例如，您是否使用诸如 Amazon EC2 Systems Manager 和 Service Catalog 之类的服务？

日志记录

您是否已安全启用该服务的所有相关日志记录？ 日志文件的示例包括以下内容：

- Amazon VPC 流日志
- Elastic Load Balancing 访问日志
- 亚马逊 CloudFront 日志
- 亚马逊 CloudWatch 日志
- Amazon Relational Database Service 日志
- 亚马逊 OpenSearch 服务慢速索引日志
- X-Ray 跟踪
- AWS Directory Service 日志
- AWS Config 物品
- 快照

保护

制定并实施适当的保护措施，以确保提供关键基础设施服务和安全编码实践。

安全访问管理

该服务是否在其 IAM 或资源策略中使用最低权限实践？

密码和密钥是否足够复杂？ 它们是否已适当轮换？

该服务是否使用 Multi-Factor Authentication (MFA)？

该服务是否避开根用户？

基于资源的策略是否允许公有访问？

安全网络配置

该服务是否避免公有和不安全的远程网络访问？

该服务是否正确使用了 VPC？ 例如，是否要求在 VPC 中运行作业？

该服务是否已正确分割和隔离敏感资源？

数据保护

静态数据加密——该服务是否加密静态数据？

加密传输中数据——该服务是否对数据进行传输中加密？

数据完整性——该服务是否验证数据的完整性？

数据删除保护——该服务是否保护数据免遭意外删除？

数据管理/使用——您是否使用 Amazon Macie 等服务来跟踪敏感数据的位置？

API 保护

该服务是否 AWS PrivateLink 用于保护服务 API 操作？

保护性服务

是否有适当的保护性服务？ 它们是否提供了正确的覆盖范围？

保护性服务可帮助您转移针对该服务的攻击和破坏。中的保护服务示例 AWS 包括 AWS Control Tower、、、Vanta AWS WAF AWS Shield Advanced、Secrets Manager、IAM Access Analyzer 和 AWS Resource Access Manager。

安全开发

您是否使用了安全编码实践？

您是否避免了诸如开放 Web 应用程序安全项目 (OWASP) 十大漏洞之类的漏洞？

Detect

制定并实施适当的活动，以识别网络安全事件的发生。

检测服务

是否有适当的检测服务？

它们是否提供了正确的覆盖范围？

AWS 检测服务的示例包括亚马逊 GuardDuty、Amazon Inspector AWS Security Hub、Amazon Detective、A CloudWatch mazon AI AWS IoT Device Defender arms 和 AWS Trusted Advisor。

响应

制定并实施适当的活动，以便对检测到的网络安全事件采取措施。

响应措施

您是否能迅速对安全事件做出响应？

您现在是否有任何“严重”或“高”严重性的结果？

取证

您是否能够安全地获取服务的取证数据？ 例如，您是否获取与实际正面调查发现相关的 Amazon EBS 快照？

您是否设立了取证账户？

恢复

制定并实施适当的活动，以维护恢复能力计划，恢复因网络安全事件而受损的任何能力或服务。

弹性

服务配置是否支持正常故障转移、弹性扩展和高可用性？

您是否已创建备份？

在所有标准中启用和禁用控件

AWS Security Hub 生成已启用的控件的调查结果，并在计算安全分数时考虑所有启用的控件。您可以选择启用和禁用所有安全标准下的控件，也可以在不同的标准中以不同的方式配置启用状态。我们建议使用前一个选项，即控件的启用状态在所有已启用的标准中保持一致。本部分介绍如何启用和禁用不同标准中的控件。要启用或禁用一个或多个特定标准中的控件，请参阅在特定标准中启用和禁用控件。

如果您设置了聚合区域，则 Security Hub 控制台会显示来自所有关联区域的控件。如果某个控件在关联区域中可用，但在聚合区域中不可用，则无法在聚合区域启用或禁用该控件。

> **Note**
>
> 启用和禁用控件的说明会因您是否使用中心配置而异。本部分介绍其中的区别。集成 Security Hub 和的用户可以使用中央配置 AWS Organizations。我们建议使用中心配置来简化在多账户、多区域环境中启用和禁用控件的过程。

启用控件

当您在标准中启用控件时，Security Hub 会开始对该控件运行安全检查并生成控件调查发现。

Security Hub 还在总体安全分数和标准安全分数的计算中包括控件状态。如果您开启了整合的控件调查发现，那么即使您已在多个标准中启用了某个控件，也将收到一份单独的安全检查调查发现。有关更多信息，请参阅 Consolidated control findings。

启用跨多个账户和区域的所有标准中的控件

要在多个账户和之间启用安全控制 AWS 区域，必须使用集中配置。

当您使用中心配置时，委托管理员可以创建 Security Hub 配置策略，这些策略可以跨已启用的标准启用指定控件。然后，您可以将配置策略与特定的账户和组织单元（OU）或根相关联。配置策略在您的主区域（也称为聚合区域）和所有关联区域中生效。

配置策略可自定义。例如，您可以选择启用一个 OU 中的所有控件，也可以选择在另一个 OU 中仅启用 Amazon Elastic Compute Cloud（EC2）控件。粒度级别取决于您的组织中安全覆盖范围的预期目标。有关创建配置策略（启用不同标准中的指定控件）的说明，请参阅创建和关联 Security Hub 配置策略。

> **Note**
>
> 授权的管理员可以创建配置策略来管理除服务管理标准之外的所有标准中的控件: AWS Control Tower。应在 AWS Control Tower 服务中配置该标准的控件。

如果您希望某些账户配置自己的控件而不是委托管理员来配置，则委托管理员可以将这些账户指定为自行管理。自行管理账户必须在每个区域中单独配置控件。

在单个账户和区域中启用所有标准的控件

如果您不使用中心配置或是自行管理账户，则无法使用配置策略在多个账户和区域中集中启用控件。但是，您可以使用以下步骤在单个账户和区域中启用控件。

Security Hub console

要在一个账户和区域中启用不同标准中的控件

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 从导航窗格中选择控件。
3. 选择已禁用选项卡。
4. 选择控件旁边的选项。
5. 选择启用控制（对于已启用的控件，此选项不会出现）。
6. 在您要在其中启用控件的每个区域中重复这些操作。

Security Hub API

要在一个账户和区域中启用不同标准中的控件

1. 调用 ListStandardsControlAssociations API。提供安全控件 ID。

   请求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. 调用 BatchUpdateStandardsControlAssociations API。提供所有未启用控件的标准的 Amazon 资源名称（ARN）。要获取标准 ARN，请运行 `DescribeStandards`。
3. 将 `AssociationStatus` 参数设置为等于 `ENABLED`。如果您对已启用的控件执行以下步骤，则该 API 将返回 HTTP 状态码 200 响应。

   请求示例：

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
   v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
   best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
   }
   ```

4. 在您要在其中启用控件的每个区域中重复这些操作。

AWS CLI

要在一个账户和区域中启用不同标准中的控件

1. 运行 list-standards-control-associations 命令。提供安全控件 ID。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. 运行 batch-update-standards-control-associations 命令。提供所有未启用控件的标准的 Amazon 资源名称（ARN）。要获取标准 ARN，请运行 `describe-standards` 命令。
3. 将 `AssociationStatus` 参数设置为等于 `ENABLED`。如果您对已启用的控件执行这些步骤，该命令将返回 HTTP 状态代码 200 响应。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. 在您要在其中启用控件的每个区域中重复这些操作。

自动启用已启用标准中的新控件

Security Hub 会定期发布新的安全控件，并将其添加到一个或多个标准中。您可以选择是否在启用的标准中自动启用新控件。

> **Note**
>
> 我们建议使用中心配置来自动启用新控件。如果您的配置策略包含要禁用的控件列表（以编程方式说明的话，反映了 `DisabledSecurityControlIdentifiers` 参数），则 Security Hub 会自动启用所有其他不同标准中的控件，包括新发布的控件。如果您的策略包含要启用的控件列表（反映了 `EnabledSecurityControlIdentifiers` 参数），则 Security Hub 会自动禁用所有其他不同标准中的控件，包括新发布的控件。有关更多信息，请参阅 Security Hub 配置策略的工作原理。

选择首选访问方法，然后按照以下步骤自动启用启用的标准中的新控件。以下说明仅在您不使用中心配置时适用。

Security Hub console

要自动启用新控件

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择设置，然后选择常规选项卡。
3. 在控件下，选择编辑。
4. 在已启用的标准中开启自动启用新控件。
5. 选择保存。

Security Hub API

要自动启用新控件

1. 调用 UpdateSecurityHubConfiguration API。
2. 要自动为启用的标准启用新控件，将 `AutoEnableControls` 设置为 `true`。如果您不想自动启用新控件，请设置 `AutoEnableControls` 为 false。

AWS CLI

要自动启用新控件

1. 运行 update-security-hub-configuration 命令。
2. 要自动为启用的标准启用新控件，请指定 `--auto-enable-controls`。如果您不想自动启用新控件，请指定 `--no-auto-enable-controls`。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

命令示例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

禁用控件

当您禁用所有标准中的控件时，会发生以下情况：

- 不再执行控件的安全检查。
- 不会为该控制生成任何其他结果。
- 现有调查发现将在 3-5 天后自动存档（请注意，这是尽最大努力的结果）。
- Security Hub 创建的所有相关 AWS Config 规则都将被删除。

您可以仅在一个或多个特定标准中禁用该控件，而不是禁用所有标准中的控件。如果您这样做，Security Hub 将不会对您禁用该控件的标准进行安全检查，因此它不会影响这些标准的安全分数。但是，如果在其他标准中启用了该 AWS Config 规则，Security Hub 会保留该规则，并继续对该控件进行安全检查。这可能会影响您的汇总安全分数。有关在特定标准中配置控件的说明，请参阅在特定标准中启用和禁用控件。

为了减少调查发现噪音，禁用与环境无关的控件可能会很有用。有关禁用哪些控件的建议，请参阅您可能希望禁用的 Security Hub 控件。

禁用标准时，所有适用于该标准的控件都将被禁用（但是，这些控件在其他标准中可能仍处于启用状态）。有关禁用标准的信息，请参阅 the section called “启用和禁用标准”。

当您禁用标准时，Security Hub 不会跟踪其哪些适用控件被禁用。如果您随后重新启用相同的标准，则所有适用于该标准的控件都会自动启用。此外，禁用控件不是永久性操作。假设您禁用一个控件，然后启用一个先前已禁用的标准。如果标准包含该控件，它将在该标准中启用。当您在 Security Hub 中启用标准时，适用于该标准的所有控件都会自动启用。您可以选择禁用特定控件。

在多个账户和区域中禁用所有标准中的控件

要禁用跨多个账户和的安全控制 AWS 区域，必须使用集中配置。

使用中心配置时，委托管理员可以创建 Security Hub 配置策略，以禁用已启用的标准中的指定控件。然后，您可以将配置策略与特定账户、OU 或根相关联。配置策略在您的主区域（也称为聚合区域）和所有关联区域中生效。

配置策略可自定义。例如，您可以选择禁用一个 OU 中的所有 AWS CloudTrail 控件，也可以选择禁用另一个 OU 中的所有 IAM 控件。粒度级别取决于您的组织中安全覆盖范围的预期目标。有关创建用于禁用不同标准中指定控件的配置策略的说明，请参阅创建和关联 Security Hub 配置策略。

> **Note**
>
> 授权的管理员可以创建配置策略来管理除服务管理标准之外的所有标准中的控件: AWS Control Tower。应在 AWS Control Tower 服务中配置该标准的控件。

如果您希望某些账户配置自己的控件而不是委托管理员来配置，则委托管理员可以将这些账户指定为自行管理。自行管理账户必须在每个区域中单独配置控件。

在单个账户和区域中禁用所有标准中的控件

如果您未使用中心配置，或是自行管理账户，则无法使用配置策略在多个账户和区域中集中禁用控件。但是，您可以使用以下步骤来禁用单个账户和区域中的控件。

Security Hub console

要在一个账户和区域中禁用不同标准中的控件

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 从导航窗格中选择控件。
3. 选择控件旁边的选项。
4. 选择禁用控制（对于已禁用的控件，此选项不会出现）。
5. 选择禁用控件的原因，然后选择禁用进行确认。
6. 在您要在其中禁用控件的每个区域中重复这些操作。

Security Hub API

要在一个账户和区域中禁用不同标准中的控件

1. 调用 ListStandardsControlAssociations API。提供安全控件 ID。

   请求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. 调用 BatchUpdateStandardsControlAssociations API。提供启用该控件的任何标准的 ARN。要获取标准 ARN，请运行 `DescribeStandards`。

3. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已禁用的控件执行以下步骤，API 将返回 HTTP 状态代码 200 响应。

   请求示例：

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
 applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. 在您要在其中禁用控件的每个区域中重复这些操作。

AWS CLI

要在一个账户和区域中禁用不同标准中的控件

1. 运行 list-standards-control-associations 命令。提供安全控件 ID。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. 运行 batch-update-standards-control-associations 命令。提供启用该控件的任何标准的 ARN。要获取标准 ARN，请运行 describe-standards 命令。

3. 将 AssociationStatus 参数设置为等于 DISABLED。如果您对已禁用的控件执行以下步骤，该命令将返回 HTTP 状态代码 200 响应。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. 在您要在其中禁用控件的每个区域中重复这些操作。

自动启用已启用标准中的新控件

AWS Security Hub 定期发布新的控件并将其添加到一个或多个标准中。您可以选择是否在启用的标准中自动启用新控件。

> **Note**
>
> 如果您使用中心配置并在配置策略中包含要禁用的特定控件列表（以编程方式说明的话，反映了 `DisabledSecurityControlIdentifiers` 参数），Security Hub 会自动启用不同标准中的所有其他控件，包括新发布的控件。有关更多信息，请参阅 Security Hub 配置策略的工作原理。

我们建议使用 Security Hub 中心配置来自动启用新的安全控件。您可以创建配置策略，其中包括不同标准中要禁用的控件列表。默认情况下，所有其他控件（包括新发布的控件）均处于启用状态。或者，您可以创建策略，其中包含不同标准中要启用的控件的列表。默认情况下，所有其他控件（包括新发布的控件）均处于禁用状态。有关更多信息，请参阅 中央配置的工作原理。

当新控件添加到您尚未启用的标准中时，Security Hub 不会启用这些控件。

以下说明仅在您不使用中心配置时适用。

选择首选访问方法，然后按照以下步骤自动启用启用的标准中的新控件。

Security Hub console

要自动启用新控件

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择设置，然后选择常规选项卡。
3. 在控件下，选择编辑。
4. 在已启用的标准中开启自动启用新控件。
5. 选择保存。

Security Hub API

要自动启用新控件

1. 运行 UpdateSecurityHubConfiguration。
2. 要自动为启用的标准启用新控件，将 AutoEnableControls 设置为 true。如果您不想自动启用新控件，请设置 AutoEnableControls 为 false。

AWS CLI

要自动启用新控件

1. 运行 update-security-hub-configuration 命令。
2. 要自动为启用的标准启用新控件，请指定 --auto-enable-controls。如果您不想自动启用新控件，请指定 --no-auto-enable-controls。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

命令示例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

如果您没有自动启用新控件，则必须手动启用它们。有关说明，请参阅the section called “在所有标准中启用和禁用控件”。

自定义控制参数

某些 Security Hub 控件使用的参数会影响控件的评估方式。通常，此类控件是根据 Security Hub 定义的默认参数值进行评估的。但是，对于这些控件的子集，您可以自定义参数值。当您为控件自定义参数值时，Security Hub 会开始根据您指定的值评估控件。如果控件底层的资源满足自定义值，Security Hub 会生成 PASSED 调查发现。如果资源不满足自定义值，Security Hub 会生成 FAILED 调查发现。

通过自定义控制参数，您可以优化 Security Hub 推荐和监控的安全最佳实践，使其符合您的业务需求和安全期望。您可以自定义控件的一个或多个参数以获得符合您安全需求的调查发现，而不是隐藏控件的调查发现。

以下是一些自定义控制参数的示例用例：

- [CloudWatch.16]- CloudWatch 日志组应在指定的时间段内保留

  您可以指定保留期限。
- [IAM.7]—IAM 用户的密码策略应具有可靠的配置

  您可以指定与密码强度相关的参数。
- [EC2.18]—安全组应只允许来自授权端口的不受限制的传入流量

  您可以指定哪些端口有权允许不受限制的传入流量。
- [Lambda.5]—VPC Lambda 函数应在多个可用区内运行

  您可以指定生成通过的调查发现的可用区的最小数量。

本部分介绍如何自定义和管理控制参数。

自定义控制参数的工作原理

一个控件可以有一个或多个可自定义的参数。单个控制参数可能具有的数据类型包括：

- 布尔值
- Double
- 枚举
- EnumList
- 整数
- IntegerList
- String
- StringList

对于某些控件，可接受的参数值还必须介于指定范围之内才有效。在这些情况下，Security Hub 会提供可接受的范围。

Security Hub 会选择默认参数值，并且可能偶尔会对其进行更新。自定义控制参数后，除非您对其值进行更改，否则它会一直为您为该参数指定的值。也就是说，即使该参数的自定义值与 Security Hub 定义的当前默认值匹配，该参数也不会再跟踪对默认 Security Hub 值的更新。以下是控件 [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订的示例：

```
{
```

```
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

在前面的示例中，daysToExpiration 参数的自定义值为 30。此参数的当前默认值也可以是 30。如果 Security Hub 将默认值更改为 14，则此示例中的参数将不会跟踪该更改。它将保留值 30。

如果要跟踪对某参数的默认 Security Hub 值的更新，请将 ValueType 字段设置为 DEFAULT，而不是 CUSTOM。有关更多信息，请参阅 在单个账户和区域中恢复为默认参数值。

更改参数值后，还会触发新的安全检查，根据新值对控件进行评估。然后，Security Hub 会根据新值生成新的控件调查发现。在定期更新控件调查发现期间，Security Hub 也会使用新的参数值。如果您更改了控件的参数值，但尚未启用任何包含该控件的标准，则 Security Hub 不会使用新值进行任何安全检查。您必须至少启用一个相关标准，Security Hub 才能根据新的参数值评估控件。

自定义参数值会应用于您启用的各种标准。您无法为当前区域不支持的控件自定义参数。有关各个控件的区域限制列表，请参阅对控件的区域限制。

自定义控制参数

自定义控制参数的说明因您是否使用中心配置而异。中央配置是一项功能，委派的 Security Hub 管理员可以使用它来跨 AWS 区域其组织中的账户和组织单位 (OU) 管理 Security Hub 功能。

如果您的组织使用中心配置，则委托管理员可以创建包含自定义控制参数的配置策略。这些策略可以与集中管理的成员账户和 OU 关联，并且在您的主区域和所有关联的区域生效。委托管理员还可以将一个或多个账户指定为自行管理，这允许账户所有者在每个区域中单独配置自己的参数。如果您的组织不使用中心配置，则必须在每个账户和区域中分别自定义控制参数。

为多个账户和区域自定义控制参数

使用中心配置时，您可以为多个账户和区域的集中管理账户和 OU 自定义控制参数。我们建议使用中心配置，因为它允许您在组织的不同部门之间调整控制参数值。例如，您的所有测试账户都可能使用特定的参数值，而所有生产账户使用的可能是不同的值。

如果您是使用中心配置的组织的委托 Security Hub 管理员，请选择您的首选方法，然后按照步骤自定义多个账户和区域之间的控制参数。

Security Hub console

要在多个账户和区域中自定义控制参数

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   确保您已登录到主区域。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。
4. 要创建包含自定义参数的新配置策略，请选择创建策略。要在现有配置策略中指定自定义参数，请选择策略，然后选择编辑。

   要使用自定义参数创建新的配置策略

   1. 在自定义策略部分，选择要启用的安全标准和控件。
   2. 选择自定义控制参数。
   3. 选择一个控件，然后为一个或多个参数指定自定义值。
   4. 要自定义更多控件的参数，请选择自定义其他控件。
   5. 在账户部分，选择要对其应用策略的账户或组织单元。
   6. 选择下一步。
   7. 选择创建策略并应用。此操作将覆盖您的主区域和所有关联区域中与此配置策略关联的账户和 OU 的现有配置设置。可以通过直接应用或从父级继承来将账户和 OU 与配置策略相关联。

   要在现有配置策略中添加或编辑自定义参数

   1. 在控制部分的自定义策略下，指定所需的新自定义参数值。
   2. 如果这是您第一次自定义此策略中的控制参数，请选择自定义控制参数，然后选择要自定义的控件。要自定义更多控件的参数，请选择自定义其他控件。
   3. 在账户部分，验证您要对其应将策略的账户或 OU。
   4. 选择下一步。

5. 再次检查您的更改，确认正确无误。完成后，选择保存策略并应用。此操作将覆盖您的主区域和所有关联区域中与此配置策略关联的账户和 OU 的现有配置设置。可以通过直接应用或从父级继承来将账户和 OU 与配置策略相关联。

Security Hub API

要在多个账户和区域中自定义控制参数

要使用自定义参数创建新的配置策略

1. 从主区域的委托管理员账户调用 CreateConfigurationPolicy API。
2. 对于 SecurityControlCustomParameters 对象，请提供要自定义的每个控件的标识符。
3. 对于 Parameters 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 CUSTOM 作为 ValueType 的值。对于 Value，请提供参数的数据类型和自定义值。当 ValueType 的值为 CUSTOM 时，该 Value 字段不能为空。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过调用 GetSecurityControlDefinition API，您可以找到控件支持的参数、数据类型和有效值。

要在现有配置策略中添加或编辑自定义参数

1. 从主区域的委托管理员账户调用 UpdateConfigurationPolicy API。
2. 对于 Identifier 字段，提供要更新配置策略的 Amazon 资源名称（ARN）或 ID。
3. 对于 SecurityControlCustomParameters 对象，请提供要自定义的每个控件的标识符。
4. 对于 Parameters 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 CUSTOM 作为 ValueType 的值。对于 Value，请提供参数的数据类型和自定义值。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过调用 GetSecurityControlDefinition API，您可以找到控件支持的参数、数据类型和有效值。

创建新配置策略的 API 请求示例：

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
```

```
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

要在多个账户和区域中自定义控制参数

要使用自定义参数创建新的配置策略

1. 从主区域的委托管理员账户运行 create-configuration-policy 命令。
2. 对于 SecurityControlCustomParameters 对象，请提供要自定义的每个控件的标识符。
3. 对于 Parameters 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 CUSTOM 作为 ValueType 的值。对于 Value，请提供参数的数据类型和自定义值。当 ValueType 的值为 CUSTOM 时，该 Value 字段不能为空。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过运行 get-security-control-definition 命令，您可以找到控件支持的参数、数据类型和有效值。

要在现有配置策略中添加或编辑参数

1. 要在现有配置策略中添加或更新自定义输入参数，请从主区域的委托管理员账户运行 update-configuration-policy 命令。
2. 对于 `identifier` 字段，提供要更新策略的 Amazon 资源名称（ARN）或 ID。
3. 对于 `SecurityControlCustomParameters` 对象，请提供要自定义的每个控件的标识符。
4. 对于 `Parameters` 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 `CUSTOM` 作为 `ValueType` 的值。对于 `Value`，请提供参数的数据类型和自定义值。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过运行 get-security-control-definition 命令，您可以找到控件支持的参数、数据类型和有效值。

创建新配置策略的命令示例：

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

在单个账户和区域中自定义控制参数

如果您不使用中心配置，或拥有自行管理账户，则可以一次在一个区域内为账户自定义控制参数

选择您的首选方法，然后按照步骤自定义控制参数。您的更改仅适用于当前区域中的账户。要自定义其他区域中的控制参数，请在要自定义参数的每个其他账户和区域中重复以下步骤。同一个控件可以在不同的区域中使用不同的参数值。

Security Hub console

要在一个账户、一个区域中自定义控制参数

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

2. 在导航窗格中，选择控件。在表中，选择支持自定义参数且想要更改其参数的控件。自定义参数列指示哪些控件支持自定义参数。
3. 在控件的详细信息页面上，选择参数选项卡，然后选择编辑。
4. 指定所需的参数值。
5. 或者，在更改原因部分中，选择自定义参数的原因。
6. 选择保存。

Security Hub API

要在一个账户、一个区域中自定义控制参数

1. 调用 UpdateSecurityControl API。
2. 对于 `SecurityControlId`，请提供要自定义的控件的 ID。
3. 对于 `Parameters` 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 `CUSTOM` 作为 `ValueType` 的值。对于 `Value`，请提供参数的数据类型和自定义值。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过调用 GetSecurityControlDefinition API，您可以找到控件支持的参数、数据类型和有效值。
4. （可选）对于 `LastUpdateReason`，提供自定义控制参数的理由。

API 请求示例：

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
        }
    },
    "LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

要在一个账户、一个区域中自定义控制参数

1. 运行 update-security-control 命令。
2. 对于 `security-control-id`，请提供要自定义的控件的 ID。
3. 对于 `parameters` 对象，请提供要自定义的每个参数的名称。对于您自定义的每个参数，请提供 `CUSTOM` 作为 `ValueType` 的值。对于 `Value`，请提供参数的数据类型和自定义值。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。通过运行 get-security-control-definition 命令，您可以找到控件支持的参数、数据类型和有效值。
4. （可选）对于 `last-update-reason`，提供自定义控制参数的理由。

命令示例：

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

检查控制参数的状态

验证和检查控制参数变更的状态很重要。这有助于确保控件按预期运行，并达到预期的安全值。要验证参数更新是否成功，您可以在 Security Hub 控制台上查看控件的详细信息。在控制台上，选择控件以显示其详细信息。参数选项卡将显示参数更改的状态。

以编程方式说明的话，如果您更新参数的请求有效，则作为对 BatchGetSecurityControls 操作的响应，字段 `UpdateStatus` 的值将为 `UPDATING`。这意味着更新有效，但您的调查发现可能还不包括更新后的参数值。当 `UpdateState` 的值更改为 `READY` 时，您的调查发现将开始包含更新后的参数值。

该 `UpdateSecurityControl` 操作返回无效参数值的 `InvalidInputException` 响应。该响应提供关于失败原因的其他详细信息。例如，您指定的值可能超出了参数的有效范围。或者，您指定的值没有使用正确的数据类型。请使用有效的输入再次提交您的请求。如果参数更新失败，Security Hub 会保留该参数的当前值。

如果您尝试更新参数值时出现内部故障，如果您已 AWS Config 启用，Security Hub 会自动重试。有关更多信息，请参阅 正在配置 AWS Config。

查看控制参数

您可以查看账户中各个控制参数的当前值。如果您使用中心配置，则委托 Security Hub 管理员还可以查看配置策略中指定的参数值。

选择您的首选方法，然后按照以下步骤查看当前控制参数值。

Security Hub console

要查看当前参数值

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择控件。选择控件。
3. 选择参数选项卡。此选项卡显示控件的当前参数值。

Security Hub API

要查看当前参数值

调用 BatchGetSecurityControls API，并提供一个或多个安全控件 ID 或 ARN。响应中的 `Parameters` 对象显示指定控件的当前参数值。

API 请求示例：

```
{
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

要查看当前参数值

运行 batch-get-security-controls 命令，并提供一个或多个安全控件 ID 或 ARN。响应中的 `Parameters` 对象显示指定控件的当前参数值。

命令示例：

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
```

```
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

选择您的首选方法以查看中心配置策略中的当前参数值。

Security Hub console

要查看配置策略中的当前参数值

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中委托 Security Hub 管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 在策略选项卡上，选择配置策略，然后选择查看详细信息。然后将显示策略详细信息，包括当前参数值。

Security Hub API

要查看配置策略中的当前参数值

1. 从主区域的委托管理员账户调用 GetConfigurationPolicy API。
2. 提供您要查看其详细信息的配置策略的 ARN 或 ID。响应包含当前参数值。

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

要查看配置策略中的当前参数值

1. 从主区域的委托管理员账户运行 get-configuration-policy 命令。
2. 提供您要查看其详细信息的配置策略的 ARN 或 ID。响应包含当前参数值。

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
```

```
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

您的控件调查发现还会显示当前的参数值。在 AWS 安全调查结果格式 (ASFF) 语法中，这些值出现在 Compliance 对象的 Parameters 字段中。要在 Security Hub 上查看调查发现，在导航窗格中选择调查发现。要以编程方式查看调查发现，请使用 GetFindings 操作。

> **Note**
>
> 自定义控制参数功能发布后，Security Hub 将更新现有控件调查发现以包含 Parameters ASFF 字段。这最多需要 24 小时。

恢复为默认控制参数值

控制参数可以具有 Security Hub 定义的默认值。我们可能会更新参数的默认值，以反映不断演变的安全最佳实践。如果您还没有为控制参数指定自定义值，则该控件会自动跟踪这些更新并使用新的默认值。

您可以恢复为使用控件的默认参数值。如何执行此操作取决于您是否使用中心配置。

> **Note**
>
> 并非所有控制参数都有默认的 Security Hub 值。在此类情况下，当 ValueType 的值设定为 DEFAULT 时，Security Hub 不会使用特定的默认值。Security Hub 会在没有自定义值的情况下，忽略该参数。

在多个账户和区域中恢复为默认参数值

如果您使用中心配置，则可以恢复多个账户和区域中集中管理的账户和 OU 的控制参数。

选择您的首选方法，然后按照以下步骤，使用中心配置在多个账户和区域中恢复为默认参数值。

Security Hub console

要在多个账户和区域中恢复为默认参数值

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。

   使用主区域中 Security Hub 委托管理员账户的凭证登录。
2. 在导航窗格中，选择设置和配置。
3. 选择策略选项卡。
4. 选择一个策略，然后选择编辑。
5. 在自定义策略下，控件部分显示了您为其指定自定义参数的控件列表。
6. 找到具有一个或多个要恢复的参数值的控件。然后，选择删除以恢复为默认值。
7. 在账户部分，验证您要对其应将策略的账户或 OU。
8. 选择下一步。
9. 再次检查您的更改，确认正确无误。完成后，选择保存策略并应用。此操作将覆盖您的主区域和所有关联区域中与此配置策略关联的账户和 OU 的现有配置设置。可以通过直接应用或从父级继承来将账户和 OU 与配置策略相关联。

Security Hub API

要在多个账户和区域中恢复为默认参数值

1. 从主区域的委托管理员账户调用 UpdateConfigurationPolicy API。
2. 对于 `Identifier` 字段，提供要更新策略的 Amazon 资源名称（ARN）或 ID。
3. 对于 `SecurityControlCustomParameters` 对象，请提供要为其恢复一个或多个参数的每个控件的标识符。
4. 在 `Parameters` 对象中，为要恢复的每个参数提供 `DEFAULT` 作为 `ValueType` 字段的值。当 `ValueType` 设置为 `DEFAULT` 时，无需为该 `Value` 字段提供值。如果您的请求中包含了值，Security Hub 会将其忽略。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。

> **Warning**
>
> 如果在 SecurityControlCustomParameters 字段中省略控件对象，Security Hub 会将该控件的所有自定义参数恢复为其默认值。SecurityControlCustomParameters 的列表完全为空会将所有控件的自定义参数恢复为其默认值。

API 请求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
             "SecurityControlsConfiguration": {
                "DisbledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "DEFAULT"
                             }
                         }
                    }
                ]
             }
        }
    }
}
```

AWS CLI

要在多个账户和区域中恢复为默认参数值

1. 从主区域的委托管理员账户运行 update-configuration-policy 命令。
2. 对于 identifier 字段，提供要更新策略的 Amazon 资源名称（ARN）或 ID。
3. 对于 SecurityControlCustomParameters 对象，请提供要为其恢复一个或多个参数的每个控件的标识符。
4. 在 Parameters 对象中，为要恢复的每个参数提供 DEFAULT 作为 ValueType 字段的值。当 ValueType 设置为 DEFAULT 时，无需为该 Value 字段提供值。如果您的请求中包含了值，Security Hub 会将其忽略。如果您的请求省略了控件支持的参数，则该参数将保留其当前值。

> **Warning**
>
> 如果在 SecurityControlCustomParameters 字段中省略控件对象，Security Hub 会将该控件的所有自定义参数恢复为其默认值。SecurityControlCustomParameters 的列表完全为空会将所有控件的自定义参数恢复为其默认值。

命令示例：

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

在单个账户和区域中恢复为默认参数值

如果您不使用中心配置或拥有自行管理账户，则可以恢复为每次在一个区域中使用账户的默认参数值。

选择您的首选方法，然后按照以下步骤在单个区域中将您的账户恢复为默认参数值。要在其他区域中恢复为默认参数值，请在每个其他区域中重复这些步骤。

> **Note**
>
> 如果您禁用 Security Hub，则您的自定义控制参数将被重置。如果您将来再次启用 Security Hub，则所有控件最开始都将使用默认参数值。

Security Hub console

要在一个账户和区域中恢复为默认参数值

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中，选择控件。选择要恢复为默认值的参数。
3. 在 `Parameters` 选项卡上，选择控制参数旁边的自定义。然后，选择删除自定义。此参数现在使用默认的 Security Hub 值，并会跟踪未来的默认值更新。
4. 对要恢复的每个参数值重复上述步骤。

Security Hub API

要在一个账户和区域中恢复为默认参数值

1. 调用 UpdateSecurityControl API。
2. 对于 `SecurityControlId`，请提供要恢复其参数的控件的 ARN 或 ID。
3. 在 `Parameters` 对象中，为要恢复的每个参数提供 `DEFAULT` 作为 `ValueType` 字段的值。当 `ValueType` 设置为 `DEFAULT` 时，无需为该 `Value` 字段提供值。如果您的请求中包含了值，Security Hub 会将其忽略。
4. （可选）对于 `LastUpdateReason`，提供恢复为默认参数值的原因。

API 请求示例：

```
{
```

```
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

要在一个账户和区域中恢复为默认参数值

1. 运行 update-security-control 命令。
2. 对于 `security-control-id`，请提供要恢复其参数的控件的 ARN 或 ID。
3. 在 `parameters` 对象中，为要恢复的每个参数提供 `DEFAULT` 作为 `ValueType` 字段的值。当 `ValueType` 设置为 `DEFAULT` 时，无需为该 `Value` 字段提供值。如果您的请求中包含了值，Security Hub 会将其忽略。
4. （可选）对于 `last-update-reason`，提供恢复为默认参数值的原因。

命令示例：

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

支持自定义参数的控件

有关支持自定义参数的安全控件列表，您可以参阅 Security Hub 控制台上的控件页面或 Security Hub 控件参考。要以编程方式检索此列表，您可以使用 ListSecurityControlDefinitions 操作。在响应中，`CustomizableProperties` 对象指示哪些控件支持可自定义的参数。

您可能想要禁用的 Security Hub 控件

我们建议禁用某些 AWS Security Hub 控件以减少查找噪音并限制成本。

处理全局资源的控件

有些 AWS 服务 支持全局资源，这意味着您可以从任何资源访问该资源 AWS 区域。为了节省成本 AWS Config，您可以禁用除一个区域以外的所有区域记录全球资源。但在完成此操作后，Security Hub 仍将在所有启用控件的区域进行安全检查，并将根据每个区域的每个账户的检查数量，向您收费。因此，为了减少查找噪音并节省 Security Hub 的成本，您还应禁用除记录全球资源的区域之外的所有区域中涉及全球资源的控件。

如果控件涉及全球资源，但仅在一个区域可用，则在该区域禁用该控件会阻止您获得底层资源的任何发现。在这种情况下，我们建议将控件保持启用状态。使用跨区域聚合时，可使用控件的区域应为聚合区域或链接区域之一。以下控制措施涉及全球资源，但仅适用于单个区域：

- 所有 CloudFront 控件 — 仅在美国东部（弗吉尼亚北部）可用
- GlobalAccelerator.1 — 仅在美国西部（俄勒冈州）提供
- Route53.2 — 仅在美国东部（弗吉尼亚北部）提供
- WAF.1、WAF.6、WAF.7 和 WAF.8 — 仅在美国东部（弗吉尼亚北部）上市

> **Note**
>
> 如果您使用中央配置，Security Hub 会自动禁用涉及除本地区以外的所有区域的全球资源的控件。您选择通过配置策略启用的其他控件将在所有可用区域中启用。要将这些控件的结果限制在一个区域内，您可以更新 AWS Config 记录器设置并关闭除主区域之外的所有区域的全局资源记录。当你使用中央配置时，你无法覆盖主区域和任何关联区域中不可用的控件。有关中心配置的更多信息，请参阅中央配置的工作原理。

对于具有定期计划类型的控件，需要在 Security Hub 中将其禁用以防止计费。将 AWS Config 参数设置`includeGlobalResourceTypes`为`false`不会影响定期的 Security Hub 控件。

以下是涉及全局资源的 Security Hub 控件列表：

- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移

- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应该有很长的持续时间 AWS Config
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作

- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

处理 CloudTrail 日志的控件

此控件用于使用 AWS Key Management Service (AWS KMS) 加密 AWS CloudTrail 跟踪日志。如果您将这些跟踪记录在集中日志账户中，则只需在进行集中日志记录的账户和区域中启用此控制即可。

> **Note**
>
> 如果您使用中心配置，则控件的启用状态将在主区域和关联区域之间保持一致。您无法在某些区域禁用某个控件而在其他区域启用该控件。在这种情况下，隐藏来自以下控件的调查发现以减少调查发现噪音。

- [CloudTrail.2] CloudTrail 应该启用静态加密

处理 CloudWatch 警报的控件

如果您更喜欢使用亚马逊而不是亚马逊警报 GuardDuty 进行异常检测，则可以禁用这些以 CloudWatch 警 CloudWatch 报为重点的控件。

- [CloudWatch.1] “root” 用户应有日志指标筛选器和警报

- [CloudWatch.2] 确保存在针对未经授权的 API 调用的日志指标筛选器和警报
- [CloudWatch.3] 确保在没有 MFA 的情况下登录管理控制台时存在日志指标筛选器和警报
- [CloudWatch.4] 确保存在针对 IAM 策略更改的日志指标筛选器和警报
- [CloudWatch.5] 确保存在针对 CloudTrail AWS Config持续时间变化的日志指标筛选器和警报
- [CloudWatch.6] 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报
- [CloudWatch.7] 确保存在用于禁用或计划删除客户托管密钥的日志指标筛选器和警报
- [CloudWatch.8] 确保存在针对 S3 存储桶策略更改的日志指标筛选器和警报
- [CloudWatch.9] 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报
- [CloudWatch.10] 确保存在针对安全组更改的日志指标筛选器和警报
- [CloudWatch.11] 确保存在针对网络访问控制列表 (NACL) 更改的日志指标筛选器和警报
- [CloudWatch.12] 确保存在针对网络网关更改的日志指标筛选器和警报
- [CloudWatch.13] 确保存在针对路由表更改的日志指标筛选器和警报
- [CloudWatch.14] 确保存在针对 VPC 更改的日志指标筛选器和警报

查看控件的详细信息

对于每个 AWS Security Hub 控件，您可以显示一个包含有用详细信息的页面。

控件详细信息页面的顶部提供控件概览，包括：

- 启用状态——页面顶部会告诉您是否在至少一个成员账户中为至少一个标准启用了该控件。如果您设置了聚合区域，则如果在至少一个区域中为至少一个标准启用了该控件，则该控件将被启用。如果该控件已禁用，则可以从此页面将其启用。如果该控件已启用，则可以从此页面将其禁用。有关更多信息，请参阅 the section called “在所有标准中启用和禁用控件”。
- 控件状态——此状态根据控件调查发现的合规性状态聚合控制的性能。Security Hub 通常会在您首次访问 Security Hub 控制台上的摘要页面或安全标准页面后 30 分钟内生成初始控件状态。状态仅适用于您访问这些页面时启用的控件。使用 `UpdateStandardsControl` API 操作启用或禁用控件。此外，必须配置 AWS Config 资源记录才能显示控制状态。首次生成控件状态后，Security Hub 会根据前 24 小时的调查发现每 24 小时更新一次控件状态。在标准详细信息页面和控制详细信息页面上，Security Hub 会显示时间戳以指示上次更新状态的时间。

  管理员账户可以看到管理员账户和成员账户的聚合控件状态。如果您设置了聚合区域，则控件状态包括所有关联区域的调查发现。有关控件状态的详细信息，请参阅 the section called “合规状态和控制状态”。

> **Note**
>
> 启用控件后，最长可能需要 24 小时才能在中国地区和 AWS GovCloud (US) Region生成首次控件状态。

标准和要求选项卡列出了可启用控件的标准以及来自不同合规框架的与该控件相关的要求。

详细信息页面的底部包含有关控件活动调查发现的信息。控件调查发现是通过对控件进行安全检查生成的。对照调查发现列表不包括存档的调查发现。

调查发现列表使用显示列表不同子集的选项卡。在大多数选项卡上，调查发现列表显示工作流程状态为 NEW、NOTIFIED 或 RESOLVED 的调查发现。单独的选项卡显示 SUPPRESSED 结果。

对于每项调查发现，该列表都提供对调查发现详细信息的访问权限，例如合规性状态和相关资源。您还可以设置每个调查发现的工作流程状态，并将结果发送到自定义操作。有关更多信息，请参阅 the section called “查看结果并采取操作”。

查看控件的详细信息

选择首选访问方法，然后按照以下步骤查看控件的详细信息。详细信息适用于当前账户和地区，包括以下内容：

- 控件的标题和描述
- 链接到失败的控件调查发现的补救说明
- 控制的严重性
- 控件的启用状态
- （在控制台上）控件的最新调查发现列表。使用 Security Hub API 或时 AWS CLI，使用`GetFindings`来检索控制结果。

Security Hub console

1. 打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 在导航窗格中选择控件。
3. 选择控件。

Security Hub API

1. 运行 ListSecurityControlDefinitions 并提供一个或多个标准 ARN 以获取该标准的控件 ID 列表。要获取标准 ARN，请运行 DescribeStandards。如果您不提供标准 ARN，此 API 将返回所有 Security Hub 控制 ID。此 API 返回与标准无关的安全控件 ID，而不是这些功能发布之前存在的基于标准的控件 ID。

   请求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 运行BatchGetSecurityControls以获取有关当前 AWS 账户 和中一个或多个控件的详细信息 AWS 区域。

   请求示例：

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. 运行 list-security-control-definitions 命令，并提供一个或多个标准 ARN 以获取控件 ID 列表。要获取标准 ARN，请运行 describe-standards 命令。如果您不提供标准 ARN，则此命令会返回所有 Security Hub 控件 ID。此命令返回与标准无关的安全控件 ID，而不是这些功能发布之前存在的基于标准的控件 ID。

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
   ```

2. 运行 batch-get-security-controls 命令以获取有关当前 AWS 账户 和 AWS 区域中一个或多个控件的详细信息。

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

筛选和排序控件列表

在控件页面上，您可以看到控件列表。您可以对列表进行筛选和排序，将重点放在控件的特定子集上。

- 全部启用（在至少一个启用的标准中启用的控件）
- 失败（带有 Failed 状态的控件）
- 未知（带有 Unknown 状态的控件）
- 已通过（带有 Passed 状态的控件）
- 已禁用（在所有标准中禁用的控件）
- 没有数据（没有调查发现的控件）
- 全部（所有控件，包括启用和禁用，不考虑控件状态或结果次数）

有关控件状态的详细信息，请参阅 合规状态和控制状态。

如果您正在使用与管理员帐户的集成 AWS Organizations 并登录到 AWS Security Hub 管理员帐户，则 “全部启用” 选项卡包含在至少一个成员帐户中启用的控件。如果您设置了聚合区域，则全部启用选项卡将包含在至少一个关联区域中启用的控件。

默认情况下显示已失败选项卡。默认情况下，每个选项卡上的控件按严重程度排序，从严重到低。您还可以按控件 ID、合规性状态、严重性或检查失败次数对控件进行排序。搜索栏允许您搜索特定的控件。

> **Tip**
>
> 如果您有基于控件调查发现的自动化工作流程，我们建议使用 SecurityControlId 或 SecurityControlArn ASFF 字段作为筛选条件，而不是 Title 或 Description。后面的字段偶尔会发生变化，而控件 ID 和 ARN 是静态标识符。

选择控件旁边的选项会弹出一个侧面板，显示当前启用该控件的标准。您还可以查看当前禁用该控件的标准。在此面板中，您可以通过在所有标准中禁用控件来禁用该控件。有关启用和禁用各类标准控件的更多信息，请参阅 在所有标准中启用和禁用控件。对于管理员账户，侧面板中显示的信息反映了所有成员账户。

在 Security Hub API 上，运行 `ListSecurityControlDefinitions` 以获取控件 ID 列表。获得感兴趣的控件 ID 后，运行`BatchGetSecurityControls`以获取有关当前 AWS 账户 和控件子集的数据 AWS 区域。

查看结果并采取操作

控件详细信息页面显示控件的活动调查发现列表。该列表不包括已存档的调查发现。

控件详细信息页面支持调查发现聚合。如果您设置了聚合区域，则控件详细信息页面上的控件状态和安全检查列表将包括来自所有链接的 AWS 区域检查。

该列表提供了对结果进行筛选和排序的工具，这样您就可以先将注意力集中在更紧急的发现上。调查发现可能包含指向相关服务控制台中资源详细信息的链接。对于基于 AWS Config 规则的控件，您可以查看有关规则和配置时间表的详细信息。

您还可以使用 AWS Security Hub API 来检索发现结果列表。有关更多信息，请参阅 the section called “查看发现详情”。

主题

- 查看有关控件调查发现和调查发现资源的详细信息
- 控件调查发现样本
- 筛选、排序和下载控件调查发现
- 对控件调查发现采取操作

查看有关控件调查发现和调查发现资源的详细信息

AWS Security Hub 提供了每项对照发现的以下详细信息，以帮助您进行调查：

- 用户对调查发现所做更改的历史记录
- 调查发现的 `.json` 文件
- 与调查发现相关的资源信息
- 与调查发现相关的配置规则
- 用户已在调查发现中添加的注意事项

以下部分介绍如何访问这些详细信息。

调查发现历史记录

调查发现历史记录是 Security Hub 的一项功能，可让您跟踪过去 90 天内对调查发现所做的更改。

调查发现历史记录可用于控件调查发现和其他 Security Hub 发现。有关更多信息，请参阅 查看发现历史记录。

查看完整的 .json 以获取调查发现

您可以显示和下载调查发现的完整 `.json`。

要显示 `.json`，请在调查发现.json 列中选择图标。

在调查发现 JSON 面板上，要下载 `.json`，请选择下载。

查看有关调查发现资源的信息

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。对于 AWS 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，信息仅包括账户 ID。

如果您有权查看原始服务中的资源，则资源标识符会显示指向该服务的链接。例如，对于 AWS 用户，资源详细信息提供了在 IAM 中查看用户详细信息的链接。

如果资源位于其他账户中，Security Hub 会显示一条消息通知您。

查看调查发现资源的配置时间表

一种调查途径是 AWS Config中资源的配置时间表。

如果您有权查看调查发现资源的配置时间表，则调查发现列表会提供指向该时间轴的链接。

如果资源在不同的账户中，Security Hub 会显示一条消息通知您。

要在中导航到配置时间表 AWS Config

1. 在调查列中，选择图标。
2. 在菜单上，选择配置时间轴。如果您无权访问配置时间线，则不会显示该链接。

查看查找资源的 AWS Config 规则

如果控件基于 AWS Config 规则，则您可能还需要查看该 AWS Config 规则的详细信息。 AWS 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。

如果您有权查看控件的 AWS Config 规则，则查找结果列表会提供指向中该 AWS Config 规则的链接 AWS Config。

如果资源在不同的账户中，Security Hub 会显示一条消息通知您。

导航到 AWS Config 规则

1. 在调查列中，选择图标。
2. 在菜单上，选择 Config 规则。如果您无权访问该 AWS Config 规则，则不会关联 Config 规则。

查看调查发现的注释

如果调查发现关联了附注，则已更新列会显示一个附注图标。

显示与调查发现关联的注释

在已更新列中，选择备注图标。

控件调查发现样本

控件调查发现的格式会有所不同，具体取决于您是否开启了整合的控件调查发现。当您打开此功能时，即使该控件适用于多个启用的标准，Security Hub 也会生成一个用于控件检查的调查发现。有关更多信息，请参阅 整合的控件调查发现。

以下章节展示了控件调查发现样本。其中包括在您的账户中关闭整合的控件调查发现时每个 Security Hub 标准的调查发现，以及启用该标准时各类标准的样本控件调查发现。

> **Note**
>
> 结果将参考中国地区和 AWS GovCloud (US) 地区的不同字段和值。有关更多信息，请参阅 合并对 ASFF 字段和值的影响。

整合的控件调查发现已关闭

- AWS 基础安全最佳实践 (FSBP) 标准的调查结果示例
- 互联网安全中心 (CIS) AWS 基金会基准测试版本 1.2.0 的样本发现
- 互联网安全中心 (CIS) AWS 基金会基准测试 v1.4.0 的样本发现
- 互联网安全中心 (CIS) AWS 基金会基准测试 v3.0.0 的样本发现

- 美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5 的调查发现样本
- 支付卡行业数据安全标准 (PCI DSS) 的调查发现样本
- AWS 资源标签标准的调查结果示例
- 服务托管标准的调查结果示例： AWS Control Tower

已开启整合的控件调查发现

- 各类标准的调查发现样本

FSBP 的调查发现样本


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
```

```
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

CIS AWS 基金会基准测试 v3.0.0 的样本发现

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
```

```
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
```

```
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```


CIS AWS 基金会基准测试 v1.4.0 的样本发现


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
```

```
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

CIS AWS 基金会基准测试 v1.2.0 的样本发现

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
```

```
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

NIST SP 800-53 Rev. 5 的调查发现样本

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
```

```
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
```

```
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

PCI DSS 的调查发现样本

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
```

```
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
```

```
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

AWS 资源标签标准的调查结果示例

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
```

```
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
```

```
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
```

```
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

服务托管标准的调查结果示例： AWS Control Tower

> **Note**
>
> 只有当您是在中创建该标准的 AWS Control Tower 用户时，您才可以使用该标准 AWS Control Tower。有关更多信息，请参阅 服务管理标准： AWS Control Tower。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
```

```
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
```

```
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

各类调查发现样本标准（启用整合的控件调查发现时）

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
```

```
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
       { "StandardsId": "standards/pci-dss/v/3.2.1"},
       { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
       { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
       { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    ]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

筛选、排序和下载控件调查发现

您可以使用筛选选项卡根据合规性状态筛选控件调查发现列表。您也可以根据其他调查发现字段值筛选列表，并从列表中下载调查发现。

对控件调查发现列表进行筛选和排序

所有检查选项卡列出了工作流程状态为 NEW、NOTIFIED 或 RESOLVED 的所有有效结果。默认情况下，列表进行排序，以便将失败的调查发现排在列表顶部。这种排序顺序可以帮助您确定需要解决的调查发现的优先顺序。

失败、未知和已通过选项卡上的列表根据 Compliance.Status 的值进行筛选。这些列表还仅包括工作流程状态为 NEW、NOTIFIED 或 RESOLVED 的活动调查发现。

已隐藏选项卡包含工作流程状态为 SUPPRESSED 的活动调查发现列表。

除了每个选项卡上的内置筛选条件外，您还可以使用以下字段中的值来筛选列表：

- 帐户 ID
- 工作流状态
- 合规性状态
- 资源 ID
- 资源类型

您可以使用任何列对每个列表进行排序。

下载控件调查发现清单

如果您导航到安全标准并选择标准，则会看到该标准的控件列表。从列表中选择控件会将您带到控件详细信息页面，其中包含该控件的发现结果列表。从这里，您可以将控件调查发现下载到 .csv 文件中。

如果您筛选调查发现列表，则下载内容仅包含与筛选条件匹配的控件。

如果您从列表中选择特定的调查发现，则下载内容仅包含选定的调查发现。

要下载结果，请选择下载。已下载当前调查结果页面。

对控件调查发现采取操作

为了反映调查的当前状态，您可以设置工作流程状态。有关更多信息，请参阅 the section called “设置调查发现的工作流程状态”。

在中 AWS Security Hub，您还可以将选定的调查结果发送给 Amazon 中的自定义操作 EventBridge。有关更多信息，请参阅 the section called “将结果发送到自定义操作”。

使用摘要控制面板

在 AWS Security Hub 控制台上，摘要页面上的控制面板可以帮助您识别 AWS 环境中存在安全问题的区域，而无需额外的分析工具或复杂的查询。您可以自定义控制面板布局、添加或删除小组件以及筛选数据，从而聚焦特别感兴趣的领域。您还可以将筛选条件保存为筛选器集，以便将来快速检索特定类型的数据。

如果您自定义了控制面板或筛选数据，Security Hub 会自动保存您的设置以供日后使用。此外，您的 Security Hub 账户将为每个用户单独保存这些设置。这意味着不同的用户可以为控制面板设置不同的布局、小组件和筛选器集。

每次打开摘要控制面板时，Security Hub 都会自动刷新大部分控制面板数据。但是，有些数据的更新频率较低。例如，安全评分和控件状态每 24 小时更新一次。

如果您为 Security Hub 配置了跨区域聚合区域，则控制面板数据将包括来自聚合区域和所有关联区域的调查发现。如果您是组织委派的 Security Hub 管理员，则数据包括您的管理员账户和成员账户的调查发现。您可选择按账户筛选数据。如果您有成员账户或独立账户，则数据仅包含您的账户的调查发现。

摘要控制面板的可用小组件

摘要控制面板包含了反映现代云安全威胁情形的小组件，以 AWS 客户的安全运营和体验为指导。有些小组件是默认显示的，而另一些则不是。您可以通过添加或删除小组件来自定义控制面板视图。

要添加小组件，请选择摘要页面右上角的添加小组件。在搜索栏中，输入小组件的标题。将小组件拖放到控制面板上。

默认显示的小组件

默认情况下，摘要控制面板包含以下小组件：

安全标准

显示您最新的摘要安全分数以及每项 Security Hub 标准的安全分数。安全分数（介于 0-100% 之间）表示已通过控件与所有已启用控件的比例。有关这些资源的更多信息，请参阅安全评分是如何计算的。此小组件可帮助您了解自己的整体安全状况。

具有最多调查发现的资产

概述具有最多调查发现的资源、账户和应用程序。该列表按调查发现的数量降序排序。在小组件中，按严重性和资源类型分组，每个选项卡显示该类别中排名前六的项目。如果您在调查发现总

数列中选择一个数字，Security Hub 会打开显示资产调查发现的页面。此小组件可帮助您快速识别哪些核心资产存在潜在的安全威胁。

按地区划分的调查发现

按严重性分组，显示每个启用了 Security Hub 的 AWS 区域 中的调查发现总数。此小组件可帮助您识别可能影响特定区域的安全问题。如果您在聚合区域中打开控制面板，则此小组件可帮助您监控每个关联区域中的潜在安全问题。

最常见的威胁类型

详细列出您的 AWS 环境中最常见的 10 种威胁类型。包括权限升级、使用公开的凭证或与恶意 IP 地址通信等威胁。

要查看这些数据，必须启用 Amazon GuardDuty。如果已启用，请在此小组件中选择一种威胁类型，打开 GuardDuty 控制台并查看与此威胁相关的调查发现。此小组件可帮助您评估其他安全问题背景下的潜在威胁。

已被利用的软件漏洞

提供 AWS 环境中已知已被利用的软件漏洞的摘要。您还可以查看有可用修复程序和没有可用修复程序的漏洞明细。

要查看这些数据，必须启用 Amazon Inspector。如果已启用，请在此小组件中选择一项统计数据，打开 Amazon Inspector 控制台并查看有关该漏洞的更多详细信息。此小组件可帮助您在其他安全问题背景下评估软件漏洞。

随着时间推移而出现的新调查发现

显示过去 90 天内每日新调查发现数量的趋势。您可以按严重性或按提供程序对数据进行细分，以获取更多背景信息。此小组件可帮助您了解在过去 90 天中的特定时间内，调查发现数量是激增还是下降。

具有最多调查发现的资源

提供按以下资源类型进行细分，具有最多调查发现的资源摘要：Amazon Simple Storage Service（Amazon S3）存储桶、Amazon Elastic Compute Cloud（Amazon EC2）实例和 AWS Lambda 函数。

在小组件中，每个选项卡都侧重于上述某个资源类型，列出了调查发现最多的 10 个资源实例。要查看特定资源的调查发现，请选择该资源实例。此小组件可帮助您对与常用 AWS 资源相关的安全调查发现进行分类。

默认隐藏的小组件

以下小组件也可用于摘要控制面板，但默认情况下处于隐藏状态：

具有最多调查发现的 AMI

提供生成调查发现最多的 10 个亚马逊机器映像（AMI）的列表。仅当您的账户启用了 Amazon EC2 时，这一数据才可用。它可以帮助您识别哪些 AMI 会带来潜在的安全风险。

调查发现最多的 IAM 主体

提供生成调查发现最多的 10 个 AWS Identity and Access Management（IAM）用户的列表。此小组件可帮助您执行管理和计费任务。它会显示那些使用 Security Hub 最多的用户。

调查发现最多的账户（按严重性分类）

显示生成调查发现最多的 10 个账户的图表，并按严重性分组。此小组件可帮助您确定要重点分析和修复哪些账户。

调查发现最多的账户（按资源类型分类）

显示生成调查发现最多的 10 个账户的图表，并按资源类型分组。此小组件可帮助您确定要优先分析和修复哪些账户和资源类型。

洞察

列出了五个 Security Hub 托管见解及其生成的调查发现数量。洞察力确定了需要关注的特定安全领域。

AWS 集成的最新调查发现

显示您在 Security Hub 中从集成 AWS 服务 中收到的调查发现数量。它还会显示您最近一次从每项集成服务中收到调查发现的时间。此小组件提供来自多个 AWS 服务 的调查发现整合数据。要深入了解，请选择集成服务。然后，Security Hub 会打开该服务的控制台。

筛选摘要控制面板

要在摘要控制面板上整理数据并仅包含与自己最相关的安全数据，您可以筛选控制面板。例如，如果您是某个应用程序团队的成员，则可以为生产环境中的关键应用程序创建专用视图。如果您是某个安全团队的成员，则可以创建一个专用视图，帮助自己专注于高严重性的调查发现。要筛选摘要控制面板上的数据，请在控制面板上方的筛选框中输入筛选条件。您应用筛选条件后，则该条件会应用于控制面板上的所有数据，但洞察和安全标准小组件中的数据除外。

您可以使用以下字段筛选数据。

- 账户名称
- 账户 ID
- 应用程序 Amazon 资源名称（ARN）
- 应用程序名称
- 产品名称（将调查发现发送到 Security Hub 的 AWS 服务 或第三方产品的名称）
- Record state
- 区域
- 资源标签
- 严重性
- 工作流状态

默认情况下，使用以下条件筛选控制面板数据：`Workflow status` 为 `NOTIFIED` 或 `NEW`、以及 `Record state` 为 `ACTIVE`。这些条件显示在控制面板上方，筛选框下方。要删除这些条件，请在要删除的条件筛选令牌中选择 X。

如果您应用了想再次使用的筛选条件，则可以将其另存为筛选器集。筛选器集是一组筛选标准，您可以创建并保存这些筛选标准，以便您在摘要控制面板上查看数据时重新应用。

> **Note**
>
> 以下字段无法保存为筛选器集的一部分：应用程序 ARN、应用程序名称和资源标签。

创建和保存筛选器集

要创建和保存筛选器集，请执行下列步骤。

要创建和保存筛选器集

1. 访问 https://console.aws.amazon.com/securityhub/，打开 AWS Security Hub 控制台。
2. 在导航窗格中，选择摘要。
3. 在摘要控制面板上方的筛选框中，为筛选器集输入筛选条件。
4. 在清除筛选条件菜单上，选择保存新筛选器集。
5. 在保存筛选器集对话框中，输入筛选器集的名称。

6. （可选）要在每次打开摘要页面时使用默认设置的筛选器集，请选择将其设置为默认视图的选项。
7. 选择 Save（保存）。

要在已创建和保存的筛选器集之间切换，请使用摘要控制面板上方的选择筛选器集菜单。当您选择筛选器集时，Security Hub 会将筛选器集的条件应用于控制面板上的数据。

更新或删除筛选器集

请按照以下步骤更新或删除现有筛选器集。如果您删除当前设置为摘要控制面板默认视图的筛选器集，则默认视图将重置为默认 Security Hub 视图。

要更新或删除筛选器集

1. 访问 https://console.aws.amazon.com/securityhub/，打开 AWS Security Hub 控制台。
2. 在导航窗格中，选择摘要。
3. 在摘要页面上方的选择筛选器集菜单中，选择筛选器集。
4. 在清除筛选条件菜单上，执行以下操作之一：
   - 要更新筛选器集，请选择更新当前筛选器集。然后在出现的对话框中输入您的更改。
   - 要删除筛选器集，请选择删除当前筛选器集。然后在出现的对话框中选择删除。

自定义摘要控制面板

您可以通过多种方式自定义摘要控制面板。您可以在控制面板中添加和删除小组件。您还可以在控制面板上重新排列小组件并调整其大小。

如果您自定义控制面板，Security Hub 会立即应用您的更改并保存新的控制面板设置。您的更改将应用于所有 AWS 区域 和浏览器中的控制面板视图。

要自定义摘要控制面板

1. 访问 https://console.aws.amazon.com/securityhub/，打开 AWS Security Hub 控制台。
2. 在导航窗格中，选择摘要。
3. 执行以下任一操作：
   - 要添加小组件，请选择页面右上角的添加小组件。在搜索栏中，输入要添加的小组件的标题。然后，将小组件拖到所需位置。

- 要删除小组件，请选择小组件右上角的三个点。
- 要移动小组件，请选择小组件左上角的图柄，然后将小组件拖到所需位置。
- 要更改小组件的大小，请选择小组件右下角的大小调整图柄。拖动小组件的边缘，使其达到您想要的大小。

要随后恢复原始设置，请选择页面顶部的重置为默认布局。

使用 AWS CloudFormation创建 Security Hub 资源

AWS Security Hub 与集成 AWS CloudFormation，这是一项可帮助您对 AWS 资源进行建模和设置的服务，这样您就可以减少创建和管理资源和基础架构所花费的时间。您可以创建一个描述所需的所有 AWS 资源（例如自动化规则）的模板，并为您 AWS CloudFormation 预置和配置这些资源。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置 Security Hub 资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中一遍又一遍地配置相同的资源。

Security Hub 和 AWS CloudFormation 模板

要为 Security Hub 和相关服务预置和配置资源，您必须了解 AWS CloudFormation 模板的工作原理。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。

如果你不熟悉 JSON 或 YAML，可以使用 D AWS CloudFormation esigner 来帮助你开始使用 AWS CloudFormation 模板。有关更多信息，请参阅什么是 AWS CloudFormation 设计器？ 在《AWS CloudFormation 用户指南》中。

您可以为以下类型的 Security Hub 资源创建 AWS CloudFormation 模板：

- 启用 Security Hub
- 为组织指定委派的 Security Hub 管理员
- 启用安全标准
- 创建自定义见解
- 创建自动化规则
- 订阅第三方产品集成

有关更多信息（包括资源的 JSON 和 YAML 模板示例），请参阅 AWS CloudFormation 用户指南中的 AWS Security Hub 资源类型参考。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation

- AWS CloudFormation 用户指南
- AWS CloudFormation API 引用
- AWS CloudFormation 命令行界面用户指南

使用 Amazon Simple Notification Service 订阅 Security Hub 公告

本节提供有关通过 Amazon Simple Notification Service (Amazon SNS)订阅AWS Security Hub 公告以接收 Security Hub 通知的信息。

订阅后，您将收到有关以下事件的通知（请注意每个事件相应的 `AnnouncementType`）：

- `GENERAL`：有关 Security Hub 服务的常规通知。
- `UPCOMING_STANDARDS_CONTROLS`：特定的 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 AWS 区域 中提供了对 Security Hub 的支持。
- `NEW_STANDARDS_CONTROLS`：添加了新的 Security Hub 控件或标准。
- `UPDATED_STANDARDS_CONTROLS`：现有的 Security Hub 控件或标准已更新。
- `RETIRED_STANDARDS_CONTROLS`：现有的 Security Hub 控件或标准已停用。
- `UPDATED_ASFF`：AWS 安全调查发现格式 (ASFF) 语法、字段或值已更新。
- `NEW_INTEGRATION`：提供了与其他AWS服务或第三方产品的新集成。
- `NEW_FEATURE`：新的 Security Hub 功能可用。
- `UPDATED_FEATURE`：现有的 Security Hub 功能已更新。

通知以 Amazon SNS 支持的所有格式提供。您可以在 Security Hub 可用的所有 AWS 区域 中订阅 Security Hub 公告。

用户必须拥有 `Subscribe` 权限才能订阅 Amazon SNS 主题。您可以通过 Amazon SNS 策略、IAM policy 或两者来实现这一目标。有关更多信息，请参阅 Amazon Simple Notification Service 开发者指南中的 IAM 和 Amazon SNS 策略。

> **Note**
>
> Security Hub 会向任何 AWS 账户 订阅者发送有关 Security Hub 服务更新的 Amazon SNS 公告。要接收有关 Security Hub 调查发现的通知，请参阅 管理和查看查找结果的详细信息和历史记录。

您可以为 Amazon SNS 主题订阅 Amazon Simple Queue Service (Amazon SQS) 队列，但必须使用同一区域内的 Amazon SNS 主题 Amazon 资源名称（ARN）。有关更多信息，请参阅 Amazon Simple Queue Service 开发人员指南中的教程：为 Amazon SQS 队列订阅 Amazon SNS 主题。

您也可以使用 AWS Lambda 函数在收到通知时调用事件。有关更多信息，包括示例函数代码，请参阅《AWS Lambda 开发者指南》中的教程：一起使用 AWS Lambda 与 Amazon Simple Notification Service。

每个区域的 Amazon SNS 主题 ARN 如下所示。

AWS 区域	Amazon SNS 主题 ARN
美国东部（俄亥俄）	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
美国东部（弗吉尼亚州北部）	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
美国西部（北加利福尼亚）	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
美国西部（俄勒冈州）	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
非洲（开普敦）	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
亚太地区（香港）	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
亚太地区（海得拉巴）	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`

AWS 区域	Amazon SNS 主题 ARN
亚太地区（雅加达）	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
Asia Pacific (Mumbai)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
亚太地区（大阪）	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
亚太地区（首尔）	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
亚太地区（新加坡）	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
亚太地区（悉尼）	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements
亚太地区（东京）	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
加拿大（中部）	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
中国（北京）	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements

AWS 区域	Amazon SNS 主题 ARN
中国（宁夏）	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
欧洲地区（法兰克福）	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
欧洲地区（爱尔兰）	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
欧洲地区（伦敦）	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
欧洲地区（米兰）	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
欧洲地区（巴黎）	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
欧洲（西班牙）	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
欧洲地区（斯德哥尔摩）	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
欧洲（苏黎世）	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements

AWS 区域	Amazon SNS 主题 ARN
以色列（特拉维夫）	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
中东（巴林）	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
中东（阿联酋）	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
南美洲（圣保罗）	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud（美国东部）	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud（美国西部）	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

分区内各区域的消息通常相同，因此您可以订阅每个分区中的一个区域，以接收影响该分区中所有区域的公告。与成员账户关联的公告不会复制到管理员账户中。因此，每个账户（包括管理员账户）将只有一份每份公告的副本。您可以决定要使用哪个账户来订阅 Security Hub 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 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在“区域”列表中，选择要在其中订阅 Security Hub 公告的区域。此示例使用`us-west-2`区域。
3. 在导航窗格中，选择订阅，然后选择创建订阅。

4. 在主题 ARN 框中，输入主题 ARN。例如，arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements。
5. 在协议中，选择您希望如何接收 Security Hub 公告。如果您选择电子邮件，请在端点中输入要用于接收公告的电子邮件地址。
6. 选择创建订阅。
7. 确认订阅。例如，如果您选择电子邮件协议，Amazon SNS 会向您提供的电子邮件发送一条订阅确认消息。

订阅 Security Hub 公告（AWS CLI）

1. 运行以下命令：

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. 确认订阅。例如，如果您选择电子邮件协议，Amazon SNS 会向您提供的电子邮件发送一条订阅确认消息。

Amazon SNS 消息格式

以下示例显示了 Amazon SNS 发布的关于引入新安全控制措施的 Security Hub 公告。消息内容因公告类型而异，但所有公告类型的格式都相同。可选择包含一个 Link 字段，提供有关公告的详细信息。

示例：Security Hub 关于新控件的公告（电子邮件协议）

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
```

```
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

示例：Security Hub 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 AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured 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" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
```

```
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

AWS Security Hub 中的安全性

AWS 十分重视云安全性。作为 AWS 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 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 AWS Security Hub 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括数据的敏感性、公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Security Hub 时应用责任共担模型 以下主题说明如何配置 Security Hub 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Security Hub 资源。

主题

AWS Security Hub 中的数据保护

AWS 责任共担模式适用于 AWS Security Hub 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 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。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得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数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 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 Amazon S3 中的敏感数据。
- 如果您在通过命令行界面或 API 访问 AWS 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（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API、AWS CLI 或 AWS SDK 处理 Security Hub 或其他 AWS 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，我们强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

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

AWS Identity and Access Management AWS Security Hub

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Security Hub 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- AWS Sec AWS urity Hub 的托管策略
- 对 AWS Security Hub 身份和访问进行故障排除

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Security Hub 中所做的工作。

服务用户 - 如果您使用 Security Hub 服务来完成工作，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，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Security Hub 中的某项功能，请参阅 对 AWS Security Hub 身份和访问进行故障排除。

服务管理员 - 如果您在公司负责管理 Security Hub 资源，则您可能具有 Security Hub 的完全访问权限。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 如何 AWS Security Hub 与 IAM 配合使用。

IAM 管理员 - 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Security Hub 的访问的详细信息。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 Security Hub 基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 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《AWS IAM Identity Center 用户指南》中的 多重身份验证和《IAM 用户指南》中的 在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。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《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，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，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员或应用程序关联，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

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。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：

- 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的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 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。
- 跨账户存取 – 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，对于某些资源 AWS 服务，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 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。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。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 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分派的 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 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 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 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向

EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该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

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。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 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM 策略定义操作的权限，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。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS 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策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。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 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资

源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持其他不太常见的策略类型。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特征，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，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。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 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS 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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Security Hub 与 IAM 配合使用

在使用 AWS Identity and Access Management (IAM) 管理访问权限之前 AWS Security Hub，请先了解哪些 IAM 功能可用于 Security Hub。

您可以搭配使用的 IAM 功能 AWS Security Hub

IAM 功能	Security Hub 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	否
策略条件键	是
访问控制列表 (ACL)	否
基于属性的访问控制 (ABAC) – 策略中的标签	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
服务相关角色	是

有关 Security Hub 和其他 AWS 服务 功能如何与大多数 IAM 功能配合使用的高级视图 AWS 服务 ，请参阅 IAM 用户指南中的如何与 IAM 配合使用。

Security Hub 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

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。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Security Hub 支持基于身份的策略。有关更多信息，请参阅 Security Hub 基于身份的策略示例。

Security Hub 基于资源=的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 IAM 用户指南中的跨账户在 IAM 中访问资源。

Security Hub 不支持基于资源的策略。您不能将 IAM 策略直接附加到 Security Hub 资源。

Security Hub 的策略操作

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS 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关联操作的权限。

Security Hub 中的策略操作在操作前使用以下前缀：

```
securityhub:
```

例如，要向用户授予启用 Security Hub（该操作与 Security Hub API 的EnableSecurityHub操作相对应的操作）的权限，请将该securityhub:EnableSecurityHub操作包含在他们的策略中。策略语句必须包含 Action 或 NotAction 元素。Security Hub 定义了一组自己的操作，以描述您可以使用该服务执行的任务。

```
"Action": "securityhub:EnableSecurityHub"
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。例如：

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 Get 开头的所有操作，包括以下操作：

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

但作为最佳实践，您应创建遵循最低权限 原则的策略。换句话说，您应创建仅包含执行特定任务所需的权限的策略。

用户必须具有DescribeStandardsControl操作访问权限才能访问BatchGetSecurityControlsBatchGetStandardsControlAssociations、和ListStandardsControlAssociations。

用户必须具有UpdateStandardsControls操作访问权限才能访问BatchUpdateStandardsControlAssociations、和UpdateSecurityControl。

有关 Securit y Hub 操作的列表，请参阅《服务授权参考》 AWS Security Hub中定义的操作。有关指定 Security Hub 操作的策略示例，请参阅Security Hub 基于身份的策略示例。

资源

支持策略资源	否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (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": "*"
```

Security Hub 定义了以下资源类型：

- 中心
- 产品
- 查找聚合器，也称为跨区域聚合器
- 自动化规则
- 配置策略

您可以通过使用 ARN 在政策中指定这些类型的资源。

有关 Security Hub 资源类型列表以及每种资源类型的 ARN 语法，请参阅《服务授权参考》 AWS Security Hub中定义的资源类型。要了解您可以为每种类型的资源指定哪些操作，请参阅《服务授权参考》 AWS Security Hub中定义的操作。有关指定资源的策略示例，请参阅 Security Hub 基于身份的策略示例。

Security Hub 的策略条件密钥

支持特定于服务的策略条件键	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

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 AWS 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，则使用逻辑OR运算来 AWS 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。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

有关 Security Hub 条件键的列表，请参阅《服务授权参考》 AWS Security Hub中的条件密钥。要了解可以将条件键与哪些操作和资源一起使用，请参阅由定义的操作 AWS Security Hub。有关使用条件密钥的策略示例，请参阅 Security Hub 基于身份的策略示例。

Security Hub 中的访问控制列表 (ACL)

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Security Hub 不支持 ACL，这意味着您无法将 ACL 附加到 Security Hub 资源。

使用 Security Hub 实现基于属性的访问控制 (ABAC)

支持 ABAC（策略中的标签）	是

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

您可以将标签附加到 Security Hub 资源。您还可以通过在策略Condition元素中提供标签信息来控制对资源的访问权限。

有关为 Security Hub 资源添加标签的信息，请参阅标记 AWS Security Hub 资源。有关基于标签控制资源访问权的基于身份的策略示例，请参阅Security Hub 基于身份的策略示例。

将临时凭证与 Security Hub 一起使用

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 AWS STS API 操作来获取临时安全证书GetFederationToken。

Security Hub 支持使用临时证书。

转发 Security Hub 的访问会话

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

例如， AWS 服务 当你将 Security Hub 与 Organiations 中的组织集成 AWS Organizations 以及为组织中的组织指定委派的 Security Hub 管理员帐户时，Security Hub 会向下游发出 FAS 请求。

对于其他任务，Security Hub 使用服务相关角色代表您执行操作。有关此角色的详细信息，请参阅Security Hub 的服务相关角色。

Security Hub 的服务角色

Security Hub 不担任或使用服务角色。为了代表您执行操作，Security Hub 使用服务相关角色。有关此角色的详细信息，请参阅Security Hub 的服务相关角色。

> **Warning**
>
> 更改服务角色的权限可能会给您使用 Security Hub 带来操作问题。仅当 Security Hub 提供相关指导时才编辑服务角色。

Security Hub 的服务相关角色

支持服务相关角色	是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Security Hub 使用服务相关角色代表您执行操作。有关此角色的详细信息，请参阅Security Hub 的服务相关角色。

Security Hub 基于身份的策略示例

默认情况下，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 AWS Management Console、AWS CLI 或 AWS API 执行任务。管理员必须创建 IAM policy，以便为用户和

角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的在 JSON 选项卡上创建策略。

主题

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Security Hub 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- AWS 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 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户中找到这些策略。建议通过定义特定于您的使用场景的 AWS 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 AWS 托管策略 或 工作职能的 AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 AWS 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 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，有助于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) – 如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。要在调用 API 操作时要求 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 AWS 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的 AWS 账户 中的 Security Hub 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

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

为确保这些用户和角色可以使用 Security Hub 控制台，还要将以下AWS托管策略附加到该实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

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

示例：允许用户查看自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联策略和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

示例：允许用户创建和管理配置策略

此示例说明如何创建允许用户创建、查看、更新和删除配置策略的 IAM 策略。此示例策略还允许用户启动、停止和查看策略关联。要使此 IAM 策略发挥作用，用户必须是组织委派的 Security Hub 管理员。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

示例：允许用户查看调查结果

此示例说明如何创建允许用户查看 Security Hub 发现结果的 IAM 策略。

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

示例：允许用户创建和管理自动化规则

此示例说明如何创建允许用户创建、查看、更新和删除 Security Hub 自动化规则的 IAM 策略。要使此 IAM 策略发挥作用，用户必须是 Security Hub 管理员。要限制权限（例如，仅允许用户查看自动化规则），您可以移除创建、更新和删除权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Security Hub 的服务相关角色

AWS Security Hub使用名AWSServiceRoleForSecurityHub为的 AWS Identity and Access Management (IAM) 服务相关角色。此服务相关角色是一个 IAM 角色，直接链接到 Security Hub。它由 Security Hub 预定义，它包括 Security Hub 代表你调用其他资源AWS 服务和监控AWS资源所需的所有权限。Security Hub 在所有可用 Security Hub AWS 区域 的地方都使用此服务相关角色。

您可以使用服务相关角色轻松设置 Security Hub，因为您不必手动添加所需的权限。Security Hub 定义其服务相关角色的权限，除非另有定义权限，否则只有 Security Hub 可以承担该角色。定义的权限包括信任策略和权限策略，您不能将该权限策略附加到任何其他 IAM 实体。

要查看服务相关角色的详细信息，请在 Security Hub 控制台的设置页面上，选择常规，然后选择查看服务权限。

您必须首先在启用了 Security Hub 的所有区域中禁用它，然后才能删除 Security Hub 服务相关角色。这会保护您的 Security Hub 资源，因为您不会无意中删除这些资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅 IAM 用户指南中与 IAM 配合使用的 AWS 服务，并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

主题

Security Hub 的服务相关角色权限

Security Hub 使用名为 AWSServiceRoleForSecurityHub 的服务相关角色。这是 AWS Security Hub 访问您资源所需的服务相关角色。服务相关角色允许 Security Hub 接收其他 AWS 服务 的调查发现，并配置必要的 AWS Config 基础架构以使控件运行安全检查。

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

- securityhub.amazonaws.com

AWSServiceRoleForSecurityHub 服务相关角色使用托管策略 AWSSecurityHubServiceRolePolicy。

必须授予权限，允许 IAM 身份（如角色、组或用户）创建、编辑或删除服务相关角色。为了成功创建 AWSServiceRoleForSecurityHub 服务相关角色，用于访问 Security Hub 的 IAM 身份必须具有所需的权限。要授予所需的权限，请将以下策略附加到此角色、组或用户。

```
{
    "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

在您首次启用 Security Hub 时，或者在以前未启用 Security Hub 的支持区域中启用它时，将自动创建 `AWSServiceRoleForSecurityHub` 服务相关角色。您还可以使用 IAM 控制台、IAM API 或 IAM API 创建 `AWSServiceRoleForSecurityHub` 服务相关角色。

> **Important**
>
> 为 Security Hub 管理员账户创建的服务相关角色，不适用于 Security Hub 成员账户。

有关手动创建角色的更多信息，请参阅 IAM 用户指南中的创建服务相关角色。

为 Security Hub 编辑服务相关角色

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。

为 Security Hub 删除服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，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**
>
> 要删除 `AWSServiceRoleForSecurityHub` 服务相关角色，您必须先在启用了 Security Hub 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 Security Hub。

禁用 Security Hub 时，`AWSServiceRoleForSecurityHub` 服务相关角色不会自动删除。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。

AWS Sec AWS urity Hub 的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：AWSSecurityHubFullAccess

您可以将 AWSSecurityHubFullAccess 策略附加到 IAM 身份。

此策略授予管理权限，允许主体完全访问所有 Security Hub 操作。在主体为其账户手动启用 Security Hub 之前，必须将此策略附加到主体。例如，拥有这些权限的主体可以查看和更新调查发现的状态。他们可以配置自定义见解并启用集成。他们可以启用和禁用标准和控件。管理员账户的主体也可以管理成员账户。

权限详细信息

该策略包含以下权限。

- securityhub：允许主体访问所有 Security Hub 操作。
- guardduty— 允许委托人在 Amazon GuardDuty 中获取有关账户状态的信息。
- iam：允许主体创建服务相关角色。
- inspector：允许主体在 Amazon Inspector 中获取有关账户状态的信息。
- pricing— 允许校长获取 AWS 服务 和产品的价目表。

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

```
        {
            "Sid": "SecurityHubAllowAll",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*",
        }
    ]
}
```

Security Hub 托管式策略：AWSSecurityHubReadOnlyAccess

您可以将 AWSSecurityHubReadOnlyAccess 策略附加到 IAM 身份。

此策略授予只读权限，允许用户查看 Security Hub 中的信息。附加了此策略的主体无法在 Security Hub 中进行任何更新。例如，拥有这些权限的主体可以查看与其账户关联的调查发现列表，但不能改变调查发现的状态。他们可以查看见解的结果，但不能创建或配置自定义见解。他们无法配置控件或产品集成。

权限详细信息

该策略包含以下权限。

- securityhub：允许用户执行返回项目列表或项目详细信息的操作。这包括以Get、List 或 Describe 开头的 API 操作。

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

AWS 托管策略：AWSSecurityHubOrganizationsAccess

您可以将 AWSSecurityHubOrganizationsAccess 策略附加到 IAM 身份。

此策略授予支持 Securit AWS Organizations y Hub 与 Organizations 集成所需的管理权限。

这些权限允许组织管理账户为 Security Hub 指定委派的管理员账户。它们还允许委托的 Security Hub 管理员账户将组织账户启用为成员账户。

此策略仅为 Organizations 提供权限。组织管理账户和委派的 Security Hub 管理员账户还需要在 Security Hub 中执行相关操作的权限。这些权限可以使用 AWSSecurityHubFullAccess 管理策略来授予。

权限详细信息

该策略包含以下权限。

- organizations:ListAccounts：允许主体检索属于某个组织的账户列表。
- organizations:DescribeOrganization：允许主体检索有关组织的信息。
- organizations:ListRoots：允许主体列出组织的根。
- organizations:ListDelegatedAdministrators：允许主体列出组织的委托管理员。

- organizations:ListAWSServiceAccessForOrganization— 允许委托人列出组织使用 AWS 服务 的。
- organizations:ListOrganizationalUnitsForParent：允许主体列出父组织单位（OU）的子 OU。
- organizations:ListAccountsForParent：允许主体列出父 OU 的子账户。
- organizations:DescribeAccount – 让委托人可以检索有关企业中某个账户的信息。
- organizations:DescribeOrganizationalUnit：允许主体检索有关组织中某个 OU 的信息。
- organizations:DescribeOrganization：允许主体检索有关组织配置的信息。
- organizations:EnableAWSServiceAccess：允许主体启用 Security Hub 与 Organions 的集成。
- organizations:RegisterDelegatedAdministrator：允许主体为 Security Hub 指定委派管理员账户。
- organizations:DeregisterDelegatedAdministrator——允许主体为 Security Hub 移除指定委派管理员账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
            "Effect": "Allow",
```

```
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS 托管策略：AWSSecurityHubServiceRolePolicy

您不能将 `AWSSecurityHubServiceRolePolicy` 附加到自己的 IAM 实体。此附加到服务相关角色的策略允许 Security Hub 代表您执行操作。有关更多信息，请参阅 the section called “服务相关角色”。

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

权限详细信息

此策略包括以下权限：

- `cloudtrail`— 检索有关 CloudTrail 路径的信息。
- `cloudwatch`— 检索当前 CloudWatch 警报。
- `logs`— 检索 CloudWatch 日志的指标筛选器。
- `sns`：检索 SNS 主题的订阅列表。

- config— 检索有关配置记录器、资源和 AWS Config 规则的信息。还允许服务相关角色创建和删除 AWS Config 规则，并根据规则运行评估。
- iam：获取和生成账户凭证报告。
- organizations：检索组织的账户和组织单位 (OU) 信息。
- securityhub：检索有关如何配置 Security Hub 服务、标准和控件的信息。
- tag：检索有关资源标签的信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
```

```
                "securityhub:BatchGetStandardsControlAssociations",
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
```

```
                }
            }
        }
    ]
}
```

Security Hub 对 AWS 托管策略的更新

查看自该服务开始跟踪这些更改以来 Security Hub AWS 托管策略更新的详细信息。有关此页面更改的自动提示，请订阅 Security Hub 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSSecurityHubFullAccess— 更新现有政策	Security Hub 更新了政策，以获取 AWS 服务 和产品的定价详情。	2024 年 4 月 24 日
AWSSecurityHubReadOnlyAccess— 更新现有政策	Security Hub 通过添加一个`Sid`字段更新了此托管策略。	2024年2月22日
AWSSecurityHubFullAccess— 更新现有政策	Security Hub 更新了政策，因此它可以确定账户中是否启用了亚马逊 GuardDuty 和亚马逊 Inspector。这可以帮助客户汇集来自多个 AWS 服务与安全相关的信息。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess— 更新现有政策	Security Hub 更新了授予额外权限的策略，现在允许以只读方式访问 AWS Organizations 委托管理员功能。这包括根、组织单位（OU）、账户、组织结构和服务访问权限等详细信息。	2023 年 11 月 16 日

更改	描述	日期
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 添加了 `BatchGetSecurityControls` 、`DisassociateFromAdministratorAccount` ，以及读取和更新可自定义安全控制属性的 `UpdateSecurityControl` 权限。	2023 年 11 月 26 日
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 增加了读取与调查发现相关的资源标签的 `tag:GetResources` 权限。	2023 年 11 月 7 日
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 在标准中添加了获取有关控件启用状态信息的 `BatchGetStandardsControlAssociations` 权限。	2023 年 9 月 27 日
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 增加了获取 AWS Organizations 数据以及读取和更新 Security Hub 配置（包括标准和控件）的新权限。	2023 年 9 月 20 日
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 将现有 `config:DescribeConfigRuleEvaluationStatus` 权限移至策略中的另一条声明。该 `config:DescribeConfigRuleEvaluationStatus` 权限现已应用于所有资源。	2023 年 3 月 17 日

更改	描述	日期
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 将现有 `config:PutEvaluations` 权限移至策略中的另一条声明。该 `config:PutEvaluations` 权限现已应用于所有资源。	2021 年 7 月 14 日
AWSSecurityHubServiceRolePolicy – 更新了现有策略	Security Hub 添加了一项新权限，允许服务相关角色将评估结果传递给 AWS Config。	2021 年 6 月 29 日
AWSSecurityHubServiceRolePolicy— 已添加到托管策略列表中	添加了有关托管策略的信息 AWSSecurityHubServiceRolePolicy，该策略由 Security Hub 服务相关角色使用。	2021 年 6 月 11 日
AWSSecurityHubOrganizationsAccess— 新政策	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 开始跟踪更改	Security Hub 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 15 日

对 AWS 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
- 我无权执行 iam：PassRole
- 我想以编程方式访问 Security Hub
- 我是管理员并希望允许其他人访问 Security Hub

- 我想允许我以外的人访问我的 S AWS 账户 ecurity Hub 资源

我无权在 Security Hub 中执行操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当用户 `mateojackson` 尝试使用控制台查看有关 *`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

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Security Hub。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Security Hub 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想以编程方式访问 Security Hub

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS Management Console。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅《软件开发工具包和AWS 工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

我是管理员并希望允许其他人访问 Security Hub

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

我想允许我以外的人访问我的 S AWS 账户 ecurity Hub 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。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 如何 AWS Security Hub 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过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的区别，请参阅 IA M 用户指南中的跨账户资源访问。

AWS Security Hub 的合规性验证

作为多个 AWS Security Hub 合规性计划的一部分，第三方审计员将评估 AWS 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 AWS 服务的列表，请参阅按合规性计划提供的范围内 AWS 服务。有关一般信息，请参阅 AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 AWS Artifact 中下载报告。

您使用 Security Hub 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 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 AWS 上部署基于安全性和合规性的基准环境的步骤。
- AWS 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。
- AWS Config – 此 AWS 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。
- AWS Security Hub – 此AWS服务提供了AWS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操。

Sec AWS urity Hub 中的弹性

AWS 全球基础设施围绕 AWS 区域和可用区而构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

AWS Security Hub 中的基础设施安全性

作为一项托管式服务，AWS Security Hub 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础设施的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问 Security Hub。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

AWS Security Hub 和接口 VPC 端点 (AWS PrivateLink)

您可以通过创建接口 VPC 端点在 VPC 和 AWS Security Hub 之间建立私有连接。接口端点由 AWS PrivateLink 提供支持，该技术支持您通过私密方式访问 Security Hub API，而无需互联网网关、NAT 设备、VPN 连接或 AWS 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。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅 AWS PrivateLink 指南中的接口 VPC 端点 (AWS PrivateLink)。

Security Hub VPC 端点的注意事项

请务必先查看 AWS PrivateLink 指南中的接口端点属性和限制，然后再为 Security Hub 设置接口 VPC 端点。

Security Hub 支持从 VPC 调用它的所有 API 操作。

> **Note**
>
> Security Hub 无法使用亚太地区（大阪）区域中的 VPC 端点。

为 Security Hub 创建接口 VPC 端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 Security Hub 服务创建 VPC 端点。有关更多信息，请参阅 AWS PrivateLink 指南中的创建接口端点。

使用以下服务名称为 Security Hub 创建 VPC 端点：

- com.amazonaws.*region*.securityhub

如果为端点启用私有 DNS，则可以通过使用区域默认的 DNS 名称向 Security Hub 发送 API 请求，例如 `securityhub.us-east-1.amazonaws.com`。

有关更多信息，请参阅 AWS PrivateLink 指南中的通过接口端点访问服务。

为 Security Hub 创建 VPC 端点策略

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

- 可执行操作的委托人。
- 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 AWS PrivateLink 指南中的使用 VPC 端点控制对服务的访问。

示例：Security Hub 操作的 VPC 端点策略

下面是用于 Security Hub 的端点策略示例。当附加到端点时，此策略会向所有资源上的所有主体授予对列出的 Security Hub 操作的访问权限。

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

共享子网

您无法在与您共享的子网中创建、描述、修改或删除 VPC 端点。但是，您可以在与您共享的子网中使用 VPC 端点。有关 VPC 共享的信息，请参阅《Amazon VPC 用户指南》中的与其他账户共享 VPC。

使用 AWS CloudTrail 记录 AWS Security Hub API 调用

AWS Security Hub 已与 AWS CloudTrail 集成，后者作为一项服务，提供 Security Hub 中由用户、角色或 AWS 服务所执行的操作的记录。CloudTrail 将 Security Hub 的API 调用作为事件捕获。捕获的调用包含来自 Security Hub 控制台和代码的 Security Hub API 操作调用。如果您创建跟踪记录，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 控制台中的事件历史记录中查看最新事件。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它详细信息。

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 AWS CloudTrail 用户指南。

CloudTrail 中的 Security Hub 信息

在您创建 AWS 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，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在账户中查看、搜索和下载最新事件。有关更多信息，请参阅 使用 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），请创建跟踪记录。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。在控制台创建跟踪时，跟踪默认应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您可以配置其他 AWS 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。

将以下操作的活动记录到 CloudTrail 时，`responseElements` 的值将设置为 `null`。这可确保 CloudTrail 日志中不包含敏感信息。

- `BatchImportFindings`

- GetFindings
- GetInsights
- GetMembers
- UpdateFindings

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是 AWS 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 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

示例：Security Hub 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日记账条目。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，该条目演示了 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 AWS Security Hub 中的见解。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

标记 AWS Security Hub 资源

标签是一个可选标签，您可以定义它并将其分配给 AWS 资源，包括某些类型的 AWS Security Hub 资源。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。例如，您可以使用标签来区分资源、识别支持某些合规性要求或工作流程的资源或分配成本。

您可以为以下类型的 Security Hub 资源分配标签：自动化规则、配置策略和 Hub 资源。

主题

标签基础知识

一个资源可具有多达 50 个标签。每个标签都包含您定义的一个标签键和一个可选的标签值。标签键是一种常见的标签，充当更具体的标签值的类别。标签值 充当标签键的描述符。

例如，如果您为不同的环境创建不同的自动化规则（一组自动化规则用于测试账户，另一组用于生产账户），则可以为这些规则分配 `Environment` 标签密钥。关联的标签值可能是适用于与测试账户关联规则的 `Test`，也可能是与生产账户和 OU 关联规则的 `Prod`。

在为 AWS Security Hub 资源定义并分配标签时，请注意以下几点：

- 每个资源最多可以有 50 个标签。
- 对于每个资源，每个标签键都必须是唯一的，并且只能有一个标签值。
- 标签键和值区分大小写。作为最佳实践，我们建议您定义标签大写的策略，并在您的资源中一致地实施该策略。
- 一个标签密钥最多可以包含 128 个 UTF-8 字符。标签值最多可以包含 256 个 UTF-8 字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @
- `aws:` 前缀专门预留供 AWS 使用。您不能在您定义的任何标签键或值中使用它。此外，您无法更改或删除使用此前缀的标签键或值。使用此前缀的标签不计入每个资源的 50 个标签配额中。

- 您分配的任何标签仅适用于您的 AWS 账户 并且仅在您分配它们的 AWS 区域 中可用。
- 如果您使用 Security Hub 为资源分配标签，则标签仅应用于直接存储在适用 AWS 区域 中的 Security Hub 的资源。它们不适用于 Security Hub 在其他 AWS 服务 为您创建、使用或维护的任何关联的支持资源。例如，如果您为更新与 Amazon Simple Storage Service (Amazon S3) Service 相关的调查发现的自动化规则分配标签，则这些标签仅应用于 Security Hub 中指定区域的自动化规则。它们不适用于您的 S3 存储桶。要同时为关联资源分配标签，您可以使用 AWS Resource Groups 或 AWS 服务 来存储资源，例如用于 S3 存储桶的 Amazon S3。为关联资源分配标签可以帮助您识别 Security Hub 资源的支持资源。
- 如果删除资源，则分配给该资源的所有标签也将被删除。

> **Important**
>
> 不要在标签中存储机密或其他类型的敏感数据。标签可供许多 AWS 服务 访问，包括 AWS Billing and Cost Management。它们不适合用于敏感数据。

要为 Security Hub 资源添加和管理标签，您可以使用 Security Hub 控制台、Security Hub API 或 AWS Resource Groups Tagging API。通过 Security Hub，在创建资源时，您可以将标签添加到资源中。您还可以为单个现有资源添加和管理标签。通过资源组，您可以为跨多个 AWS 服务（包括 Security Hub）的多个现有资源批量添加和管理标签。

有关其他添加标签的提示和最佳实践，请参阅《为 AWS 资源添加标签用户指南》中的为 AWS 资源添加标签。

在 IAM policy 中使用标签

开始为资源添加标签后，您可在 AWS Identity and Access Management (IAM) policy 中定义基于标签的资源级权限。通过这种方式使用标记，您可以更全面地控制您 AWS 账户 中的哪些用户和角色有权创建和标记资源，以及哪些用户和角色有权添加、编辑和删除标签。要基于标签控制访问，您可以在 IAM policy 的条件元素中使用与标签关联的条件密钥。

例如，您可以创建一个 IAM policy，允许用户拥有对所有 AWS Security Hub 资源的完全访问权限（如果资源的 `Owner` 标签指定了用户名）：

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

```
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

如果您定义基于标签的资源级权限，该权限立即生效。这意味着，您的资源在创建后会更安全，而且您可以快速开始将标签用于新资源。您还可以使用资源级权限来控制哪些标签键和值可以与新的和现有资源关联。有关更多信息，请参阅 IAM 用户指南中的使用标签控制对 AWS 资源的访问权限。

向 AWS Security Hub 资源添加标签

要向单个 AWS Security Hub 资源添加标签，您可以使用 Security Hub 控制台或 Security Hub API。控制台不支持向 Hub 资源添加标签。

要同时向多个 Security Hub 资源添加标签，请使用 AWS Resource Groups Tagging API 的标记操作。

> **Important**
>
> 向资源添加标签可能会影响对该资源的访问。在向资源添加标签之前，请查看任何可能使用标签控制资源访问权限的 AWS Identity and Access Management (IAM) 策略。

Console

要将标签添加到资源中

创建自动化规则或配置策略时，Security Hub 控制台会提供向其添加标签的选项。您可以在标签部分中提供标签密钥和标签值。

Security Hub API & AWS CLI

要将标签添加到资源中

要创建资源并以编程方式向其添加一个或多个标签，请使用适合您要创建的资源类型的操作：

- 要创建配置策略并向其添加一个或多个标签，请调用 CreateConfigurationPolicy API，或者如果你使用的是 AWS CLI，则运行 create-configuration-policy 命令。
- 要创建自动化规则并向其添加一个或多个标签，请调用 CreateAutomationRule API，或者，如果您使用的是 AWS CLI，则运行 create-automation-rule 命令。
- 要启用 Security Hub 并向 Hub 资源添加一个或多个标签，请调用 EnableSecurityHub API，或者如果您使用的是 AWS Command Line Interface (AWS CLI)，则运行 enable-security-hub 命令。

在您的请求中，使用 `tags` 参数指定要添加到资源的每个标签的标签键和可选标签值。该 `tags` 参数指定对象数组。每个对象都指定一个标签密钥及其关联的标签值。

要将一个或多个标签添加到现有资源，请使用 Security Hub API 的 TagResource 操作，或者如果您使用的是 AWS CLI，请运行 tag-resource 命令。在您的请求中，指定您要向其添加标签的资源的 Amazon 资源名称（ARN）。使用 `tags` 参数为要添加的每个标签指定标签密钥 (`key`) 和可选的标签值 (`value`)。`tags` 参数指定一个对象数组，每个标签密钥对应一个对象及其关联的标签值。

例如，以下 AWS CLI 命令将具有 `Prod` 标签值的 `Environment` 标签键添加到指定配置策略。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

示例 CLI 命令：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

其中：

- `resource-arn` 指定要向其添加标签的配置策略的 ARN。
- *`Environment`* 是要添加到规则中的标签的标签密钥。
- *`Prod`* 是指定标签键（*`Environment`*）的标签值。

在以下示例中，该命令向配置策略添加了多个标签。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
```

```
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-doe
```

对于 tags 数组中的每个对象，都需要 key 和 value 参数。但是，value 参数的值可以是空字符串。如果您不想将标签值与标签密钥相关联，请不要为 value 参数指定值。例如，以下命令添加一个没有关联标签值的 Owner 标签键：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

如果标记操作成功，Security Hub 将返回一个空的 HTTP 200 响应。否则，Security Hub 会返回 HTTP 4 xx 或 500 响应，说明操作失败的原因。

查看 AWS Security Hub 资源的标签

您可以使用 Security Hub 控制台或 Security Hub API 查看 Security Hub 自动化规则或配置策略的标签（包括标签键和标签值）。控制台不支持查看 Hub 资源的标签。

要同时查看多个 Security Hub 资源的标签，请使用 AWS Resource Groups Tagging API 的标记操作。

Console

查看资源的标签

1. 使用 Security Hub 管理员的凭证，打开 AWS Security Hub 控制台，网址为 https://console.aws.amazon.com/securityhub/。
2. 根据要添加标签的资源类型，请执行以下操作之一：
   - 要查看自动化规则的标签，请在导航窗格中选择自动化。然后，选择自动化规则。
   - 要查看配置策略的标签，请在导航窗格中选择配置。然后，在策略选项卡上，选择配置策略旁边的选项。将打开一个侧面板，其中显示分配给策略的标签数量。您可以展开标签标头以查看标签键和标签值。

标签部分列出当前分配给该资源的所有标签。

Security Hub API & AWS CLI

查看资源的标签

要检索和查看现有资源的标签，请调用 ListTagsForResource API。在您的请求中，使用 resourceArn 参数指定资源的 Amazon 资源名称（ARN）。

如果您使用的是 AWS CLI，请运行 list-tags-for-resource 命令并使用参数 resource-arn 指定资源的 ARN。例如：

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

如果操作成功，Security Hub 将返回一个 tags 数组。数组中的每个对象都指定了当前分配给资源的标签（包括标签密钥和标签值）。例如：

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

其中 Environment、CostCenter 和 Owner 是分配给资源的标签键。Prod 是与 Environment 标签键关联的标签值。12345 是与 CostCenter 标签键关联的标签值。Owner 标签密钥没有关联的标签值。

要检索所有带有标签的 Security Hub 资源以及分配给每个资源的所有标签的列表，请使用 AWS Resource Groups Tagging API 的 GetResources 操作。在您的请求中，将 ResourceTypeFilters 参数的值设置为 securityhub。要执行此操作，使用 AWS CLI，并请运行 get-resources 命令并将 resource-type-filters 参数的值设置为 securityhub。例如：

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

如果操作成功，Resource Groups 将返回一个 `ResourceTagMappingList` 数组。该数组包含每个带有标签的 Security Hub 资源的一个对象。每个对象都指定 Security Hub 资源的 ARN 以及分配给该资源的标签键和值。

编辑 AWS Security Hub 资源的标签

要编辑 AWS Security Hub 资源的标签（标签键或标签值），可以使用 Security Hub API。Security Hub 控制台目前不支持标签编辑。

要同时编辑多个 Security Hub 资源的标签，请使用 AWS Resource Groups Tagging API 的标记操作。

> **Important**
>
> 编辑资源的标签可能会影响对资源的访问。在编辑资源的标签密钥或值之前，请查看可能使用该标签控件资源访问权限的任何 AWS Identity and Access Management (IAM) 策略。

Security Hub API & AWS CLI

编辑资源的标签

当您以编程方式编辑资源的标签时，会用新值覆盖现有标签。因此，编辑标签的最佳方法取决于您是要编辑标签密钥、标签值还是两者都有。要编辑标签密钥，请删除当前标签并添加新标签。

要仅编辑或删除与标签密钥关联的标签值，请使用 Security Hub API 的 TagResource 操作覆盖现有值。如果您使用的是 AWS CLI，请运行 tag-resource 命令。在您的请求中，指定要编辑或删除标签值的资源的 Amazon 资源名称（ARN）。

要编辑标签值，请使用 `tags` 参数指定要更改其标签值的标签密钥。您还应该为密钥指定新的标签值。例如，以下 AWS CLI 命令将分配给指定自动化规则的 `Environment` 标签键的标签值从 `Prod` 更改为 `Test`。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

其中：

- `resource-arn` 指定配置策略的 ARN。
- *`Environment`* 是与要更改的标签值关联的标签键。
- *`Test`* 是指定标签键 (*`Environment`*) 的新标签值。

要从标签密钥中移除标签值，请不要在 `value` 参数中为该密钥的 `tags` 参数指定值。例如：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

如果操作成功，Security Hub 将返回空的 HTTP 200 响应。否则，Security Hub 会返回 HTTP 4 xx 或 500 响应，说明操作失败的原因。

从 AWS Security Hub 资源中移除标签

要从 AWS Security Hub 资源中移除标签，您可以使用 Security Hub API。Security Hub 控制台目前不支持移除标签。

要同时从多个 Security Hub 资源中移除标签，请使用 AWS Resource Groups Tagging API 的标记操作。

> **Important**
>
> 从资源中删除标签可能对影响资源访问。在移除标签之前，请查看可能使用该标签控件资源访问权限的任何 AWS Identity and Access Management (IAM) 策略。

Security Hub API & AWS CLI

要从资源中删除标签

要以编程方式从资源中删除一个或多个标签，请使用 Security Hub API 的 UntagResource 操作。在请求中，使用 `resourceArn` 参数指定要从中删除标签的资源的 Amazon 资源名称（ARN）。使用 `tagKeys` 参数指定要删除的标签的标签键。要移除多个标签，请为要移除的每个标签附加 `tagKeys` 参数，并用和号 (&) 分隔，例如，`tagKeys=`*`key1`*`&tagKeys=`*`key2`*。如果仅从资源中删除特定的标签值（而不是标签键），请编辑标签而不是删除标签。

如果您使用的是 AWS CLI，请运行 untag-resource 命令从资源中移除一个或多个标签。在 `resource-arn` 参数中，指定要从中移除标签的资源的 ARN。使用 `tag-keys` 参数指定要删除的标签的标签键。例如，以下命令从指定配置策略中移除 `Environment` 标签（包括标签键和标签值）：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

其中，`resource-arn` 指定要移除标签的配置策略的 ARN，*`Environment`* 是要移除的标签的标签键。

要从资源中移除多个标签，请添加每个额外的标签密钥作为 `tag-keys` 参数的参数。例如：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

如果操作成功，Security Hub 将返回空的 HTTP 200 响应。否则，Security Hub 会返回 HTTP 4 xx 或 500 响应，说明操作失败的原因。

Security Hub 配额

对于每个 AWS 服务，您的 AWS 账户 都具有一些默认配额（以前称为限制）。这些限额是您的账户使用的服务资源或操作的最大数量。本主题链接到适用于您账户的 AWS Security Hub 资源和操作的配额。除非另有说明，每个配额适用于您在每个 AWS 区域 中的账户。

一些配额可以提升，而另一些配额不能提升。要请求增加配额，您可以使用服务限额控制台。要了解如何申请增加配额，请参阅服务限额用户指南中的请求增加配额。如果服务限额控制台上没有配额，请使用 AWS Support Center Console 上的提高服务限制表单申请增加配额。

最大配额

有关适用于 Security Hub 资源的配额列表，请参阅 AWS 一般参考 中的 AWS Security Hub 端点和配额。

速率配额

有关适用于 Security Hub API 操作的配额列表，请参阅《AWS Security Hub API Reference》。

如果您已设置 跨区域聚合，则只需调用一次 `BatchImportFindings` 和 `BatchUpdateFindings` 即可影响关联区域和聚合区域。该 `GetFindings` 操作从关联区域和聚合区域检索结果。但是，`BatchEnableStandards` 和 `UpdateStandardsControl` 操作是特定于区域的。

Security Hub 区域限制

某些 S AWS ecurity Hub 功能仅在某些情况下可用 AWS 区域。以下各节详细说明了这些区域限制。

有关提供 Security Hub 的区域列表，请参阅 AWS 一般参考 中的 AWS Security Hub 端点和配额。

跨区域聚合限制

在中 AWS GovCloud (US)，跨区域聚合 AWS GovCloud (US) 仅适用于调查结果、查找更新和见解。具体而言，您只能汇总 AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）之间的调查结果、最新发现和见解。

在中国区域，跨区域聚合仅可用于在中国区域的调查发现、调查发现更新和见解。具体而言，您只能聚合中国（北京）和中国（宁夏）之间的调查发现、调查发现更新和见解。

您不能使用默认禁用的区域作为聚合区域。有关默认禁用的区域列表，请参阅 AWS 一般参考 中的启用区域。

按区域划分的集成可用性

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，该集成不会在 Security Hub 控制台的集成页面上列出。

中国（北京）和中国（宁夏）区域支持的集成

中国（北京）和中国（宁夏）区域仅支持以下AWS 服务集成：

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager 补丁管理器

中国（北京）和中国（宁夏）区域仅支持以下第三方集成：

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）支持的集成

AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）地区仅支持以下服务集成： AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）地区仅支持以下第三方集成：

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie

- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series（仅在 AWS GovCloud （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

按区域划分的标准的可用性

服务管理标准： AWS Control Tower 仅在 AWS Control Tower 支持的区域中可用，包括 AWS GovCloud (US)。有关 AWS Control Tower 支持的区域列表，请参阅《AWS Control Tower 用户指南》 AWS Control Tower中的 “如何 AWS 区域 使用”。

AWS 资源标签标准不适用于加拿大西部（卡尔加里）、中国和。 AWS GovCloud (US)

Security Hub 可用的所有区域均提供其他安全标准。

按地区划分的控件可用性

Security Hub 控件可能并未在所有区域提供。要查看每个区域中不可用的控件列表，请参阅 对控件的区域限制。如果某个控件在您登录的区域中不可用，则该控件不会出现在 Security Hub 控制台的控件列表中。当您登录到聚合区域时例外。在这种情况下，您可以看到聚合区域或一个或多个关联区域中可用的控件。

对控件的区域限制

AWS Security Hub 控件可能并非全部可用 AWS 区域。此页面显示哪些控件在特定区域不可用。如果某个控件在您登录的区域中不可用，则该控件不会出现在 Security Hub 控制台的控件列表中。当您登录到聚合区域时例外。在这种情况下，您可以看到聚合区域或一个或多个关联区域中可用的控件。

目录

- 中国（北京）
- 中国（宁夏）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（米兰）
- 欧洲地区（巴黎）
- 欧洲（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 中东（巴林）
- 中东（阿联酋）
- 南美洲（圣保罗）
- AWS GovCloud （美国东部）
- AWS GovCloud （美国西部）

美国东部（弗吉尼亚州北部）

美国东部（弗吉尼亚州北部）不支持以下控件。

- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组

- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

美国东部（俄亥俄州）

美国东部（俄亥俄州）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型

- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

美国西部（北加利福尼亚）

美国西部（北加利福尼亚）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查

- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

美国西部（俄勒冈州）

美国西部（俄勒冈州）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联

- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

非洲（开普敦）

非洲（开普敦）不支持以下控制。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)
- [EC2.12] 应删除未使用的 Amazon EC2 EIP
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中

- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.1] GuardDuty 应该启用
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

亚太地区（香港）

亚太地区（香港）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象

- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份

- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

亚太地区（海得拉巴）

亚太地区（海得拉巴）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能

- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CodeArtifact.1] 应标记CodeArtifact 存储库

- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.22] 应删除未使用的 Amazon EC2 安全组

- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.9] ECS 任务定义应具有日志配置
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.5] 应启用应用程序和经典负载均衡器日志记录
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告

- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess

- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录

- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config
- [RDS.7] RDS 集群应启用删除保护
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级

- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件

- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

亚太地区（雅加达）

亚太地区（雅加达）不支持以下控件。

- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密

- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS

- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.2] ECS 服务不应自动分配公有 IP 地址
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应该使用容器详情
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中

- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施

- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.9] Redshift 集群不应使用默认的数据库名称
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.11] S3 通用存储桶应启用事件通知
- [S3.13] S3 通用存储桶应具有生命周期配置
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密

- [SQS.2] 应标记 SQS 队列
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

亚太地区（孟买）

亚太地区（孟买）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签

- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

亚太地区（墨尔本）

亚太地区（墨尔本）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签

- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.1] Amazon EBS 快照不应公开恢复
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)

- [EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [EC2.52] 应标记 EC2 传输网关
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.9] ECS 任务定义应具有日志配置
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置

- [EKS.8] EKS 集群应启用审核日志记录
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移
- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy

- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.10] IAM 用户的密码策略应该有很长的持续时间 AWS Config
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略

- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误

- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.3] RDS 数据库实例应启用静态加密
- [RDS.7] RDS 集群应启用删除保护
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.14] S3 通用存储桶应启用版本控制
- [S3.15] S3 通用存储桶应启用对象锁定
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限

- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

亚太地区（大阪）

亚太地区（大阪）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联

- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.4] 应 AWS Backup 标记报告计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制

- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.1] Amazon EBS 快照不应公开恢复
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.7] 应启用 EBS 默认加密
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址
- [EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [EC2.52] 应标记 EC2 传输网关

- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.2] ECS 服务不应自动分配公有 IP 地址
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应该使用容器详情
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头
- [ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.9] 经典负载均衡器应启用跨区域负载均衡器
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch

- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.1] GuardDuty 应该启用
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- AWS KMS keys 不应无意中删除 [KMS.3]
- [Lambda.1] Lambda 函数策略应禁止公共访问
- [Lambda.2] Lambda 函数应使用受支持的运行时系统
- [Lambda.3] Lambda 函数应位于 VPC 中
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch

- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.4] RDS 集群快照和数据库快照应进行静态加密
- [RDS.6] 应为 RDS 数据库实例配置增强监控
- [RDS.7] RDS 集群应启用删除保护
- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级

- [Redshift.1] Amazon Redshift 集群应禁止公共访问
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.15] S3 通用存储桶应启用对象锁定
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SecretsManager.1] Secrets Manager 密钥应启用自动轮换
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

亚太地区（首尔）

亚太地区（首尔）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch

- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

亚太地区（新加坡）

亚太地区（新加坡）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密

- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

亚太地区（悉尼）

亚太地区（悉尼）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移

- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接

- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

亚太地区（东京)

亚太地区（东京）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器

- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

加拿大（中部）

加拿大（中部）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库

- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

中国（北京）

中国（北京）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ACM.3] 应标记 ACM 证书
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.9] CloudTrail 路径应加标签
- [CloudWatch.15] CloudWatch 警报应配置指定操作

- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.5] 应标记 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关

- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL
- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应给亚马逊 VPC 加标签
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接进行标记
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [EC2.52] 应标记 EC2 传输网关
- [EC2.53] EC2 安全组不应允许从 0.0.0.0/0 进入远程服务器管理端口
- [EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager

- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.23] 应标记 IAM 访问分析器分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IAM.28] 应启用 IAM 访问分析器外部访问分析器
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施

- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.2] Kinesis 直播应该被标记
- [Lambda.6] 应标记 Lambda 函数
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密

- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS Private CA 根证书颁发机构
- [RDS.7] RDS 集群应启用删除保护
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由

- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应该标记 Redshift 集群
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.14] S3 通用存储桶应启用版本控制
- [S3.22] S3 通用存储桶应记录对象级写入事件
- [S3.23] S3 通用存储桶应记录对象级读取事件
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 话题
- [SQS.2] 应标记 SQS 队列
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则

- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

中国（宁夏）

中国（宁夏）不支持以下控制。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ACM.3] 应标记 ACM 证书
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.9] CloudTrail 路径应加标签
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.5] 应标记 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.28] 备份计划应涵盖 EBS 卷

- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关
- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL
- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应给亚马逊 VPC 加标签
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接进行标记
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [EC2.52] 应标记 EC2 传输网关
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联

- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.23] 应标记 IAM 访问分析器分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户

- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IAM.28] 应启用 IAM 访问分析器外部访问分析器
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.2] Kinesis 直播应该被标记
- [Lambda.1] Lambda 函数策略应禁止公共访问
- [Lambda.2] Lambda 函数应使用受支持的运行时系统
- [Lambda.3] Lambda 函数应位于 VPC 中
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Lambda.6] 应标记 Lambda 函数
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [Neptune.3] Neptune 数据库集群快照不应公开
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS Private CA 根证书颁发机构
- [RDS.7] RDS 集群应启用删除保护
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.3] Amazon Redshift 集群应启用自动快照

- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应该标记 Redshift 集群
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.14] S3 通用存储桶应启用版本控制
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 话题
- [SQS.2] 应标记 SQS 队列
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

欧洲地区（法兰克福）

欧洲地区（法兰克福）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [ECR.4] 应标记 ECR 公共存储库
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [RDS.31] 应标记 RDS 数据库安全组
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

欧洲地区（爱尔兰）

欧洲地区（爱尔兰）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1

- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

欧洲地区（伦敦）

欧洲地区（伦敦）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

欧洲地区（米兰）

欧洲地区（米兰）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量

- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)
- [EC2.12] 应删除未使用的 Amazon EC2 EIP
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.12] ECS 集群应该使用容器详情
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头

- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.1] GuardDuty 应该启用
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- AWS KMS keys 不应无意中删除 [KMS.3]
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署

- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.4] RDS 集群快照和数据库快照应进行静态加密
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

欧洲地区（巴黎）

欧洲地区（巴黎）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级

- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

欧洲（西班牙）

欧洲（西班牙）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址

- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书

- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.1] DynamoDB 表应根据需求自动扩展容量
- [DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.1] Amazon EBS 快照不应公开恢复
- [EC2.2] VPC 默认安全组不应允许入站或出站流量
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
- [EC2.7] 应启用 EBS 默认加密
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址
- [EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量

- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.9] ECS 任务定义应具有日志配置
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥

- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头
- [ELB.5] 应启用应用程序和经典负载均衡器日志记录
- [ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.9] 经典负载均衡器应启用跨区域负载均衡器
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签

- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.4] 应启用 AWS KMS 密钥轮换
- [Lambda.1] Lambda 函数策略应禁止公共访问
- [Lambda.2] Lambda 函数应使用受支持的运行时系统
- [Lambda.3] Lambda 函数应位于 VPC 中
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行

- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志

- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config
- [RDS.3] RDS 数据库实例应启用静态加密
- [RDS.4] RDS 集群快照和数据库快照应进行静态加密
- [RDS.5] RDS 数据库实例应配置多个可用区
- [RDS.6] 应为 RDS 数据库实例配置增强监控
- [RDS.7] RDS 集群应启用删除保护
- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch
- [RDS.10] 应为 RDS 实例配置 IAM 身份验证
- [RDS.11] RDS 实例应启用自动备份
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.1] Amazon Redshift 集群应禁止公共访问

- [Redshift.2] 与 Amazon Redshift 集群的连接应在传输过程中进行加密
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.5] S3 通用存储桶应要求请求使用 SSL
- [S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.9] S3 通用存储桶应启用服务器访问日志记录
- [S3.15] S3 通用存储桶应启用对象锁定
- [S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态

- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

欧洲地区（斯德哥尔摩）

欧洲地区（斯德哥尔摩）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密

- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件

- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

欧洲（苏黎世）

欧洲（苏黎世）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudTrail.7] 确保在 S3 存储桶上启用 S CloudTrail 3 存储桶访问日志记录
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch

- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.1] DynamoDB 表应根据需求自动扩展容量
- [DynamoDB.2] DynamoDB 表应该启用恢复功能 point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.2] VPC 默认安全组不应允许入站或出站流量
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 实例不应拥有公有 IPv4 地址
- [EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库

- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.9] ECS 任务定义应具有日志配置
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.9] 经典负载均衡器应启用跨区域负载均衡器
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志

- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名

- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护

- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.3] RDS 数据库实例应启用静态加密
- [RDS.5] RDS 数据库实例应配置多个可用区
- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.8] S3 通用存储桶应阻止公共访问
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动

- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

以色列（特拉维夫）

以色列（特拉维夫）不支持以下控件。

- [ACM.1] 导入的证书和 ACM 颁发的证书应在指定的时间段后续订
- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度

- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密

- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
- [EC2.10] 应将 Amazon EC2 配置为使用为 Amazon EC2 服务创建的 VPC 端点
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.18] 安全组应只允许授权端口不受限制的传入流量

- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [EC2.52] 应标记 EC2 传输网关
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.9] ECS 任务定义应具有日志配置
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志记录
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS

- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.4] 应将应用程序负载均衡器配置为删除 http 标头
- [ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移
- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [ES.1] Elasticsearch 域应启用静态加密
- [ES.2] Elasticsearch 域名不可供公共访问
- [ES.3] Elasticsearch 域应加密节点之间发送的数据
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签

- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.7] IAM 用户的密码策略应具有可靠的配置
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.10] IAM 用户的密码策略应该有很长的持续时间 AWS Config
- [IAM.11] 确保 IAM 密码策略要求包含至少一个大写字母
- [IAM.12] 确保 IAM 密码策略要求包含至少一个小写字母
- [IAM.13] 确保 IAM 密码策略要求包含至少一个符号
- [IAM.14] 确保 IAM 密码策略要求包含至少一个数字
- [IAM.15] 确保 IAM 密码策略要求最短密码长度不低于 14
- [IAM.16] 确保 IAM 密码策略阻止重复使用密码
- [IAM.17] 确保 IAM 密码策略使密码在 90 天或更短时间内失效
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.23] 应标记 IAM 访问分析器分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IAM.28] 应启用 IAM 访问分析器外部访问分析器
- [IoT.1] 应 AWS IoT Core 标记安全配置文件

- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.2] Kinesis 直播应该被标记
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Macie.1] 应该启用亚马逊 Macie
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组

- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS Private CA 根证书颁发机构
- [RDS.1] RDS 快照应为私有
- [RDS.4] RDS 集群快照和数据库快照应进行静态加密
- [RDS.7] RDS 集群应启用删除保护
- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.31] 应标记 RDS 数据库安全组

- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.3] Amazon Redshift 集群应启用自动快照
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.9] Redshift 集群不应使用默认的数据库名称
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.2] S3 通用存储桶应阻止公共读取权限
- [S3.3] S3 通用存储桶应阻止公共写入权限
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.9] S3 通用存储桶应启用服务器访问日志记录
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.1] Secrets Manager 密钥应启用自动轮换
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager

- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [SSM.3] 由 Systems Manager 管理的 Amazon EC2 实例的关联合规状态应为 COMPLIANT
- [SSM.4] SSM 文档不应公开
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch

中东（巴林）

中东（巴林）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源

- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.20] 用于点对 AWS 点 VPN 连接的两个 VPN 隧道都应处于开启状态
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.1] GuardDuty 应该启用
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级

- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.7] RDS 集群应启用删除保护
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.31] 应标记 RDS 数据库安全组
- [Redshift.6] Amazon Redshift 应该启用自动升级到主要版本的功能
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SSM.2] 由 Systems Manager 管理的 Amazon EC2 实例在安装补丁后应具有 COMPLIANT 的补丁合规性状态
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

中东（阿联酋）

中东（阿联酋）不支持以下控件。

- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ApigateWay.1] 应启用 API Gateway REST 和 WebSocket API 执行日志记录
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证

- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查
- [Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
- [CloudTrail.6] 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config

- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.1] Database Migration Service 复制实例不应公开
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.3] 挂载的 Amazon EBS 卷应进行静态加密
- [EC2.4] 停止的 EC2 实例应在指定时间段后删除
- [EC2.6] 应在所有 VPC 中启用 VPC 流日志记录
- [EC2.8] EC2 实例应使用实例元数据服务版本 2 (IMDSv2)
- [EC2.12] 应删除未使用的 Amazon EC2 EIP
- [EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量
- [EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量
- [EC2.22] 应删除未使用的 Amazon EC2 安全组

- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.9] ECS 任务定义应具有日志配置
- [EFS.1] 应将弹性文件系统配置为使用以下方法加密静态文件数据 AWS KMS
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS
- [ELB.3] 应将经典负载均衡器侦听器配置为 HTTPS 或 TLS 终止
- [ELB.9] 经典负载均衡器应启用跨区域负载均衡器
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移
- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证

- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.1] IAM policy 不应允许完整的“*”管理权限
- [IAM.2] IAM 用户不应附加 IAM policy
- [IAM.3] IAM 用户访问密钥应每 90 天或更短时间轮换一次
- [IAM.4] 不应存在 IAM 根用户访问密钥
- [IAM.5] 应为拥有控制台密码的所有 IAM 用户启用 MFA
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.8] 应移除未使用的 IAM 用户凭证
- [IAM.9] 应为根用户启用 MFA
- [IAM.18] 确保已创建支持角色来管理事件 AWS Support
- [IAM.19] 应为所有 IAM 用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.22] 应移除在 45 天内未使用的 IAM 用户凭证
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书

- [IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [KMS.1] IAM 客户托管策略不应允许对所有 KMS 密钥执行解密操作
- [KMS.2] IAM 主体不应有允许对所有 KMS 密钥进行解密操作的 IAM 内联策略
- [KMS.4] 应启用 AWS KMS 密钥轮换
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空

- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.10] OpenSearch 域名应安装最新的软件更新
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.1] RDS 快照应为私有
- [RDS.2] RDS 数据库实例应禁止公共访问，具体取决于持续时间 PubliclyAccessible AWS Config
- [RDS.3] RDS 数据库实例应启用静态加密
- [RDS.5] RDS 数据库实例应配置多个可用区
- [RDS.6] 应为 RDS 数据库实例配置增强监控
- [RDS.8] RDS 数据库实例应启用删除保护
- [RDS.11] RDS 实例应启用自动备份
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.9] Redshift 集群不应使用默认的数据库名称
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口

- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.2] S3 通用存储桶应阻止公共读取权限
- [S3.3] S3 通用存储桶应阻止公共写入权限
- [S3.5] S3 通用存储桶应要求请求使用 SSL
- [S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户
- [S3.14] S3 通用存储桶应启用版本控制
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.1] Secrets Manager 密钥应启用自动轮换
- [SecretsManager.2] 配置了自动轮换功能的 Secrets Manager 密钥应成功轮换
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS
- [SNS.3] 应标记 SNS 话题
- [SQS.1] 应对 Amazon SQS 队列进行静态加密
- [SQS.2] 应标记 SQS 队列
- [SSM.1] Amazon EC2 实例应由以下人员管理 AWS Systems Manager
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组

- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录

南美洲（圣保罗）

南美洲（圣保罗）不支持以下控件。

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [ECR.4] 应标记 ECR 公共存储库
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷

- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [RDS.7] RDS 集群应启用删除保护
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.16] 应将 RDS 数据库集群配置为将标签复制到快照
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组

AWS GovCloud（美国东部）

AWS GovCloud（美国东部）不支持以下控件。

- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ACM.3] 应标记 ACM 证书

- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.2] Amazon EC2 Auto Scaling 组应覆盖多个可用区
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密
- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求

- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.9] CloudTrail 路径应加标签
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权
- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开

- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.1] DynamoDB 表应根据需求自动扩展容量
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.5] 应标记 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关
- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL
- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应给亚马逊 VPC 加标签

- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接进行标记
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.52] 应标记 EC2 传输网关
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应该使用容器详情
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联
- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置

- [EKS.8] EKS 集群应启用审核日志记录
- [ELB.2] 带有 SSL/HTTPS 侦听器的经典负载均衡器应使用由提供的证书 AWS Certificate Manager
- [ELB.8] 带有 SSL 侦听器的经典负载均衡器应使用持续时间较长的预定义安全策略 AWS Config
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移
- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器
- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.1] GuardDuty 应该启用
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签

- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.23] 应标记 IAM 访问分析器分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书
- [IAM.28] 应启用 IAM 访问分析器外部访问分析器
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.2] Kinesis 直播应该被标记
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Lambda.6] 应标记 Lambda 函数
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控
- [Neptune.1] 应对 Neptune 数据库集群进行静态加密

- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS Private CA 根证书颁发机构
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证
- [RDS.13] 应启用 RDS 自动次要版本升级

- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.9] Redshift 集群不应使用默认的数据库名称
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应该标记 Redshift 集群
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.10] 启用版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知
- [S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限

- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.14] S3 通用存储桶应启用版本控制
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [SageMaker.1] Amazon SageMaker 笔记本实例不应直接访问互联网
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 话题
- [SQS.2] 应标记 SQS 队列
- [SSM.4] SSM 文档不应公开
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch

AWS GovCloud （美国西部）

AWS GovCloud （美国西部）不支持以下控件。

- [ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度
- [ACM.3] 应标记 ACM 证书
- [Account.1] 应为以下人员提供安全联系信息 AWS 账户
- [账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分
- [APIGateway.2] 应将 API Gateway REST API 阶段配置为使用 SSL 证书进行后端身份验证
- [APIGateway.3] API Gateway REST API 阶段应启用 AWS X-Ray 追踪功能
- [APIGateway.4] API Gateway 应与 WAF Web ACL 关联
- [APIGateway.8] API Gateway 路由应指定授权类型
- [APIGateway.9] 应为 API Gateway V2 阶段配置访问日志
- [AppSync.2] AWS AppSync 应该启用字段级日志记录
- [AppSync.4] 应标记 AWS AppSync GraphQL API
- [AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证
- [Athena.2] 应标记 Athena 数据目录
- [Athena.3] 应标记 Athena 工作组
- [AutoScaling.2] Amazon EC2 Auto Scaling 组应覆盖多个可用区
- [AutoScaling.3] Auto Scaling 组启动配置应将 EC2 实例配置为需要实例元数据服务版本 2 (imdsv2)
- [AutoScaling.6] Auto Scaling 组应在多个可用区域中使用多种实例类型
- [AutoScaling.9] 亚马逊 EC2 Auto Scaling 小组应使用亚马逊 EC2 启动模板
- [AutoScaling.10] 应标记 EC2 Auto Scaling 群组
- [Autoscaling.5] 使用自动扩缩组启动配置启动的 Amazon EC2 实例不应具有公有 IP 地址
- [Backup.2] 应标记 AWS Backup 恢复点
- [Backup.3] 应 AWS Backup 标记文件库
- [Backup.4] 应 AWS Backup 标记报告计划
- [Backup.5] 应 AWS Backup 标记备份计划
- [CloudFormation.2] 应 CloudFormation 标记堆栈
- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [CloudFront.3] CloudFront 发行版在传输过程中应要求加密

- [CloudFront.4] CloudFront 发行版应配置源站故障转移
- [CloudFront.5] CloudFront 发行版应启用日志记录
- [CloudFront.6] CloudFront 发行版应启用 WAF
- [CloudFront.7] CloudFront 发行版应使用自定义 SSL/TLS 证书
- [CloudFront.8] CloudFront 发行版应使用 SNI 来处理 HTTPS 请求
- [CloudFront.9] CloudFront 发行版应加密发往自定义来源的流量
- [CloudFront.10] CloudFront 分发版不应在边缘站点和自定义源站之间使用已弃用的 SSL 协议
- [CloudFront.12] CloudFront 发行版不应指向不存在的 S3 来源
- [CloudFront.13] CloudFront 发行版应使用源站访问控制
- [CloudFront.14] 应该给 CloudFront 发行版加标签
- [CloudTrail.9] CloudTrail 路径应加标签
- [CloudWatch.15] CloudWatch 警报应配置指定操作
- [CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留
- [CloudWatch.17] 应激 CloudWatch 活警报动作
- [CodeArtifact.1] 应标记CodeArtifact 存储库
- [CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证
- [CodeBuild.2] CodeBuild 项目环境变量不应包含明文凭证
- [CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [CodeBuild.4] CodeBuild 项目环境应该有一个日志持续时间 AWS Config
- [DataFirehose.1] Firehose 传输流应在静态状态下进行加密
- [Detective.1] 应标记侦探行为图
- [DMS.2] 应标记 DMS 证书
- [DMS.3] 应标记 DMS 活动订阅
- [DMS.4] 应标记 DMS 复制实例
- [DMS.5] 应标记 DMS 复制子网组
- [DMS.6] DMS 复制实例应启用自动次要版本升级
- [DMS.7] 目标数据库的 DMS 复制任务应启用日志记录
- [DMS.8] 源数据库的 DMS 复制任务应启用日志记录
- [DMS.9] DMS 端点应使用 SSL
- [DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权

- [DMS.11] MongoDB 的 DMS 端点应启用身份验证机制
- [DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS
- [DocumentDB.1] Amazon DocumentDB 集群应进行静态加密
- [DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期
- [DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开
- [documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch
- [DocumentDB.5] Amazon DocumentDB 集群应启用删除保护
- [DynamoDB.1] DynamoDB 表应根据需求自动扩展容量
- [DynamoDB.3] DynamoDB Accelerator (DAX) 集群应在静态状态下进行加密
- [DynamoDB.4] 备份计划中应有 DynamoDB 表
- [DynamodB.5] 应标记 DynamoDB 表
- [DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密
- [EC2.15] Amazon EC2 子网不应自动分配公有 IP 地址
- [EC2.16] 应删除未使用的网络访问控制列表
- [EC2.17] Amazon EC2 实例不应使用多个 ENI
- [EC2.21] 网络 ACL 不应允许从 0.0.0.0/0 进入端口 22 或端口 3389
- [EC2.22] 应删除未使用的 Amazon EC2 安全组
- [EC2.23] Amazon EC2 中转网关不应自动接受 VPC 附件请求
- [EC2.24] 不应使用 Amazon EC2 半虚拟化实例类型
- [EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP
- [EC2.28] 备份计划应涵盖 EBS 卷
- [EC2.33] 应标记 EC2 传输网关附件
- [EC2.34] 应标记 EC2 传输网关路由表
- [EC2.35] 应标记 EC2 网络接口
- [EC2.36] 应标记 EC2 客户网关
- [EC2.37] 应标记 EC2 弹性 IP 地址
- [EC2.38] 应标记 EC2 实例
- [EC2.39] 应标记 EC2 互联网网关
- [EC2.40] 应标记 EC2 NAT 网关
- [EC2.41] 应标记 EC2 网络 ACL

- [EC2.42] 应标记 EC2 路由表
- [EC2.43] 应标记 EC2 安全组
- [EC2.44] 应标记 EC2 子网
- [EC2.45] 应标记 EC2 卷
- [EC2.46] 应给亚马逊 VPC 加标签
- [EC2.47] 应标记 Amazon VPC 终端节点服务
- [EC2.48] 应标记 Amazon VPC 流日志
- [EC2.49] 应标记 Amazon VPC 对等连接进行标记
- [EC2.50] 应标记 EC2 VPN 网关
- [EC2.52] 应标记 EC2 传输网关
- [ECR.1] ECR 私有存储库应配置图像扫描
- [ECR.2] ECR 私有存储库应配置标签不可变性
- [ECR.3] ECR 存储库应至少配置一个生命周期策略
- [ECR.4] 应标记 ECR 公共存储库
- [ECS.1] Amazon ECS 任务定义应具有安全的联网模式和用户定义。
- [ECS.3] ECS 任务定义不应共享主机的进程命名空间
- [ECS.4] ECS 容器应以非特权身份运行
- [ECS.5] ECS 容器应限制为仅对根文件系统具有只读访问权限。
- [ECS.8] 密钥不应作为容器环境变量传递
- [ECS.9] ECS 任务定义应具有日志配置
- [ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行
- [ECS.12] ECS 集群应该使用容器详情
- [ECS.13] 应标记 ECS 服务
- [ECS.14] 应标记 ECS 群集
- [ECS.15] 应标记 ECS 任务定义
- [EFS.2] Amazon EFS 卷应包含在备份计划中
- [EFS.3] EFS 接入点应强制使用根目录
- [EFS.4] EFS 接入点应强制使用用户身份
- [EFS.5] 应标记 EFS 接入点
- [EFS.6] EFS 挂载目标不应与公有子网关联

- [EKS.1] EKS 集群端点不应公开访问
- [EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行
- [EKS.3] EKS 集群应使用加密的 Kubernetes 密钥
- [EKS.6] 应标记 EKS 集群
- [EKS.7] 应标记 EKS 身份提供商配置
- [EKS.8] EKS 集群应启用审核日志记录
- [ELB.10] 经典负载均衡器应跨越多个可用区
- [ELB.12] 应用程序负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.13] 应用程序、网络和网关负载均衡器应跨越多个可用区
- [ELB.14] 经典负载均衡器应配置为防御性或最严格的异步缓解模式
- [ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF
- [ElastiCache.1] ElastiCache Redis 集群应启用自动备份
- [ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级
- [ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移
- [ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密
- [ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密
- [ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证
- [ElastiCache.7] ElastiCache 群集不应使用默认子网组
- [ElasticBeanstalk.1] Elastic Beanstalk 环境应启用增强型运行状况报告
- [ElasticBeanstalk.2] 应启用 Elastic Beanstalk 托管平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch
- [EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置
- [ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志
- [ES.9] 应标记 Elasticsearch 域名
- [EventBridge.2] 应标记 EventBridge 活动总线
- [EventBridge.3] EventBridge 自定义事件总线应附加基于资源的策略
- [EventBridge.4] EventBridge 全局端点应启用事件复制
- [fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷
- [fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份
- [GlobalAccelerator.1] 应标记全球加速器加速器

- [Glue.1] 应该给 AWS Glue 工作加标签
- [GuardDuty.2] 应该给 GuardDuty 过滤器加标签
- [GuardDuty.3] 应 GuardDuty 标记 IP 集
- [GuardDuty.4] 应 GuardDuty 标记探测器
- [IAM.6] 应该为根用户启用硬件 MFA
- [IAM.9] 应为根用户启用 MFA
- [IAM.21] 您创建的 IAM 客户托管策略不应允许对服务执行通配符操作
- [IAM.23] 应标记 IAM 访问分析器分析器
- [IAM.24] 应标记 IAM 角色
- [IAM.25] 应标记 IAM 用户
- [IAM.28] 应启用 IAM 访问分析器外部访问分析器
- [IoT.1] 应 AWS IoT Core 标记安全配置文件
- [IoT.2] 应 AWS IoT Core 标记缓解措施
- [IoT.3] 应为 AWS IoT Core 维度加标签
- [IoT.4] 应给 AWS IoT Core 授权者加标签
- [Iot.5] 应标记 AWS IoT Core 角色别名
- [IoT.6] AWS IoT Core 策略应该被标记
- [Kinesis.1] Kinesis 直播应在静态状态下进行加密
- [Kinesis.2] Kinesis 直播应该被标记
- [Lambda.5] VPC Lambda 函数应在多个可用区内运行
- [Lambda.6] 应标记 Lambda 函数
- [Macie.1] 应该启用亚马逊 Macie
- [Macie.2] 应启用 Macie 自动发现敏感数据
- [MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch
- [MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级
- [MQ.4] 应给亚马逊 MQ 经纪商加标签
- [MQ.5] ActiveMQ 代理应使用主动/备用部署模式
- [MQ.6] RabbitMQ 代理应该使用集群部署模式
- [MSK.1] MSK 集群应在代理节点之间传输时进行加密
- [MSK.2] MSK 集群应配置增强型监控

- [Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch
- [Neptune.3] Neptune 数据库集群快照不应公开
- [Neptune.4] Neptune 数据库集群应启用删除保护
- [Neptune.5] Neptune 数据库集群应启用自动备份
- [Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密
- [Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [Neptune.9] Neptune 数据库集群应跨多个可用区部署
- [NetworkFirewall.1] Network Firewall 防火墙应部署在多个可用区域中
- [NetworkFirewall.2] 应启用 Network Firewall 日志记录
- [NetworkFirewall.3] Network Firewall 策略应至少关联一个规则组
- [NetworkFirewall.4] Network Firewall 策略的默认无状态操作应为丢弃或转发已满数据包
- [NetworkFirewall.5] 对于分段的数据包，Network Firewall 策略的默认无状态操作应为丢弃或转发
- [NetworkFirewall.6] 无状态 Network Firewall 规则组不应为空
- [NetworkFirewall.7] 应标记 Network Firewall 防火墙
- [NetworkFirewall.8] 应标记 Network Firewall 防火墙策略
- [NetworkFirewall.9] Network Firewall 防火墙应启用删除保护
- [Opensearch.1] OpenSearch 域名应启用静态加密
- [Opensearch.2] OpenSearch 域名不应向公众开放
- [Opensearch.3] OpenSearch 域应加密节点之间发送的数据
- [Opensearch.4] OpenSearch 应该启用记录到 CloudWatch 日志的域名错误
- [Opensearch.5] OpenSearch 域应启用审核日志
- [Opensearch.6] OpenSearch 域名应至少有三个数据节点
- [Opensearch.7] OpenSearch 域名应启用精细的访问控制
- [Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密
- [Opensearch.9] 应该给 OpenSearch 域名加标签
- [Opensearch.11] OpenSearch 域名应至少有三个专用的主节点
- [PCA.1] 应禁用 AWS Private CA 根证书颁发机构
- [RDS.12] 应为 RDS 集群配置 IAM 身份验证

- [RDS.13] 应启用 RDS 自动次要版本升级
- [RDS.14] Amazon Aurora 集群应启用回溯功能
- [RDS.15] 应为多个可用区配置 RDS 数据库集群
- [RDS.24] RDS 数据库集群应使用自定义管理员用户名
- [RDS.25] RDS 数据库实例应使用自定义管理员用户名
- [RDS.26] RDS 数据库实例应受备份计划保护
- [RDS.27] 应对 RDS 数据库集群进行静态加密
- [RDS.28] 应标记 RDS 数据库集群
- [RDS.29] 应标记 RDS 数据库集群快照
- [RDS.30] 应标记 RDS 数据库实例
- [RDS.31] 应标记 RDS 数据库安全组
- [RDS.32] 应标记 RDS 数据库快照
- [RDS.33] 应标记 RDS 数据库子网组
- [RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch
- [RDS.35] RDS 数据库集群应启用自动次要版本升级
- [Redshift.7] Redshift 集群应使用增强型 VPC 路由
- [Redshift.8] Amazon Redshift 集群不应使用默认的管理员用户名
- [Redshift.9] Redshift 集群不应使用默认的数据库名称
- [Redshift.10] Redshift 集群应在静态状态下进行加密
- [Redshift.11] 应该标记 Redshift 集群
- [Redshift.12] 应标记 Redshift 事件通知订阅
- [Redshift.13] 应标记 Redshift 集群快照
- [Redshift.14] 应标记 Redshift 集群子网组
- [Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口
- [Route53.1] 应标记 Route53 运行状况检查
- [Route53.2] Route 53 公有托管区域应记录 DNS 查询
- [S3.1] S3 通用存储桶应启用阻止公共访问设置
- [S3.8] S3 通用存储桶应阻止公共访问
- [S3.10] 启用版本控制的 S3 通用存储桶应具有生命周期配置
- [S3.11] S3 通用存储桶应启用事件通知

- [S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限
- [S3.13] S3 通用存储桶应具有生命周期配置
- [S3.14] S3 通用存储桶应启用版本控制
- [S3.20] S3 通用存储桶应启用 MFA 删除
- [SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1
- [SES.1] 应标记 SES 联系人列表
- [SES.2] 应标记 SES 配置集
- [SecretsManager.3] 移除未使用的 Secrets Manager 密钥
- [SecretsManager.4] Secrets Manager 密钥应在指定的天数内轮换
- [SecretsManager.5] 应标记 Secrets Manager 机密
- [ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享
- [SNS.3] 应标记 SNS 话题
- [SQS.2] 应标记 SQS 队列
- [SSM.4] SSM 文档不应公开
- [StepFunctions.1] Step Functions 状态机应该开启日志功能
- [StepFunctions.2] 应标记 Step Functions 活动
- [Transfer.1] 应标记 AWS Transfer Family 工作流程
- [Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接
- [WAF.1] 应启用 AWS WAF 经典全局 Web ACL 日志记录
- [WAF.2] AWS WAF 经典区域规则应至少有一个条件
- [WAF.3] AWS WAF 经典区域规则组应至少有一条规则
- [WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组
- [WAF.6] AWS WAF 经典全局规则应至少有一个条件
- [WAF.7] AWS WAF 经典全局规则组应至少有一条规则
- [WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组
- [WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组
- [WAF.11] 应启 AWS WAF 用 Web ACL 日志记录
- [WAF.12] AWS WAF 规则应启用指标 CloudWatch

禁用 Security Hub

> **Note**
>
> 如果使用中心配置，则 AWS Security Hub 委托管理员可以创建配置策略，以在特定账户和组织单位（OU）中禁用 Security Hub，并在其他账户和组织单位中保持启用状态。配置策略将在主区域和所有关联区域生效。有关更多信息，请参阅中央配置的工作原理。

您可以使用 Security Hub 控制台、Security Hub API 或 AWS CLI 禁用 Security Hub。

当您为某个账户禁用 Security Hub 时，会出现以下情况：

- 将不再为该账户处理任何新的调查发现。
- 在 90 天后，您现有的调查发现和见解以及任何 Security Hub 配置设置将被删除，并且无法恢复。

  如果您要保存现有调查发现，则必须先导出它们，然后再禁用 Security Hub。有关更多信息，请参阅the section called “账户操作对 Security Hub 数据的影响”。
- 任何启用的标准和控件都将被禁用。

在以下情况下，您无法禁用 Security Hub：

- 账户为组织指定指定 Security Hub 管理员账户。如果使用中心配置，则无法将禁用 Security Hub 的配置策略与委托管理员账户关联。其他账户的关联可能会成功，但 Security Hub 不会将此类策略应用于委托管理员账户。
- 您的账户是受邀的 Security Hub 管理员账户，并且您有已启用的成员账户。在禁用 Security Hub 之前，您必须取消关联所有成员账户。请参阅the section called “取消关联成员账户”。

在为成员账户禁用 Security Hub 之前，必须先解除该账户与其管理员账户的关联。对于组织账户，只有管理员账户可以取消成员账户的关联。有关更多信息，请参阅the section called “解除组织成员账户”。对于手动邀请的账户，管理员账户或成员账户都可以取消其与成员账户的关联。有关更多信息，请参阅 the section called “取消关联成员账户”或 the section called “取消关联您的管理员账户”。如果使用中心配置，则不需要解除关联，因为您可以创建一个策略，在特定成员账户中禁用 Security Hub。

在账户中禁用 Security Hub 时，仅在当前区域禁用。但如果使用中心配置在特定账户中禁用了 Security Hub，则会导致在主区域和所有关联区域禁用 Security Hub。

选择您首选的方法，然后按照以下步骤禁用 Security Hub。

Security Hub console

要禁用 Security Hub

1. 打开 AWS Security Hub 控制台，登陆：https://console.aws.amazon.com/securityhub/。
2. 在导航窗格上，选择设置。
3. 在设置页面上，选择常规。
4. 在禁用 AWS Security Hub下，选择禁用 AWS Security Hub。然后再次选择禁用 AWS Security Hub。

Security Hub API

要禁用 Security Hub

调用 `DisableSecurityHub` API。

AWS CLI

要禁用 Security Hub

运行 `disable-security-hub`命令。

命令示例：

```
aws securityhub disable-security-hub
```

Security Hub 控件的更改日志

以下变更日志跟踪对现有 AWS Security Hub 安全控制措施的重大更改，这些更改可能会导致控制的整体状态及其发现的合规性状态发生变化。有关 Security Hub 如何评估控件状态的信息，请参阅合规状态和控制状态。更改在输入此日志后可能需要几天时间才能影响所有 AWS 区域 可用的控件。

此日志跟踪自 2023 年 4 月以来发生的更改。

选择控件可查看有关该控件的更多详细信息。标题变更会在每个控件的详细描述中注明 90 天。

变更日期	控件 ID 和标题	更改的说明
2024年6月25日	AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录	此控件检查 AWS Config 是否已启用，使用服务相关角色并记录已启用控件的资源。Security Hub 更新了控件标题以反映控件评估的内容。
2024年6月14日	[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch	此控件检查是否将 Amazon Aurora MySQL 数据库集群配置为向亚马逊日志发布审核 CloudWatch 日志。Security Hub 更新了控件，使其不会为 Aurora Serverless v1 数据库集群生成调查结果。
2024 年 6 月 10 日	AWS Config 应启用 [Config.1] 并使用服务相关角色进行资源记录	此控件检查资源记录 AWS Config 是否已启用， AWS Config 资源记录是否已开启。以前，只有在为所有资源配置了

变更日期	控件 ID 和标题	更改的说明
		录制时，控件才会生成PASSED调查结果。Security Hub 更新了控件，以便在为启用控件所需的资源开启录制时生成PASSED结果。控件也已更新，以检查是否使用了 AWS Config 服务相关角色，该角色提供了记录必要资源的权限。
2024 年 5 月 8 日	[S3.20] S3 通用存储桶应启用 MFA 删除	此控件检查 Amazon S3 通用版本存储桶是否启用了多重身份验证 (MFA) 删除。以前，该控件会为具有生命周期配置的存储分区生成FAILED结果。但是，无法在具有生命周期配置的存储桶上启用带版本控制的 MFA 删除。Security Hub 更新了控件，使其不对具有生命周期配置的存储桶生成任何结果。控件描述已更新，以反映当前行为。

变更日期	控件 ID 和标题	更改的说明
2024年5月2日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	Security Hub 更新了 Kubernetes 支持的最早版本，Amazon EKS 集群可以在该版本上运行，以得出通过的调查发现。目前支持的最旧版本是 Kubernetes 1.26。
2024 年 4 月 30 日	[CloudTrail.3] 应至少启用一条 CloudTrail 跟踪	将控件标题从“CloudTrail 应启用”更改为“至少应启用一条 CloudTrail 跟踪”。如果启用 AWS 账户 了至少一条 CloudTrail 跟踪，则此控件当前会生成PASSED查找结果。标题和描述已更改，以准确反映当前行为。
2024 年 4 月 29 日	[AutoScaling.1] 与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查	已更改的控制标题从与 Classic Load Balancer 关联的 Auto Scaling 组应使用负载均衡器运行状况检查更改为与负载均衡器关联的 Auto Scaling 组应使用 ELB 运行状况检查。此控件当前评估应用程序、网关、网络和经典负载均衡器。标题和描述已更改，以准确反映当前行为。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 19 日	[CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪	该控件检查 AWS CloudTrail 是否启用并配置了至少一个包含读写管理事件的多区域跟踪。以前，当账户 CloudTrail 启用并配置了至少一个多区域跟踪时，即使没有跟踪捕获读写管理事件，控件也会错误地生成PASSED调查结果。现在，只有在启用并配置了至少一个捕获读写管理事件的多区域跟踪时 CloudTrail ，该控件才会生成PASSED查找结果。
2024 年 4 月 10 日	[Athena.1] Athena 工作组应进行静态加密	Security Hub 停用了此控件，并将其从所有标准中删除。Athena 工作组将日志发送到亚马逊简单存储服务 (Amazon S3) Service 存储桶。Amazon S3 现在使用 S3 托管式密钥 (SS3-S3) 为新的和现有的 S3 存储桶提供默认加密。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 10 日	[AutoScaling.4] Auto Scaling 组启动配置的元数据响应跳跃限制不应大于 1	Security Hub 停用了此控件，并将其从所有标准中删除。Amazon Elastic Compute Cloud (Amazon EC2) 实例的元数据响应跳跃限制取决于工作负载。
2024 年 4 月 10 日	[CloudFormation.1] CloudFormation 堆栈应与简单通知服务 (SNS) 集成 Simple Notification Service	Security Hub 停用了此控件，并将其从所有标准中删除。将 AWS CloudFormation 堆栈与 Amazon SNS 主题集成不再是一种最佳安全实践。尽管将重要的 CloudFormation 堆栈与 SNS 主题集成可能很有用，但并非所有堆栈都需要这样做。
2024 年 4 月 10 日	[CodeBuild.5] CodeBuild 项目环境不应启用特权模式	Security Hub 停用了此控件，并将其从所有标准中删除。在 CodeBuild 项目中启用特权模式不会给客户环境带来额外的风险。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 10 日	[IAM.20] 避免使用 root 用户	Security Hub 停用了此控件，并将其从所有标准中删除。此控件的目的由另一个控件覆盖[CloudWatch.1] “root” 用户应有日志指标筛选器和警报。
2024 年 4 月 10 日	[SNS.2] 应为发送到主题的通知消息启用传送状态记录	Security Hub 停用了此控件，并将其从所有标准中删除。记录 SNS 主题的传送状态不再是最佳安全实践。尽管记录重要 SNS 主题的传送状态可能很有用，但并非所有主题都必须这样做。
2024 年 4 月 10 日	[S3.10] 启用版本控制的 S3 通用存储桶应具有生命周期配置	Security Hub 从《 AWS 基础安全最佳实践》和《服务管理标准》中删除了此控件:。 AWS Control Tower此控件的目的由另外两个控件覆盖：[S3.13] S3 通用存储桶应具有生命周期配置和[S3.14] S3 通用存储桶应启用版本控制。此控件仍然是 NIST SP 800-53 Rev. 5 的一部分。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 10 日	[S3.11] S3 通用存储桶应启用事件通知	Security Hub 从《 AWS 基础安全最佳实践》和《服务管理标准》中删除了此控件:。 AWS Control Tower尽管在某些情况下，S3 存储桶的事件通知很有用，但这不是通用的安全最佳实践。此控件仍然是 NIST SP 800-53 Rev. 5 的一部分。
2024 年 4 月 10 日	[SNS.1] SNS 主题应使用以下方法进行静态加密 AWS KMS	Security Hub 从《 AWS 基础安全最佳实践》和《服务管理标准》中删除了此控件:。 AWS Control Tower由于 SNS 已在默认情况下对主题 AWS KMS 进行加密，因此不再建议使用加密主题作为安全最佳实践。此控件仍然是 NIST SP 800-53 Rev. 5 的一部分。

变更日期	控件 ID 和标题	更改的说明
2024 年 4 月 8 日	[ELB.6] 应用程序、网关和网络负载均衡器应启用删除保护	应将控制标题从 Application Load Balancer 删除保护更改为应用程序、网关和网络负载均衡器应启用删除保护。此控件当前评估应用程序、网关和网络负载均衡器。标题和描述已更改，以准确反映当前行为。
2024 年 3 月 22 日	[Opensearch.8] 应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密	将控制标题从应使用 TLS 1.2 加密到 OpenSearch 域的连接更改为应使用最新的 TLS 安全策略对与 OpenSearch 域的连接进行加密。以前，该控件仅检查与 OpenSearch 域的连接是否使用 TLS 1.2。现在，该控件会PASSED发现 OpenSearch 域名是否使用最新的 TLS 安全策略进行加密。控件标题和描述已更新，以反映当前行为。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 22 日	[ES.8] 应使用最新的 TLS 安全策略对与 Elasticsearch 域的连接进行加密	将控制标题从 Elasticsearch 域名的连接更改为应使用 TLS 1.2 加密到 Elasticsearch 域的连接应使用最新的 TLS 安全策略进行加密。以前，该控件仅检查与 Elasticsearch 域的连接是否使用 TLS 1.2。现在，该控件可以PASSED发现 Elasticsearch 域名是否使用最新的 TLS 安全策略进行加密。控件标题和描述已更新，以反映当前行为。
2024 年 3 月 12 日	[S3.1] S3 通用存储桶应启用阻止公共访问设置	应将标题从 S3 阻止公共访问设置更改为 S3 通用存储桶应启用阻止公共访问设置。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.2] S3 通用存储桶应阻止公共读取权限	已更改 S3 存储桶的标题应禁止对 S3 的公共读取权限通用存储桶应阻止公共读取权限。Security Hub 将标题更改为说明新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.3] S3 通用存储桶应阻止公共写入权限	已更改 S3 存储桶的标题应禁止对 S3 的公共写入权限。通用存储桶应阻止公共写入权限。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.5] S3 通用存储桶应要求请求使用 SSL	从 S3 存储桶更改后的标题应要求请求使用安全套接字层，改为 S3 通用存储桶应要求请求使用 SSL。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户	从授予其他 AWS 账户存储桶策略的 S3 权限更改后的标题应仅限于 S3 通用存储桶策略应限制其他存储桶策略的访问权限 AWS 账户。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.7] S3 通用存储桶应使用跨区域复制	从 S3 存储桶更改后的标题应启用跨区域复制，改为 S3 通用存储桶应使用跨区域复制。Security Hub 将标题更改为说明新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.7] S3 通用存储桶应使用跨区域复制	从 S3 存储桶更改后的标题应启用跨区域复制，改为 S3 通用存储桶应使用跨区域复制。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.8] S3 通用存储桶应阻止公共访问	应在存储桶级别启用 S3 阻止公共访问设置的标题更改为 S3 通用存储桶应阻止公共访问。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.9] S3 通用存储桶应启用服务器访问日志记录	应启用 S3 存储桶服务器访问日志的标题更改为应为 S3 通用存储桶启用服务器访问日志记录。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.10] 启用版本控制的 S3 通用存储桶应具有生命周期配置	已启用版本控制的 S3 存储桶的标题应将生命周期策略配置为启用版本控制的 S3 通用存储桶应具有生命周期配置。Security Hub 将标题更改为说明新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.11] S3 通用存储桶应启用事件通知	从 S3 存储桶更改的标题应启用事件通知，改为 S3 通用存储桶应启用事件通知。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.12] 不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限	从 S3 访问控制列表 (ACL) 更改后的标题不应用于管理用户对存储桶的访问权限，而不应使用 ACL 来管理用户对 S3 通用存储桶的访问权限。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.13] S3 通用存储桶应具有生命周期配置	从 S3 存储桶更改后的标题应将生命周期策略配置为 S3 通用存储桶应具有生命周期配置。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.14] S3 通用存储桶应启用版本控制	从 S3 存储桶更改后的标题应使用版本控制，改为 S3 通用存储桶应启用版本控制。Security Hub 将标题更改为说明新的 S3 存储桶类型。

变更日期	控件 ID 和标题	更改的说明
2024 年 3 月 12 日	[S3.15] S3 通用存储桶应启用对象锁定	应将标题从 S3 存储桶配置为使用对象锁定，S3 通用存储桶应启用对象锁定。Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 12 日	[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys	已更改的标题从 S3 存储桶应使用静态加密 AWS KMS keys到 S3 通用存储桶应使用静态加密。 AWS KMS keys Security Hub 将标题更改为说明新的 S3 存储桶类型。
2024 年 3 月 7 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持`nodejs20.x` 和`ruby3.3`作为参数。
2024年2月22日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持 `dotnet8` 作为参数。

变更日期	控件 ID 和标题	更改的说明
2024年2月5日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	Security Hub 更新了 Kubernetes 支持的最早版本，Amazon EKS 集群可以在该版本上运行，以得出通过的调查发现。目前支持的最旧版本是 Kubernetes 1.25。
2024 年 1 月 10 日	[CodeBuild.1] CodeBuild Bitbucket 源存储库网址不应包含敏感凭证	已更改标题CodeBuild GitHub 或 Bitbucket 源存储库网址应使用 OAuth 到 CodeBuild Bitbucket 源存储库网址不应包含敏感凭据。Security Hub 删除了对 OAuth 的提及，因为其他连接方法也可以是安全的。Security Hub 删除了提及， GitHub 因为不再可能在 GitHub 源存储库 URL 中包含个人访问令牌或用户名和密码。

变更日期	控件 ID 和标题	更改的说明
2024 年 1 月 8 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 不再支持 `go1.x` 和 `java8` 作为参数，因为这些运行时系统都已停用。
2023 年 12 月 29 日	[RDS.8] RDS 数据库实例应启用删除保护	RDS.8 会检查使用某个受支持数据库引擎的 Amazon RDS 数据库实例是否启用了删除保护。Security Hub 现在支持 `custom-oracle-ee`、`oracle-ee-cdb`、和 `oracle-se2-cdb` 作为数据库引擎。
2023 年 12 月 22 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持 `java21` 和 `python3.12` 作为参数。Security Hub 不再支持 `ruby2.7` 作为参数。

变更日期	控件 ID 和标题	更改的说明
2023 年 12 月 15 日	[CloudFront.1] CloudFront 发行版应配置默认根对象	CloudFront.1 检查 Amazon CloudFront 分配是否配置了默认根对象。Security Hub 将此控件的严重性从“关键”降低到“高”，因为添加默认根对象是一个建议操作，具体取决于用户应用程序及特定需求。
2023 年 12 月 5 日	[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量	将控件标题从安全组不应允许从 0.0.0.0/0 到端口 22 的入口流量更改为安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量。
2023 年 12 月 5 日	[EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量	将控件标题从 确保没有安全组允许从 0.0.0.0/0 到端口 3389 的入口流量更改为安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量。

变更日期	控件 ID 和标题	更改的说明
2023 年 12 月 5 日	[RDS.9] RDS 数据库实例应将日志发布到日志 CloudWatch	应将控制标题从数据库日志记录更改为 RDS 数据库实例应将日志发布到 CloudWatch 日志。Security Hub 发现，此控件仅检查日志是否已发布到 Amazon CloudWatch Logs，而不检查是否已启用 RDS 日志。如果PASSED将 RDS 数据库实例配置为将日志发布到 CloudWatch 日志，则该控件会生成一个结果。控件标题已更新，以反映当前行为。
2023 年 11 月 17 日	[EC2.19] 安全组不应允许不受限制地访问高风险端口	EC2.19 检查被认为高风险的指定端口是否可以访问安全组的不受限制的传入流量。Security Hub 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果此前缀列表包含字符串“0.0.0.0/0”或“::/0”，则该控件会生成 FAILED 调查发现。

变更日期	控件 ID 和标题	更改的说明
2023 年 11 月 16 日	[CloudWatch.15] CloudWatch 警报应配置指定操作	将控制标题从CloudWatch 警报更改为应为警报状态配置动作，而 CloudWatch 警报则应配置指定操作。
2023 年 11 月 16 日	[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留	更改后的控制标题应从CloudWatch 日志组保留至少 1 年，而 CloudWatch 日志组应在指定的时间段内保留。
2023 年 11 月 16 日	[Lambda.5] VPC Lambda 函数应在多个可用区内运行	将控件标题从 VPC Lambda 函数应在一个以上可用区中运行更改为 VPC Lambda 函数应在多个可用区中运行。
2023 年 11 月 16 日	[AppSync.2] AWS AppSync 应该启用字段级日志记录	将控件标题从 AWS AppSync 应开启请求级和字段级日志记录更改为 AWS AppSync 应启用字段级日志记录。
2023 年 11 月 16 日	[EMR.1] Amazon EMR 集群主节点不应有公有 IP 地址	控制标题从 Amazon Elastic MapReduce 集群主节点不应具有公有 IP 地址更改为 Amazon EMR 集群主节点不应具有公有 IP 地址。

变更日期	控件 ID 和标题	更改的说明
2023 年 11 月 16 日	[Opensearch.2] OpenSearch 域名不应向公众开放	将控制标题从OpenSearch 域名应在 VPC 中更改为不应公开访问的OpenSearch域。
2023 年 11 月 16 日	[ES.2] Elasticsearch 域名不可供公共访问	将控件标题从 Elasticsearch 域名应位于 VPC 中更改为 Elasticsearch 域名不可供公共访问。
2023 年 10 月 31 日	[ES.4] 应启用 Elasticsearch 域错误日志记录到 CloudWatch 日志	ES.4 检查 Elasticsearch 域是否配置为向亚马逊日志发送错误日志。 CloudWatch 该控件之前对一个 Elasticsearch 域生成了PASSED调查结果，该域将所有日志配置为发送到 CloudWatch 日志。Security Hub 更新了控件，PASSED使其仅针对配置为向日志发送错误日志的 Elasticsearch 域生成查找结果。CloudWatch 该控件也进行了更新，将不支持错误日志的 Elasticsearch 版本排除在评估之外。

变更日期	控件 ID 和标题	更改的说明
2023 年 10 月 16 日	[EC2.13] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 22 的入口流量	EC2.13 检查安全组是否允许对端口 22 进行不受限制的入口访问。Security Hub 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串“0.0.0.0/0”或“::/0”，则该控件会生成 FAILED 调查发现。
2023 年 10 月 16 日	[EC2.14] 安全组不应允许从 0.0.0.0/0 或 ::/0 到端口 3389 的入口流量	EC2.14 检查安全组是否允许对端口 3389 进行不受限制的入口访问。Security Hub 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串“0.0.0.0/0”或“::/0”，则该控件会生成 FAILED 调查发现。

变更日期	控件 ID 和标题	更改的说明
2023 年 10 月 16 日	[EC2.18] 安全组应只允许授权端口不受限制的传入流量	EC2.18 检查正在使用的安全组是否允许不受限制的入口流量。Security Hub 更新了此控件，以考虑到将托管前缀列表作为安全组规则来源的情况。如果前缀列表包含字符串“0.0.0.0/0”或“::/0”，则该控件会生成 FAILED 调查发现。
2023 年 10 月 16 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持 python3.11 作为参数。
2023 年 10 月 4 日	[S3.7] S3 通用存储桶应使用跨区域复制	Security Hub 添加了值为 CROSS-REGION 的参数 ReplicationType，以确保 S3 存储桶启用了跨区域复制，而非同区域复制。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 27 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	Security Hub 更新了 Kubernetes 支持的最早版本，Amazon EKS 集群可以在该版本上运行，以得出通过的调查发现。目前支持的最旧版本是 Kubernetes 1.24。
2023 年 9 月 20 日	CloudFront.2 — CloudFront 发行版应启用来源访问身份	Security Hub 停用了此控件，并将其从所有标准中删除。请改为参阅[CloudFront.13] CloudFront 发行版应使用源站访问控制。“源访问标识”是当前的安全最佳实践。此控件将在 90 天后从文档中删除。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 20 日	[EC2.22] 应删除未使用的 Amazon EC2 安全组	Security Hub 从 AWS 基础安全最佳实践 (FSBP) 和美国国家标准与技术研究院 (NIST) SP 800-53 Rev. 5 中删除了此控件。它仍然是服务管理标准的一部分: AWS Control Tower. 如果安全组连接到 EC2 实例或弹性网络接口，此 控件会生成一个通过的调查发现。但是，对于某些用例，未附加的安全组不会构成安全风险。您可以使用其他 EC2 控件（例如 EC2.2、EC2.13、EC2.14、EC2.18 和 EC2.19）来监控您的安全组。
2023 年 9 月 20 日	EC2.29：EC2 实例应在 VPC 中启动	Security Hub 停用了此控件，并将其从所有标准中删除。Amazon EC2 已将 EC2-Classic 实例迁移到 VPC。此控件将在 90 天后从文档中删除。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 20 日	S3.4：S3 存储桶应启用服务器端加密	Security Hub 停用了此控件，并将其从所有标准中删除。Amazon S3 现在使用 S3 托管式密钥 (SS3-S3) 为新的和现有的 S3 存储桶提供默认加密。使用 SS3-S3 或 SS3-KMS 服务器端加密的现有存储桶的加密设置保持不变。此控件将在 90 天后从文档中删除。
2023 年 9 月 14 日	[EC2.2] VPC 默认安全组不应允许入站或出站流量	已将控件标题从 VPC 默认安全组不应允许入站和出站流量更改为 VPC 默认安全组不应允许入站或出站流量。
2023 年 9 月 14 日	[IAM.9] 应为根用户启用 MFA	已将控件标题从应为根用户启用虚拟 MFA更改为应为根用户启用 MFA。
2023 年 9 月 14 日	[RDS.19] 应为关键集群事件配置现有 RDS 事件通知订阅	已将控件标题从应为关键集群事件配置 RDS 事件通知订阅更改为应为关键集群事件配置现有 RDS 事件通知订阅。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 14 日	[RDS.20] 应为关键数据库实例事件配置现有 RDS 事件通知订阅	已将控件标题从应为关键数据库实例事件配置 RDS 事件通知订阅更改为应为关键数据库实例事件配置现有 RDS 事件通知订阅。
2023 年 9 月 14 日	[WAF.2] AWS WAF 经典区域规则应至少有一个条件	已将控件标题从WAF Regional 规则应至少有一个条件更改为AWS WAF Classic Regional 规则应至少有一个条件。
2023 年 9 月 14 日	[WAF.3] AWS WAF 经典区域规则组应至少有一条规则	已将控件标题从 WAF Regional 规则组应至少包含一条规则更改为AWS WAF Classic Regional 规则组应至少包含一条规则。
2023 年 9 月 14 日	[WAF.4] AWS WAF 经典区域性 Web ACL 应至少有一个规则或规则组	已将控件标题从 WAF Regional web ACL 应至少有一个规则或规则组更改为AWS WAF Classic Regional Web ACL 应至少有一个规则或规则组。
2023 年 9 月 14 日	[WAF.6] AWS WAF 经典全局规则应至少有一个条件	已将控件标题从全局 WAF 规则应至少有一个条件更改为 Classic 全局AWS WAF 规则应至少有一个条件。

变更日期	控件 ID 和标题	更改的说明
2023 年 9 月 14 日	[WAF.7] AWS WAF 经典全局规则组应至少有一条规则	已将控件标题从全局 WAF 规则组应至少包含一条规则更改为 Classic 全局AWS WAF 规则组应至少包含一条规则。
2023 年 9 月 14 日	[WAF.8] AWS WAF 经典全局 Web ACL 应至少有一个规则或规则组	已将控件标题从 WAF 全局 Web ACL 应至少包含一个规则或规则组更改为AWS WAF Classic 全局 Web ACL 应至少有一个规则或规则组。
2023 年 9 月 14 日	[WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组	已将控件标题从 WAFv2 Web ACL 至少有一个规则或规则组更改为AWS WAF Web ACL 应至少有一个规则或规则组。
2023 年 9 月 14 日	[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录	已将控件标题从应激活AWS WAF v2 Web ACL 日志记录更改为应启用AWS WAF Web ACL 日志记录。

变更日期	控件 ID 和标题	更改的说明
2023 年 7 月 20 日	S3.4：S3 存储桶应启用服务器端加密	S3.4 检查一个 Amazon S3 存储桶是否启用了服务器端加密，或者 S3 存储桶策略是否明确拒绝了没有服务器端加密的 `PutObject` 请求。Security Hub 更新了此控件，以加入具有 KMS 密钥的双层服务器端加密 (DSSE-KMS)。当使用 SSE-S3、SSE-KMS 或 DSSE-KMS 加密 S3 存储桶时，控件会生成已通过的调查发现。
2023 年 7 月 17 日	[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys	S3.17 检查 Amazon S3 存储桶是否使用了 AWS KMS key加密。Security Hub 更新了此控件，以加入具有 KMS 密钥的双层服务器端加密 (DSSE-KMS)。当使用 SSE-KMS 或 DSSE-KMS 加密 S3 存储桶时，该控件会生成已通过的调查发现。

变更日期	控件 ID 和标题	更改的说明
2023 年 6 月 9 日	[EKS.2] EKS 集群应在支持的 Kubernetes 版本上运行	EKS.2 检查 Amazon EKS 集群是否在受支持的 Kubernetes 版本上运行。现在支持的最旧版本是 `1.23`。
2023 年 6 月 9 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持 `ruby3.2` 作为参数。
2023 年 6 月 5 日	[APIGateway.5] API Gateway REST API 缓存数据应进行静态加密	APIGateway.5. 检查 Amazon API Gateway REST API 阶段中的所有方法是否都处于静态加密状态。Security Hub 更新了控件，使其仅在为特定方法启用缓存时才评估该方法的加密。
2023 年 5 月 18 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持 `java17` 作为参数。

变更日期	控件 ID 和标题	更改的说明
2023 年 5 月 18 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 不再支持 `nodejs12.x` 作为参数。
2023 年 4 月 23 日	[ECS.10] ECS Fargate 服务应在最新的 Fargate 平台版本上运行	ECS.10 会检查 Amazon ECS Fargate 服务是否运行最新的 Fargate 平台版本。客户可以直接通过 ECS 部署 Amazon ECS，也可以使用部署 CodeDeploy。Security Hub 更新了此控件，以便在您使用 CodeDeploy 部署 ECS Fargate 服务时生成通过调查结果。
2023 年 4 月 20 日	[S3.6] S3 通用存储桶策略应限制对其他存储桶的访问 AWS 账户	S3.6 检查亚马逊简单存储服务 (Amazon S3) 存储桶策略是否阻止 AWS 账户 其他人的委托人对 S3 存储桶中的资源执行被拒绝的操作。考虑存储桶策略中的条件，Security Hub 更新了控件。

变更日期	控件 ID 和标题	更改的说明
2023 年 4 月 18 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 现在支持 `python3.10` 作为参数。
2023 年 4 月 18 日	[Lambda.2] Lambda 函数应使用受支持的运行时系统	Lambda.2 检查运行时的 AWS Lambda 函数设置是否与为每种语言支持的运行时设置的预期值相匹配。Security Hub 不再支持 `dotnetcore3.1` 作为参数。
2023 年 4 月 17 日	[RDS.11] RDS 实例应启用自动备份	RDS.11 会检查 Amazon RDS 实例是否启用了自动备份，其备份保留期大于或等于七天。Security Hub 更新了此控件，将只读副本排除在评估范围之外，因为并非所有引擎都支持对只读副本进行自动备份。此外，RDS 不提供在创建只读副本时指定备份保留期的选项。默认情况下，只读副本创建时的备份保留期为 `0`。

《Sec AWS urity Hub 用户指南》的文档历史记录

下表介绍了 Sec AWS urity Hub 文档的更新。

> **Note**
>
> 在发布安全控件时，指定的日期是所有账户和地区都可以使用这些控件的日期。控件可能需要 1-2 周才能在所有账户和区域中可用。

变更	说明	日期
独联体 AWS 基金会基准测试版本 3.0.0 发布	Security Hub 发布了互联网安全中心 (CIS) AWS 基金会基准 v3.0.0。该版本包括以下新控件，以及与多个现有控件的映射。 • the section called “[EC2.53] EC2 安全组不应允许从 0.0.0.0/0 进入远程服务器管理端口” • the section called “[EC2.54] EC2 安全组不应允许从:: /0 进入远程服务器管理端口” • the section called “[IAM.26] 应移除在 IAM 中管理的过期 SSL/TLS 证书” • the section called “[IAM.27] IAM 身份不应附加策略 AWSCloudShellFullAccess ” • the section called “[IAM.28] 应启用 IAM 访问分析器外部访问分析器”	2024年5月13日

- the section called “[S3.22] S3 通用存储桶应记录对象级写入事件”
- the section called “[S3.23] S3 通用存储桶应记录对象级读取事件”

新的安全控件	以下新的 Security Hub 控件可用： • the section called “[DataFirehose.1] Firehose 传输流应在静态状态下进行加密” • the section called “[DMS.10] Neptune 数据库的 DMS 终端节点应启用 IAM 授权” • the section called “[DMS.11] MongoDB 的 DMS 端点应启用身份验证机制” • the section called “[DMS.12] 适用于 Redis 的 DMS 终端节点应启用 TLS” • the section called “[DynamodB.7] DynamoDB 加速器集群应在传输过程中进行加密” • the section called “[EFS.6] EFS 挂载目标不应与公有子网关联” • the section called “[EKS.3] EKS 集群应使用加密的 Kubernetes 密钥” • the section called “[fsx.2] 应将适用于 Lustre 文件系统的 FSx 配置为将标签复制到备份” • the section called “[MQ.2] ActiveMQ 代理应将审计日志流式传输到 CloudWatch” • the section called “[MQ.3] 亚马逊 MQ 经纪商应启用自动次要版本升级”	2024 年 5 月 3 日

	• the section called “[Opensearch.11] OpenSearch 域名应至少有三个专用的主节点” • the section called “[Redshift.15] Redshift 安全组应仅允许从受限来源进入集群端口” • the section called “[SageMaker.4] SageMaker 端点生产变体的初始实例数应大于 1” • the section called “[ServiceCatalog.1] Service Catalog 产品组合只能在 AWS 组织内部共享” • the section called “[Transfer.2] Transfer Family 服务器不应使用 FTP 协议进行端点连接”	
AWS 资源标签标准	S AWS ecurity Hub 的资源标签标准现已正式发布，同时还有适用于该标准的新控件。	2024 年 4 月 30 日
更新现有托管策略	Security Hub 更新了名为`AmazonSecurityHubFullAccess` 的AWS 托管策略，以获取 AWS 服务 和产品的定价详情。	2024 年 4 月 24 日
在上下文中配置控制参数	如果您使用中央配置，则现在可以从 Security Hub 控制台上控件的详细信息页面在上下文中配置控制参数。	2024 年 3 月 29 日

更新现有托管策略	Security Hub `AWSSecurityHubReadOnlyAccess` 通过添加`Sid`字段更新了名为的AWS 托管策略。	2024年2月22日
新的安全控制	应启用 Macie 自动发现敏感数据的控件 [Macie.2] 现已可用。有关此控件的区域限制，请参阅按地区划分的控件可用性。	2024年2月19日
Security Hub 已在加拿大西部（卡尔加里）上线	Security Hub 现已在加拿大西部（卡尔加里）上线。除某些安全控件外，所有 Security Hub 功能现已在该地区提供。有关更多信息，请参阅根据区域的控件可用性。	2023 年 12 月 20 日

新的安全控件	以下新的 Security Hub 控件可用： • the section called “[Backup.1] 应在静态状态下对 AWS Backup 恢复点进行加密” • the section called “[DynamodB.6] DynamoDB 表应启用删除保护” • the section called “[EC2.51] EC2 Client VPN 端点应启用客户端连接日志记录” • the section called “[EKS.8] EKS 集群应启用审核日志记录” • the section called “[EMR.2] 应启用 Amazon EMR 屏蔽公共访问权限设置” • the section called “[fsx.1] 应将适用于 OpenZFS 的 FSX 文件系统配置为将标签复制到备份和卷” • the section called “[Macie.1] 应该启用亚马逊 Macie” • the section called “[MSK.2] MSK 集群应配置增强型监控” • the section called “[Neptune.9] Neptune 数据库集群应跨多个可用区部署” • the section called “[Network Firewall.1] Network Firewall 防火墙应部署在多个可用区域中”	2023 年 12 月 14 日

	• the section called “[Network Firewall.2] 应启用 Network Firewall 日志记录” • the section called “[Opensearch.10] OpenSearch 域名应安装最新的软件更新” • the section called “[PCA.1] 应禁用 AWS Private CA 根证书颁发机构” • the section called “[S3.19] S3 接入点已启用屏蔽公共访问权限设置” • the section called “[S3.20] S3 通用存储桶应启用 MFA 删除”	
调查发现富集	Security Hub 在 AWS 安全查找格式 (ASFF) 中添加了新的查找字段`AwsAccountName` `ApplicationArn` 、和`ApplicationName` 。	2023 年 11 月 27 日
摘要控制面板的增强功能	现在，您可以在 Security Hub 控制台的摘要页面上访问更多控制面板小组件，保存控制面板筛选器集以快速关注特定的安全问题，还可以自定义控制面板布局。	2023 年 11 月 27 日
中心配置	中央配置现已可用。通过中心配置，Security Hub 委托管理员可以跨多个组织账户、组织单元（OU）和区域配置 Security Hub、标准和控件。	2023 年 11 月 27 日

托管式策略的更新	Security Hub 为 AWSSecurityHubServiceRolePolicy 托管策略添加了新的权限，允许 Security Hub 读取和更新可自定义的安全控件属性。	2023 年 11 月 26 日
自定义控制参数	现在，您可以为所选 Security Hub 控件自定义参数值。这可以使特定控件的调查发现与您的业务需求和安全期望更加相关。	2023 年 11 月 26 日
托管式策略的更新	Security Hub 更新了AWSSecurityHubFullAccess 允许您分别使用 Security Hub 功能和与集成的AWSSecurityHubOrganizationsAccess 托管策略 AWS Organizations。	2023 年 11 月 16 日

服务管理标准中添加的现有安全控制措施： AWS Control Tower	以下现有的 Security Hub 控件已添加到服务管理标准中：AWS Control Tower。 • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	2023 年 11 月 14 日
托管式策略更新	Security Hub 为 `AWSSecurityHubServiceRolePolicy` 托管策略添加了新的标记权限，允许 Security Hub 读取与调查发现相关的资源标签。	2023 年 11 月 7 日

新的安全控件	以下新的 Security Hub 控件可用： • the section called “[AppSync.5] 不应使用 API AWS AppSync 密钥对 GraphQL API 进行身份验证” • the section called “[DMS.6] DMS 复制实例应启用自动次要版本升级” • the section called “[DMS.7] 目标数据库的 DMS 复制任务应启用日志记录” • the section called “[DMS.8] 源数据库的 DMS 复制任务应启用日志记录” • the section called “[DMS.9] DMS 端点应使用 SSL” • the section called “[DocumentDB.3] Amazon DocumentDB 手动集群快照不应公开” • the section called “[documentDB.4] Amazon DocumentDB 集群应将审计日志发布到日志 CloudWatch ” • the section called “[DocumentDB.5] Amazon DocumentDB 集群应启用删除保护” • the section called “[ECS.9] ECS 任务定义应具有日志配置” • the section called “[EventBridge.3] EventBridge 自定义	2023 年 10 月 10 日

事件总线应附加基于资源的策略”

- the section called “[EventBridge.4] EventBridge 全局端点应启用事件复制”
- the section called “[MSK.1] MSK 集群应在代理节点之间传输时进行加密”
- the section called “[MQ.5] ActiveMQ 代理应使用主动/备用部署模式”
- the section called “[MQ.6] RabbitMQ 代理应该使用集群部署模式”
- the section called “[NetworkFirewall.9] Network Firewall 防火墙应启用删除保护”
- the section called “[RDS.34] Aurora MySQL 数据库集群应将审计日志发布到日志 CloudWatch ”
- the section called “[RDS.35] RDS 数据库集群应启用自动次要版本升级”
- the section called “[Route53.2] Route 53 公有托管区域应记录 DNS 查询”
- the section called “[WAF.12] AWS WAF 规则应启用指标 CloudWatch ”

托管式策略更新	Security Hub 为 `AWSSecurityHubServiceRolePolicy` 托管策略添加了新的组织操作，允许 Security Hub 检索账户和组织单位 (OU) 信息。我们还添加了新的 Security Hub 操作，允许 Security Hub 读取和更新服务配置，包括标准和控件。	2023 年 9 月 27 日

服务管理标准中添加的现有安全控制措施： AWS Control Tower	以下现有的 Security Hub 控件已添加到服务管理标准中：AWS Control Tower。 • the section called “[Athena.1] Athena 工作组应进行静态加密” • the section called “[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密” • the section called “[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期” • the section called “[Neptune.1] 应对 Neptune 数据库集群进行静态加密” • the section called “[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch ” • the section called “[Neptune.3] Neptune 数据库集群快照不应公开” • the section called “[Neptune.4] Neptune 数据库集群应启用删除保护” • the section called “[Neptune.5] Neptune 数据库集群应启用自动备份” • the section called “[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密”	2023 年 9 月 26 日

	• the section called “[Neptune .7] Neptune 数据库集群应启用 IAM 数据库身份验证” • the section called “[Neptune .8] 应将 Neptune 数据库集群配置为将标签复制到快照” • the section called “[RDS.27] 应对 RDS 数据库集群进行静态加密”	
合并的控制视图和合并的控制结果可在中找到 AWS GovCloud (US)	整合的控件视图和整合的控件调查发现现已在 AWS GovCloud (US) Region中提供。Security Hub 控制台的控件页面显示了您跨标准的所有控件。每个控件在不同标准中都具有相同的控件 ID。当您启用整合的控件调查发现时，即使一项控件适用于多个启用的标准，您也会收到每项安全检查的单个调查发现。	2023 年 9 月 6 日
中国地区提供整合的控件视图和整合的控件调查发现	整合的控件视图和整合的控件调查发现现已在中国区域提供。Security Hub 控制台的控件页面显示了您跨标准的所有控件。每个控件在不同标准中都具有相同的控件 ID。当您启用整合的控件调查发现时，即使一项控件适用于多个启用的标准，您也会收到每项安全检查的单个调查发现。	2023 年 8 月 28 日

Security Hub 已在以色列（特拉维夫）区域可用	Security Hub 现已在以色列（特拉维夫）提供。除某些安全控件外，所有 Security Hub 功能现已在该地区提供。有关更多信息，请参阅根据区域的控件可用性。	2023 年 8 月 8 日

新的安全控件	以下新的 Security Hub 控件可用： • the section called “[Athena.1] Athena 工作组应进行静态加密” • the section called “[DocumentDB.1] Amazon DocumentDB 集群应进行静态加密” • the section called “[DocumentDB.2] Amazon DocumentDB 集群应有足够的备份保留期” • the section called “[Neptune.1] 应对 Neptune 数据库集群进行静态加密” • the section called “[Neptune.2] Neptune 数据库集群应将审计日志发布到日志 CloudWatch ” • the section called “[Neptune.3] Neptune 数据库集群快照不应公开” • the section called “[Neptune.4] Neptune 数据库集群应启用删除保护” • the section called “[Neptune.5] Neptune 数据库集群应启用自动备份” • the section called “[Neptune.6] 应在静态状态下对 Neptune 数据库集群快照进行加密”	2023 年 7 月 28 日

	• the section called “[Neptune .7] Neptune 数据库集群应启用 IAM 数据库身份验证” • the section called “[Neptune .8] 应将 Neptune 数据库集群配置为将标签复制到快照” • the section called “[RDS.27] 应对 RDS 数据库集群进行静态加密”	
自动化规则标准的新运算符	现在，您可以将 CONTAINS 和 NOT_CONTAINS 比较运算符用于自动化规则映射和字符串条件。	2023 年 7 月 25 日
自动化规则	Security Hub 现已提供自动化规则，这些规则会根据您指定的条件自动更新调查发现。	2023 年 6 月 13 日
新的第三方集成	Snyk 是一项新的第三方集成，会将结果发送到 Security Hub。	2023 年 6 月 12 日

服务管理标准中添加的现有安全控制措施： AWS Control Tower	以下现有的 Security Hub 控件已添加到服务管理标准中：AWS Control Tower。 • the section called “[Account.1] 应为以下人员提供安全联系信息 AWS 账户” • the section called “[APIGateway.8] API Gateway 路由应指定授权类型” • the section called “[APIGateway.9] 应为 API Gateway V2 阶段配置访问日志” • the section called “[CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密” • the section called “[EC2.25] Amazon EC2 启动模板不应为网络接口分配公有 IP” • the section called “[ELB.1] 应用程序负载均衡器应配置为将所有 HTTP 请求重定向到 HTTPS” • the section called “[Redshift.10] Redshift 集群应在静态状态下进行加密” • the section called “[SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动” • the section called “[SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限”	2023 年 6 月 12 日

	• the section called “[WAF.10] AWS WAF Web ACL 应至少有一个规则或规则组”	
新的安全控件	以下新的 Security Hub 控件可用： • the section called “[ACM.2] 由 ACM 托管的 RSA 证书应使用至少 2,048 位的密钥长度” • the section called “[AppSync.2] AWS AppSync 应该启用字段级日志记录” • the section called “[CloudFront.13] CloudFront 发行版应使用源站访问控制” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk 应该将日志流式传输到 CloudWatch” • the section called “[S3.17] S3 通用存储桶应使用静态加密 AWS KMS keys” • the section called “[StepFunctions.1] Step Functions 状态机应该开启日志功能”	2023 年 6 月 6 日
Security Hub 已在亚太地区（墨尔本）可用	Security Hub 现已在亚太地区（墨尔本）可用。除某些安全控件外，所有 Security Hub 功能现已在该地区提供。有关更多信息，请参阅根据区域的控件可用性。	2023 年 5 月 25 日

调查发现历史记录	Security Hub 现在可以追踪过去 90 天内调查发现的历史记录。	2023 年 5 月 4 日
新的安全控件	以下新的 Security Hub 控件可用： • the section called “[EKS.1] EKS 集群端点不应公开访问” • the section called “[ELB.16] 应用程序负载均衡器应与 Web ACL 关联 AWS WAF” • the section called “[Redshift.10] Redshift 集群应在静态状态下进行加密” • the section called “[S3.15] S3 通用存储桶应启用对象锁定”	2023 年 3 月 29 日
扩大对整合的控件调查发现的支持	AWS v2.0.0 上的自动安全响应现在支持整合的控制结果。	2023 年 3 月 24 日
Security Hub 已推出全新版本 AWS 区域	Security Hub 现已在亚太地区（海得拉巴）、欧洲(西班牙)和欧洲(苏黎世)推出。这些区域中可用的控件存在限制。	2023 年 3 月 21 日
托管式策略的更新	Security Hub 已更新 `AWSSecurityHubServiceRolePolicy` 托管策略中的现有权限。	2023 年 3 月 17 日

适用于 NIST 800-53 标准的新安全控件	Security Hub 增加了以下安全控件，这些控件适用于 NIST 800-53 标准： • the section called “[账户.2] AWS 账户 应该是 AWS Organizations 组织的一部分” • the section called “[CloudWatch.15] CloudWatch 警报应配置指定操作” • the section called “[CloudWatch.16] CloudWatch 日志组应在指定的时间段内保留” • the section called “[CloudWatch.17] 应激 CloudWatch 活警报动作” • the section called “[DynamoDB.4] 备份计划中应有 DynamoDB 表” • the section called “[EC2.28] 备份计划应涵盖 EBS 卷” • EC2.29 - EC2 实例应在 VPC 中启动（已停用） • the section called “[RDS.26] RDS 数据库实例应受备份计划保护” • the section called “[S3.14] S3 通用存储桶应启用版本控制” • the section called “[WAF.11] 应启 AWS WAF 用 Web ACL 日志记录”	2023 年 3 月 3 日

美国国家标准与技术研究院 (NIST) 800-53 Rev. 5	Security Hub 现在支持 NIST 800-53 Rev. 5 标准，具有 200 多种适用的安全控件。	2023 年 2 月 28 日
整合的控件视图和整合的控件调查发现	随着整合的控件视图发布，Security Hub 控制台的控件页面显示了您跨标准的所有控件。每个控件在不同标准中都具有相同的控件 ID。当您启用整合的控件调查发现时，即使一项控件适用于多个启用的标准，您也会收到每项安全检查的单个调查发现。	2023 年 2 月 23 日

新的安全控件	以下新的 Security Hub 控件可用。某些控件有区域限制。 • the section called “[ElastiCache.1] ElastiCache Redis 集群应启用自动备份” • the section called “[ElastiCache.2] ElastiCache 对于 Redis 缓存集群，应启用自动次要版本升级” • the section called “[ElastiCache.3] ElastiCache 对于 Redis 复制组，应启用自动故障转移” • the section called “[ElastiCache.4] ElastiCache 对于 Redis，复制组应进行静态加密” • the section called “[ElastiCache.5] ElastiCache 对于 Redis，复制组应在传输过程中进行加密” • the section called “[ElastiCache.6] ElastiCache 对于 6.0 版本之前的 Redis 复制组，应使用 Redis 身份验证” • the section called “[ElastiCache.7] ElastiCache 群集不应使用默认子网组”	2023 年 2 月 16 日

新的 ASFF 字段	Security Hub 已添加 ProductFields。 ArchivalReasons:0/描述和。 ProductFields ArchivalReasons:0/ 改ReasonCode 为 AWS 安全调查结果格式 (ASFF)。	2023 年 2 月 8 日
新的 ASFF 字段	Security Hub 增加了合规性。 AssociatedStandards 和合规。 SecurityControlId 改为 AWS 安全调查结果格式 (ASFF)。	2023 年 1 月 31 日
漏洞详情现已公布	现在，您可以在 Security Hub 控制台中查看漏洞详情，查看 Amazon Inspector 发送给 Security Hub 的调查发现。	2023 年 1 月 14 日
Security Hub 在中东（阿联酋）推出	Security Hub 现已在中东（阿联酋）推出 有些控件有区域限制。	2023 年 1 月 12 日
添加了与 MetricStream 的第三方集成	Security Hub 现在支持MetricStream在除中国以外的所有地区进行第三方集成 AWS GovCloud (US)。	2023 年 1 月 11 日
提高了组织账户限制	Security Hub 现在支持每个区域的每个 Security Hub 管理员账户最多 11,000 个成员账户。	2022 年 12 月 27 日
ElasticBeanstalk.3 向后滚动	Security Hub 撤销了控制权 [ElasticBeanstalk.3] Elastic Beanstalk 应该将所有区域的CloudWatch日志从 FSBP 标准流式传输到。	2022 年 12 月 21 日

Security Hub 添加了新的安全控件	启用了 FSBP 标准的客户可以使用新的 Security Hub 控件。某些控件有区域限制。	2022 年 12 月 15 日
即将推出的功能指南	Security Hub 计划发布两项新功能：整合的控件视图和整合的控件调查发现。这些即将推出的功能可能会影响依赖控件调查发现字段和值的现有工作流程。	2022 年 12 月 9 日
Amazon Security Lake 集成现已推出	Security Lake 现在通过接收 Security Hub 的调查发现与 Security Hub 集成。	2022 年 11 月 29 日
Support 对服务管理标准的支持： AWS Control Tower	Security Hub 支持一项名为 “服务管理标准” 的新安全标准：AWS Control Tower。 AWS Control Tower 管理这个标准。	2022 年 11 月 28 日
CIS AWS 基金会基准测试 v1.4.0 现已在中国地区推出	Security Hub 现在支持中国 AWS 地区的独联体基金会基准测试 v1.4.0。	2022 年 11 月 18 日
Jira 服务管理云集成现已推出	Jira 服务管理云现在可以接收除中国区域之外的所有支持区域的 Security Hub 调查发现。	2022 年 11 月 17 日
AWS IoT Device Defender 集成现已推出	AWS IoT Device Defender 现在将所有可用区域的发现结果发送到 Security Hub。	2022 年 11 月 17 日
Support 对 CIS AWS 基金会基准测试 v1.4.0	Security Hub 现在提供支持 CIS AWS 基金会基准测试 v1.4.0 的安全控制。该标准在除中国区域之外的所有支持区域可用。	2022 年 11 月 9 日

支持中的 Security Hub 公告 AWS GovCloud (US)	现在，您可以通过亚马逊简单通知服务 (Amazon SNS)（美国东部）AWS GovCloud 和（美国西部）订阅 S AWS GovCloud ecurity Hub 公告，以接收有关 Security Hub 的通知。	2022 年 10 月 3 日
AWS Security Hub 添加了新的安全控件	启用了 FSBP 标准的客户可以使用新的 Security Hub 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，您可以通过 Amazon Simple Notification Service (Amazon SNS) 订阅 Security Hub 公告，以接收有关 Security Hub 的通知。	2022 年 8 月 29 日
跨区域聚合的区域扩展	跨区域聚合现已在 AWS GovCloud (US)可用于调查发现、发现更新和见解。	2022 年 8 月 2 日
新的第三方产品集成	Fortinet - FortiCNP 是接收 Security Hub 调查发现的第三方集成，而 JFrog 是将调查发现发送到 Security Hub 的第三方集成。	2022 年 7 月 26 日
EC2.27 已停用	Security Hub 已停用 EC2.27-运行 EC2 实例不应使用密钥对，密钥对以前是 AWS 基础安全最佳实践 (FSBP) 标准中的控件。	2022 年 7 月 20 日

Lambda.2 不再支持 python3.6	Security Hub 不再支持 python3.6 作为 Lambda.2 的参数。Lambda 函数应使用支持的运行时，这是基础安全最佳实践 (FSB P) 标准中的控件。AWS	2022 年 7 月 19 日
AWS Security Hub 添加了新的安全控件	启用了 FSBP 标准的客户可以使用新的 Security Hub 控件。某些控件有区域限制。	2022 年 6 月 22 日
AWS Security Hub 支持新区域	Security Hub 现已在亚太地区（雅加达）推出。某些控件在此区域不可用。	2022 年 6 月 7 日
改进了 Sec AWS urity Hub 和之间的集成 AWS Config	Security Hub 用户可以在 Security Hub 中将 AWS Config 规则评估结果作为发现结果进行查看。	2022 年 6 月 6 日
增加了选择退出自动启用标准的功能	对于已与集成的用户 AWS Organizations，此功能允许您登录 Security Hub 管理员帐户，并选择新的成员帐户退出自动启用的标准。	2022 年 4 月 25 日
扩展的跨区域聚合	添加了跨区域聚合以控制状态和安全分数。	2022 年 4 月 20 日
CompanyName 现在 ProductName 是顶级属性	添加了新的顶级属性，用于设置与自定义集成关联的公司和产品名称	2022 年 4 月 1 日
为 AWS 基础安全最佳实践标准添加了新的控件	在 AWS 基础安全最佳实践标准中添加了 5 个新的控件	2022 年 3 月 31 日

在 ASFF 中添加了新的资源详细信息对象	在 ASFF 中添加了 `AwsRdsDbSecurityGroup` 资源类型。	2022 年 3 月 25 日
在 ASFF 中添加了其他资源详情	在 `AwsAutoScalingScalingGroup` 、`AwsElbLoadBalancer` 、`AwsRedshiftCluster` 和 `AwsCodeBuildProject` 中添加了更多详细信息。	2022 年 3 月 25 日
为 AWS 基础安全最佳实践标准添加了新的控件	在 AWS 基础安全最佳实践标准中添加了 15 个新的控件。	2022 年 3 月 16 日
为 AWS 基础安全最佳实践标准和支付卡行业数据安全标准 (PCI DSS) 添加了新的控件	为亚马逊 OpenSearch 服务、亚马逊 RDS、Amazon EC2、Elastic Load Balancin CloudFront g 以及 AWS 基础安全最佳实践标准添加了新的控件。还在 PCI DSS 中添加了两个新的 OpenSearch 服务控件。	2022 年 2 月 15 日
在 ASFF 中添加了新字段	添加了新字段：示例。	2022 年 1 月 26 日
增加了与的集成 AWS Health	AWS Health 使用 service-to-service 事件消息将发现结果发送到 Security Hub。	2022 年 1 月 19 日
增加了与的集成 AWS Trusted Advisor	Trusted Advisor 将其检查结果作为 Security Hub 的调查结果发送给 Security Hub。Security Hub 将其 AWS 基础安全最佳实践检查结果发送至。 Trusted Advisor	2022 年 1 月 18 日

更新了 ASFF 中的资源详细信息对象	已将 `MixedInstancesPolicy` 和 `AvailabilityZones` 添加到 `AwsAutoScalingAutoScalingGroup` 。已将 `MetadataOptions` 添加到 `AwsAutoScalingLaunchConfiguration` 。已将 `BucketVersioningConfiguration` 添加到 `AwsS3Bucket` 。	2021 年 12 月 20 日
更新了 ASFF 文档的输出	ASFF 属性的描述以前是在一个主题中进行的。现在，每个顶级对象和每个资源详细信息对象都在自己的主题中。ASFF 语法主题包含指向这些主题的链接。	2021 年 12 月 20 日
在 ASFF 中添加了新的资源详细信息对象 AWS Network Firewall	为 AWS Network Firewall，添加了以下资源详细信息对象：`AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy` 、和`AwsNetworkFirewallRuleGroup` 。	2021 年 12 月 20 日
增加了对新版 Amazon Inspector 的支持	Security Hub 已与新版本的 Amazon Inspector 以及 Amazon Inspector Classic 集成。Amazon Inspector 将调查发现发送到 Security Hub。	2021 年 11 月 29 日
已更改 EC2.19 的严重性	EC2.19（安全组不应允许不受限制地访问具有高风险的端口）的严重性从“高”更改为“严重”。	2021 年 11 月 17 日

与 Sonrai Dig 的新集成	Security Hub 现在提供了与 Sonrai Dig 的集成。Sonrai Dig 监控云环境以识别安全风险。Sonrai Dig 将调查发现发送到 Security Hub。	2021 年 11 月 12 日
更新了 CIS 2.1 和 CloudTrail .1 控件的检查	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
添加了对 VPC 端点的支持	Security Hub 现已与 VPC 终端节点集成 AWS PrivateLink 并支持。	2021 年 11 月 3 日
为 AWS 基础安全最佳实践标准添加了控件	为 Elastic Load Balancing（ELB.2 和 ELB.8）和 AWS Systems Manager（SSM.4）添加了新的控件。	2021 年 11 月 2 日
在 EC2.19 控件的检查中添加了端口	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（替代 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 从 Security Hub 接收调查发现。	2021 年 10 月 25 日
增加了对调查发现的跨区域聚合的支持	跨区域聚合使您无需更改区域即可查看所有调查发现。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发现从关联的区域汇总到聚合区域。	2021 年 10 月 20 日
更新了 ASFF 中的资源详细信息对象	向 `AwsCloudFrontDistribution` 中添加了查看器证书详细信息。向 `AwsCodeBuildProject` 中添加了更多详细信息。向 `AwsElbV2LoadBalancer` 添加了负载均衡器属性。已将 S3 存储桶所有者账户标识符添加到 `AwsS3Bucket` 。	2021 年 10 月 8 日
向 ASFF 添加了新的资源详细信息对象	向 ASFF 添加了以下新的资源详细信息对象：`AwsEc2VpcEndpointService` 、`AwsEcrRepository` 、`AwsEksCluster` 、`AwsOpenSearchServiceDomain` 、`AwsWafRateBasedRule` 、`AwsWafRegionalRateBasedRule` 、`AwsXrayEncryptionConfig`	2021 年 10 月 8 日

从 Lambda.2 控件中移除了已弃用的运行时	在 AWS 基础安全最佳实践标准中，从 [Lambda.2] 中删除的**dotnetcore2.1** 运行时 Lambda 函数应使用支持的运行时。	2021 年 10 月 6 日
检查点集成的新名称	与 Check Point Dome9 Arc 的集成现在是 Check Point CloudGuard 姿势管理。集成 ARN 没有改变。	2021 年 10 月 1 日
移除了与 Alcide 的集成	与 Alcide kAudit 的集成已停止。	2021 年 9 月 30 日
已更改 EC2.19 的严重性	EC2.19（安全组不应允许不受限制地访问具有高风险的端口）的严重性已从“中”更改为“高”。	2021 年 9 月 30 日
中国区域 AWS Organizations 现已支持与集成	Security Hub 与 Organizations 集成功能现已在中国（北京）和中国（宁夏）推出。	2021 年 9 月 20 日
S3.1 和 PCI.S3.6 控件的新 AWS Config 规则	S3.1 和 PCI.S3.6 均验证 Amazon S3 屏蔽公共访问权限设置是否已启用。这些控件的 AWS Config 规则已从更改`s3-account-level-public-access-blocks` 为`s3-account-level-public-access-blocks-periodic` 。	2021 年 9 月 14 日
从 Lambda.2 控件中移除了已弃用的运行时系统	在 AWS 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

已更改 CIS 2.2 控件的严重性	在 CIS AWS 基金会基准标准中，严重性为 2.2。— 确保启用 CloudTrail 日志文件验证已从 “低” 更改为 “中”。	2021 年 9 月 13 日
更新了基础安全最佳实践标准中的 ECS.1、Lambda.2 和 SSM.1 AWS	在 AWS 基础安全最佳实践标准中，ECS.1 现在有一个`SkipInactiveTaskDefinitions` 参数设置为。`true`这样可以确保控件仅检查活动任务定义。对于 Lambda.2，将 Python 3.9 添加到运行时系统列表中。SSM.1 现在会同时检查已停止和正在运行的实例。	2021 年 9 月 7 日
PCI.Lambda.2 控件现在不包括 Lambda @Edge 资源	在支付卡行业数据信息安全标准 (PCI DSS) 中，PCI.Lambda.2 控件现已将 Lambda @Edge 资源排除在外。	2021 年 9 月 7 日
添加了与 HackerOne Vulnerability Intelligence 的集成	Security Hub 现在提供了与 HackerOne Vulnerability Intelligence 的集成。该集成会将调查发现发送到 Security Hub。	2021 年 9 月 7 日
更新了 ASFF 中的资源详细信息对象	为 `AwsKmsKey` 添加了 `KeyRotationStatus` 。对于 `AwsS3Bucket` ，已添加 `AccessControlList` 、`BucketLoggingConfiguration` 、`BucketNotificationConfiguration` 和 `BucketWebsiteConfiguration` 。	2021 年 9 月 2 日

向 ASFF 添加了新的资源详细信息对象	在 ASFF 中添加了以下新的资源详细信息对象：AwsAutoScalingLaunchConfiguration 、AwsEc2VpnConnection 和 AwsEcrContainerImage 。	2021 年 9 月 2 日
在 ASFF 中为 Vulnerabilities 对象添加了细节	在 Cvss 中添加了 Adjustments 和 Source。在 VulnerablePackages 中添加了文件路径和包管理器。	2021 年 9 月 2 日
中国区域现已支持 Systems Manager Explorer 和 OpsCenter 集成	Security Hub 与 SSM Explorer 集成，现已在中国（北京）和中国（宁夏）支持。OpsCenter	2021 年 8 月 31 日
停用 Lambda.4 控件	Security Hub 即将停用控件 [Lambda.4] Lambda 函数应该配置死信队列。控件停用后，它将不再显示在控制台上，Security Hub 也不会对其进行检查。	2021 年 8 月 31 日
停用 PCI.EC2.3 控件	Security Hub 即将停用控件 [PCI.EC2.3] 应移除未使用的 EC2 安全组。控件停用后，它将不再显示在控制台上，Security Hub 也不会对其进行检查。	2021 年 8 月 27 日
更改了 Security Hub 将调查发现发送到自定义操作的方式	现在，当您将调查发现发送到自定义操作时，Security Hub 会在单独的 Security Hub Findings - Custom Action 事件中发送每个调查发现。	2021 年 8 月 20 日

为自定义 Lambda 运行时系统添加了新的合规状态原因代码	添加了新的 LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE 合规状态原因代码。此原因代码表明 Security Hub 无法对自定义 Lambda 运行时执行检查。	2021 年 8 月 20 日
AWS Firewall Manager 中国区域现已支持集成	Security Hub 与 Firewall Manager 集成功能现已在中国（北京）和中国（宁夏）推出。	2021 年 8 月 19 日
与 Caveonix Cloud 和 Forcepoint Cloud Security Gateway 的新集成	Security Hub 现在提供与 Caveonix Cloud 和 Forcepoint Cloud Security Gateway 的集成。这两种集成都会将调查发现发送到 Security Hub。	2021 年 8 月 10 日
在 ASFF 中添加了新的 CompanyName 、ProductName 和 Region 属性	在 ASFF 的顶层添加了 CompanyName 、ProductName 和 Region 字段。这些字段是自动填充的，除自定义产品集成外，无法使用 BatchImportFindings 或 BatchUpdateFindings 进行更新。在控制台上，调查发现筛选条件使用这些新字段。在 API 中，CompanyName 和 ProductName 筛选条件使用 ProductFields 下方的属性。	2021 年 7 月 23 日

在 ASFF 中添加和更新了资源详细信息对象	添加了新的 AwsRdsEventSubscription 资源类型和资源详细信息。为 AwsEcsService 资源类型添加了资源详细信息。为 AwsElasticsearchDomain 资源详细信息对象添加了属性。	2021 年 7 月 23 日
为 AWS 基础安全最佳实践标准添加了控件	为亚马逊 API Gateway.5、亚马逊 EC2（EC2.19）、亚马逊 ECS（ECS.2）、Elastic Load Balancing（ELB.7）、亚马逊服务（ES.5 到 ES.8）、亚马逊 RDS（RDS.16 到 RDS.23）、 OpenSearch 亚马逊 Redshift（Redshift.4）和亚马逊 SQS 添加了新的控件 S(SQS.1)。	2021 年 7 月 20 日
在服务相关角色托管式策略中移动权限	在托管策略 AWSSecurityHubServiceRolePolicy 中移动了 config:PutEvaluations 权限，使其适用于所有资源。	2021 年 7 月 14 日

为 AWS 基础安全最佳实践标准添加了控件	为亚马逊 API Gateway.4、亚马逊（.5 和. CloudFront 6）、亚马逊 EC2CloudFront（EC2.17 和 EC2.18）、 CloudFront 亚马逊 EC2（EC2.17 和 EC2.18）、亚马逊 ECS（ECS.1）、亚马逊服务（ES.4）、（IAM.21）、亚马逊 RDS（RDS.15）和 OpenSearch 亚马逊 S3（S3.8） AWS Identity and Access Management 添加了新的控件。	2021 年 7 月 8 日
为控件调查发现添加了新的合规状态原因代码	`INTERNAL_SERVICE_ERROR` 表示出现未知错误。`SNS_TOPIC_CROSS_ACCOUNT` 表示 SNS 主题由其他账户拥有。`SNS_TOPIC_INVALID` 表示关联的 SNS 主题无效。	2021 年 7 月 6 日
添加了与的集成 AWS Chatbot	添加了与的集成 AWS Chatbot。Security Hub 将调查结果发送到 AWS Chatbot。	2021 年 6 月 30 日
为服务相关的角色托管策略添加了新权限	为托管策略 `AWSSecurityHubServiceRolePolicy` 添加了新权限，允许服务相关角色向 AWS Config提供评估结果。	2021 年 6 月 29 日

ASFF 中新增的和更新的资源详细信息对象	为 ECS 群集和 ECS 任务定义添加了新的资源详细信息对象。更新了 EC2 实例对象以列出相关的网络接口。为 API Gateway V2 阶段添加了客户端证书 ID。为 S3 存储桶添加了生命周期配置。	2021 年 6 月 24 日
更新了汇总控件状态和标准安全分数的计算	现在，Security Hub 每 24 小时计算一次总体控件状态和标准安全分数。对于管理员账户，分数现在反映了每个账户是启用还是禁用了每个控件。	2021 年 6 月 23 日
有关 Security Hub 处理暂停账户的更新信息	添加了有关 Security Hub 如何处理 AWS中被暂停的账户的信息。	2021 年 6 月 23 日
添加了选项卡以显示个人管理员账户的启用和禁用控件	对于管理员账户，标准详细信息页面上的主要选项卡包含跨账户的汇总信息。新的为此账户启用和为此账户禁用选项卡列出了为单个管理员账户启用或禁用的账户。	2021 年 6 月 23 日
添加 `java8.al2` 到 `Lambda.2` 的参数	在 AWS 基础安全最佳实践标准中，已`java8.al2` 添加到控件支持的运行时中。`Lambda.2`	2021 年 6 月 8 日
与 NETSCOUT 网络 MicroFocus ArcSight 调查员的新集成	增加了与 NETSCOUT 网络 MicroFocus ArcSight 调查员的集成。 MicroFocus ArcSight 接收来自 Security Hub 的调查结果。NETSCOUT 网络调查员将调查发现发送到 Security Hub。	2021 年 6 月 7 日

为 AWSSecurityHubServiceRolePolicy 添加了详细信息	更新了托管式策略部分以添加现有托管式策略 AWSSecurityHubServiceRolePolicy 的详细信息，该策略由 Security Hub 服务相关角色使用。	2021 年 6 月 4 日
与 Jira 服务管理的新集成	Jira 的 AWS 服务管理连接器将调查结果发送到 Jira，并使用它们来创建 Jira 事务。当 Jira 问题更新时，Security Hub 中的相应调查发现也会更新。	2021 年 5 月 26 日
更新了亚太地区（大阪）区域支持的控件列表	更新了 CIS AWS 基金会标准和支付卡行业数据安全标准 (PCI DSS)，以指明亚太地区（大阪）不支持的控制措施。	2021 年 5 月 21 日
与适用于云的 Sysdig Secure 的新集成	添加了与 Sysdig Secure 云的集成。该集成会将调查发现发送到 Security Hub。	2021 年 5 月 14 日

为 AWS 基础安全最佳实践标准添加了控件	为亚马逊 API Gateway（Apigateway.2 和 Apigateway.3）、（. AWS CloudTrail 4 和 .5）、亚马逊 EC2（EC2.15 CloudTrail 和 EC2.16 CloudTrail）、（.1 和 .2）、（Lambda.4）、亚马逊 RDS AWS Elastic Beanstalk（RDS.12 — RDS ElasticBeanstalk .14）、亚马逊 Redshift AWS Lambda（Redshift.7）、（.3 和 ElasticBeanstalk .4）和 (WAF.1)。 AWS Secrets Manager SecretsManager SecretsManager AWS WAF	2021 年 5 月 10 日
Amazon RDS 控件的更新 GuardDuty 和	已将 `GuardDuty.1` 和 `PCI.GuardDuty.1` 的严重程度从“中”更改为“高”。向 `RDS.8` 中添加了一个 `databaseEngines` 参数。	2021 年 5 月 4 日
向 ASFF 添加了新的资源详细信息	在 `Resources.Details` 中，为 Amazon EC2 网络 ACL、Amazon EC2 子网和 AWS Elastic Beanstalk 环境添加了新的资源详细信息对象。	2021 年 5 月 3 日
添加了控制台字段以提供 Amazon EventBridge 规则的筛选值	Security Hub EventBridge 规则的新预定义筛选模式提供了可用于指定筛选值的控制台字段。	2021 年 4 月 30 日

添加了与 AWS Systems Manager Explorer 的集成和 OpsCenter	Security Hub 现在支持与 Systems Manager Explorer 的集成 OpsCenter。该集成接收来自 Security Hub 的调查发现，并在 Security Hub 中更新这些调查发现。	2021 年 4 月 26 日
产品集成的新类型	新的集成类型 `UPDATE_FINDINGS_IN_SECURITY_HUB` 表示产品集成更新了从 Security Hub 收到的调查发现。	2021 年 4 月 22 日
将“主账户”更改为“管理员账户”	术语 “主账户” 已更改为 “管理员账户”。该术语也在 Security Hub 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 Websocket	更新了 APIGateway.1 的标题、描述和修复。该控件现在会检查 Websocket API 执行日志记录，而不是 HTTP API 执行日志记录。	2021 年 4 月 9 日
北京和宁夏现已支持亚马逊 GuardDuty 集成	现在，中国（北京）和中国（宁夏）区域支持与 GuardDuty Security Hub 的集成。	2021 年 4 月 5 日
已添加 `nodejs14.x` 到 Lambda.2 控件支持的运行时系统中	基础安全最佳实践标准中的 Lambda.2 控件现在支持 `nodejs14.x` 运行时系统。	2021 年 3 月 30 日
Security Hub 在亚太地区（大阪）推出	Security Hub 现已在亚太地区（大阪）区域中可用。	2021 年 3 月 29 日

在调查发现详细信息中添加了调查发现提供商字段	在调查发现详细信息面板上，新的调查发现提供商字段部分包含置信度、重要性、相关调查发现、严重性和类型的调查发现提供商值。	2021 年 3 月 24 日
增加了接收来自 Amazon Macie 的敏感调查发现的选项	现在可以将与 Macie 的集成配置为将敏感调查发现发送到 Security Hub。	2021 年 3 月 23 日
正在过渡到 AWS Organizations 用于账户管理	对于现有管理员账户和成员账户的客户，添加了有关如何从受邀管理账户改为使用 Organizations 管理账户的新信息。	2021 年 3 月 22 日
ASFF 中的新对象用于了解有关 Amazon S3 公共访问屏蔽设置的信息	在 `Resources` 中，新的 `AwsS3AccountPublicAccessBlock` 资源类型和详细信息对象提供了有关账户的 Amazon S3 公共访问屏蔽设置的信息。在 `AwsS3Bucket` 资源详细信息对象中，该 `PublicAccessBlockConfiguration` 对象提供了 S3 存储桶的公共访问屏蔽设置。	2021 年 3 月 18 日

ASFF 中的新对象允许调查发现提供商更新特定字段	ASFF 中的新 FindingProviderFields 对象用于在 BatchImportFindings 中为 Confidence 、Criticality 、RelatedFindings 、Severity 和 Types 提供值。只能使用 BatchUpdateFindings 更新原始字段。	2021 年 3 月 18 日
ASFF 中资源的新 DataClassification 对象	ASFF 中的新 Resources.DataClassification 对象用于提供有关在资源上检测到的敏感数据的信息。	2021 年 3 月 18 日
为可用的合规性状态代码增添了 CONFIG_RETURNS_NOT_APPLICABLE 值	对于 NOT_AVAILABLE 合规性状态，删除了原因代码 RESOURCE_NO_LONGER_EXISTS 并添加了原因代码 CONFIG_RETURNS_NOT_APPLICABLE 。	2021 年 3 月 16 日
用于与集成的新托管策略 AWS Organizations	新的托管策略 AWSSecurityHubOrganizationsAccess 提供了组织管理账户和委托的 Security Hub 管理员账户所需的组织权限。	2021 年 3 月 15 日
托管策略和服务相关角色信息已移至“安全”一章	对有关托管政策的信息进行了修订和扩展。托管策略信息和服务相关角色信息均已移至“安全”一章。	2021 年 3 月 15 日

与 SecureCloud数据库的新集成	将 SecureCloud DB 添加到第三方集成列表中。 SecureCloud数据库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。SecureCloud数据库将调查结果发送到 Security Hub。	2021 年 3 月 4 日
修订了 CIS 1.1 和 CIS 3.1 — CIS 3.14 控件的严重性	CIS 1.1 和 CIS 3.1 — CIS 3.14 控件的严重性更改为“低”。	2021 年 3 月 3 日
已移除 RDS.11 控件	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，可以发送和接收调查发现。	2021 年 2 月 26 日
为基础安全最佳实践标准添加了控件	为亚马逊 API Gateway (ApiGateway.1)、亚马逊 EC2 (EC2.9 和 EC2.10)、亚马逊弹性文件系统 (EFS.2)、亚马逊 OpenSearch 服务 (ES.2 和 ES.3)、Elastic Load Balancing (ELB.6) 和 () (KMS.3) 添加了新的控件。 AWS Key Management Service AWS KMS	2021 年 2 月 11 日
在 `DescribeProducts` API 中添加了可选 `ProductArn` 筛选条件	`DescribeProducts` API 操作现在包含一个可选 `ProductArn` 参数。`ProductArn` 参数用于标识要返回其详细信息的特定产品集成。	2021 年 2 月 3 日
云存储安全与适用于 Amazon S3 的防病毒软件的新集成	与 Amazon S3 防病毒软件的集成会将病毒扫描结果作为调查发现发送到 Security Hub。	2021 年 1 月 27 日

更新了管理员账户的安全评分计算流程	对于管理员帐户，Security Hub 使用单独的过程来计算安全分数。新流程可确保分数包括对成员账户启用、但对管理员账户禁用的控件。	2021 年 1 月 21 日
ASFF 中的新字段和对象	添加了一个新 `Action` 对象来跟踪对资源执行的操作。在 `AwsEc2NetworkInterface` 对象中添加了用于跟踪 DNS 名称和 IP 地址的字段。在资源详细信息中添加了一个新 `AwsSsmPatchCompliance` 对象。	2021 年 1 月 21 日
为基础安全最佳实践标准添加了控件	为亚马逊 CloudFront（CloudFront.1 到. CloudFront 4）、亚马逊 DynamoDB（DynamoDB.1 到 DynamodB. 3）、Elastic Load Balancing（ELB.3 到 ELB.5）、亚马逊 RDS（RDS.9 到 RDS.11）、亚马逊 Redshift（Redshift.1 到 Redshift.3 和 Redshift.6）和亚马逊 SNS（SNS.1)。	2021 年 1 月 15 日
根据记录状态或合规性状态重置工作流状态	如果存档的调查发现处于活动状态，或者调查发现的合规性状态从 `PASSED` 更改为 `FAILED`、`WARNING` 或 `NOT_AVAILABLE` ，Security Hub 将自动将工作流状态从 `NOTIFIED` 或 `RESOLVED` 重置为 `NEW`。这些变化表明需要进一步调查。	2021 年 1 月 7 日

为基于控件的调查发现添加了 `ProductFields` 信息	对于通过控件生成的调查发现，添加了有关 AWS 安全调查发现格式（ASFF）中 `ProductFields` 对象内容的信息。	2020 年 12 月 29 日
托管见解的更新	更改了 见解 5 的标题。添加了新的见解 32，用于检查是否存在可疑活动的 IAM 用户。	2020 年 12 月 22 日
IAM.7 和 Lambda.1 控件的更新	在 AWS 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
扩展了与 ServiceNow ITSM 的集成	ServiceNow ITSM 集成允许用户在收到 Security Hub 的调查结果时自动创建事件或问题。对这些事件或问题的更新会导致对 Security Hub 中调查发现进行更新。	2020 年 12 月 11 日
与 Audit Manag AWS er 的新集成	Security Hub 现在提供与 Audit Man AWS ager 的集成。该集成允许 Audit Manager 接收来自 Security Hub 的基于控件的调查发现。	2020 年 12 月 8 日
与 Aqua Security Kube-bench 的新集成	Security Hub 增加了与 Aqua Security Kube-bench 的集成。该集成会将调查发现发送到 Security Hub。	2020 年 11 月 24 日
云托管现已在中国区域推出	与云托管的集成，现已在中国（北京）和中国（宁夏）区域推出。	2020 年 11 月 24 日

BatchImportFindings 现在可以用来更新其他字段	以前，您无法使用 BatchImportFindings 更新 Confidence 、Criticality 、RelatedFindings 、Severity 和 Types 字段。现在，如果这些字段尚未由 BatchUpdateFindings 更新，则可以通过 BatchImportFindings 进行更新。它们一旦被 BatchUpdateFindings 更新，就不能由 BatchImportFindings 更新。	2020 年 11 月 24 日
Security Hub 现已与 AWS Organizations	客户现在可以使用他们的 Organizations 账户配置来管理成员账户。组织管理账户指定 Security Hub 管理员账户，该账户确定要在 Security Hub 中启用哪些组织账户。对于不属于组织的账户，仍可使用手动邀请流程。	2020 年 11 月 23 日
删除了高容量控件的单独调查发现列表格式	当存在大量调查发现时，控件的调查发现列表不再使用调查发现页面格式。	2020 年 11 月 19 日
新的和更新的第三方集成	Security Hub 现在支持与 cloudtamer.io、3CoreSec、Prowler 和 Kubernetes Security 集成。 StackRox IBM QRadar 不再发送调查发现。它只接收调查发现。	2020 年 10 月 30 日

添加了从控件详细信息页面下载调查发现列表的选项。	在控件详细信息页面上，新的下载选项允许您将调查发现列表下载到 .csv 文件。下载的列表会考虑列表中的所有筛选条件。如果您选择了特定的调查发现，则下载的列表仅包含这些调查发现。	2020 年 10 月 26 日
添加了从标准详细信息页面下载控件列表的选项。	在标准详细信息页面上，新的下载选项允许您将控制列表下载到 .csv 文件。下载的列表会考虑列表中的所有筛选条件。如果您选择了特定控件，则下载的列表仅包含该控件。	2020 年 10 月 26 日
新增的和更新的合作伙伴集成	Security Hub 现已与集成 ThreatModeler。更新了以下合作伙伴集成，以反映他们的新产品名称。Twistlock 企业版现在是 Palo Alto Networks-Prisma Cloud Compute。Demisto 同样来自 Palo Alto Networks，现在是 Cortex XSOAR，Redlock 现在是 Prisma Cloud Enterprise。	2020 年 10 月 23 日
Security Hub 在中国（北京）和中国（宁夏）推出	Security Hub 现已在中国（北京）和中国（宁夏）区域推出。	2020 年 10 月 21 日
修改了 ASFF 属性和第三方集成的格式	ASFF 属性和合作伙伴集成现在使用基于列表的格式，而不是表格。ASFF 语法、属性和类型分类法现在位于不同的主题中。	2020 年 10 月 15 日

重新设计的标准详情页面	启用标准的标准详细信息页面现在会显示选项卡式控件列表。这些选项卡根据控件状态筛选控制列表。	2020 年 10 月 7 日
将 CloudWatch 事件替换为 EventBridge	将提及亚马逊 CloudWatch 活动的内容替换为亚马逊 EventBridge。	2020 年 10 月 1 日
与 Blue Hexagon AWS、Alcide kAudit 和 Palo Alto Networks VM 系列的新集成。	Security Hub 现已与 Blue Hexagon AWS、Alcide kAudit 和 Palo Alto Networks VM 系列集成。Blue Hexagon for AWS 和 kAudit 将调查结果发送到 Security Hu VM 系列可接收来自 Security Hub 的调查发现。	2020 年 9 月 30 日
ASFF 中新增和更新的资源详细信息对象	为 `AwsApiGatewayRestApi` 、`AwsApiGatewayStage` 、`AwsApiGatewayV2Api` 、`AwsApiGatewayV2Stage` 、`AwsCertificateManagerCertificate` 、`AwsElbLoadBalancer` 、`AwsIamGroup` 和 `AwsRedshiftCluster` 添加了新 `Resources.Details` 对象。为 `AwsCloudFrontDistribution` 、`AwsIamRole` 和 `AwsIamAccessKey` 对象添加了详细信息。	2020 年 9 月 30 日

ASFF 中资源的新 ResourceRole 属性，用于跟踪资源是角色还是目标。	资源的 ResourceRole 属性表示资源是调查发现活动的目标还是调查发现活动的实施者。有效值为 ACTOR 和 TARGET。	2020 年 9 月 30 日
在可用的 AWS 服务集成中添加了 AWS Systems Manager 补丁管理器	AWS Systems Manager 补丁管理器现已与 Security Hub 集成。当客户实例集中的实例不符合其补丁合规性标准时，Patch Manager 会将结果发送给 Security Hub。	2020 年 9 月 22 日
为 AWS 基础安全最佳实践标准添加了新的控件	为以下服务添加了新的控件：亚马逊 EC2（EC2.7 和 EC2.8）、亚马逊 EMR（EMR.1）、IAM（IAM .8）、亚马逊 RDS（RDS.4 到 RDS.8）、亚马逊 S3（S3.6）和（.1 和 .2）。 AWS Secrets Manager SecretsManager SecretsManager	2020 年 9 月 15 日
用于控制 BatchUpdateFindings 字段访问权限的 IAM policy 的新上下文密钥	现在可以将 IAM policy 配置为在使用 BatchUpdateFindings 时限制对字段和字段值的访问。	2020 年 9 月 10 日
扩大了成员账户 BatchUpdateFindings 的访问权限	默认情况下，成员账户现在具有与管理员账户BatchUpdateFindings 相同的访问权限。	2020 年 9 月 10 日

基础安全最佳实践标准 AWS KMS 中的新控件	在基础安全最佳实践标准中添加了两个新控件（KMS.1 和 KMS.2）。新的控制措施会检查 IAM 策略是否限制对 AWS KMS 解密操作的访问。	2020 年 9 月 9 日
删除了账户级别的控件调查发现	Security Hub 不再为控件生成账户级别的调查发现。仅生成资源级别的调查发现。	2020 年 9 月 1 日
ASFF 中的新 PatchSummary 对象	已将 `PatchSummary` 对象添加到 ASFF 中。`PatchSummary` 对象提供有关资源相对于所选合规性标准的补丁合规性的信息。	2020 年 9 月 1 日
重新设计的控件详情页面	重新设计了控件详细信息页面。控件调查发现列表提供选项卡，允许您根据合规性状态快速筛选列表。您还可以快速查看隐藏的调查发现。每个条目都允许访问有关查找资源、AWS Config 规则和查找结果注释的其他详细信息。	2020 年 8 月 28 日
新的调查发现筛选选项	对于调查发现筛选条件，可以使用 is not 筛选条件来查找字段值不等于筛选条件值的调查发现。您可以使用 does not start with 来查找字段值不是以指定筛选值开头的调查发现。	2020 年 8 月 28 日

ASFF 中的新资源详细信息对象	为以下资源类型添加了新 `Resources.Details` 对象：`AwsDynamoDbTable` 、`AwsEc2Eip` 、`AwsIamPolicy` 、`AwsIamUser` 、`AwsRdsDbCluster` 、`AwsRdsDbClusterSnapshot` 、`AwsRdsDbSnapshot` 、`AwsSecretsManagerSecret`	2020 年 8 月 18 日
与 RSA Archer 的新集成	Security Hub 现已与 RSA Archer 集成。RSA Archer 从 Security Hub 接收调查发现。	2020 年 8 月 18 日
新的 “描述” 字段 AwsKmsKey	为 `Resources.Details` 下面的 `AwsKmsKey` 对象添加了一个 `Description` 字段。	2020 年 8 月 18 日
向添加了字段 AwsRdsDbInstance	为 `Resources.Details` 下面的 `AwsRdsDbInstance` 对象添加了几个属性。	2020 年 8 月 18 日
更新了 Security Hub 确定控件总体状态的方式	对于没有调查发现的控件，状态为无数据，而不是未知。控制状态包括账户级别和资源级别的调查发现。控制状态不使用调查发现的工作流状态，但忽略隐藏的调查发现除外。	2020 年 8 月 13 日

更新了 Security Hub 计算标准安全分数的方式	在计算标准的安全分数时，Security Hub 现在会忽略状态为无数据的控件。安全分数是已通过的控件与已启用的控件的比例，不包括没有数据的控件。	2020 年 8 月 13 日
在已启用的标准中自动启用新控件的新选项	添加了设置选项，以自动启用已启用的标准中的新控件。您还可以使用 `UpdateSecurityHubConfiguration` API 操作配置此选项。	2020 年 7 月 31 日
支付卡行业数据安全标准 (PCI DSS) 标准的新控件	在 PCI DSS 标准中添加了新的控件。新控件的标识符是 PCI.DMS.1、PCI.EC2.5、PCI.EC2.6、PCI.ELBV2.1、PCI。 GuardDuty.1、PCI.IAM.7、PCI.IAM.8、PCI.S3.5、PCI.S3.6、PCI。 SageMaker.1、PCI.SSM.2 和 PCI.SSM.3。	2020 年 7 月 29 日
基础安全最佳实践标准中新增的和更新的控件	在基础安全最佳实践标准中添加了新的控件。新控件的标识符是 AutoScaling .1、DMS.1、EC2.4、EC2.6、S3.5 和 SSM.3。更新了 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，该对象提供与调查发现相关的漏洞的相关信息。	2020 年 7 月 1 日

ASFF 中适用于自动扩缩组、EC2 卷和 EC2 VPC 的新 Resource.Details 对象	在 Resource.Details 中新增了 AwsAutoScalingAutoScalingGroup 、AWSEc2Volume 和 AwsEc2Vpc 对象。	2020 年 7 月 1 日
ASFF 中的新 NetworkPath 对象	添加了 NetworkPath 对象，它提供与调查发现相关的网络路径的相关信息。	2020 年 7 月 1 日
当 Compliance.Status 为 PASSED 时自动解决发现的问题	对于来自控件的调查发现，如果 Compliance.Status 是 PASSED，则 Security Hub 会自动设置 Workflow.Status 为 RESOLVED。	2020 年 6 月 24 日
AWS Command Line Interface 例子	为多个 Security Hub 任务添加了 AWS 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，与控件状态的详细信息有关	添加了 Compliance.StatusReasons 对象，该对象为控制的当前状态提供了附加上下文。	2020 年 5 月 20 日
新的 AWS 基础安全最佳实践标准	添加了新的 AWS 基础安全最佳实践标准，该标准是一组控件，用于检测您部署的账户和资源何时偏离安全最佳实践。	2020 年 4 月 22 日

用于更新调查发现工作流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
用于客户更新调查发现的新 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
AWS 安全调查结果格式 (ASFF) 的更新	添加了几种新的资源类型。向 Severity 对象添加了一个新的 Label 属性。Label 将用于替换 Normalized 字段。添加了一个新的 Workflow 对象来跟踪调查过程以获得结果。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
对“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，此页面现在显示集成类别，以及每个集成是向 Security Hub 发送调查发现还是从中接收调查发现。它还提供了启用每个集成所需的特定步骤。	2020 年 2 月 26 日

新的第三方产品集成	添加了以下新产品集成：Cloud Custodian、FireEye Helix、Forcepoint CASB、Forcepoint DLP、Forcepoint NGFW、Rackspace 云原生安全和 Vectra.ai Cognito Detect。	2020 年 2 月 21 日
支付卡行业数据安全标准 (PCI DSS) 的新安全标准	为支付卡行业数据安全标准 (PCI DSS) 添加了 Security Hub 安全标准。如果启用了该标准，Security Hub 将针对与 PCI DSS 要求相关的控制执行自动检查。	2020 年 2 月 13 日
AWS 安全调查结果格式 (ASFF) 的更新	为标准控制的相关要求添加了一个字段。添加了新的资源类型和新的资源详细信息。ASFF 现在还允许您提供最多 32 个资源。	2020 年 2 月 5 日
禁用各个安全标准控件的新选项	添加了有关如何控制是否启用每个单独的安全标准控制的信息。	2020 年 1 月 15 日
对术语和概念的更新	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
AWS Security Hub 正式发布版本	更新内容以反映预览期间对 Security Hub 所做的改进。	2019 年 6 月 25 日
为 CIS AWS 基金会检查添加了补救步骤	在 Security Hub 支持的安全标准中 AWS添加了补救步骤。	2019 年 4 月 15 日
Sec AWS urity Hub 的预览版	发布了 AWS Security Hub 用户指南的预览版。	2018 年 11 月 18 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。