实施指南

AWS 上的自动安全响应

AWS 上的自动安全响应: 实施指南

Table of Contents

在 AWS Security Hub 中使用预定义的响应和补救措施自动应对安全威胁

本实施指南概述了 AWS 上的自动安全响应解决方案、其参考架构和组件、部署规划注意事项、将 AWS 上的自动安全响应解决方案部署到 Amazon Web Services (AWS) 云的配置步骤。

使用以下导航表可快速找到这些问题的答案：

如果您想. . .	阅读. . .
了解运行此解决方案的成本	成本
了解此解决方案的安全注意事项	安全性
知道如何为该解决方案规划配额	配额
了解此解决方案支持哪些 AWS 区域	支持的 AWS 区域
查看或下载此解决方案中包含的 AWS CloudFormation 模板，以自动部署此解决方案的基础设施资源（“堆栈”）	AWS CloudFormation 模板
访问源代码，也可以选择使用 AWS Cloud Development Kit (AWS CDK) 来部署解决方案。	GitHub 存储库

安全的持续发展需要采取积极措施来保护数据，这会使安全团队难以做出反应，而且成本高昂且耗时。AWS 上的自动安全响应解决方案可根据行业合规标准和最佳实践提供预定义的响应和补救措施，从而帮助您快速应对安全问题。

AWS 上的自动安全响应是一种 AWS 解决方案，可与 AWS Sec urity Hub 配合使用，以提高您的安全性，并帮助您的工作负载与 Well-Architected 安全支柱最佳实践 SEC1 (0) 保持一致。该解决方案让 AWS Security Hub 的客户可以更轻松地解决常见的安全问题并改善他们在 AWS 中的安全状况。

您可以选择要在您的 Security Hub 主账户中部署的特定攻略手册。每本手册都包含在单个 A WS 账户或多个账户中启动补救工作流程所需的必要自定义操作、身份和访问管理 (IAM) 角色、亚马逊 EventBridge 规则、AWS S ystems Manager 自动化文档、AWS Lambda 函数和 AWS Step

Functions。补救措施可通过 AWS Security Hub 的 “操作” 菜单进行，允许授权用户通过单一操作修复其所有 AWS Security Hub 管理的账户中的发现。例如，您可以应用互联网安全中心 (CIS) AWS Foundations Benchmark（一项保护 AWS 资源的合规标准）的建议，确保密码在 90 天内过期，并对存储在 AWS 中的事件日志强制加密。

> **Note**
>
> 补救措施旨在应对需要立即采取行动的紧急情况。只有在您通过 AWS Security Hub 管理控制台启动或使用特定控制的 Amazon EventBridge 规则启用自动补救时，此解决方案才会对发现的修复进行更改。要恢复这些更改，必须手动将资源恢复到其原始状态。
>
> 修复作为 CloudFormation 堆栈一部分部署的 AWS 资源时，请注意这可能会导致偏差。如果可能，请通过修改定义堆栈资源的代码并更新堆栈来修复堆栈资源。有关更多信息，请参阅什么是漂移？ 在 AWS CloudFormation 用户指南中。

AWS 上的自动安全响应包括针对以下内容中定义的安全标准的行动手册补救措施：

- 互联网安全中心 (CIS) AWS 基金会基准测试 v1.2.0
- CIS AWS 基金会基准测试 v1.4.0
- CIS AWS 基金会基准测试 v3.0.0
- AWS 基础安全最佳实践 (FSBP) v.1.0.0
- 支付卡行业数据安全标准 (PCI-DSS) v3.2.1
- 美国国家标准与技术研究所 (NIST) SP 800-53 Rev. 5

该解决方案还包括 AWS Security Hub 整合控制结果功能的安全控制 (SC) 手册。有关更多信息，请参阅行动手册。我们建议使用 SC 手册以及 Security Hub 中的综合控制结果。

本实施指南讨论了在 AWS 云中部署 AWS 上的自动安全响应解决方案的架构注意事项和配置步骤。它包括指向 AWS CloudFormation 模板的链接，这些模板使用 AWS 安全性和可用性最佳实践启动、配置和运行在 AWS 上部署此解决方案所需的 AWS 计算、网络、存储和其他服务。

本指南面向在 AWS 云中具有架构实践经验的 IT 基础设施架构师、管理员和 DevOps 专业人士。

功能和优势

AWS 上的自动安全响应提供以下功能：

自动修复针对特定控制措施的调查结果

激活亚马逊控件 EventBridge 规则，以便在该控件的发现出现在 AWS Security Hub 中后立即自动对其进行修复。

从一个位置管理多个账户和区域的补救措施

在配置为组织账户和区域聚合目标的 AWS Security Hub 管理员账户中，针对部署解决方案的任何账户和区域中的发现启动补救措施。

获取补救措施和结果的通知

订阅解决方案部署的 Amazon SNS 主题，即可在启动补救措施以及补救是否成功时收到通知。

使用 Web 用户界面启动、查看和管理修正

在部署管理堆栈时，您可以选择启用解决方案的 Web UI，这将提供一个全面的用户友好型视图，用于运行修复和查看该解决方案过去执行的所有补救措施。

与 Jira 或 Jira 等票务系统集成 ServiceNow

为了帮助您的组织对补救措施做出反应（例如，更新基础架构代码），此解决方案可以将票证推送到您的外部票务系统。

在 GovCloud 和中国分区中使用 AWSConfig补救措施

该解决方案中包含的一些补救措施是重新打包 AWS 自 AWSConfig有的 Remention 文档，这些文档在商业区可用，但在中国却没有。 GovCloud 部署此解决方案以在这些分区中使用这些文档。

通过自定义补救和 Playbook 实施来扩展解决方案

该解决方案旨在实现可扩展和可定制。要指定替代补救措施，请部署自定义的 AWS Systems Manager 自动化文档和 AWS IAM 角色。要支持解决方案未实现的全新控件集，请部署自定义 Playbook。

使用案例

在贵组织的账户和地区强制遵守标准

部署标准攻略手册（例如，AWS 基础安全最佳实践），以便能够使用所提供的补救措施。自动或手动启动对部署解决方案的任何账户和区域中的资源进行修复，以修复不合规的资源。

部署自定义补救措施或 Playbook 以满足组织的合规性需求

使用提供的 Orchestrator 组件作为框架。根据组织的特定需求构建自定义补救措施以解决 out-of-compliance资源问题。

概念和定义

本节介绍重要概念并定义此解决方案特有的术语：

修复，修复操作手册

实施一组解决发现的步骤。例如，针对控制安全控制 (SC) Lambda.1 “Lambda 函数策略应禁止公开访问” 的补救措施将修改相关 AWS Lambda 函数的策略，以删除允许公开访问的语句。

控制运行手册

一组 AWS Systems Manager (SSM) 自动化文档之一，Orchestrator 使用这些文档将针对特定控制的已启动补救措施发送到正确的补救运行手册。例如，SC Lambda.1 和 AWS 基础安全最佳实践 (FSBP) Lambda.1 的补救措施是使用相同的修复操作手册实施的。Orchestrator 为每个控件调用控制运行手册，这些控件分别命名为 asr-afsbp_Lambda.1 和 asr-sc_2.0.0_Lambda.1。每个控制运行手册都调用相同的修复运行手册，在本例中为 ASR-。RemoveLambdaPublicAccess

管弦乐师

解决方案部署的 Step Functions 将来自 AWS Security Hub 的查找对象作为输入，并在目标账户和区域中调用正确的控制运行手册。当修复开始以及修复成功或失败时，Orchestrator 还会通知解决方案 SNS 主题。

标准

组织作为合规框架的一部分定义的一组控制措施。例如，AWS Security Hub 和该解决方案支持的标准之一是 AWS FSBP。

控制

对资源为了合规而应该或不应该拥有的属性的描述。例如，控件 AWS FSBP Lambda.1 规定 AWS Lambda Functions 应禁止公开访问。允许公共访问的函数将无法进行此控制。

整合控制结果、安全控制、安全控制视图

AWS Security Hub 的一项功能，激活后，它会显示带有合并控制的结果 IDs ， IDs 而不是与特定标准相对应的控制结果。例如，控件 AWS FSBP S3.2、CIS v1.2.0 2.3、CIS v1.4.0 2.1.5.2 和 PCI-DSS

v3.2.1 S3.1 都映射到整合 (SC) 控件 S3.2 “S3 存储桶应禁止公共读取权限”。开启此功能后，将使用 SC 运行手册。

[解决方案 Web UI] 委派管理员

在解决方案的 Web UI 环境中，委派管理员是受管理员邀请并拥有运行修正和查看修复历史记录的完全访问权限的用户。该用户还可以查看和管理其他账户操作员用户。

[解决方案 Web UI] 账户操作员

在解决方案的 Web UI 环境中，账户操作员是管理员或委托管理员邀请访问解决方案的 Web UI 的用户。该用户与邀请中提供的 AWS 账户 ID 列表相关联；他们只能运行补救措施并查看与这些账户中的资源相关的修复历史记录。

有关 AWS 术语的一般参考，请参阅 AWS 术语表。

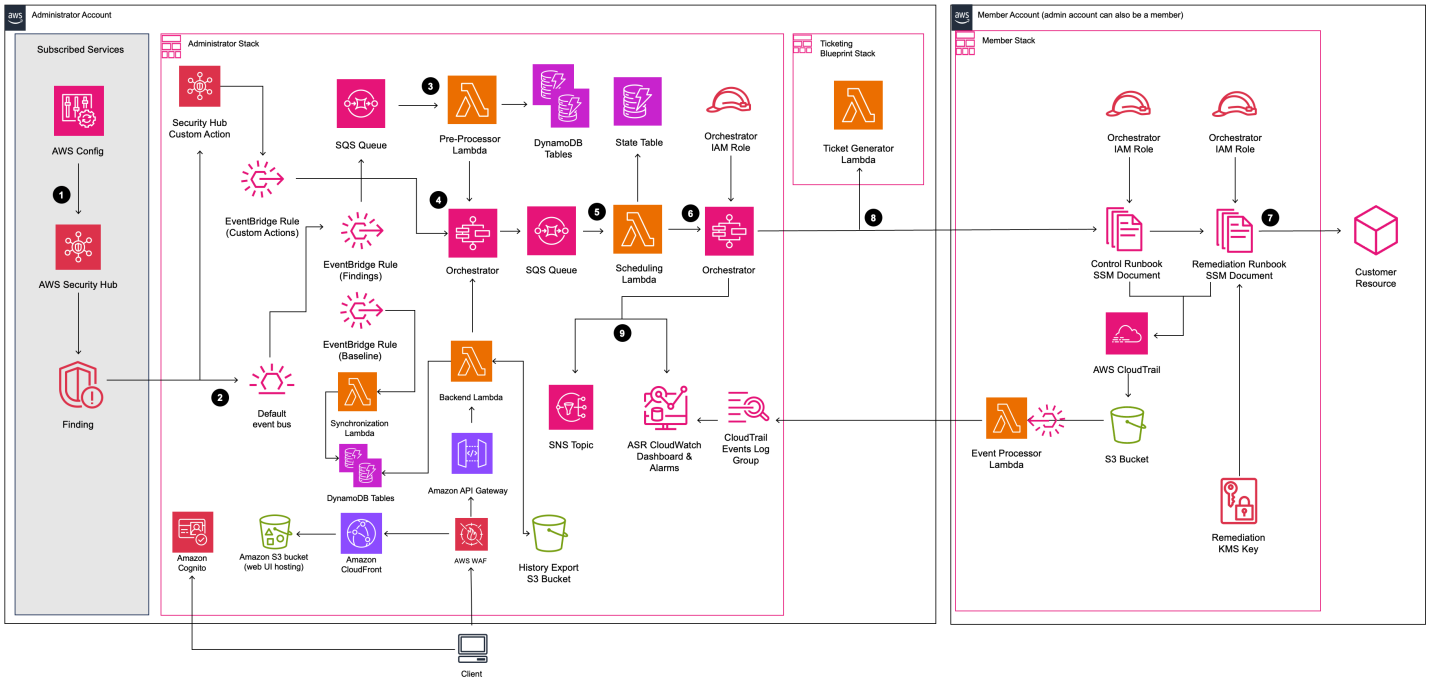
架构概述

本节提供了此解决方案所部署组件的参考实施架构图。

架构图

使用默认参数部署此解决方案将在 AWS 云中构建以下环境。

AWS 架构上的自动安全响应



> **Note**
>
> AWS CloudFormation 资源是基于 AWS Cloud Development Kit (AWS CDK) 结构创建的。

使用 AWS CloudFormation 模板部署的解决方案组件的高级流程如下：

1. 检测：AWS Security Hub 为客户提供其 AWS 安全状态的全面视图。它可以帮助他们根据安全行业标准和最佳实践来衡量自己的环境。它的工作原理是从其他 AWS 服务（例如 AWS Config、Amazon Guard Duty 和 AWS Firewall Manager）收集事件和数据。这些事件和数据是根据安全标准进行分析的，例如 CIS AWS 基金会基准。异常会在 AWS Security Hub 控制台中作为发现结果进行断言。新发现将作为 Amazon EventBridge 事件发送。

2. 收听：AWS Security Hub 会针对该服务创建或修改的每个发现发出 EventBridge 事件。AWS 上的自动安全响应 (ASR) 部署了两 EventBridge 条规则，用于监听 AWS Security Hub 生成的查找事件：
   - 自定义操作 EventBridge 规则：当用户触发 “使用 ASR 修复” 自定义操作时，监听 AWS Security Hub CSPM 发出的自定义操作事件。该事件将转发给 Orchestrator 进行修复。
   - 调查结果 EventBridge 规则：监听 AWS Security Hub 和 AWS Security Hub CSPM 发出的所有查找、创建或更新事件。这些事件被转发到预处理器的 SQS 队列进行进一步处理。
3. 启动：您可以手动启动修复，也可以将其配置为自动运行。要手动运行修复，您可以使用解决方案部署的 Web 用户界面或 AWS Security Hub CSPM 中的自定义操作功能。在非生产环境中进行仔细测试后，您还可以激活自动修复。您可以为单个修正激活自动化，而无需激活所有修正的自动启动。要将修正配置为自动运行，请参阅启用全自动修复页面。
4. 预修复：在管理员账户中，AWS Step Fun ctions 处理修复事件并做好计划准备。
5. 计划：该解决方案调用调度 AWS Lambda 函数将修复事件置于 Amazon DynamoD B 状态表中。
6. 编排：在管理员账户中，Step Functions 使用跨账户 AWS 身份和访问管理 (IAM) 角色。Step Functions 在包含产生安全发现的资源的成员账户中调用补救措施。
7. 补救：成员账户中的 A WS Systems Manager A utomation 文档执行修复目标资源发现所需的操作，例如禁用 Lambda 公共访问权限。

   或者，您可以使用日志参数在成员堆栈中启用操作EnableCloudTrailForASRAction日志功能。此功能可记录解决方案在您的成员账户中执行的操作，并将其显示在解决方案的 Amazon CloudWatch 控制面板中。
8. （可选）创建票证：如果您使用TicketGenFunctionName参数在管理堆栈中启用票证，则解决方案将调用提供的票证生成器 Lambda 函数。在成员账户中成功执行补救措施后，此 Lambda 函数会在您的票务服务中创建票证。我们提供用于与 Jira 集成的堆栈，以及. ServiceNow
9. 通知并记录：该剧本将结果记录到 CloudWatch 日志组，向亚马逊简单通知服务 (Amazon SNS) 主题发送通知，并更新 Security Hub 的调查结果。该解决方案在调查结果说明中保留了对操作的审计跟踪。

AWS Well-Architected 设计注意事项

该解决方案是根据 AWS Well-Architected Framework 中的最佳实践设计的，可帮助客户在云中设计和运行可靠、安全、高效且经济实惠的工作负载。本节介绍在构建此解决方案时如何应用 Well-Architected Framework 的设计原则和最佳实践。

卓越运营

本节介绍我们是如何使用卓越运营支柱的原则和最佳实践来设计此解决方案的。

- 使用 CloudFormation定义为 IaC 的资源。
- 在可能的情况下，实施的补救措施应具有以下特征：
  - 幂等性
  - 错误处理和报告
  - 日志记录
  - 出现故障时将资源恢复到已知状态

安全性

本节介绍我们是如何使用安全性支柱的原则和最佳实践来设计此解决方案的。

- 使用 IAM 进行身份验证和授权。
- 尽可能缩小角色权限范围，但在许多情况下，该解决方案需要通配符权限才能对任何资源采取行动。
- 出于安全考虑，

可靠性

本节介绍我们是如何使用可靠性支柱的原则和最佳实践来设计此解决方案的。

- 如果补救措施未能解决发现的根本原因，Security Hub 会继续创建调查结果。
- 无服务器服务允许该解决方案根据需要进行扩展。

性能效率

本节介绍我们是如何使用性能效率支柱的原则和最佳实践来设计此解决方案的。

- 该解决方案旨在成为一个无需自己实施协调和权限即可进行扩展的平台。

成本优化

本节介绍我们是如何使用成本优化支柱的原则和最佳实践来设计此解决方案的。

- 无服务器服务允许您只对使用的服务付费。
- 在每个账户中使用免费套餐实现 SSM 自动化

可持续性

本节介绍我们是如何使用可持续性支柱的原则和最佳实践来设计此解决方案的。

- 无服务器服务允许您根据需求扩展或缩减规模。

架构详情

本节介绍构成此解决方案的组件和 AWS 服务，以及这些组件如何协同工作的架构详情。

AWS Security Hub 集成

部署`automated-security-response-admin`堆栈可以与 AWS Security Hub CSPM 的自定义操作功能集成。当 AWS Security Hub CSPM 控制台用户单击 “操作” > “使用 ASR 修复” 时，所选结果将发送到 EventBridge 并触发修复工作流程。

必须使用和模板将跨账户权限和 AWS Systems Manager 运行手册部署到所有 AWS Security Hub 账户（管理员`automated-security-response-member.template`和`automated-security-response-member-roles.template` CloudFormation 成员）。有关更多信息，请参阅行动手册。此模板允许对目标账户进行自动修复。

用户可以使用 Amazon DynamoDB 在每个控制的基础上配置全自动补救措施。此选项将在发现结果报告给 AWS Security Hub 后立即激活全自动补救措施。默认情况下，自动启动处于关闭状态。安装后，可以通过修改修复配置 DynamoDB 表随时更改此选项。

跨账户补救

AWS 上的自动安全响应使用跨账户角色，使用跨账户角色跨主账户和次要账户工作。这些角色将在解决方案安装期间部署到成员帐户。每个补救措施都被分配了一个单独的角色。主账户中的修正过程被授予在需要补救的账户中担任修正角色的权限。补救由在需要补救的账户中运行的 AWS Systems Manager 运行手册执行。

剧本

一组补救措施被分组为一个名为 p layb ook 的包。使用此解决方案的模板安装、更新和移除 Playbook。有关每本 playbook 中支持的补救措施的信息，请参阅《开发者指南》→《攻略手册》。该解决方案目前支持以下攻略手册：

- 《安全控制》是一本与 AWS Security Hub 的整合控制结果功能一致的手册，于 2023 年 2 月 23 日发布。

> **Important**
>
> 在 Security Hub 中启用整合控制结果后，这是解决方案中唯一应启用的行动手册。

- 互联网安全中心 (CIS) Amazon Web Services Foundations 基准测试，版本 1.2.0，于 2018 年 5 月 18 日发布。
- 互联网安全中心 (CIS) Amazon Web Services Foundations 基准测试，版本 1.4.0，于 2022 年 11 月 9 日发布。
- 互联网安全中心 (CIS) Amazon Web Services Foundations 基准测试，3.0.0 版，于 2024 年 5 月 13 日发布。
- AWS 基础安全最佳实践 (FSBP) 版本 1.0.0，于 2021 年 3 月发布。
- 支付卡行业数据安全标准 (PCI-DSS) 3.2.1 版，于 2018 年 5 月发布。
- 美国国家标准与技术研究院 (NIST) 版本 5.0.0，于 2023 年 11 月发布。

集中式日志记录

AWS 日志上的自动安全响应到单个 CloudWatch 日志组 SO0111-ASR。这些日志包含解决方案中的详细日志记录，用于解决方案的故障排除和管理。

通知

此解决方案使用亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题来发布补救结果。您可以使用本主题的订阅来扩展解决方案的功能。例如，您可以发送电子邮件通知和更新故障单。

- so0111-asr_Topic — 用于发送与已执行的修正相关的一般信息和错误消息。
- s@@ o0111-asr_alarm_Topic — 用于在解决方案的其中一个警报被触发时发出通知，表示解决方案未按预期运行。

此解决方案中的 AWS 服务

该解决方案使用以下服务。使用该解决方案需要核心服务，而支持服务则连接核心服务。

AWS 服务	描述
Amazon EventBridge	核心。 EventBridge 规则用于监听和触发 AWS Security Hub 和 AWS Security Hub CSPM 发出的事件。
AWS IAM	核心。部署许多角色以允许对不同的资源进行修复。
AWS Lambda	核心。部署多个 lambda 函数，步进函数协调器将使用这些函数来修复问题。 用作与 API Gateway 集成的解决方案 Web 用户界面的后端。
AWS Security Hub	核心。为客户提供其 AWS 安全状态的全面视图。
AWS Step Functions	核心。部署一个协调器，该协调器将通过 AWS Systems Manager API 调用调用补救文档。
AWS Systems Manager	核心。部署 System Manager 自动化文档，其中包含要由解决方案执行的补救逻辑。 使用参数存储来维护解决方案元数据和配置设置。
AWS DynamoDB	核心。在每个账户和区域中存储上次运行的修复，以优化补救计划。 存储 AWS Security Hub 和 AWS Security Hub CSPM 生成的调查结果。 存储补救和解决方案配置元数据。 为访问解决方案的 Web UI 的用户存储数据。
AWS CloudTrail	支持。记录解决方案对您的 AWS 资源所做的更改并将其显示在 CloudWatch 控制面板上。

AWS 服务	描述
Amazon CloudWatch	支持。部署日志组，不同的攻略手册将使用这些日志组来记录结果。收集指标以显示在带有警报的自定义仪表板上。
Amazon Simple Notification Service	支持。部署修复完成后会收到通知的 SNS 主题。
AWS SQS	支持。协助安排修复，以便解决方案可以并行运行修复。 使用 Lambda 映射缓冲执行 Lamb EventSource da。
AWS Key Management Service	支持。用于加密数据以进行修复。
AWS Config	支持。记录所有可用于 AWS Security Hub 的资源。
Amazon S3	支持。存储导出的修复历史记录和日志数据。 将解决方案的 Web UI 作为单页应用程序 (SPA) 托管。
Amazon CloudFront	支持。提供解决方案的 Web 用户界面
Amazon API Gateway	支持。创建解决方案的 REST API 以支持用户界面。
AWS WAF	支持。保护解决方案的 Web 用户界面。
Amazon Cognito	支持。用于对解决方案的 Web UI 进行身份验证和授权。

规划您的部署

本节介绍部署解决方案之前的成本、网络安全、支持的 AWS 区域、配额和其他注意事项。

费用

您负责支付用于运行此解决方案的 AWS 服务的费用。

自本次修订以来，估计的每月费用为：

- 小型部署（10 个账户，1 个区域-美国）East/N. Virginia): Approximately $20.73 for 300 remediations/month
- 中型部署（100 个账户，1 个区域-美国）East/N. Virginia): Approximately $136.57 for 3,000 remediations/month
- 大规模部署（1,000 个账户，10 个区域）：大约 10,460.80 美元，用于每月修复 30,000 次

> **Important**
>
> 价格可能会发生变化。有关完整详情，请参阅本解决方案中使用的每项 AWS 服务的定价页面。

> **Note**
>
> 许多 AWS 服务都包含免费套餐，即客户可以免费使用的基本服务量。实际成本可能高于或低于提供的定价示例。

我们建议通过 AWS Cost Explorer 创建预算，以帮助管理成本。价格可能会发生变化。有关完整详情，请参阅本解决方案中使用的每项 AWS 服务的定价网页。

费用表示例

运行此解决方案的总成本取决于以下因素：

- AWS Security Hub 成员账户的数量
- 主动自动调用的修正的数量

- 补救频率

此解决方案使用以下 AWS 组件，这些组件会根据您的配置产生费用。为小型、中型和大型组织提供了定价示例。

服务	免费套餐	定价 [美元]
AWS Systems Manager Automation Systems	没有免费套餐	每个基本步骤的费用为每步 0.002 美元。对于多账户自动化，所有步骤，包括在任何儿童账户中运行的步骤，都仅计入原始账户。
AWS Systems Manager Automation Systems	没有免费套餐	每个`aws:executeScript` 操作步骤的费用为每秒 0.00003 美元。
AWS Systems Manager Automation Autom	没有免费套餐	每月每 GB 0.046 美元
AWS Systems Manager Automation Systems	没有免费套餐	每 GB 转账 0.900 美元（跨账户或） out-of-Region
AWS Security Hub CSPM-安全检查	没有免费套餐	前 10 万张每张支票的checks/account/Region/month费用为 0.0010 美元 接下来的 40 万张每张支票的 checks/account/Region/month 费用为 0.0008 美元 超过 50 万张每张支票的checks/account/Region/month费用为 0.0005 美元
AWS Security Hub CSPM-查找摄取事件	前 10,000 events/account/Region/month 是免费的。查找与	超过 10,000 人每场events/account/Region/month活动的费用为 0.00003 美元

服务	免费套餐	定价 [美元]
	Security Hub 的安全检查相关的摄取事件。	
亚马逊 CloudWatch -指标	基本监控指标（每隔 5 分钟）10 详细监控指标（以 1 分钟为频率）1 100 万个 API 请求（不适用于 GetMetricData、 GetInsightRuleReport 和 GetMetricWidgetImage）	前 10,000 个指标每月的费用为 0.30 美元 接下来的 240,000 个指标每月花费 0.10 美元 接下来的 750,000 个指标每月花费 0.05 美元 超过 100 万个指标的费用为每月 0.02 美元 API 调用每 1,000 个请求的费用为 0.01 美元
亚马逊 CloudWatch -控制面板	3 个控制面板，每月最多可显示 50 个指标	每个控制面板每月 3.00 美元
Amazon CloudWatch -警报	10 个警报指标（不适用于高分辨率警报）	标准分辨率（60 秒）费用为每个警报 0.10 美元 高分辨率（10 秒）的费用为每个警报指标 0.30 美元 标准分辨率异常检测费用为每个警报 0.30 美元 高分辨率异常检测费用为每个警报 0.90 美元 每个警报的复合费用为 0.50 美元

服务	免费套餐	定价 [美元]
Amazon CloudWatch -日志收集	5GB 数据（摄取、存档存储以及通过 Logs Insights 查询扫描的数据）	每 GB 0.50 美元
Amazon CloudWatch -日志存储	5GB 数据（摄取、存档存储以及通过 Logs Insights 查询扫描的数据）	扫描的每 GB 数据为 0.005 美元
AWS Lambda-请求	每月 100 万次免费请求	每 100 万个请求 0.20 美元
AWS Lambda-持续时间	每月 400,000 GB 秒的计算时间	每 GB 秒 0.0000166667 美元。持续时间的价格取决于您为函数分配的内存量。您可以为函数分配介于 128MB 到 10,240MB 之间任意数量的内存，以 1MB 为增量。
AWS Step Functions — 状态转换	每月 4,000 次自由状态转换	此后每 1,000 个状态转换为 0.025 美元
Amazon EventBridge	AWS 服务发布的所有状态变更事件都是免费的	自定义事件每发布一百万个自定义事件的成本 第三方 (SaaS) 事件每发布一百万个事件的成本为100万美元 跨账户事件的费用为每发送一百万次跨账户事件
Amazon SNS	每月前 100 万个 Amazon SNS 请求是免费的	此后每100万个请求0.50美元
Amazon SQS	每月前 100 万个 Amazon SQS 请求是免费的	此后每100万至1000亿个请求0.40美元
Amazon DynamoDB	前 25GB 的存储空间是免费的	此后每 100 万次持续读取和写入 2.00 美元

服务	免费套餐	定价 [美元]
AWS Key Management Service	每月 20,000 个请求	每个 1 KMS 密钥 1.00 美元。对于自动轮换或按需轮换的 KMS 密钥，密钥的第一次和第二次轮换会增加 1 美元/月（按小时按比例分配）的成本。
Amazon Cognito	在 Essentials 套餐中，前 10,000 名月活跃用户免费。 注意：当用户通过外部 IdP (SAML/OIDC) 进行身份验证时，此免费套餐为 50 个月活跃用户。	超过 10,000 名用户每位月活跃用户 0.015 美元。
Amazon CloudFront	免费套餐包括每月 1 TB 的数据传输和一千万个 HTTP 或 HTTPS 请求。	(US/Canada/Mexico) 前 9 TB 为每月 0.085 美元。接下来的40TB为每月0.080美元。 每个 HTTP 请求 0.0075 美元。每个 HTTPS 请求 0.0100 美元。
Amazon S3	没有免费套餐	前 50 TB 的费用为每月每 GB 0.023 美元。 每 1,000 个 PUT、COPY、POST、LIST 请求 0.005 美元。 每 1,000 个 GET、SELECT 和所有其他请求 0.0004 美元。
Amazon API Gateway	在使用的前 12 个月内，有 100 万次 REST API 调用。	前 3.33 亿个 API 调用每百万美元 3.50 美元。

定价示例（每月）

示例 1：每月修复 300 次

- 10 个账户，1 个区域
- 每次 30 次修复 account/Region/month
- 每人处理了 500 个 Security Hub 调查结果 account/Region/month
- 网页用户界面已禁用
- 操作日志已禁用
- 每月总花费 20.73 美元

服务	假设	每月费用 [美元]
AWS Systems Manager Automation	步骤：大约 4 个步骤 * 300 次修复 * 0.002 美元 = 2.40 美元 时长：10 秒 * 300 次修复 * 0.00003 美元 = 0.09 美元	2.49 美元
AWS Security Hub	未使用任何可计费的服务	$0
Amazon CloudWatch 日志	每 GB 0.50 美元	< 0.01
AWS Lambda-请求	300 次补救 * 7 个请求 = 2,100 个请求 5,000 个发现 * 1 个请求 = 5,000 个请求 0.20 美元/1,000,000 个请求 = 每个请求 0.0000002 美元	0.00142
AWS Lambda-持续时间	(512MB 内存) 4,000ms * 300 次修复 * 0.0000000083 = 0.00996 美元	0.029 美元

服务	假设	每月费用 [美元]
	449ms * 5,000 个调查结果 * 0.0000000083 = .0186 美元	
AWS Step Functions	19 次状态转换 * 300 次修复 = 5,700 0.025 美元 * (5,700/1,000) 状态转换 = 0.14 美元	0.14 美元
亚马逊 EventBridge 规则	规则不收费	$0
AWS Key Management Service	1 个密钥 * 10 个账户 * 1 个区域 * $1 = 10 美元 （加密/解密 API 请求） （300 次补救 * 2 个请求）+（5,000 个调查结果 * 4 个请求）= 20,600 个请求 每 10,000 个请求 0.03 美元 ⇒ 0.03 美元 * (20,600 /10,000) = 0.06 美元	10.06 美元
Amazon DynamoDB	2.00 * 1,000,000 次读取和写入 = 2.00 美元 （调查结果表）15MB * 10 个账户 * 1 个区域 = 150MB （历史表）10MB * 10 个账户 * 1 个区域 = 100MB 每月每 GB 0.25 美元 * 0.25 GB = 0.0625 美元	2.0625
Amazon SQS	0.40 * 1,000,000 个请求 = 0.40 美元	0.40 美元

服务	假设	每月费用 [美元]
Amazon SNS	0.50 美元 * （600 份/1,000,000 份通知）= 0.0003 美元	0.0003
亚马逊 CloudWatch -指标	（已禁用增强指标） 0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元*（300 个看跌期权指标 API 调用/1,000）= 0.003 美元	2.10 美元
亚马逊 CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
Amazon CloudWatch -警报	（已禁用增强指标） 0.10 美元 * 4 个警报 = 0.40 美元	0.40 美元
亚马逊 CloudWatch -X-Ray Traces	300 次补救 * 7 个请求 = 2,100 次 Lambda 调用 5,000 个发现 * 1 个请求 = 5,000 次 Lambda 调用 每条跟踪 0.000005 美元 * 7,100 条跟踪 = 0.0355 美元	0.0355 美元
总计		20.73 美元

示例 2：每月修复 300 次（已启用 Web 用户界面）

- 10 个账户，1 个区域
- 每次 30 次修复 account/Region/month
- 每人处理 5,000 个 Security Hub 发现 account/Region/month
- 网页用户界面已启用

- 操作日志已禁用
- 每月总费用为 36.35 美元

服务	假设	每月费用 [美元]
AWS Systems Manager Automation	步骤：大约 4 个步骤 * 300 次修复 * 0.002 美元 = 2.40 美元 时长：10 秒 * 300 次修复 * 0.00003 美元 = 0.09 美元	2.49 美元
AWS Security Hub	未使用任何可计费的服务	$0
Amazon CloudWatch 日志	每 GB 0.50 美元	< 0.01
AWS Lambda-请求	300 次补救 * 7 个请求 = 2,100 个请求 5,000 个发现 * 1 个请求 = 5,000 个请求 0.20 美元/1,000,000 个请求 = 每个请求 0.0000002 美元	0.00142
AWS Lambda-持续时间	(512MB 内存) 4,000ms * 300 次修复 * 0.0000000083 = 0.00996 美元 449ms * 5,000 个调查结果 * 0.0000000083 = .0186 美元	0.029 美元
AWS Step Functions	19 次状态转换 * 300 次修复 = 5,700 0.025 美元 * (5,700/1,000) 状态转换 = 0.14 美元	0.14 美元
亚马逊 EventBridge 规则	规则不收费	$0

服务	假设	每月费用 [美元]
AWS Key Management Service	1 个密钥 * 10 个账户 * 1 个区域 * $1 = 10 美元 （加密/解密 API 请求） （300 次补救 * 2 个请求）+（5,000 个调查结果 * 4 个请求）= 20,600 个请求 每 10,000 个请求 0.03 美元 ⇒ 0.03 美元 * (20,600 /10,000) = 0.06 美元	10.06 美元
Amazon DynamoDB	2.00 * 1,000,000 次读取和写入 = 2.00 美元 （调查结果表）15MB * 10 个账户 * 1 个区域 = 150MB （历史表）10MB * 10 个账户 * 1 个区域 = 100MB 每月每 GB 0.25 美元 * 0.25 GB = 0.0625 美元	2.0625
Amazon SQS	0.40 * 1,000,000 个请求 = 0.40 美元	0.40 美元
Amazon SNS	0.50 美元 *（600 份/1,000,000 份通知）= 0.0003 美元	0.0003

服务	假设	每月费用 [美元]
亚马逊 CloudWatch -指标	（已禁用增强指标） 0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元*（300 个看跌期权指标 API 调用/1,000）= 0.003 美元	2.10 美元
亚马逊 CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
Amazon CloudWatch -警报	（已禁用增强指标） 0.10 美元 * 4 个警报 = 0.40 美元	0.40 美元
亚马逊 CloudWatch -X-Ray Traces	300 次补救 * 7 个请求 = 2,100 次 Lambda 调用 5,000 个发现 * 1 个请求 = 5,000 次 Lambda 调用 每条跟踪 0.000005 美元 * 7,100 条跟踪 = 0.0355 美元	0.0355 美元
Amazon Cognito	（基本等级） 500 个月活跃用户	$0

服务	假设	每月费用 [美元]
Amazon CloudFront	向源站传输的区域数据（每 GB）= 0.020 美元 向互联网传输的区域数据（每 GB）= 0.085 美元 所有 HTTP 方法的请求定价（每 10,000 个）= 0.0075 美元	0.1125 美元
Amazon S3	（用户界面托管） 每 GB 0.023 美元 * 0.002 GB = 0.000046 美元 （历史导出）每 GB 0.023 美元 * 0.50 GB = 0.0125 美元 每 1,000 个 GET 请求 0.0004 美元	0.0125 美元
AWS WAF	1 个 Web ACL = 每月 5.00 美元 7 条规则 * 每条规则 1.00 美元 = 7.00 美元	12 美元
Amazon API Gateway	每百万个 REST API 调用 3.50 美元	3.50 美元
总计		36.35 美元

示例 3：每月修复 3,000 次

- 100 个账户，1 个区域
- 每次 30 次修复 account/Region/month
- 每人处理了 500 个 Security Hub 调查结果 account/Region/month

- 网页用户界面已禁用
- 操作日志已禁用
- 每月总花费 136.57 美元

服务	假设	每月费用 [美元]
AWS Systems Manager Automation	步骤：大约 4 个步骤 * 3,000 次补救 * 0.002 美元 = 24.00 美元 时长：10 秒 * 3,000 次修复 * 0.00003 美元 = 0.90 美元	24.90 美元
AWS Security Hub	未使用任何可计费的服务	$0
Amazon CloudWatch 日志	每 GB 0.50 美元	< 0.01
AWS Lambda-请求	3,000 次补救 * 7 个请求 = 2,100 个请求 50,000 个结果 * 1 个请求 = 50,000 个请求 0.20 美元/1,000,000 个请求 = 每个请求 0.0000002 美元	0.01 美元
AWS Lambda-持续时间	(512MB 内存) 4,000ms * 3,000 次修复 * 0.0000000083 = 0.0996 美元 449ms * 50,000 个调查结果 * 0.0000000083 = 0.186 美元	0.29 美元
AWS Step Functions	19 次状态转换 * 3,000 次修复 = 57,000 0.025 美元 * (57,000/1,000) 状态转换 = 1.425 美元	1.425 美元

服务	假设	每月费用 [美元]
亚马逊 EventBridge 规则	规则不收费	$0
AWS Key Management Service	1 个密钥 * 100 个账户 * 1 个区域 * $1 = 100 美元 （加密/解密 API 请求） （3,000 次补救 * 2 个请求）+（50,000 个调查结果 * 4 个请求）= 20.6万份请求 每 10,000 个请求 0.03 美元 ⇒ 0.03 美元 * (206,000 /10,000) = 0.618 美元	100.618 美元
Amazon DynamoDB	2.00 * 1,000,000 次读取和写入 = 2.00 美元 （调查结果表）15MB * 100 个账户 * 1 个区域 = 1,500MB （历史表）10MB * 100 个账户 * 1 个区域 = 1,000MB 每月每 GB 0.25 美元 * 2.5 GB = 0.625 美元	2.625 美元
Amazon SQS	0.40 * 1,000,000 个请求 = 0.40 美元	0.40 美元
Amazon SNS	0.50 美元 * 1,000,000 个通知 = 0.50 美元	0.50 美元

服务	假设	每月费用 [美元]
亚马逊 CloudWatch -指标	（已禁用增强指标） 0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元* (3000/1,000) 看跌指标 API 调用 = 0.03 美元	2.13 美元
亚马逊 CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
Amazon CloudWatch -警报	0.10 美元 * 4 个警报 = 0.40 美元	0.40 美元
亚马逊 CloudWatch -X-Ray Traces	3,000 次补救 * 7 个请求 = 2,100 次 Lambda 调用 50,000 个发现 * 1 个请求 = 50,000 次 Lambda 调用 每条跟踪 0.000005 美元 * 52,100 条跟踪 = 0.2605 美元	0.2605 美元
总计		136.57 美元

示例 4：每月修复 30,000 次

- 1,000 个账户，10 个区域
- 每次 30 次修复 account/Region/month
- 每人处理了 500 个 Security Hub 调查结果 account/Region/month
- 网页用户界面已禁用
- 操作日志已禁用
- 每月总花费 10,460.80 美元

服务	假设	每月费用 [美元]
AWS Systems Manager Automation	步骤：大约 4 个步骤 * 30,000 次补救 * 0.002 美元 = 240.00 美元 时长：10 秒 * 30,000 次修复 * 0.00003 美元 = 9.00 美元	249.00 美元
AWS Security Hub	未使用任何可计费的服务	$0
Amazon CloudWatch 日志	每 GB 0.50 美元	< 0.01
AWS Lambda-请求	30,000 次补救 * 7 次请求 = 210,000 次请求 500 万个调查结果 * 1 个请求 = 500 万个请求 0.20 美元/1,000,000 个请求 = 每个请求 0.0000002 美元	1.042
AWS Lambda-持续时间	(512MB 内存) 4,000ms * 30,000 次补救 * 0.0000000083 = 0.996 美元 449ms * 500万个调查结果 * 0.0000000083 = 18.63 美元	19.63 美元
AWS Step Functions	19 个状态转换 * 30,000 次修复 = 570,000 0.025 美元 * (570,000/1,000) 状态转换 = 14.25 美元	14.25 美元
亚马逊 EventBridge 规则	规则不收费	$0
AWS Key Management Service	(1 个密钥) 1 美元 * 1,000 个账户 * 10 个区域 = 10,000 美元	10,060.18 美元

服务	假设	每月费用 [美元]
	（加密/解密 API 请求） （30,000 次补救 * 2 次请求）+（500万次调查结果 * 4 次请求）= 20,060,000 次请求 每 10,000 个请求 0.03 美元 ⇒ 0.03 美元 * (20,060,000 /10,000) = 60.18 美元	
Amazon DynamoDB	2.00 美元 *（1,000,000 次读取和写入/100万次）= 20.00 美元 （调查结果表）15MB * 1000 个账户 * 10 个区域 = 150GB （历史表）10MB * 1000 个账户 * 10 个区域 = 100GB 每月每 GB 0.25 美元 * 250 GB = 62.50 美元	82.50 美元
Amazon SQS	0.40 美元*（5,060,000 个请求/100万个）= 2.024 美元	2.024
Amazon SNS	0.000005 * 1,000,000 个通知 = 0.50 美元	0.50 美元
亚马逊 CloudWatch -指标	（已禁用增强指标） 0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元* (30,000 /1,000) 看跌指标 API 调用 = 0.30 美元	2.40 美元
亚马逊 CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元

服务	假设	每月费用 [美元]
Amazon CloudWatch -警报	（已禁用增强指标） 0.10 美元 * 4 个警报 = 0.40 美元	0.40 美元
亚马逊 CloudWatch -X-Ray Traces	30,000 次补救 * 7 个请求 = 210,000 次 Lambda 调用 500 万个发现 * 1 个请求 = 500 万次 Lambda 调用 每条跟踪 0.000005 美元 * 5,210,000 条跟踪 = 26.05 美元	26.05 美元
总计		10,460.80 美元

示例 5：每月修复 30,000 次（已启用 Web 用户界面）

- 1,000 个账户，10 个区域
- 每次 30 次修复 account/Region/month
- 每人处理了 500 个 Security Hub 调查结果 account/Region/month
- 网页用户界面已启用
- 操作日志已禁用
- 每月总费用 10,480.90 美元

服务	假设	每月费用 [美元]
AWS Systems Manager Automation	步骤：大约 4 个步骤 * 30,000 次补救 * 0.002 美元 = 240.00 美元 时长：10 秒 * 30,000 次修复 * 0.00003 美元 = 9.00 美元	249.00 美元

服务	假设	每月费用 [美元]
AWS Security Hub	未使用任何可计费的服务	$0
Amazon CloudWatch 日志	每 GB 0.50 美元	< 0.01
AWS Lambda-请求	30,000 次补救 * 7 次请求 = 210,000 次请求 500 万个调查结果 * 1 个请求 = 500 万个请求 0.20 美元/1,000,000 个请求 = 每个请求 0.0000002 美元	1.042
AWS Lambda-持续时间	(512MB 内存) 4,000ms * 30,000 次补救 * 0.0000000083 = 0.996 美元 449ms * 500万个调查结果 * 0.0000000083 = 18.63 美元	19.63 美元
AWS Step Functions	19 个状态转换 * 30,000 次修复 = 570,000 0.025 美元 * (570,000/1,000) 状态转换 = 14.25 美元	14.25 美元
亚马逊 EventBridge 规则	规则不收费	$0

服务	假设	每月费用 [美元]
AWS Key Management Service	(1 个密钥) 1 美元 * 1,000 个账户 * 10 个区域 = 10,000 美元 （加密/解密 API 请求） （30,000 次补救 * 2 次请求）+（500万次调查结果 * 4 次请求）= 20,060,000 次请求 每 10,000 个请求 0.03 美元 ⇒ 0.03 美元 * (20,060,000 /10,000) = 60.18 美元	10,060.18 美元
Amazon DynamoDB	2.00 美元 *（1,000,000 次读取和写入/100万次）= 20.00 美元 （调查结果表）15MB * 1000 个账户 * 10 个区域 = 150GB （历史表）10MB * 1000 个账户 * 10 个区域 = 100GB 每月每 GB 0.25 美元 * 250 GB = 62.50 美元	82.50 美元
Amazon SQS	0.40 美元*（5,060,000 个请求/100万个）= 2.024 美元	2.024
Amazon SNS	0.000005 * 1,000,000 个通知 = 0.50 美元	0.50 美元
亚马逊 CloudWatch -指标	（已禁用增强指标） 0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元* (30,000 /1,000) 看跌指标 API 调用 = 0.30 美元	2.40 美元

服务	假设	每月费用 [美元]
亚马逊 CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
Amazon CloudWatch -警报	（已禁用增强指标） 0.10 美元 * 4 个警报 = 0.40 美元	0.40 美元
亚马逊 CloudWatch -X-Ray Traces	30,000 次补救 * 7 个请求 = 210,000 次 Lambda 调用 500 万个发现 * 1 个请求 = 500 万次 Lambda 调用 每条跟踪 0.000005 美元 * 5,210,000 条跟踪 = 26.05 美元	26.05 美元
Amazon Cognito	（基本等级） 5,000 个月活跃用户	$0
Amazon CloudFront	向源站传输的区域数据（每 GB）= 0.020 美元 向互联网传输的区域数据（每 GB）= 0.085 美元 所有 HTTP 方法的请求定价（每 10,000 个）= 0.0075 美元	0.1125 美元

服务	假设	每月费用 [美元]
Amazon S3	（用户界面托管） 每 GB 0.023 美元 * 0.002 GB = 0.000046 美元 （历史导出）每 GB 0.023 美元 * 100 GB = 2.30 美元 每 1,000 个 GET 请求 0.0004 美元 * 5,000 个请求 = 2.00 美元	4.30 美元
AWS WAF	1 个 Web ACL = 每月 5.00 美元 7 条规则 * 每条规则 1.00 美元 = 7.00 美元	12 美元
Amazon API Gateway	每百万个 REST API 调用 3.50 美元	3.50 美元
总计		10,480.90 美元

Important

KMS 密钥轮换成本 AWS Key Management Service (KMS) 在启用轮换后，每年自动轮换客户托管密钥一次。每次轮换每年会产生每个密钥1.00美元的成本。例如，如果单个区域有 1000 个账户，则每年可额外获得 1000 美元（1 次轮换 × 1000 个密钥 × 1.00 美元）。

可选功能的额外费用

本节列出了与该解决方案的可选功能相关的额外成本。

增强的 CloudWatch 指标

如果您在部署管理堆栈时选择yes该EnableEnhancedCloudWatchMetrics参数，则该解决方案会为每个控件 ID 创建两个自定义指标和一个警报。费用取决于您要修复 IDs 的控制数量。在下表中，我们假设您 IDs 每月要修复所有96种不同的控制措施，以确定成本的上限。

服务	假设 96 个控件 IDs * 2 = 192 个自定义指标	每月费用 [美元]
亚马逊 CloudWatch -指标	0.30 美元 * 192 个自定义指标 = 57.60 美元	57.60 美元
Amazon CloudWatch -警报	0.10 美元 * 96 个警报 = 9.60 美元	9.60 美元
总计		67.20 美元

CloudTrail 操作日志

在您为其启用操作日志功能的每个成员账户中，解决方案都会创建一个记录所有写入管理事件的 CloudTrail 跟踪。Lambda 函数会筛选出与解决方案无关的事件。这意味着费用与您账户中的管理事件总数有关，因为与解决方案无关的事件仍由跟踪捕获并由 Lambda 函数处理。

在下表中，我们假设账户中每月有 150,000 个管理事件。实际费用取决于您账户中的实际管理活动活动。

服务	假设	每月费用 [美元]
AWS CloudTrail	150,000 * 2.00美元/100,000 美元 = 3.00 美元	3.00 美元
Lambda	150,000 * 0.2 * 0.125 = 3,750 Gb-秒 3,750 * 0.0000166667 美元 = 0.0625 美元的计算时间成本 0.15 * 0.20 美元 = 0.03 美元请求费用	0.0925

服务	假设	每月费用 [美元]
	0.0625 美元 + 0.03 美元 = Lambda 总成本 0.0952 美元	
总计		每个会员账户 3.09 美元

安全性

当您在 AWS 基础设施上构建系统时，安全责任由您和 AWS 共同承担。这种共享模式减轻了您的运营负担，因为 AWS 运营、管理和控制组件，包括主机操作系统、虚拟化层和服务运行设施的物理安全。有关 AWS 安全的更多信息，请访问 AWS 云安全。

API Gateway 安全政策

如果您选择启用解决方案的 Web 用户界面，则会将 API Gateway REST API 与管理 CloudFormation 堆栈一起部署，后者是 Web UI 中所有操作的后端。该解决方案部署的 REST API 使用适用于 API Gateway 的默认 TLS 安全策略，该策略`TLS-1-0`适用于区域 APIs。

但是，部署管理 CloudFormation 堆栈后，您可以选择通过添加更严格的 TLS 安全策略来自定义解决方案的 REST API。例如，您可以使用 TLSv1 .2 或. TLSv1 3 选择限制流量。`TLS_1_2` `security policy`你可以在 API Gateway 控制台的名称下找到该解决方案的 REST API AutomatedSecurityResponseApi。

要为解决方案的 REST API 选择安全策略，必须先配置自定义域名。有关更多信息，请参阅 API Gateway APIs 中的公共 REST 自定义域名。

有关向 REST API 添加安全策略的更多信息，请参阅 API Gatew ay 指南中的在 API Gateway 中为 REST API 自定义域选择安全策略。

IAM 角色

AWS Identity and Access Management (IAM) 角色允许客户向 AWS 云中的服务和用户分配精细的访问策略和权限。此解决方案创建 IAM 角色，这些角色授予解决方案的自动功能访问权限，以便在特定于每项补救的狭窄权限范围内执行补救操作。

管理员帐户的 Step Function 已分配给 SO0111-ASR-Orchestrator-Admin 角色。只有此角色才允许在每个成员账户中担任 so0111-Orchestrator-Member。每个修复角色都允许成员角色将其传递给 AWS Systems Manager 服务，以运行特定的修复运行手册。修复角色名称以 SO0111 开头，后面是与修复

运行手册名称相匹配的描述。例如，so0111-Remov VPCDefault SecurityGroupRules e 是 ASR 删除修复运行手册的角色。VPCDefault SecurityGroupRules

支持的 AWS 区域

> **Important**
>
> 在解决方案中启用可选功能可能会减少支持部署的区域列表。换句话说，以下列表仅适用于解决方案的核心组件。例如，如果您选择启用 Web UI，则从 2025 年 11 月起CloudFront ，您将无法在 GovCloud 地区部署该解决方案，因为 GovCloud （美国）不支持。

区域名称	区域代码
美国东部（俄亥俄州）	us-east-2
美国东部（弗吉尼亚州北部）	us-east-1
美国西部（加利福尼亚北部）	us-west-1
美国西部（俄勒冈州）	us-west-2
非洲（开普敦）	af-south-1
亚太地区（香港）	ap-east-1
亚太地区（海得拉巴）	ap-south-2
亚太地区（雅加达）	ap-southeast-3
亚太地区（墨尔本）	ap-southeast-4
亚太地区（孟买）	ap-south-1
亚太地区（大阪）	ap-northeast-3
亚太地区（首尔）	ap-northeast-2
亚太地区（新加坡）	ap-southeast-1

区域名称	区域代码
亚太地区（悉尼）	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
加拿大（中部）	ca-central-1
欧洲地区（法兰克福）	eu-central-1
欧洲地区（爱尔兰）	eu-west-1
欧洲地区（伦敦）	eu-west-2
欧洲地区（米兰）	eu-south-1
欧洲地区（巴黎）	eu-west-3
欧洲（西班牙）	eu-south-2
欧洲地区（斯德哥尔摩）	eu-north-1
欧洲（苏黎世）	eu-central-2
中东（巴林）	me-south-1
中东（阿联酋）	me-central-1
南美洲（圣保罗）	sa-east-1
AWS GovCloud （美国东部）	us-gov-east-1
AWS GovCloud （美国西部）	us-gov-west-1
中国（北京）	cn-north-1
中国（宁夏）	cn-northwest-1
以色列（特拉维夫）	il-central-1
加拿大西部（卡尔加里）	ca-west-1

区域名称	区域代码
墨西哥（墨西哥城）	mx-central-1
亚太地区（泰国）	ap-southeast-7
亚太地区（马来西亚）	ap-southeast-5

> **Note**
>
> 任何未列出的新 AWS 区域都可以通过本地部署获得支持，但不能通过一键部署来支持。

限额

服务限额（也称为限制）是您的 AWS 账户使用的服务资源或操作的最大数量。

此解决方案中 AWS 服务的配额

请确保此解决方案中实施的每项服务都有足够的限额。有关更多信息，请参阅 AWS 服务配额。

使用以下链接转到该服务的页面。要在不切换页面的情况下查看文档中所有 AWS 服务的服务配额，请改为查看 PDF 中服务终端节点和配额页面中的信息。

AWS CloudFormation 配额

您的 AWS 账户有 AWS CloudFormation 配额，在此解决方案中启动堆栈时应注意这些配额。通过了解这些限额，可以避免阻碍成功部署此解决方案的限制错误。有关更多信息，请参阅 AWS CloudFormation 用户指南中的 AWS CloudFormation 配额。

AWS CloudWatch 配额

您的 AWS 账户的 AWS CloudWatch 配额与 CloudWatch 资源策略相关联，每个账户每个区域仅允许 10 个资源策略，并且不能申请增加配额，请参阅 AWS CloudWatch 用户指南中的 AWS CloudWatch 日志配额。在部署之前，请检查您当前的使用情况，以确保在部署解决方案时不会超过此阈值。

AWS Organizations

该解决方案的 Lambda 函数调用 AWS Organizations API，以获取当前账户的别名，以包含在发布到解决方案的 SNS 主题的消息中。这样便于在解决方案的通知中看到人类可读的帐户名，以便进行调试和跟踪。

AWS Organizations 对客户调用其 API 终端节点的频率施加了限制。如果您发现解决方案超出了为您的账户设置的限制，则可以禁用获取和显示账户别名的功能。

为此，请导航到名为的 Lambda 函数，该函数`SO0111-ASR-sendNotifications`位于部署管理堆栈的区域和账户中。然后，找到名为的环境变量`DISABLE_ACCOUNT_ALIAS_LOOKUP`并将该值从 “False” 更改为 “True”。解决方案通知中的账户别名字段现在将变为 “未知”，但这不会影响解决方案的功能。

AWS Security Hub 部署

AWS Security Hub 的部署和配置是该解决方案的先决条件。有关设置 AWS Security Hub CSPM 的更多信息，请参阅 AWS Sec urity Hub 用户指南中的设置 AWS S ec urity Hub CSPM。该解决方案还支持 AWS Security Hub（非 CSPM 版本）。有关设置 AWS Security Hub 的更多信息，请参阅启用 Security Hub。

至少，您的主账户中必须配置一个可以正常运行的 Security Hub。您可以将此解决方案部署在与 Security Hub 主账户相同的账户（和 AWS 区域）中。在每个 Security Hub 主账户和辅助账户中，您还必须部署成员模板，该模板允许 AssumeRole 该解决方案的 AWS Step Functions 在账户中运行修复运行手册。

堆栈与 StackSets 部署

堆栈集允许您使用单个 AWS CloudFormation 模板在各个 AWS 区域的 AWS 账户中创建堆栈。从版本 1.4 开始，此解决方案支持堆栈集部署，方法是根据资源的部署位置和方式拆分资源。多账户客户，尤其是使用 AWS Organizations 的客户，可以从使用堆栈集在多个账户中部署中受益。它减少了安装和维护解决方案所需的工作量。有关的更多信息 StackSets，请参阅使用 AWS CloudFormation StackSets。

部署解决方案

> **Important**
>
> 如果在 Security Hub 中启用了整合控制结果功能（这是新部署中的默认设置），则只有在部署此解决方案时才启用安全控制 (CS) 行动手册。如果该功能未开启，则仅启用在 Security Hub 中启用的安全标准的行动手册。启用其他剧本可能会导致达到 EventBridge 规则的配额。

该解决方案使用 AWS CloudFormation 模板和堆栈来自动部署。这些 CloudFormation 模板指定了此解决方案中包含的 AWS 资源及其属性。 CloudFormation 堆栈提供模板中描述的资源。

为了使解决方案发挥作用，必须部署三个模板。首先，决定将模板部署到何处，然后决定如何部署模板。

本概述将描述模板以及如何决定将其部署在何处和如何部署。接下来的章节将详细说明如何将每个堆栈部署为堆栈或 StackSet。

决定将每个堆栈部署到何处

这三个模板将使用以下名称来引用，并包含以下资源：

- 管理堆栈：协调器步骤函数、事件规则和 Security Hub 自定义操作。
- 成员堆栈：补救 SSM 自动化文档。
- 成员角色堆栈：用于补救的 IAM 角色。

管理员堆栈必须在单个账户和单个区域中部署一次。它必须部署到您已配置为组织的 Security Hub 结果聚合目标的账户和区域中。如果您希望使用操作日志功能来监控管理事件，则必须在组织的管理帐户或委派的管理员帐户中部署管理员堆栈。

该解决方案对 Security Hub 的发现进行操作，因此，如果未将特定账户和区域配置为聚合 Security Hub 管理员账户和区域中的调查结果，则该解决方案将无法对来自该账户和地区的发现进行操作。

> **Important**
>
> 如果您使用的是 AWS Security Hub（非 CSPM），则您有责任确保您注册了 AWS Security Hub CSPM 的成员账户也已加入 AWS Security Hub（非 CSPM）。AWS Security Hub CSPM 中聚合的区域也应与 AWS Security Hub（非 CSPM）中汇总的区域相匹配。

例如，一个组织拥有在区域运营的账户us-west-2，在区域us-east-1中拥有111111111111作为 Security Hub 委托管理员的账户us-east-1。账户222222222222和333333333333必须是委托管理员账户的 Security Hub 成员账户111111111111。必须将所有三个帐户配置为汇总us-west-2到的结果us-east-1。必须将管理堆栈部署到111111111111中的账户us-east-1。

有关查找聚合的更多详细信息，请参阅有关 Security Hub 委托管理员帐户和跨区域聚合的文档。

管理员堆栈必须先完成部署，然后再部署成员堆栈，这样才能创建从成员账户到中心账户的信任关系。

成员堆栈必须部署到您要修复发现的每个账户和区域。这可能包括您之前部署了 ASR 管理堆栈的 Security Hub 委托管理员帐户。自动化文档必须在成员账户中执行，才能使用 SSM 自动化的免费套餐。

使用前面的示例，如果您要修复所有账户和区域的调查结果，则必须将成员堆栈部署到所有三个账户（111111111111222222222222、和333333333333）以及两个区域（us-east-1和us-west-2）。

成员角色堆栈必须部署到每个账户，但它包含每个账户只能部署一次的全球资源（IAM 角色）。在哪个区域部署成员角色堆栈并不重要，因此为简单起见，我们建议部署到部署管理堆栈的同一区域。

使用前面的示例，我们建议将成员角色堆栈部署到中的所有三个账户（111111111111222222222222、和333333333333）us-east-1。

决定如何部署每个堆栈

部署堆栈的选项有

- CloudFormation StackSet（自行管理权限）
- CloudFormation StackSet（服务管理权限）
- CloudFormation 堆栈

StackSets 使用服务管理权限最为方便，因为它们不需要部署您自己的角色，并且可以自动部署到组织中的新帐户。不幸的是，此方法不支持嵌套堆栈，我们在管理堆栈和成员堆栈中都使用嵌套堆栈。唯一可以通过这种方式部署的堆栈是成员角色堆栈。

请注意，在部署到整个组织时，不包括组织管理帐户，因此，如果您要修复组织管理帐户中的调查结果，则必须单独部署到该帐户。

成员堆栈必须部署到每个账户和区域，但不能使用服务管理权限 StackSets 进行部署，因为它包含嵌套堆栈。因此，我们建议使用 StackSets 自我管理权限部署此堆栈。

管理员堆栈仅部署一次，因此可以将其部署为普通 CloudFormation 堆栈，也可以在单个账户和区域中部署为 StackSet 具有自我管理权限的堆栈。

整合的控件调查发现

可以在开启或关闭 Security Hub 的合并控制结果功能的情况下对组织中的账户进行配置。请参阅 AWS Security Hub 用户指南中的整合控制结果。

> **Important**
>
> 如果启用，则必须使用该解决方案的 v2.0.0 或更高版本。此外，您必须为 “SC” 或 “安全控制” 标准部署管理员和成员嵌套堆栈。这将部署自动化文档和 EventBridge 规则，以便与启用此功能时 IDs 生成的合并控件一起使用。使用此功能时，无需针对特定标准（例如 AWS FSBP）部署管理员或成员嵌套堆栈。

中国部署

该解决方案确实支持在中国区域部署，但是您必须使用以下 Launch 按钮在中国地区进行一键部署，而不是使用本指南其他部分中提供的启动按钮。如果您在中国地区部署，则无法使用本指南后续章节中提供的 “启动解决方案” 按钮。您仍然可以从任何 S3 存储桶链接下载模板并通过上传模板文件来部署堆栈。

- automated-security-response-admin。模板：

Launch solution

- automated-security-response-member-roles.模板：

- automated-security-response-member。模板：

GovCloud （美国）部署

该解决方案确实支持在 GovCloud （美国）地区进行部署，但是您必须使用以下 Launch 按钮在 GovCloud （美国）地区进行一键部署，而不是使用本指南其他部分中提供的启动按钮。如果您在 GovCloud （美国）地区进行部署，则无法使用本指南后续章节中提供的 “启动解决方案” 按钮。您仍然可以从任何 S3 存储桶链接下载模板并通过上传模板文件来部署堆栈。

- automated-security-response-admin。模板：

- automated-security-response-member-roles.模板：

- automated-security-response-member。模板：

AWS CloudFormation 模板

automa
security-response-admin.template-使用此模板启动 AWS 上的自动安全响应解决方案。该模板安装解

决方案的核心组件、AWS Step Functions 日志的嵌套堆栈以及您选择激活的每个安全标准的一个嵌套堆栈。

使用的服务包括亚马逊简单通知服务、AWS 密钥管理服务、AWS 身份和访问管理、AWS Lambda、AWS Step Functions、亚马逊 CloudWatch 日志、亚马逊 S3 和 AWS Systems Manager。

管理员账号支持

以下模板安装在 AWS Security Hub 管理员账户中，用于开启您想要支持的安全标准。在安装时，您可以选择要安装以下哪个模板`automated-security-response-admin.template`。

automated-security-response-orchestrator-log.template-为 Orchestrator Step 函数创建 CloudWatch 日志组。

automated-security-response-webui-nested-stack.template-创建资源以支持解决方案的 Web 用户界面。

AFSBPStack.template-AWS 基础安全最佳实践 v1.0.0 规则。

CIS120stack.Template-独联体亚马逊 Web Services Foundations 基准测试，v1.2.0 规则。

CIS140stack.Template-独联体亚马逊 Web Services Foundations 基准测试，v1.4.0 规则。

CIS300stack.Template-独联体亚马逊 Web Services Foundations 基准测试，v3.0.0 规则。

PCI321Stack.template-PCI-DSS v3.2.1 规则。

NISTStack.template-美国国家标准与技术研究院 (NIST)，v5.0.0 规则。

SCStack.template-安全控制 v2.0.0 规则。

成员角色

View template

automa security-response-member-roles.templ ate-定义每个 AWS Security Hub 成员账户所需的补救角色。

成员账户

View template

automa security-response-member.templat e-在设置核心解决方案后，使用此模板在每个 AWS Security Hub

成员账户（包括管理员账户）中安装 AWS Systems Manager 自动化运行手册和权限。此模板允许您选择要安装的安全标准手册。

将根据您的选择`automated-security-response-member.template`安装以下模板：

automated-security-response-remediation-runbooks.templat e-一项或多项安全标准使用的常用补救代码。

AFSBPMemberStack.template- AWS 基础安全最佳实践 v1.0.0 设置、权限和补救运行手册。

CIS120 MemberStack .template-CIS Amazon Web Services Foundations 基准测试、1.2.0 版设置、权限和补救运行手册。

CIS140 MemberStack .template-CIS Amazon Web Services Foundations 基准测试、1.4.0 版设置、权限和补救运行手册。

CIS300 MemberStack .template-CIS Amazon Web Services Foundations 基准测试、3.0.0 版设置、权限和补救运行手册。

PCI321MemberStack.tem plate-PCI-DSS v3.2.1 设置、权限和补救操作手册。

NISTMemberStack.Template-美国国家标准与技术研究院 (NIST)，v5.0.0 设置、权限和补救运行手册。

SCMemberStack.Template-安全控制设置、权限和补救操作手册。

automated-security-response-member-cloudtrail.temp late-在操作日志功能中用于跟踪和审计以及服务活动。

票务系统集成

使用以下模板之一与您的票务系统集成。

View template

JiraBlu

如果您使用 Jira 作为票务系统，请进行部署。

View template

Service

如果您 ServiceNow 用作票务系统，请进行部署。

如果您想集成不同的外部票务系统，则可以使用这两个堆栈中的任何一个作为蓝图，以了解如何实现自己的自定义集成。

自动部署- StackSets

> **Note**
>
> 我们建议使用进行部署 StackSets。但是，对于单账户部署或出于测试或评估目的，请考虑使用堆栈部署选项。

在启动解决方案之前，请查看本指南中讨论的架构、解决方案组件、安全性和设计注意事项。按照本节中的 step-by-step说明配置解决方案并将其部署到您的 AWS Organizations 中。

部署时间：每个账户大约 30 分钟，具体取决于 StackSet 参数。

先决条件

AWS O rganizations 可帮助您集中管理和管理您的多账户 AWS 环境和资源。 StackSets 最适合与 AWS Organiations 合作。

如果您之前部署过此解决方案的 1.3.x 或更早版本，则必须卸载现有解决方案。有关更多信息，请参阅更新解决方案。

在部署此解决方案之前，请查看您的 AWS Security Hub 部署情况：

- 您的 AWS 组织中必须有一个委托的 Security Hub 管理员账户。
- 应将 Security Hub 配置为汇总各区域的调查结果。有关更多信息，请参阅 AWS Security Hub 用户指南中的跨区域汇总结果。
- 您应该在每个使用 AWS 的地区为您的组织激活 Security Hub。

此过程假设您有多个使用 AWS Organizations 的账户，并且已经委托了一个 AWS Organizations 管理员账户和一个 AWS Security Hub 管理员账户。

请注意，此解决方案同时适用于 AWS Security Hub 和 AWS Security Hub CSPM。

部署概述

> **Note**
>
> StackSets 此解决方案的部署使用了服务管理和自我 StackSets管理的组合。当前 StackSets 必须使用自我管理，因为它们使用的是嵌套 StackSets，而服务 StackSets管理尚不支持嵌套。

使用您的 StackSets AWS Organizati ons 中的委托管理员账户进行部署。

规划

使用以下表格来帮助进行 StackSets 部署。准备好数据，然后在部署期间复制并粘贴这些值。

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

（可选）步骤 0：部署工单集成堆栈

- 如果您打算使用工单功能，请先将工单集成堆栈部署到您的 Security Hub 管理员帐户中。
- 从该堆栈中复制 Lambda 函数名称并将其作为输入提供给管理堆栈（参见步骤 1）。

第 1 步：在委派的 Security Hub 管理员账户中启动管理堆栈

- 使用自我管理 StackSet，将 `automated-security-response-admin.template` AWS CloudFormation 模板启动到您的 AWS Security Hub 管理员账户中，该账户与您的 Security Hub 管理员位于同一区域。此模板使用嵌套堆栈。
- 选择要安装的安全标准。默认情况下，仅选择 SC（推荐）。
- 选择要使用的现有 Orchestrator 日志组。`Yes`如果之前的安装中`SO0111-ASR- Orchestrator`已经存在，请选择此选项。
- 选择是否启用解决方案的 Web UI。如果您选择启用此功能，则还必须输入要分配管理员角色的电子邮件地址。
- 选择收集与解决方案运行状况相关的 CloudWatch 指标的首选项。

有关自我管理的更多信息 StackSets，请参阅 AW S CloudFormation 用户指南中的授予自我管理权限。

第 2 步：将修复角色安装到每个 AWS Security Hub 成员账户中

请等待步骤 1 完成部署，因为步骤 2 中的模板引用了步骤 1 创建的 IAM 角色。

- 使用服务托管 StackSet，将 `automated-security-response-member-roles.template` AWS CloudFormation 模板启动到您的 AWS Organizations 中每个账户的单个区域。
- 选择在新账户加入组织时自动安装此模板。
- 输入您的 AWS Security Hub 管理员账户的账户 ID。
- 输入一个值，`namespace`该值将用于防止资源名称与同一个账户中的先前或并发部署发生冲突。输入最多 9 个小写字母数字字符的字符串。

第 3 步：将成员堆栈启动到每个 AWS Security Hub 成员账户和区域

- 使用自我管理 StackSets，将 `automated-security-response-member.template` AWS CloudFormation 模板启动到所有区域，在该区域中，您的 AWS 组织中的每个账户都有 AWS 资源，由同一 Security Hub 管理员管理。

> **Note**
>
> 在服务管理 StackSets 支持嵌套堆栈之前，您必须为加入组织的所有新帐户执行此步骤。

- 选择要安装的 “安全标准” 行动手册。
- 提供 CloudTrail 日志组的名称（用于某些补救措施）。

- 输入您的 AWS Security Hub 管理员账户的账户 ID。
- 输入一个值，namespace该值将用于防止资源名称与同一个账户中的先前或并发部署发生冲突。输入最多 9 个小写字母数字字符的字符串。这应该与您为成员角色堆栈选择的namespace值相匹配，此外，每个成员账户的命名空间值不必是唯一的。

（可选）步骤 0：启动工单系统集成堆栈

1. 如果您打算使用票证功能，请先启动相应的集成堆栈。
2. 为 Jira 或选择提供的集成堆栈 ServiceNow，或者将其用作蓝图来实现您自己的自定义集成。

   要部署 Jira 堆栈，请执行以下操作：

   a. 输入堆栈的名称。

   b. 为您的 Jira 实例提供 URI。

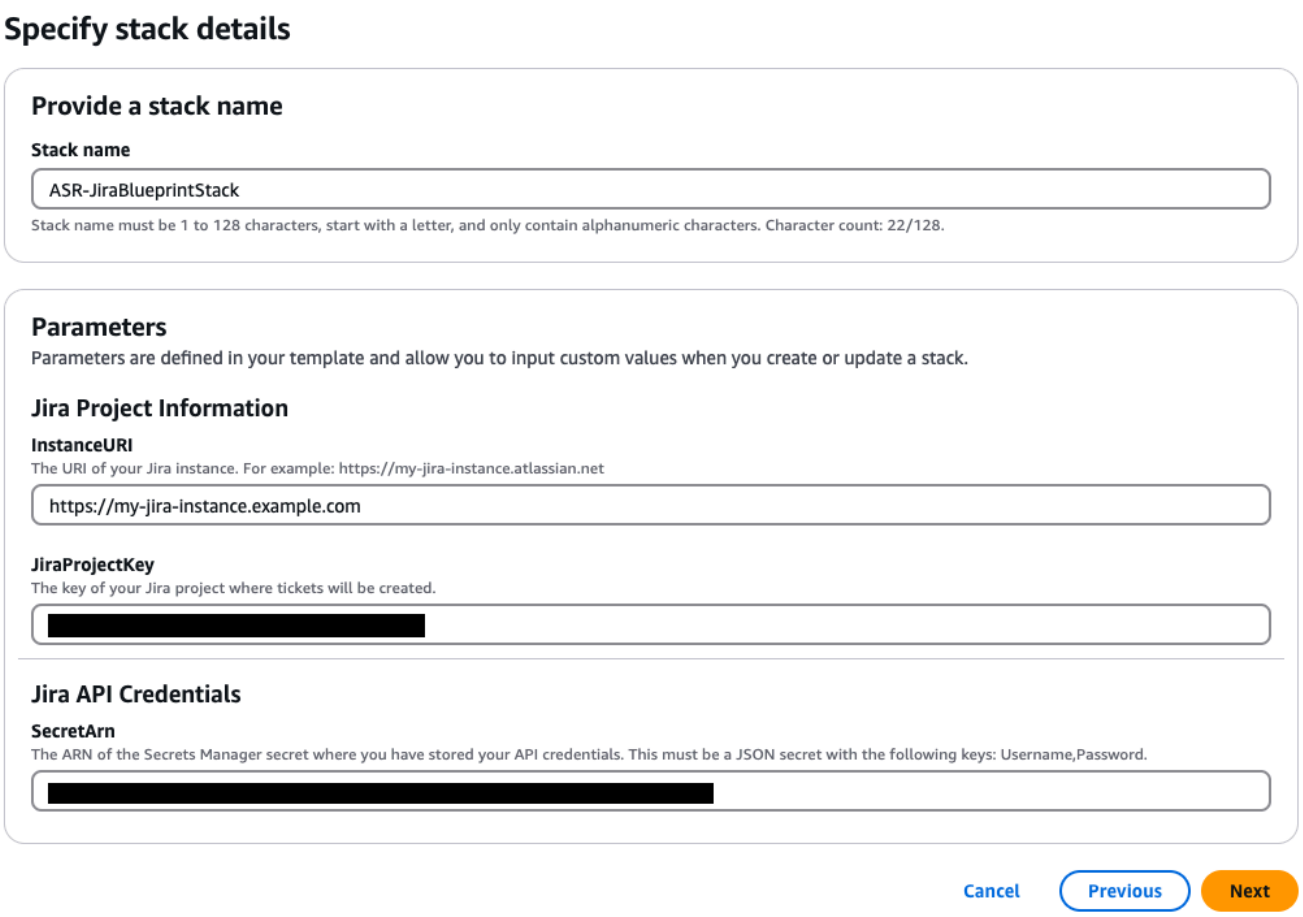
   c. 为要向其发送工单的 Jira 项目提供项目密钥。

   d. 在 Secrets Manager 中创建一个新的键值密钥，用于存放你的 Jira Username 和。Password

   > **Note**
   >
   > 您可以选择使用 Jira API 密钥代替密码，方法是提供用户名为Username，API 密钥作为。Password

   e. 将此密钥的 ARN 作为输入添加到堆栈中。

   提供堆栈名称 Jira 项目信息以及 Jira API 凭证。



要部署 ServiceNow 堆栈，请执行以下操作：

f. 输入堆栈的名称。

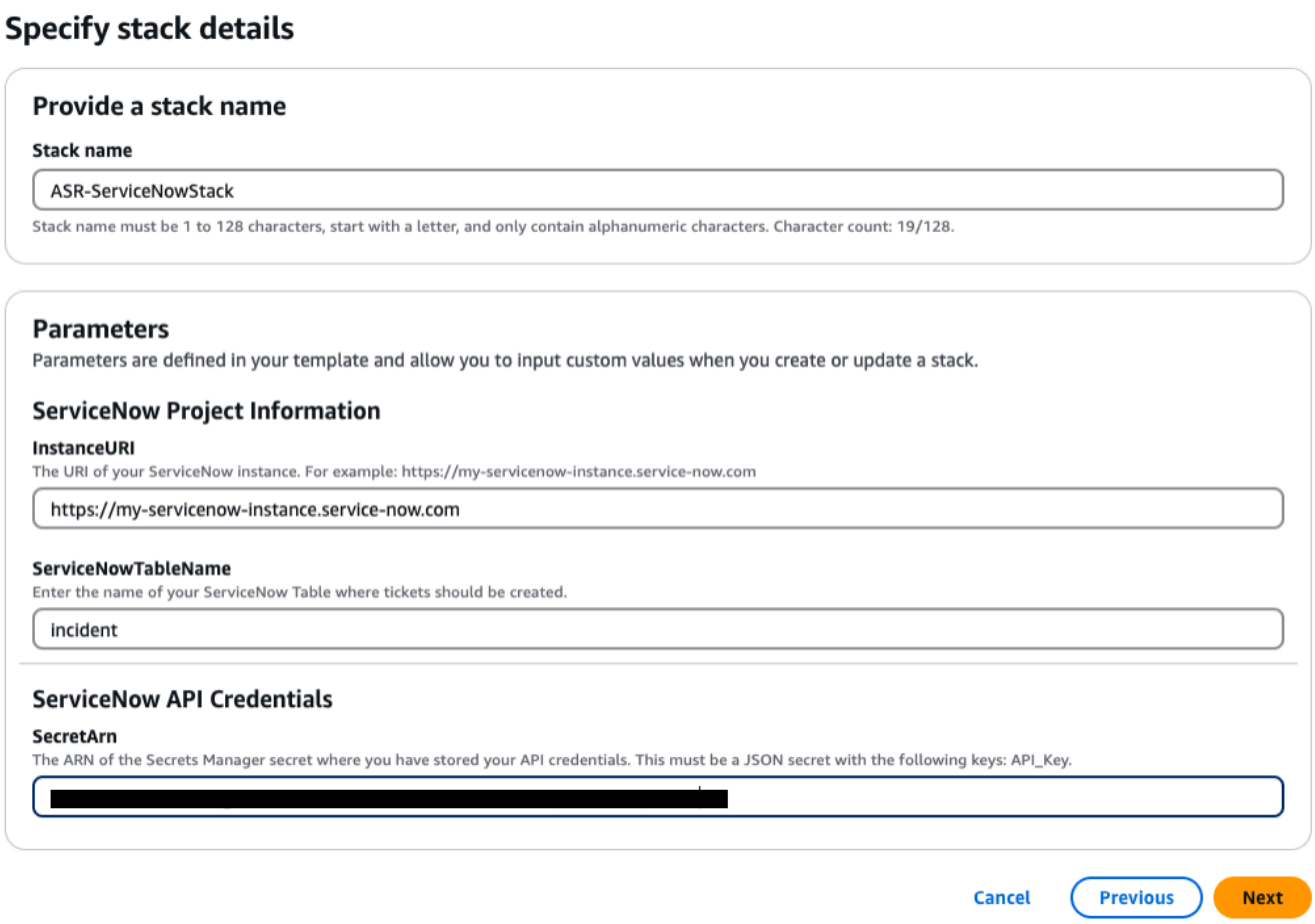
g. 提供您的 ServiceNow 实例的 URI。

h. 提供您的 ServiceNow 表名。

i. 在中创建 API 密钥，该密钥 ServiceNow 具有修改您要写入的表的权限。

j. 使用密钥在 Secrets Manager 中创建密钥，`API_Key`然后将密钥 ARN 作为堆栈的输入提供给堆栈。

提供堆栈名称、 ServiceNow 项目信息和 ServiceNow API 凭证。



要创建自定义集成堆栈，请执行以下操作：添加一个 Lambda 函数，解决方案协调器 Step Functions 可以在每次修复中调用该函数。Lambda 函数应采用 Step Functions 提供的输入，根据票务系统的要求构造有效负载，然后向您的系统请求创建票证。

第 1 步：在委派的 Security Hub 管理员账户中启动管理堆栈

1. 使用您的 Securit `automated-security-response-admin.template` y Hub 管理员帐户启动管理堆栈。通常，在单个区域中每个组织一个。由于此堆栈使用嵌套堆栈，因此您必须将此模板部署为自 StackSet管理模板。

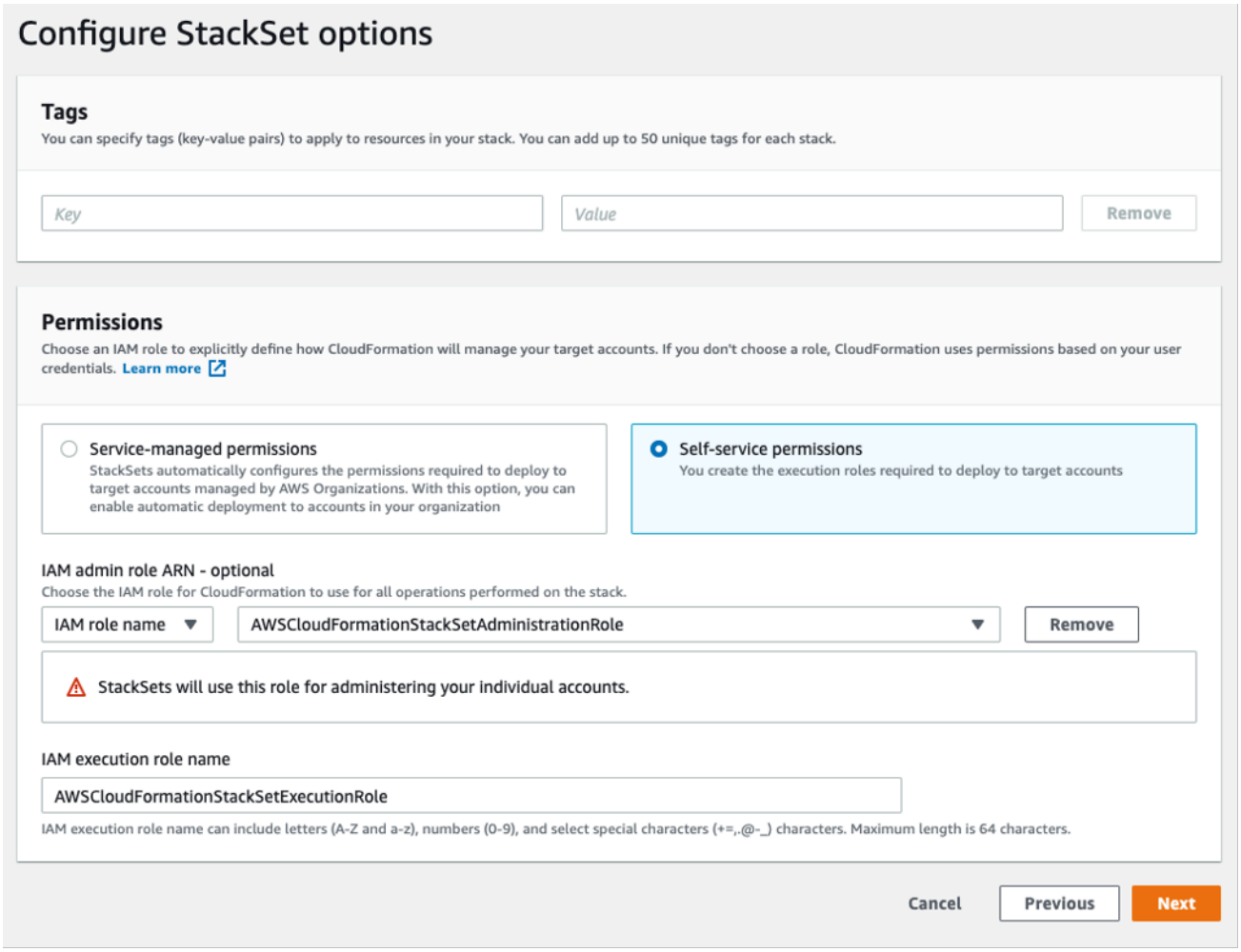
Parameters

参数	默认值	描述
加载 SC 管理堆栈	yes	指定是否安装用于自动修复 SC 控件的管理组件。
加载 AFSBP 管理堆栈	no	指定是否安装用于自动修复 FSBP 控件的管理组件。
加载 CIS12 0 管理堆栈	no	指定是否安装管理组件以自动修复 CIS12 0 个控件。
加载 CIS14 0 管理堆栈	no	指定是否安装管理组件以自动修复 CIS14 0 个控件。
加载 CIS3 00 管理堆栈	no	指定是否安装管理组件以自动修复 CIS3 00 个控件。
加载 PC1321 管理堆栈	no	指定是否安装管理组件以自动修复 PC1321 控件。
加载 NIST 管理堆栈	no	指定是否安装用于自动修复 NIST 控件的管理组件。
重用 Orchestrator 日志组	no	选择是否重复使用现有的SO0111-ASR-Orchestrator CloudWatch 日志组。这简化了重新安装和升级，而不会丢失先前版本的日志数据。yes如果此账户中Orchestrator Log Group仍存在先前部署的现有Orchestrator Log Group选择，否则，请重复使用现有选择no。如果您要从低于 v2.3.0 的版本执行堆栈更新，请选择 no

参数	默认值	描述
ShouldDeployWeb用户界面	yes	部署 Web 用户界面组件，包括 API Gateway、Lambda 函数和 CloudFront 分发。选择“是” 以启用基于 Web 的用户界面，用于查看发现结果和补救状态。如果您选择禁用此功能，您仍然可以使用 Security Hub CSPM 自定义操作配置自动修复并按需运行修复。
AdminUserEmail	（可选输入）	初始管理员用户的电子邮件地址。此用户将拥有对 ASR Web UI 的完全管理权限。仅在启用 Web 用户界面时才需要。
使用 CloudWatch 指标	yes	指定是否启用用于监控解决方案的 CloudWatch 指标。这将创建一个用于查看指标的 CloudWatch 控制面板。
使用 CloudWatch 指标警报	yes	指定是否为解决方案启用 CloudWatch 指标警报。这将为解决方案收集的某些指标创建警报。
RemediationFailureAlarmThreshold	5	为每个控件 ID 指定修复失败百分比的阈值。例如，如果您输入5，则如果控制 ID 在给定日期失败超过 5% 的补救措施，则会收到警报。 此参数仅在创建警报后才起作用（请参阅使用 CloudWatch 指标警报参数）。

参数	默认值	描述
EnableEnhancedCloudWatchMetrics	no	如果yes，则会创建其他 CloudWatch 指标，以便在 CloudWatch 仪表板上 IDs 单独跟踪所有控制并作为 CloudWatch 警报进行跟踪。 要了解由此产生的额外成本，请参阅 “成本” 部分。
TicketGenFunctionName	（可选输入）	可选。如果您不想集成票务系统，请留空。否则，请提供步骤 0 的堆栈输出中的 Lambda 函数名称，例如：。SO0111-ASR-ServiceNow-TicketGenerator

配置 StackSet 选项



1. 在账号参数中，输入 AWS Security Hub 管理员账户的账户 ID。
2. 在 “指定区域” 参数中，仅选择开启 Security Hub 管理员的区域。等待此步骤完成后再进入步骤 2。

第 2 步：将修复角色安装到每个 AWS Security Hub 成员账户中

使用服务托管 StackSets 部署成员角色模板。`automated-security-response-member-roles.template`每个成员账户 StackSet 必须将其部署在一个区域。它定义了允许通过 ASR Orchestrator 步骤函数进行跨账户 API 调用的全局角色。

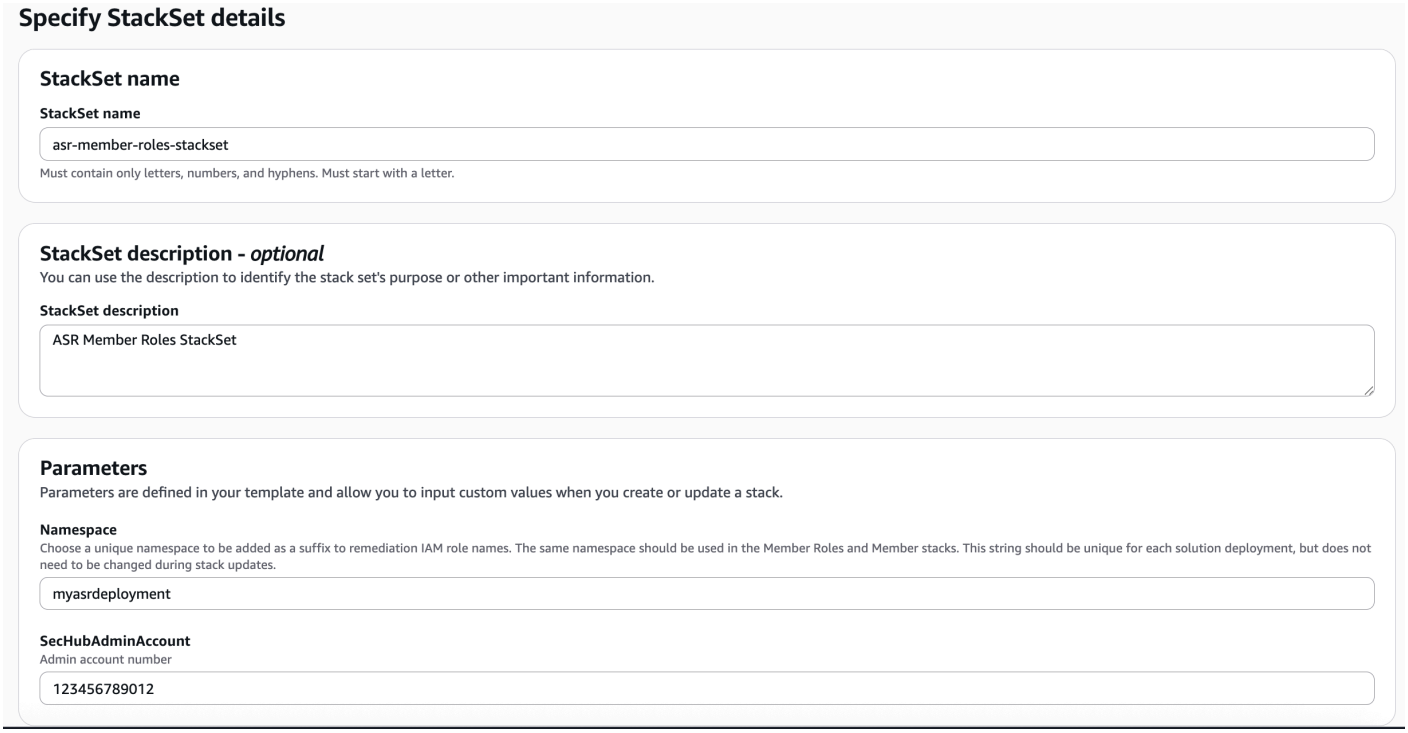
Parameters

参数	默认值	描述
命名空间	*<Requires input>*	输入最多 9 个小写字母数字字符的字符串。将添加为修复

参数	默认值	描述
		IAM 角色名称的后缀的唯一命名空间。成员角色和成员堆栈中应使用相同的命名空间。对于每个解决方案部署，此字符串应是唯一的，但在堆栈更新期间无需更改。每个成员账户的命名空间值不必是唯一的。
Sec Hub 账户管理员	*<Requires input>*	输入 AWS Security Hub 管理员账户的 12 位数账户 ID。此值向管理员账户的解决方案角色授予权限。

1. 根据您的组织政策，部署到整个组织（典型值）或组织单位。
2. 开启自动部署，这样 AWS Organizations 中的新账户就可以获得这些权限。
3. 在 “指定区域” 参数中，选择单个区域。IAM 角色是全球性的。 StackSet 部署期间，您可以继续执行步骤 3。

指定 StackSet 细节



步骤 3：将成员堆栈启动到每个 AWS Security Hub 成员账户和区域

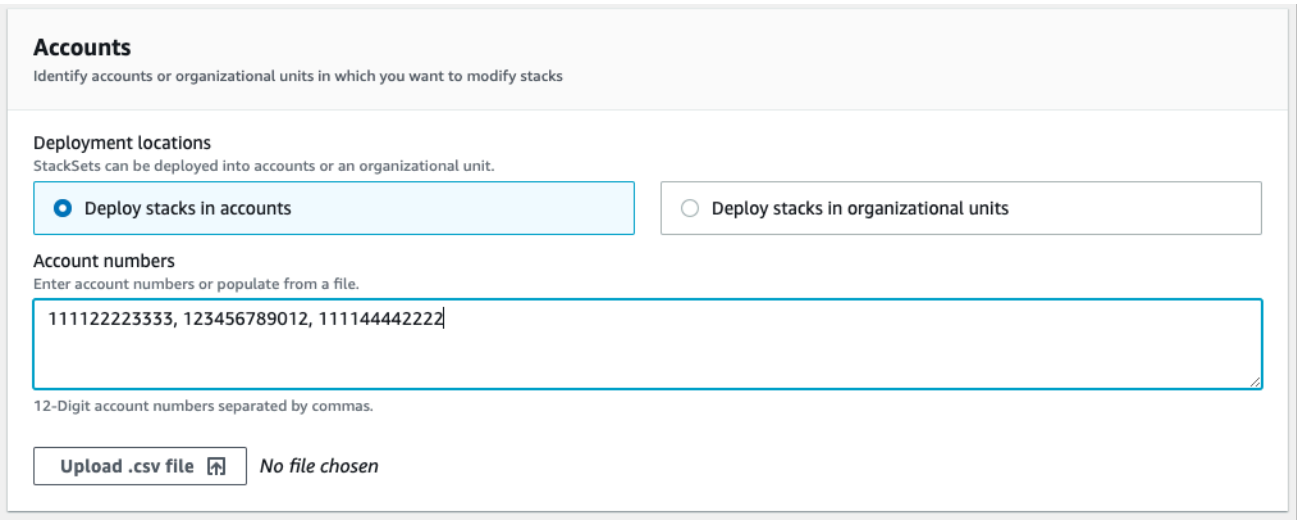
由于成员堆栈使用嵌套堆栈，因此您必须部署为自 StackSet管理堆栈。这不支持自动部署到 AWS 组织中的新账户。

Parameters

参数	默认值	描述
提供用于创建指标筛选器和警报的名称 LogGroup	*<Requires input>*	指定用于记录 API 调用的 CloudWatch CloudTrail 日志组的名称。这用于 CIS 3.1-3.14 的补救措施。
加载 SC 成员堆栈	yes	指定是否安装用于自动修复 SC 控件的成员组件。
加载 AFSBP 成员堆栈	no	指定是否安装用于自动修复 FSBP 控件的成员组件。
加载 CIS12 0 成员堆栈	no	指定是否安装成员组件以自动修复 CIS12 0 个控件。
加载 CIS14 0 成员堆栈	no	指定是否安装成员组件以自动修复 CIS14 0 个控件。
加载 CIS3 00 个成员堆栈	no	指定是否安装用于自动修复 CIS3 00 控件的成员组件。
加载 PC1321 成员堆栈	no	指定是否安装成员组件以自动修复 PC1321 控件。
加载 NIST 成员堆栈	no	指定是否安装用于自动修复 NIST 控件的成员组件。
为 Redshift 审计日志创建 S3 存储桶	no	选择yes是否应为 FSBP RedShift .4 修复创建 S3 存储桶。有关 S3 存储桶和补救措施的详细信息，请查看 AWS

参数	默认值	描述
		Security Hub 用户指南中的 Redshift.4 补救措施。
Sec Hub 管理员账户	*<Requires input>*	输入 AWS Security Hub 管理员账户的 12 位数账户 ID。
命名空间	*<Requires input>*	输入最多 9 个小写字母数字字符的字符串。此字符串成为 IAM 角色名称和 Action Log S3 存储桶的一部分。对成员堆栈部署和成员角色堆栈部署使用相同的值。每个解决方案部署的字符串都应是唯一的，但在堆栈更新期间无需更改。
EnableCloudTrailForASRAction日志	no	选择yes是否要在 CloudWatch 仪表板上监控解决方案执行的管理事件。该解决方案会在您选择的每个成员账户中创建一个 CloudTrail 跟踪yes。您必须将解决方案部署到 AWS 组织中才能启用此功能。此外，您只能在同一个账户的单个地区启用此功能。要了解由此产生的额外成本，请参阅“成本”部分。

账户



部署地点：您可以指定账号或组织单位列表。

指定区域：选择要修复结果的所有区域。您可以根据账户数量和区域数量调整部署选项。区域并发可以是并行的。

自动部署-堆栈

> **Note**
>
> 对于多账户客户，我们强烈建议使用进行部署。 StackSets

在启动解决方案之前，请查看本指南中讨论的架构、解决方案组件、安全性和设计注意事项。按照本节中的 step-by-step说明配置解决方案并将其部署到您的账户。

部署时间：大约 30 分钟

先决条件

在部署此解决方案之前，请确保 AWS Security Hub 与您的主账户和次要账户位于相同的 AWS 区域。如果您之前部署过此解决方案，则必须卸载现有解决方案。有关更多信息，请参阅更新解决方案。

部署概述

使用以下步骤在 AWS 上部署此解决方案。

（可选）步骤 0：启动工单系统集成堆栈

- 如果您打算使用工单功能，请先将工单集成堆栈部署到您的 Security Hub 管理员帐户中。
- 从该堆栈中复制 Lambda 函数名称并将其作为输入提供给管理堆栈（参见步骤 1）。

步骤 1：启动管理堆栈

- 将 `automated-security-response-admin.template` AWS CloudFormation 模板启动到您的 AWS Security Hub 管理员账户。
- 选择要安装的安全标准。
- 选择要使用的现有 Orchestrator 日志组（`Yes`如果先前安装中`SO0111-ASR-Orchestrator`已存在，请选择）。

第 2 步：将修复角色安装到每个 AWS Security Hub 成员账户中

- 将 `automated-security-response-member-roles.template` AWS CloudFormation 模板启动到每个成员账户的一个区域。
- 输入 AWS Security Hub 管理员账户的 12 位数账户 IG。

步骤 3：启动成员堆栈

- 指定要用于 CIS 3.1-3.14 修正的 CloudWatch 日志组的名称。它必须是接收 CloudWatch CloudTrail 日志的日志组的名称。
- 选择是否安装修复角色。每个账户只能安装一次这些角色。
- 选择要安装的剧本。
- 输入 AWS Security Hub 管理员账户的账户 ID。

步骤 4：（可选）调整可用的补救措施

- 以每个成员账户为单位删除所有补救措施。此为可选步骤。

（可选）步骤 0：启动工单系统集成堆栈

1. 如果您打算使用票证功能，请先启动相应的集成堆栈。
2. 为 Jira 或选择提供的集成堆栈 ServiceNow，或者将其用作蓝图来实现您自己的自定义集成。

   要部署 Jira 堆栈，请执行以下操作：

a. 输入堆栈的名称。

b. 为您的 Jira 实例提供 URI。

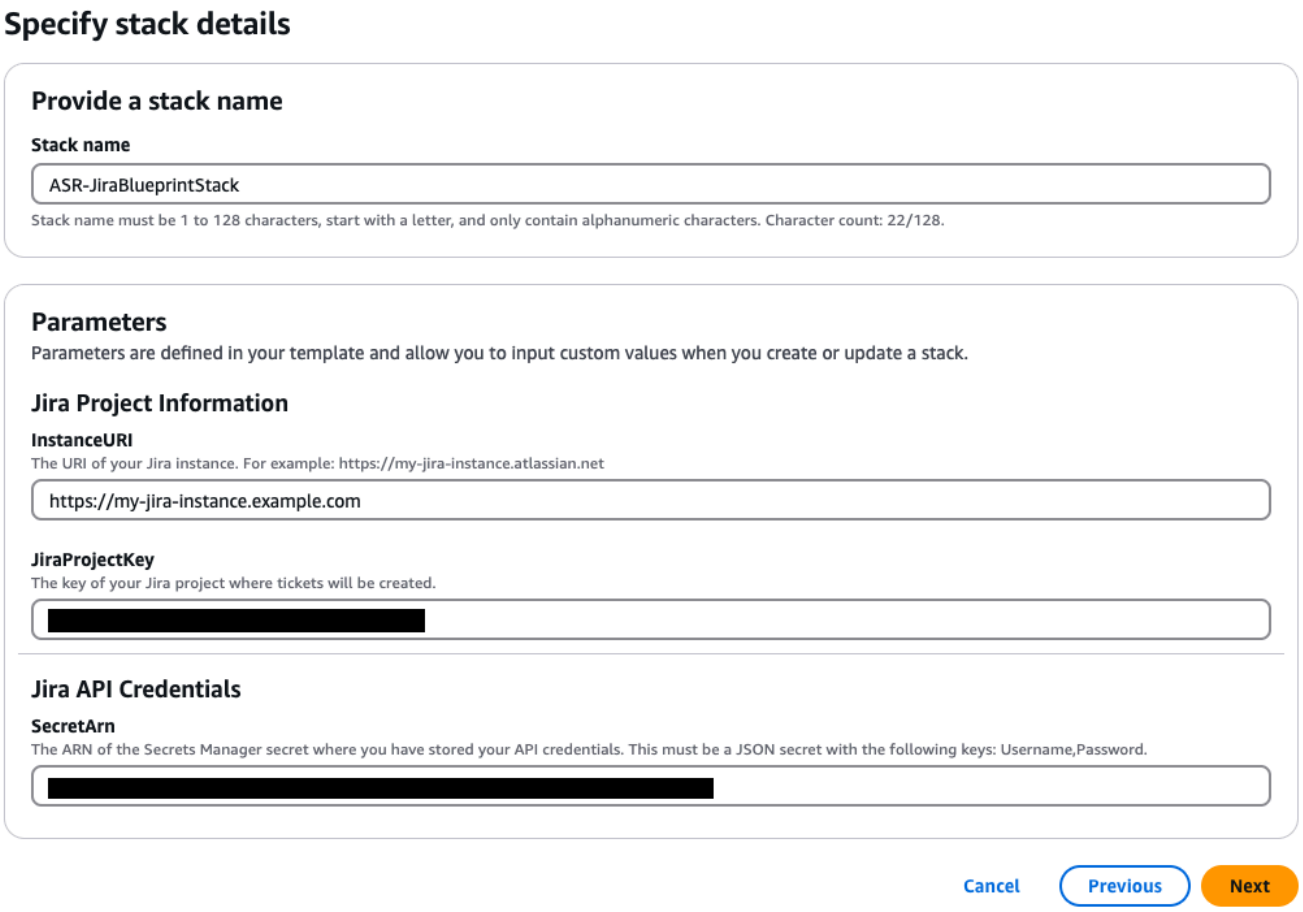
c. 为要向其发送工单的 Jira 项目提供项目密钥。

d. 在 Secrets Manager 中创建一个新的键值密钥，用于存放你的 Jira `Username` 和。`Password`

> **Note**
>
> 您可以选择使用 Jira API 密钥代替密码，方法是提供用户名为`Username`，API 密钥作为。`Password`

e. 将此密钥的 ARN 作为输入添加到堆栈中。

“提供堆栈名称 Jira 项目信息和 Jira API 凭证。



要部署 ServiceNow 堆栈，请执行以下操作：

f. 输入堆栈的名称。

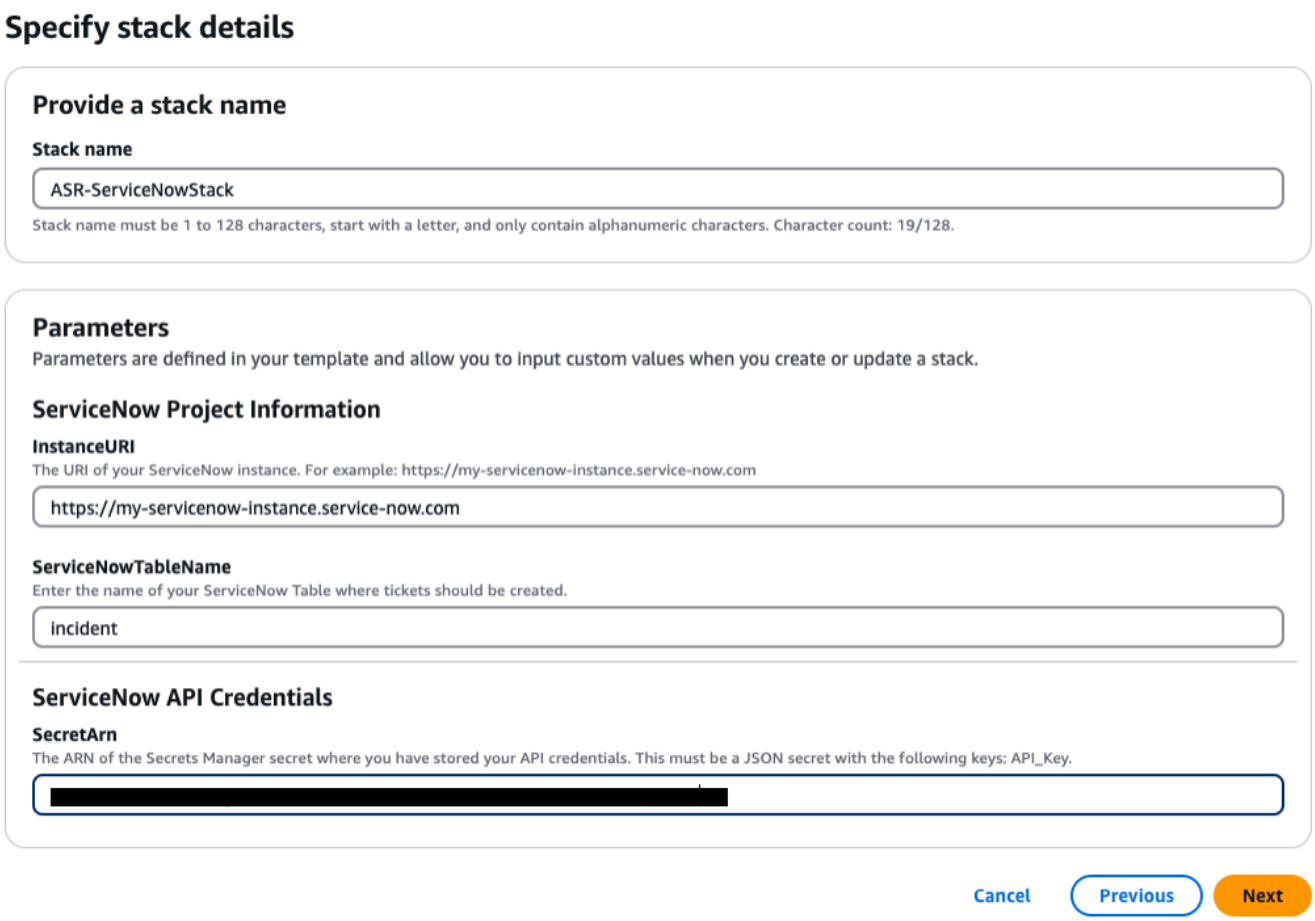
g. 提供您的 ServiceNow 实例的 URI。

h. 提供您的 ServiceNow 表名。

i. 在中创建 API 密钥，该密钥 ServiceNow 具有修改您要写入的表的权限。

j. 使用密钥在 Secrets Manager 中创建密钥，`API_Key`然后将密钥 ARN 作为堆栈的输入提供给堆栈。

提供堆栈名称、 ServiceNow 项目信息和 ServiceNow API 凭证。



要创建自定义集成堆栈，请执行以下操作：添加一个 Lambda 函数，解决方案协调器 Step Functions 可以在每次修复中调用该函数。Lambda 函数应采用 Step Functions 提供的输入，根据票务系统的要求构造有效负载，然后向您的系统请求创建票证。

步骤 1：启动管理堆栈

> **Important**
>
> 该解决方案包括数据收集。我们使用这些数据来更好地了解客户如何使用此解决方案以及相关服务和产品。AWS 拥有通过本次调查收集的数据。数据收集受 AWS 隐私声明的约束。

此自动化 AWS CloudFormation 模板在 AWS 云中部署了 AWS 上的自动安全响应解决方案。在启动堆栈之前，必须启用 Security Hub 并完成先决条件。

> **Note**
>
> 运行此解决方案时使用的 AWS 服务的费用由您承担。有关更多详情，请访问本指南中的成本部分，并参阅本解决方案中使用的每项 AWS 服务的定价网页。

1. 使用当前配置 AWS Security Hub 的账户登录 AWS 管理控制台，然后使用下面的按钮启动 `automated-security-response-admin.template` AWS CloudFormation 模板。

   Launch solution

   您也可以下载模板作为自己实施的起点。
2. 默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要在不同的 AWS 区域启动此解决方案，请使用 AWS 管理控制台导航栏中的区域选择器。

   > **Note**
   >
   > 此解决方案使用 AWS Systems Manager，该管理器目前仅在特定的 AWS 区域可用。该解决方案适用于所有支持该服务的地区。有关各地区的最新可用性，请参阅 AWS 区域服务列表。
3. 在创建堆栈页面上，确认 Amazon S3 URL 文本框中的模板 URL 是否正确，然后选择下一步。
4. 在指定堆栈详细信息页面上，为您的解决方案堆栈分配一个名称。有关命名字符限制的信息，请参阅 AWS Identity an d A ccess Management 用户指南中的 IAM 和 STS 限制。
5. 在 “参数” 页面上，选择 “下一步”。

参数	默认值	描述
加载 SC 管理堆栈	yes	指定是否安装用于自动修复 SC 控件的管理组件。
加载 AFSBP 管理堆栈	no	指定是否安装用于自动修复 FSBP 控件的管理组件。
加载 CIS12 0 管理堆栈	no	指定是否安装管理组件以自动修复 CIS12 0 个控件。
加载 CIS14 0 管理堆栈	no	指定是否安装管理组件以自动修复 CIS14 0 个控件。
加载 CIS3 00 管理堆栈	no	指定是否安装管理组件以自动修复 CIS3 00 个控件。
加载 PC1321 管理堆栈	no	指定是否安装管理组件以自动修复 PC1321 控件。
加载 NIST 管理堆栈	no	指定是否安装用于自动修复 NIST 控件的管理组件。
重用 Orchestrator 日志组	no	选择是否重复使用现有的SO0111-ASR-Orchestrator CloudWatch 日志组。这简化了重新安装和升级，而不会丢失先前版本的日志数据。yes如果此账户中Orchestrator Log Group仍存在先前部署的现有Orchestrator Log Group选择，否则，请重复使用现有选择no。如果您要从低于 v2.3.0 的版本执行堆栈更新，请选择 no

参数	默认值	描述
ShouldDeployWeb用户界面	yes	部署 Web 用户界面组件，包括 API Gateway、Lambda 函数和 CloudFront 分发。选择“是” 以启用基于 Web 的仪表板以查看发现结果和补救状态。
AdminUserEmail	（可选输入）	初始管理员用户的电子邮件地址。此用户将拥有对 ASR Web UI 的完全管理权限。仅在启用 Web 用户界面时才需要。
使用 CloudWatch 指标	yes	指定是否启用用于监控解决方案的 CloudWatch 指标。这将创建一个用于查看指标的 CloudWatch 控制面板。
使用 CloudWatch 指标警报	yes	指定是否为解决方案启用 CloudWatch 指标警报。这将为解决方案收集的某些指标创建警报。
RemediationFailure AlarmThreshold	5	为每个控件 ID 指定修复失败百分比的阈值。例如，如果您输入5，则如果控制 ID 在给定日期失败超过 5% 的补救措施，则会收到警报。 此参数仅在创建警报后才起作用（请参阅使用 CloudWatch 指标警报参数）。

参数	默认值	描述
EnableEnhancedCloudWatchMetrics	no	如果yes，则会创建其他 CloudWatch 指标，以便在 CloudWatch 仪表板上 IDs 单独跟踪所有控制并作为 CloudWatch 警报进行跟踪。 要了解由此产生的额外成本，请参阅 “成本” 部分。
TicketGenFunctionName	（可选输入）	可选。如果您不想集成票务系统，请留空。否则，请提供步骤 0 的堆栈输出中的 Lambda 函数名称，例如：。SO0111-ASR-ServiceNow-TicketGenerator

> **Note**
>
> 部署或更新解决方案 CloudFormation 堆栈后，您必须在管理员帐户中手动启用自动修复。

1. 在配置堆栈选项页面上，请选择下一步。
2. 在 Review 页面上，审核并确认设置。选中确认模板将创建 AWS Identity and Access Management (IAM) 资源的复选框。
3. 选择 Create stack（创建堆栈）以部署堆栈。

您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。大约 15 分钟后，您应该会收到 “创建完成” 状态。

第 2 步：将修复角色安装到每个 AWS Security Hub 成员账户中

每个成员账户automated-security-response-member-roles.template StackSet 只能部署在一个区域。它定义了允许通过 ASR Orchestrator 步骤函数进行跨账户 API 调用的全局角色。

1. 登录每个 AWS Security Hub 成员账户（包括同时也是成员的管理员账户）的 AWS 管理控制台。选择按钮启动 A `automated-security-response-member-roles.template` WS CloudFormation 模板。您也可以下载模板作为自己实施的起点。

2. 默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要在不同的 AWS 区域启动此解决方案，请使用 AWS 管理控制台导航栏中的区域选择器。
3. 在创建堆栈页面上，确认 Amazon S3 URL 文本框中的模板 URL 是否正确，然后选择下一步。
4. 在指定堆栈详细信息页面上，为您的解决方案堆栈分配一个名称。有关命名字符限制的信息，请参阅 AWS Identity and Access Management 用户指南中的 IAM 和 STS 限制。
5. 在 “参数” 页面上，指定以下参数并选择 “下一步”。

参数	默认值	描述
命名空间	*<Requires input>*	输入最多 9 个小写字母数字字符的字符串。将添加为修复 IAM 角色名称的后缀的唯一命名空间。成员角色和成员堆栈中应使用相同的命名空间。对于每个解决方案部署，此字符串应是唯一的，但在堆栈更新期间无需更改。每个成员账户的命名空间值不必是唯一的。
Sec Hub 账户管理员	*<Requires input>*	输入 AWS Security Hub 管理员账户的 12 位数账户 ID。此值向管理员账户的解决方案角色授予权限。

6. 在配置堆栈选项页面上，请选择下一步。
7. 在 Review 页面上，审核并确认设置。选中确认模板将创建 AWS Identity and Access Management (IAM) 资源的复选框。
8. 选择 Create stack（创建堆栈）以部署堆栈。

您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。您将在大约 5 分钟后看到 CREATE_COMPLETE 状态。在加载此堆栈的同时，您可以继续执行下一步。

步骤 3：启动成员堆栈

> **Important**
>
> 该解决方案包括数据收集。我们使用这些数据来更好地了解客户如何使用此解决方案以及相关服务和产品。AWS 拥有通过本次调查收集的数据。数据收集受 AWS 隐私政策的约束。

`automated-security-response-member`堆栈必须安装到每个 Security Hub 成员账户中。此堆栈定义了自动修复的运行手册。每个成员账户的管理员都可以通过此堆栈控制可用的补救措施。

1. 登录每个 AWS Security Hub 成员账户（包括同时也是成员的管理员账户）的 AWS 管理控制台。选择按钮启动 A `automated-security-response-member.template` WS CloudFormation 模板。

   Launch solution

您也可以下载模板作为自己实施的起点。默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要在不同的 AWS 区域启动此解决方案，请使用 AWS 管理控制台导航栏中的区域选择器。

+

> **Note**
>
> 该解决方案使用 AWS Systems Manager，该管理器目前已在大多数 AWS 区域提供。该解决方案适用于所有支持这些服务的地区。有关各地区的最新可用性，请参阅 AWS 区域服务列表。

1. 在创建堆栈页面上，确认 Amazon S3 URL 文本框中的模板 URL 是否正确，然后选择下一步。
2. 在指定堆栈详细信息页面上，为您的解决方案堆栈分配一个名称。有关命名字符限制的信息，请参阅 AWS Identity an d A ccess Management 用户指南中的 IAM 和 STS 限制。

3. 在 “参数” 页面上，指定以下参数并选择 “下一步”。

参数	默认值	描述
提供用于创建指标筛选器和警报的名称 LogGroup	*<Requires input>*	指定用于记录 API 调用的 CloudWatch CloudTrail 日志组的名称。这用于 CIS 3.1-3.14 的补救措施。
加载 SC 成员堆栈	yes	指定是否安装用于自动修复 SC 控件的成员组件。
加载 AFSBP 成员堆栈	no	指定是否安装用于自动修复 FSBP 控件的成员组件。
加载 CIS12 0 成员堆栈	no	指定是否安装成员组件以自动修复 CIS12 0 个控件。
加载 CIS14 0 成员堆栈	no	指定是否安装成员组件以自动修复 CIS14 0 个控件。
加载 CIS3 00 个成员堆栈	no	指定是否安装用于自动修复 CIS3 00 控件的成员组件。
加载 PC1321 成员堆栈	no	指定是否安装成员组件以自动修复 PC1321 控件。
加载 NIST 成员堆栈	no	指定是否安装用于自动修复 NIST 控件的成员组件。
为 Redshift 审计日志创建 S3 存储桶	no	选择yes是否应为 FSBP RedShift .4 修复创建 S3 存储桶。有关 S3 存储桶和补救措施的详细信息，请查看 AWS Security Hub 用户指南中的 Redshift.4 补救措施。
Sec Hub 管理员账户	*<Requires input>*	输入 AWS Security Hub 管理员账户的 12 位数账户 ID。

参数	默认值	描述
命名空间	*<Requires input>*	输入最多 9 个小写字母数字字符的字符串。此字符串成为 IAM 角色名称和 Action Log S3 存储桶的一部分。对成员堆栈部署和成员角色堆栈部署使用相同的值。每个解决方案部署的字符串都应是唯一的，但在堆栈更新期间无需更改。
EnableCloudTrailForASRAction日志	no	选择yes是否要在 CloudWatch 仪表板上监控解决方案执行的管理事件。该解决方案会在您选择的每个成员账户中创建一个 CloudTrail 跟踪yes。您必须将解决方案部署到 AWS 组织中才能启用此功能。此外，您只能在同一个账户的单个地区启用此功能。要了解由此产生的额外成本，请参阅“成本”部分。

4. 在配置堆栈选项页面上，请选择下一步。
5. 在 Review 页面上，审核并确认设置。选中确认模板将创建 AWS Identity and Access Management (IAM) 资源的复选框。
6. 选择 Create stack（创建堆栈）以部署堆栈。

您可以在 AWS CloudFormation 控制台的“状态”列中查看堆栈的状态。大约 15 分钟后，您应该会收到“创建完成”状态。

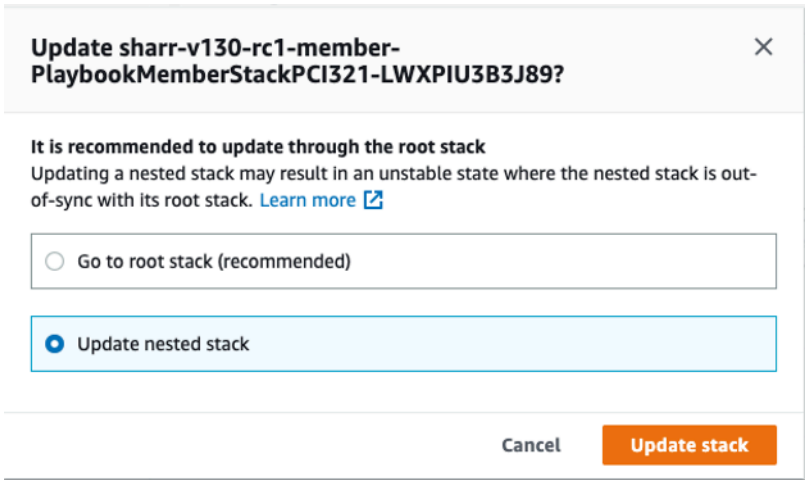
步骤 4：（可选）调整可用的补救措施

如果要从成员账户中删除特定的补救措施，可以通过更新安全标准的嵌套堆栈来实现。为简单起见，嵌套堆栈选项不会传播到根堆栈。

1. 登录 A WS CloudFormation 控制台并选择嵌套堆栈。

2. 选择更新。
3. 选择 “更新嵌套堆栈”，然后选择 “更新堆栈”。

   更新嵌套堆栈



4. 选择 “使用当前模板”，然后选择 “下一步”。
5. 调整可用的补救措施。将所需控件的值更改为 ，将不需要`Available`的控件的值更改为。`Not available`

   > **Note**
   >
   > 关闭补救措施会移除针对安全标准和控制的解决方案补救操作手册。

6. 在配置堆栈选项页面上，请选择下一步。
7. 在 Review 页面上，审核并确认设置。选中确认模板将创建 AWS Identity and Access Management (IAM) 资源的复选框。
8. 选择更新堆栈。

您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。大约 15 分钟后，您应该会收到 “创建完成” 状态。

Control Tower (CT) 部署

AWS Control Tower 定制 (cfcT) 指南适用于想要为公司和客户定制和扩展 AWS Control Tower 环境的管理员、 DevOps 专业人士、独立软件供应商、IT 基础设施架构师和系统集成商。它提供了有关使用 CfCT 自定义包自定义和扩展 AWS Control Tower 环境的信息。

部署时间：大约 30 分钟

先决条件

在部署此解决方案之前，请确保它适用于 AWS Control Tower 管理员。

当您准备好使用 AWS Control Tower 控制台设置着陆区时 APIs，或者按照以下步骤操作：

要开始使用 AWS Control Tower，请参阅：AWS Control Tower 入门

要了解如何自定义着陆区，请参阅：自定义着陆区

要启动和部署您的着陆区，请参阅：着陆区部署指南

部署概述

使用以下步骤在 AWS 上部署此解决方案。

步骤 1：构建和部署 S3 存储桶

> **Note**
>
> S3 存储桶配置-仅适用于管理员。这是一次性设置步骤，最终用户不应重复此步骤。S3 存储桶存储部署包，包括 ASR 运行所需的 AWS CloudFormation 模板和 Lambda 代码。这些资源是使用 CfCt 或部署的 StackSet。

1. 配置 S3 存储桶

设置用于存储和提供部署包的 S3 存储桶。

2. 设置 环境

准备构建和部署过程所需的必要环境变量、凭证和工具。

3. 配置 S3 存储桶策略

定义并应用适当的存储桶策略来控制访问和权限。

4. 准备构建

编译、打包或以其他方式准备您的应用程序或资产以进行部署。

5. 将软件包部署到 S3

将准备好的构建项目上传到指定的 S3 存储桶。

第 2 步：将堆栈部署到 AWS Control Tower

1. 为 ASR 组件创建生成清单

定义一份列出所有 ASR 组件及其版本、依赖关系和编译说明的构建清单。

2. 更新 CodePipeline

修改 AWS CodePipeline 配置以包括部署 ASR 组件所需的新构建步骤、项目或阶段。

步骤 1：构建并部署到 S3 存储桶

AWS Solutions 使用两个存储桶：一个用于全球访问模板的存储桶（通过 HTTPS 进行访问）和用于访问区域内资产（例如 Lambda 代码）的区域存储桶。

1. 配置 S3 存储桶

选择一个唯一的存储桶名称，例如 asr-staging。在您的终端上设置两个环境变量，一个应该是基本存储桶名称，后缀为-reference，另一个应以您的预期部署区域作为后缀：

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. 环境设置

在您的 AWS 账户中，使用这些名称创建两个存储桶，例如 asr-staging-reference和 asr-staging-us-east -1。（参考存储桶将存放 CloudFormation 模板，区域存储桶将存放所有其他资产，例如 lambda 代码包。）您的存储桶应经过加密且不允许公开访问

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> 创建存储桶时，请确保它们不可公开访问。使用随机存储桶名称。禁用公共访问。使用 KMS 加密。并在上传之前验证存储桶所有权。

3. S3 存储桶策略设置

更新 $TEMPLATE_BUCKET_NAME S3 存储桶策略以包含 PutObject 执行账户 ID 的权限。将此权限分配给执行账户中有权写入存储桶的 IAM 角色。此设置允许您避免在管理账户中创建存储桶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "org-id"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::account-id:role/iam-role-name"
                }
            }
        }
    ]
}
```

更改资产 S3 存储桶策略以包含权限。将此权限分配给执行账户中有权写入存储桶的 IAM 角色。对每个区域资产存储桶（例如 asr-staging-us-east -1、 asr-staging-eu-west -1 等）重复此设置，允许跨多个区域进行部署，而无需在管理账户中创建存储桶。

4. 编译准备

- 先决条件：
  - AWS CLI v2
  - 带有 pip 的 Python 3.11+
  - AWS CDK 2.171.1+
  - Node.js 20+ 带有 npm
  - 带导出插件的 Poetry v2
- Git clon https://github.com/aws-solutions/automated-security-response-one-aws .git

首先，请确保你已经在源文件夹中运行了 npm install。

接下来，从克隆存储库的部署文件夹中运行 build-s3-dist.sh，传递存储桶的根名称（例如 mybucket）和您正在构建的版本（例如 v1.0.0）。我们建议根据下载的版本使用 semver 版本 GitHub （例如 GitHub: v1.0.0，你的版本：v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5。将软件包部署到 S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

第 2 步：将堆栈部署到 AWS Control Tower

1. 为 ASR 组件生成清单

将 ASR 工件部署到 S3 存储桶后，更新 Control Tower 管道清单以引用新版本，然后触发管道运行，请参阅：controltower 部署

> **Important**
>
> 为确保正确部署 ASR 解决方案，请参阅 AWS 官方文档，了解有关 CloudFormation 模板概述和参数描述的详细信息。以下信息链接：CloudFormation 模板参数概述指南

ASR 组件的清单如下所示：

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: ShouldDeployWebUI
        parameter_value: "yes"
      - parameter_key: AdminUserEmail
        parameter_value: "<YOUR EMAIL ADDRESS>"
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
```

```
        parameter_value: "no"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
        parameter_value: "yes"
      - parameter_key: LoadPCI321MemberStack
        parameter_value: "no"
      - parameter_key: LoadCIS140MemberStack
        parameter_value: "no"
```

```
    - parameter_key: EnableCloudTrailForASRActionLog
      parameter_value: "no"
    - parameter_key: LogGroupName
      parameter_value: <LOG_GROUP_NAME>
    - parameter_key: LoadCIS300MemberStack
      parameter_value: "no"
  deploy_method: stack_set
  deployment_targets:
   accounts: # :type: list
      - <ACCOUNT_NAME> # and/or
      - <ACCOUNT_NUMBER>
  organizational_units:
    - <ORG UNIT>
  regions: # :type: list
    - <REGION_NAME>
```

2. 代码管道更新

将清单文件添加到 custom-control-tower-configuration .zip 并运行 CodePipeline，请参阅：代码管道概述

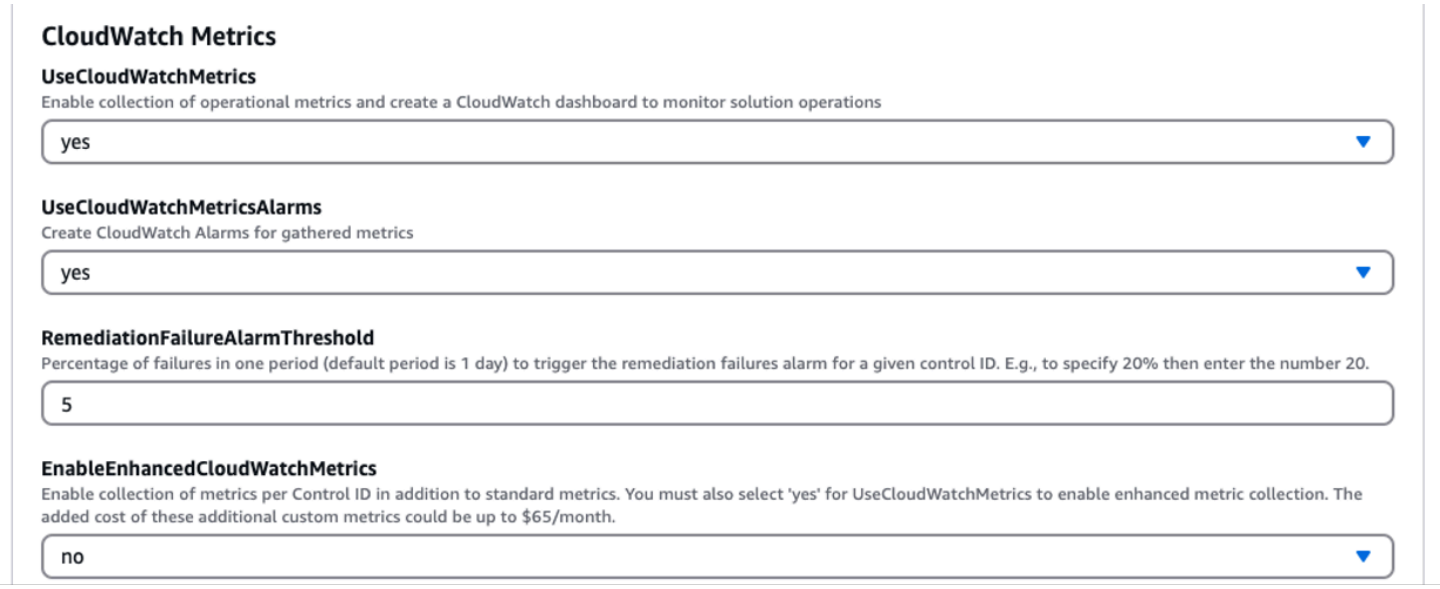
使用 Amazon CloudWatch 控制面板监控解决方案的运营

此解决方案包括在 Amazon CloudWatch 控制面板上显示的自定义指标和警报。

CloudWatch 仪表板和警报监控解决方案的运行情况，并在出现潜在问题时发出警报。

启用 CloudWatch 指标、警报和控制面板

有四个用于 CloudWatch 功能的 CloudFormation 模板参数。



1. UseCloudWatchMetrics-将其设置为yes允许收集运营指标，并创建一个 CloudWatch 仪表板来查看这些指标。
2. UseCloudWatchAlarms-将其设置为yes启用解决方案的默认警报。
3. RemediationFailureAlarmThreshold-在发出警报的一段时间内，补救失败的百分比。
4. EnableEnhancedCloudWatchMetrics-将此参数设置为，yes以收集每个控件 ID 的单个指标。默认情况下，此参数设置为no，因此仅收集所有控件 IDs 中修正总数的指标。每个控件 ID 的单独指标和警报会产生额外费用。

使用 CloudWatch 控制面板

查看控制面板：

1. 导航到 Amazon CloudWatch ，然后导航到控制面板。

2. 选择名为 “ASR 修复指标控制面板” 的仪表板。

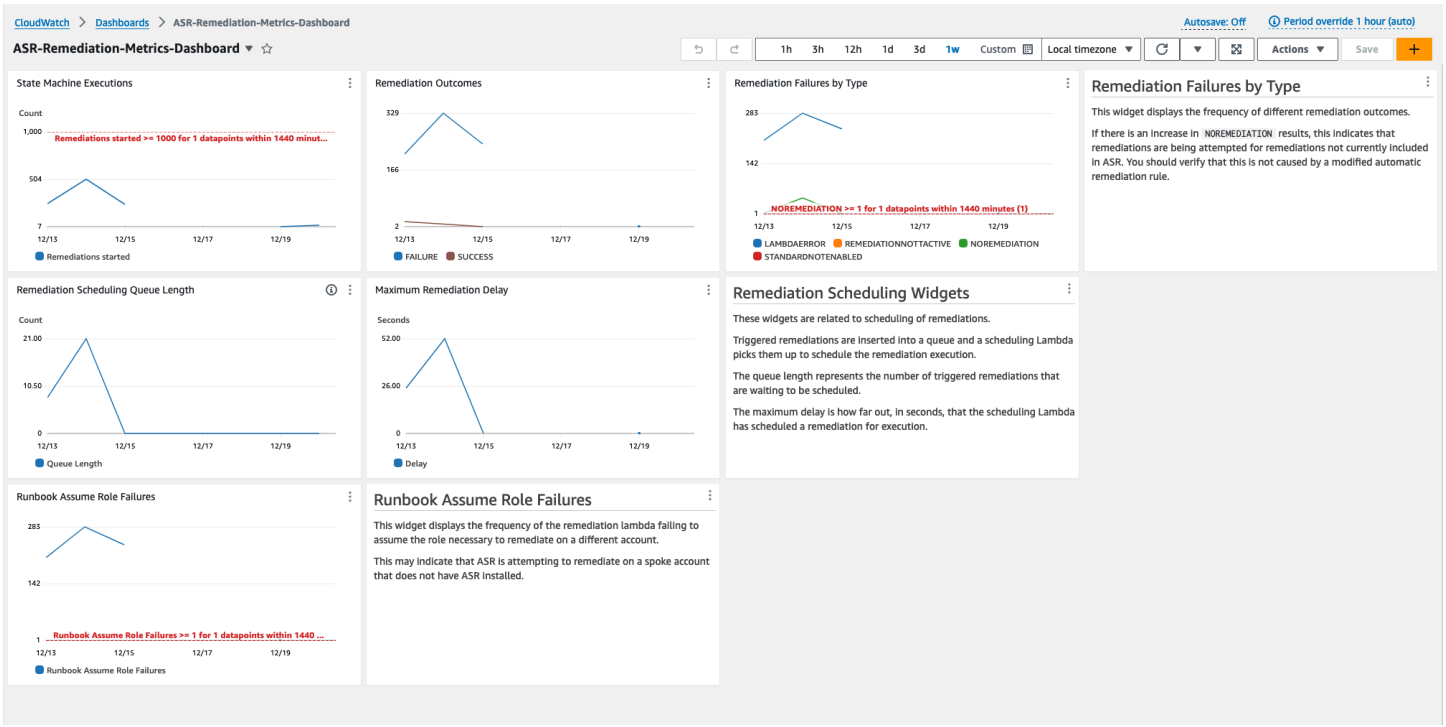
CloudWatch 仪表板包含以下部分：

1. 成功修复总数-让您深入了解该解决方案已成功修复的 Security Hub 发现的数量。
2. 修复失败-显示失败的修复总数和百分比，以及失败原因。大量的故障可能暗示解决方案存在技术问题，您可能需要对其进行更详细的调查。
3. 按控制 ID 列出的修复成功/失败-如果您在部署时启用了增强指标，则本部分按控件 ID 列出修复结果。当 “修复失败” 部分显示的总体故障率较高时，此部分将向您显示故障是分布在多个控制中 IDs，还是只有某些控制 IDs 失败。
4. Runbook 假设角色失败-显示由于在未安装解决方案成员角色的账户中尝试修复而出现的失败次数。由于缺少角色而导致的自动修复尝试反复失败会导致不必要的成本。通过在相关账户中安装成员角色堆栈、禁用解决方案创建的所有 EventBridge 规则或在 Security Hub 中取消关联账户来缓解这种情况。
5. ASR 的 Cloud Trail 管理操作 -列出解决方案在部署时使用日志参数启用操作日志的所有成员账户的 EnableCloudTrailForASRAction管理操作。当您发现任何 AWS 账户出现意外资源变化时，此小组件可以帮助您了解解决方案是否修改了资源。

CloudWatch 仪表板还带有预定义的警报，可提醒常见的操作错误。

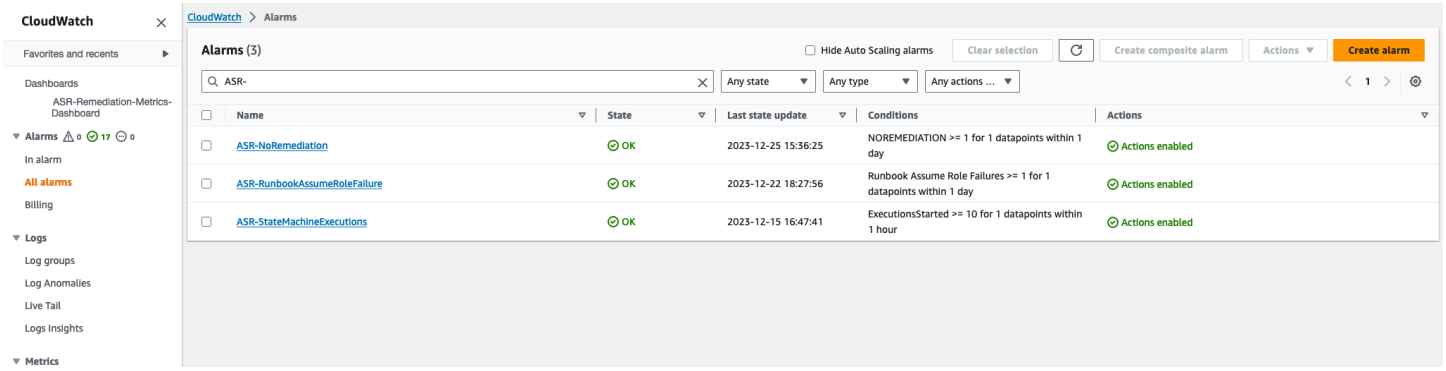
1. 在 24 小时内状态机执行次数 > 1000。
   a. 补救执行的大幅激增可能表明事件规则的启动频率高于预期。
   b. 可以使用 CloudFormation 参数更改阈值。
2. 按类型划分的修复失败 = 不修复 > 0
   a. 正在尝试对未包含在 ASR 中的补救措施进行补救。这可能表示对事件规则进行了修改，使其包含的补救措施超过了预期的补救措施。
3. 运行手册扮演角色失败 > 0
   a. 正在尝试对未正确部署解决方案的账户或区域进行补救。这可能表示已修改事件规则，使其包含的账户数量超出了预期的范围。

可以修改所有警报阈值以适应个人部署需求。

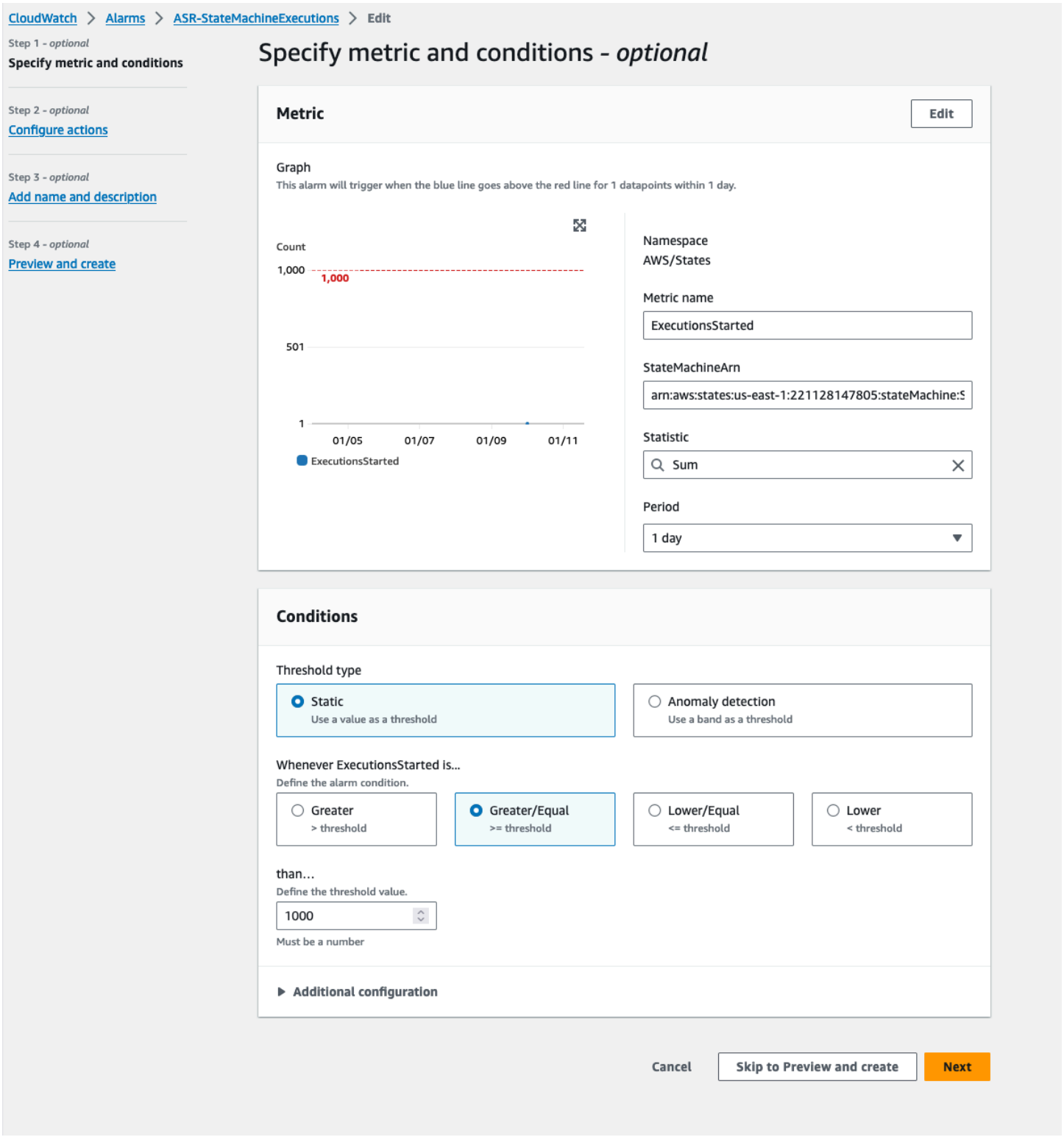


修改警报阈值

1. 导航至 Amazon CloudWatch → 警报 → 所有警报。
2. 选择您要修改的警报，然后选择操作 → 编辑。



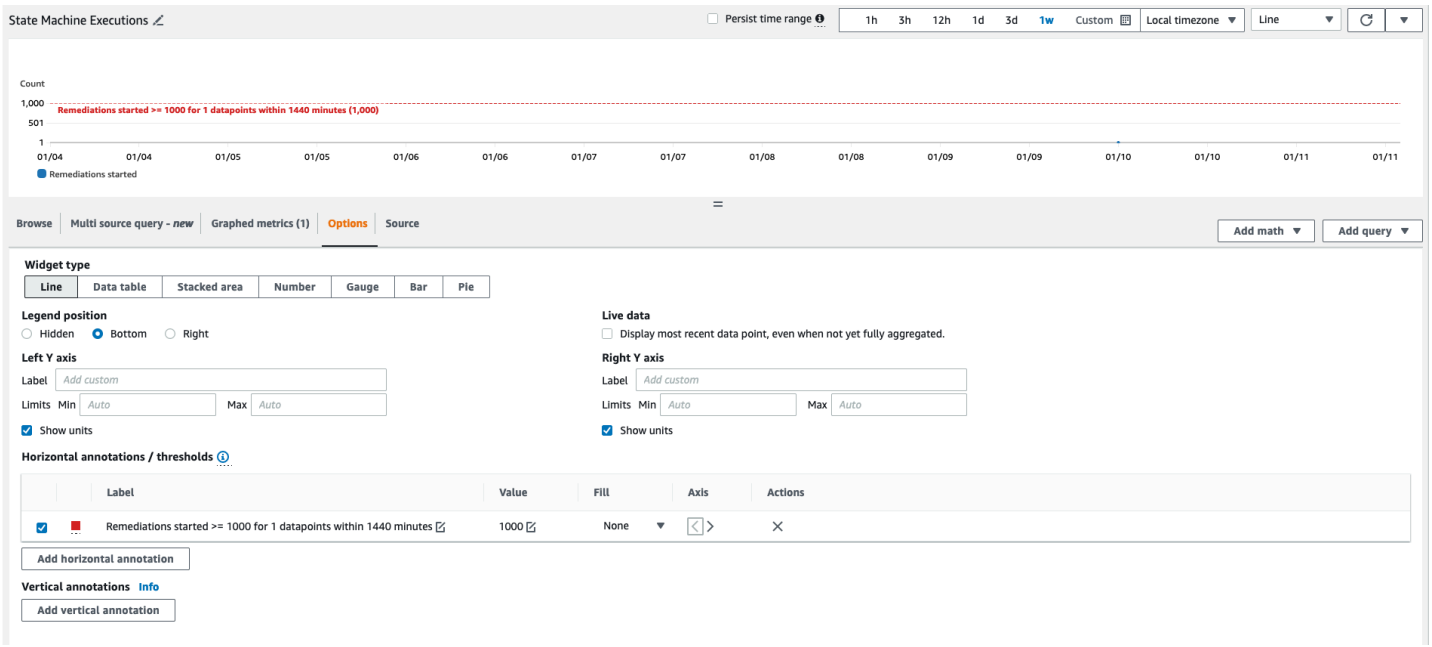
1. 将阈值更改为所需值并保存。



1. 导航到 CloudWatch 仪表板以修改那里的图表以匹配新设置。
   a. 选择相应控件右上角的省略号。
   b. 选择编辑。

c. 切换到 “选项” 选项卡。

d. 修改警报注释以匹配新设置。



订阅警报通知

在管理员账户中，订阅由管理堆栈创建的 Amazon SNS 主题 so0111-asr_alarm_Topic。当警报进入警报状态时，这将通知您。

更新此解决方案

Important

- 更新解决方案时，可能需要在管理员帐户中手动重新启用自动修复规则。请参阅启用全自动修复。
- 如果您使用`Reuse Orchestrator Log Group`参数来保留日志，请确保在堆栈更新期间对其进行适当设置，以避免重新创建日志组或丢失日志保留设置。请参阅部署解决方案。如果您要从较早版本更新到 v2.3.0+ 的堆栈，请选择 “否”

从 v1.4 之前的版本升级

如果您之前部署过 v1.4.x 之前的解决方案，请卸载，然后安装最新版本：

1. 卸载先前部署的解决方案。请参阅卸载解决方案。
2. 启动最新的模板。请参阅部署解决方案。

Note

如果您要从 1.2.1 或更早版本升级到 v1.3.0 或更高版本，请将 “使用现有的 Orchestrator 日志组” 设置为。`No`如果您要重新安装 v1.3.0 或更高版本，则可以选择此选项`Yes`。此选项允许你继续登录到 Orchestrator Step Functions 的同一个日志组。

从 v1.4 及更高版本升级

如果您要从 v1.4.x 升级，请更新所有堆栈或按以下步骤更新： StackSets

1. 使用最新模板更新 Security Hub 管理员帐户中的堆栈。
2. 在每个成员账户中，更新最新模板中的权限。
3. 在当前部署的所有地区的每个成员账户中，使用最新模板更新成员堆栈。

从 v2.0.x 升级

如果您要从 v2.0.x 升级，请升级到 v2.1.2 或更高版本。更新到 v2.1.0-v2.1.1 将失败。CloudFormation

从 v2.1.4 或更早版本升级

如果您要从 v2.1.4 或更早版本升级，则必须先升级到 v2.3.0，然后才能升级到任何高于 v2.3.0 的版本。否则，堆栈更新操作将失败。或者，您可以删除并重新部署解决方案的堆栈，而不必执行堆栈更新。

故障排除

已知问题解决方案提供了缓解已知错误的说明。如果这些说明无法解决您的问题，请联系 AWS Support 提供有关如何为该解决方案提出 AWS Support 案例的说明。

解决方案日志

本节包含此解决方案的故障排除信息，有关主题，请参阅左侧导航。

此解决方案收集在 AWS Systems Manager 下运行的修复运行手册的输出，并将结果记录到 AWS Security Hub 管理员账户的 CloudWatch 日志组`SO0111-ASR`中。每天每个控件只有一个数据流。

Orchestrator Step Functions 将所有步骤转换记录到 AWS Security Hub 管理员账户中的`SO0111-ASR-Orchestrator` CloudWatch 日志组。此日志是一种审计跟踪，用于记录 Step Functions 每个实例的状态转换。每次执行 Step Functions 都有一个日志流。

两个日志组均使用 AWS KMS 客户经理密钥 (CMK) 进行加密。

以下故障排除信息使用`SO0111-ASR`日志组。使用此日志以及 AWS Systems Manager Automation 控制台、自动化执行日志、Step Function 控制台和 Lambda 日志来解决问题。

如果修复失败，则将在日志流`SO0111-ASR`中记录一条类似于以下内容的消息，以了解标准、控制和日期。例如：CIS -2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

以下消息提供了更多详细信息。此输出来自安全标准和控制的 ASR 运行手册。例如：AS R-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

此信息将您指向失败，在本例中为成员帐户中运行的儿童自动化。要解决此问题，您必须使用成员账户（来自上面的消息）登录 AWS 管理控制台，前往 AWS Systems Manager，导航到自动化，然后检查执行 ID 的日志输出`eecdef79-9111-4532-921a-e098549f525`。

已知问题解决方案

- 问题：解决方案部署失败，错误提示资源已在 Amazon 中可用 CloudWatch。

  解决方案：检查 “ CloudFormation 资源/事件” 部分中是否有错误消息，指出日志组已存在。ASR 部署模板允许重复使用现有的日志组。确认您已选择重复使用。

- 问题：解决方案部署失败，在 playbook 嵌套堆栈中出现错误， EventBridge 规则创建失败

  解决方案：随着部署的剧本数量，你可能已经达到了 EventBridge 规则的配额。您可以通过将 Security Hub 中的整合控制结果与本解决方案中的 SC 剧本配对、仅部署所用标准的行动手册或请求增加 EventBridge 规则配额来避免这种情况。

- 问题：我使用同一个账户在多个区域运行 Security Hub。我想在多个区域部署此解决方案。

  解决方案：在与 Security Hub 管理员相同的账户和区域中部署管理堆栈。将成员模板安装到配置了 Security Hub 成员的每个账户和区域。在 Security Hub 中启用聚合。

- 问题：部署后，SO0111-asr-Orchestrator 立即在 “获取自动化文档” 状态下失败，并显示 502 错误：“由于 KMS 访问被拒绝，Lambda 无法解密环境变量。请检查该功能的 KMS 密钥设置。KMS 异常： UnrecognizedClientExceptionKMS 消息：请求中包含的安全令牌无效。（服务：AWSLambda；状态码：502；错误代码： KMSAccessDeniedException；请求编号：... `”

  解决方案：在运行修复之前，让解决方案稳定下来大约 10 分钟。如果问题仍然存在，请提交支持请求或 GitHub 问题。

- 问题：我尝试补救一个发现，但什么也没发生。

  解决方案：查看调查结果的注释，了解未得到补救的原因。一个常见的原因是该发现没有自动补救措施。目前，除了通过备注之外，如果不存在任何补救措施，则无法直接向用户提供反馈。查看解决方案日志。在控制台中打开 “ CloudWatch 日志”。查找 SO0111-ASR CloudWatch 日志组。对列表进行排序，使最近更新的直播排在最前面。选择您尝试运行的结果的日志流。你应该在那里发现任何错误。失败的一些原因可能是：发现控制与补救控制不匹配、跨账户补救（尚不支持），或者发现已得到补救。如果无法确定失败的原因，请收集日志并提交支持请求。

- 问题：开始修复后，Security Hub 控制台中的状态尚未更新。

  解决方案：Security Hub 控制台不会自动更新。刷新当前视图。调查结果的状态应更新。调查结果可能需要几个小时才能从 “失败” 转换为 “通过”。调查结果是根据其他服务（例如 AWS Config）发送到 AWS Security Hub 的事件数据创建的。重新评估规则之前的时间取决于底层服务。如果这不能解决问题，请参考前面的解决方案，“`我试图纠正发现但什么也没发生。 `”

- 问题：Orchestrator 步骤函数在 “获取自动化文档状态” 中失败：调用操作时出现错误 (AccessDenied)。 AssumeRole

  解决方案：成员模板尚未安装在 ASR 正在尝试修正发现的成员账户中。按照成员模板的部署说明进行操作。

- 问题：Config.1 运行手册失败，因为录制器或交付渠道已经存在。

  解决方案：仔细检查您的 AWS Config 设置，确保配置设置正确。在某些情况下，自动修复无法修复现有的 AWS Config 设置。

- 问题：修复成功但返回消息 `"No output available yet because the step is not successfully executed."`

  解决方案：这是此版本中的一个已知问题，其中某些补救运行手册不返回响应。如果修复运行手册不起作用，则会正确失败并发出解决方案信号。

- 问题：解析失败并发送了堆栈跟踪。

  解决方案：有时，我们会错过处理导致堆栈跟踪而不是错误消息的错误情况的机会。尝试从跟踪数据中解决问题。如果您需要帮助，请提交支持请求。

- 问题：在自定义操作资源上移除 v1.3.0 堆栈失败。

  解决方案：移除自定义操作后，移除管理模板可能会失败。这是一个已知问题，将在下一个版本中修复。如果发生这种情况：

  a. 登录 AWS Security Hub 管理控制台。

  b. 在管理员帐户中，前往 “设置”。

  c. 选择 “自定义操作” 选项卡

  d. 手动删除条目 “使用 ASR 修复”。

  e. 再次删除堆栈。

- 问题：重新部署管理堆栈后，步骤功能失败。`AssumeRole`

  解决方案：重新部署管理员堆栈会破坏管理员账户中的管理员角色和成员账户中的成员角色之间的信任联系。您必须在所有成员账户中重新部署成员角色堆栈。

- 问题：超过 24 小时PASSED后未显示 CIS 3.x 补救措施。

  解决方案：如果您在成员账户中没有订阅 `SO0111-ASR_LocalAlarmNotification` SNS 主题，这种情况很常见。

特定补救措施存在问题

设置SSLBucket策略失败并 AccessDenied 出现错误

相关控件：AWS FSBP v1.0.0 S3.5、PCI v3.2.1 PCI.S3.5、CIS v1.4.0 2.1.2、SC v2.0.0 S3.5

问题：“设置SSLBucket策略” 失败并 AccessDenied 出现错误：

调用 PutBucketPolicy 操作时出错 (AccessDenied)：访问被拒绝

如果已为存储桶启用了阻止公共访问设置，则尝试放置包含允许公开访问的语句的存储桶策略将失败，并显示此错误。通过放置包含此类语句的存储桶策略，然后为该存储桶启用公共访问屏蔽，即可达到此状态。

补救措施 ConfigureS3BucketPublicAccessBlock （相关控件：AWS FSBP v1.0.0 S3.2、PCI v3.2.1 PCI.S3.2、CIS v1.4.0 2.1.5.2、SC v2.0.0 S3.2）也可以将存储桶置于此状态，因为它在不更改存储桶策略的情况下设置了公共访问封锁设置。

Set SSLBucket Policy 在存储桶策略中添加了一条声明，用于拒绝不使用 SSL 的请求。它不会修改策略中的其他语句，因此，如果存在允许公开访问的声明，则尝试放置仍包含这些语句的修改后的存储桶策略时，补救措施将失败。

解决方案：修改存储桶策略以删除允许公开访问的声明，这些声明与存储桶上的阻止公共访问设置相冲突。

Puts3 失败BucketPolicyDeny 了

相关控件：AWS FSBP v1.0.0 S3.6、(1)、 NIST.800-53.r5 CA-9 nist.800-53.r5 CM-2

问题：PutS3 BucketPolicyDeny 出现以下错误：

```
Unable to create an explicit deny statement for {bucket_name}.
```

如果目标存储桶上所有策略的委托人均为 “*”，则该解决方案无法将拒绝策略添加到目标存储桶，因为它会阻止所有委托人执行的所有存储桶操作。

解决方案：修改存储桶策略以允许对特定账户执行操作，而不是使用 “*” 委托人并限制被拒绝的操作。

如何禁用该解决方案

在发生事件时，您可能会发现需要在不移除任何基础架构的情况下禁用该解决方案。这些场景详细说明了如何在解决方案中禁用不同的组件。

场景 1：禁用单个控件的自动修复。

1. 在 AWS CloudFormation 控制台 EventBridge 中导航至。
2. 在侧栏中选择 “规则”。
3. 选择默认事件总线并搜索要禁用的控件。
4. 在规则上选择，然后选择 “禁用” 按钮。

场景 2：禁用所有控件的自动修复。

1. 在控制台 EventBridge 中导航至。
2. 在侧栏中选择 “规则”。
3. 选择 “默认” 事件总线，然后选择以下所有规则。
4. 在 “禁用” 按钮上选择。请注意，对于多页规则，您可能需要这样做。

场景 3：禁用账户的手动修复

1. 在控制台 EventBridge 中导航至。
2. 在侧栏中选择 “规则”。
3. 选择 “默认” 事件总线并搜索 “remediate_with_asr_CustomAction”
4. 在规则上选择，然后选择 “禁用” 按钮。

请联系 Support。

如果您有 AWS 开发者支持、AWS 商业支持或 AWS 企业支持，则可以使用支持中心获取有关此解决方案的专家帮助。以下部分提供了说明。

创建案例

1. 登录 Su pport Center。
2. 选择创建案例。

我们能帮上什么忙？

1. 选择 “技术”。

2. 对于 “服务”，选择 “解决方案”。
3. 在 “类别” 中，选择 “其他解决方案”。
4. 在 “严重性” 中，选择与您的用例最匹配的选项。
5. 当您输入 “服务”、“类别” 和 “严重性” 时，界面会填充常见疑难解答问题的链接。如果您无法通过这些链接解决问题，请选择下一步：其他信息。

其他信息

1. 在 “主题” 中，输入总结您的问题或问题的文本。
2. 在描述中，详细描述问题。
3. 选择 “附加文件”。
4. 附上 Support 处理请求所需的信息。

帮助我们更快地解决您的问题

1. 输入所需的信息。
2. 选择下一步：立即解决或联系我们。

立即解决或联系我们

1. 查看 “立即解决” 解决方案。
2. 如果您无法使用这些解决方案解决问题，请选择 “联系我们”，输入所需信息，然后选择 “提交”。

卸载此解决方案

使用以下步骤通过 AWS 管理控制台卸载解决方案。

V1.0.0-V1.2.1

对于 v1.0.0 到 v1.2.1 的版本，请使用 Service Catalog 卸载 CIS FSBP Playbook。 and/or 在 v1.3.0 中，不再使用 Service Catalog。

1. 登录 AWS CloudFormation 控制台并导航到 Security Hub 主账户。
2. 选择 S ervice Catalog 以终止所有已配置的 playbook，移除任何安全组、角色或用户。
3. 从 Security Hub 成员账户中移除分支`CISPermissions.template`模板。
4. 从 Security Hub 管理员和成员账户中移除分支`AFSBPMemberStack.template`模板。
5. 导航到 Security Hub 主帐户，选择解决方案的安装堆栈，然后选择删除。

> **Note**
>
> CloudWatch 保留日志组日志。我们建议根据贵组织的日志保留政策的要求保留这些日志。

v1.3.x

1. `automated-security-response-member.template`从每个成员账户中删除。
2. `automated-security-response-admin.template`从管理员帐户中删除。

> **Note**
>
> 移除自定义操作后，在 v1.3.0 中移除管理模板可能会失败。这是一个已知问题，将在下一个版本中修复。按照以下说明修复此问题：
>
> 1. 登录 AWS Security Hub 管理控制台。
> 2. 在管理员帐户中，前往 “设置”。
> 3. 选择自定义操作选项卡。
> 4. 手动删除条目 “使用 ASR 修复”。
> 5. 再次删除堆栈。

V1.4.0 及更高版本

堆栈部署

1. automated-security-response-member.template从每个成员账户中删除。
2. automated-security-response-admin.template从管理员帐户中删除。

StackSet 部署

对于每个堆栈 StackSet，请移除堆栈，然后按与 StackSet 部署顺序相反的顺序移除。

请注意，即使删除了模板automated-security-response-member-roles.template，也会保留中的 IAM 角色。这样，使用这些角色的补救措施就可以继续发挥作用。在验证这些 SO0111-* 角色已不再使用后，可以通过主动补救措施（例如 CloudWatch 日志记录或 RDS 增强监控） CloudTrail 将其手动删除。

管理员指南

启用和禁用解决方案的某些部分

作为解决方案管理员，您可以通过以下方式控制启用解决方案的哪些功能。

成员和成员角色堆栈的部署位置：

- 管理员堆栈只能在已部署成员和成员角色堆栈且以管理员账号作为参数值的账户中启动修复（通过自定义操作或全自动 EventBridge 规则）。
- 要完全免除账户或区域对解决方案的控制，请勿将成员或成员角色堆栈部署到这些账户或区域。

在 Security Hub 中查找聚合配置的账户和区域：

- 管理员堆栈只能针对到达管理员账户和区域的调查结果启动补救（通过自定义操作或全自动 EventBridge 规则）。
- 要完全免除账户或区域对解决方案的控制，请不要将这些账户或区域包括在内，以便将调查结果发送到部署管理堆栈的同一个管理员账户和区域。

部署了哪些标准嵌套堆栈：

- 管理员堆栈只能针对在目标成员账户和区域中部署了控制运行手册的控件启动修复（通过自定义操作或全自动 EventBridge 规则）。它们由每个标准的成员堆栈部署。
- 管理员堆栈只能使用控件规则启动全自动修复，这些 EventBridge 规则由管理员堆栈针对该标准部署的规则。它们已部署到管理员帐户。
- 为简单起见，我们建议您在管理员和成员账户中统一部署标准。如果您关心 AWS FSBP 和 CIS v1.2.0，请将这两个嵌套的管理堆栈部署到管理员账户，然后将这两个嵌套的成员堆栈部署到每个成员账户和区域。

在每个嵌套成员堆栈中部署了哪些控制运行手册：

- 管理员堆栈只能针对在目标成员账户中部署控制运行手册的控件启动修复（通过自定义操作或全自动 EventBridge 规则），并按每个标准的成员堆栈按成员堆栈部署了控制运行手册。
- 为了更精细地控制为特定标准启用了哪些控件，标准的每个嵌套堆栈都有部署控制运行手册的参数。将控件的参数设置为 “不可用” 值以取消部署该控件运行手册。

用于启用和禁用标准的 SSM 参数：

- 对于通过标准管理堆栈部署的 SSM Parameter 启用的标准，管理员堆栈只能启动修复（通过自定义操作或全自动 EventBridge 规则）。
- <standard_name><standard_version>要禁用标准，请将路径 “/solutions/so0111/ /status” 的 SSM 参数值设置为 “否”。

访问解决方案的 Web 用户界面：

- 部署管理堆栈后，您将收到一封电子邮件，其中包含使用您在部署期间提供的电子邮件地址登录 Web UI 的临时证书。
- 使用 “邀请用户” 页面，管理员和授权管理员可以邀请其他用户访问 Web UI 并委托对解决方案的访问权限。
- 使用 “查看用户” 页面，管理员和授权管理员可以查看和管理现有用户。
- 要详细了解权限以及如何使用解决方案的 Web UI，请参阅 Web UI 开发者指南。

SNS 通知示例

何时启动修复

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

补救成功时


```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```


当补救失败时


```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

教程

本教程将指导您完成首次部署 ASR。它将从部署解决方案的先决条件开始，最后是你修复成员账户中的示例发现。

教程：AWS 上的自动安全响应入门

本教程将指导您完成首次部署。它将从部署解决方案的先决条件开始，最后是你修复成员账户中的示例发现。

准备账目

为了演示该解决方案的跨账户和跨区域修复功能，本教程将使用两个账户。您也可以将解决方案部署到单个帐户。

以下示例使用账户111111111111和222222222222来演示解决方案。 111111111111将是管理员帐户，也222222222222将是成员帐户。我们将制定解决方案，以修复各地区us-east-1和us-west-2地区的资源调查结果。

下表举例说明了我们将针对每个账户和地区的每个步骤采取的行动。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	无	无
222222222222	成员	无	无

管理员帐户是执行解决方案管理操作的帐户，即手动启动补救或使用 EventBridge 规则启用全自动修复。此账户还必须是您想要修复发现的所有账户的 Security Hub 委托管理员账户，但它不必是，也不应是您的账户所属的 AWS 组织的 AWS Organizations 管理员账户。

启用 AWS Config

请查看以下文档：

- AWS Config 文档
- AWS Config 定价
- 启用 AWS Config

在两个账户和两个区域中启用 AWS Config。这将产生费用。

> **Important**
>
> 确保选择 “包括全球资源（例如 AWS IAM 资源）” 选项。如果您在启用 AWS Config 时未选择此选项，则不会看到与全球资源（例如 AWS IAM 资源）相关的调查结果

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启用 AWS Config	启用 AWS Config
222222222222	成员	启用 AWS Config	启用 AWS Config

启用 AWS 安全中心

请查看以下文档：

- AWS Security Hub 文档
- AWS Security Hub 定价
- 启用 AWS Security Hub

在两个账户和两个区域中启用 AWS Security Hub。这将产生费用。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启用 AWS Security Hub	启用 AWS Security Hub
222222222222	成员	启用 AWS Security Hub	启用 AWS Security Hub

启用整合的控制结果

请查看以下文档：

- 生成和更新控制结果

在本教程中，我们将演示在启用 AWS Security Hub 的合并控制结果功能（这是推荐的配置）的情况下如何使用该解决方案。在截至撰写本文时还不支持此功能的分区中，您需要部署特定于标准的剧本，而不是 SC（安全控制）。

在两个账户和两个区域中启用合并控制结果。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启用整合的控制结果	启用整合的控制结果
222222222222	成员	启用整合的控制结果	启用整合的控制结果

使用新功能可能需要一些时间才能生成调查结果。您可以继续本教程，但是如果没有新功能，您将无法修复生成的发现。使用新要素生成的结果可以通过`GeneratorId`字段值来识别`security-control/<control_id>`。

配置跨区域查找结果聚合

请查看以下文档：

- 跨区域聚合
- 启用跨区域聚合

在两个账户中配置从 us-west-2 到 us-east-1 的查找聚合。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	从 us-west-2 配置聚合	无
222222222222	成员	从 us-west-2 配置聚合	无

调查结果可能需要一些时间才能传播到聚合区域。您可以继续本教程，但是在其他区域的发现结果开始出现在聚合区域中之前，您将无法对其进行修复。

指定 Security Hub 管理员帐户

请查看以下文档：

- 在 AWS Security Hub 中管理账户
- 管理组织成员账户
- 通过邀请管理成员账户

在接下来的示例中，我们将使用手动邀请方法。对于一组生产账户，我们建议通过 AWS Organizations 管理 Security Hub 的委托管理。

在 AWS Security Hub 控制台的管理员账户 (111111111111) 中，邀请成员账户 (222222222222) 以 Security Hub 授权管理员的身份接受管理员账户。从成员账户接受邀请。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	邀请成员账号	无
222222222222	成员	接受邀请	无

调查结果可能需要一些时间才能传播到管理员帐户。您可以继续本教程，但是在成员帐户中发现的结果开始出现在管理员帐户中之前，您将无法对其进行修复。

为自行管理 StackSets 的权限创建角色

请查看以下文档：

- AWS CloudFormation StackSets
- 授予自我管理权限

我们将向多个账户部署 CloudFormation 堆栈，因此我们将使用 StackSets。我们无法使用服务管理权限，因为管理堆栈和成员堆栈都有嵌套堆栈，服务不支持这些堆栈，因此我们必须使用自我管理的权限。

部署堆栈以获得基本的 StackSet 操作权限。对于生产账户，您可能希望根据 “高级权限选项” 文档缩小权限范围。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	部署 StackSet 管理员角色堆栈 部署 StackSet 执行角色堆栈	无
222222222222	成员	部署 StackSet 执行角色堆栈	无

创建将生成示例结果的不安全资源

请查看以下文档：

- Security Hub 控件参考
- AWS Lambda 控件

以下示例资源配置不安全，用于演示补救措施。示例控件是 Lambda.1：Lambda 函数策略应禁止公开访问。

> **Important**
>
> 我们将故意创建配置不安全的资源。请查看控制的性质，并评估在您的环境中为自己创建此类资源的风险。请注意您的组织可能拥有的任何用于检测和报告此类资源的工具，并在适当时申请例外。如果我们选择的示例控件不适合您，请选择该解决方案支持的另一个控件。

在成员账户的第二个区域中，导航到 AWS Lambda 控制台并在最新的 Python 运行时中创建函数。在“配置”→“权限”下，添加一条策略声明，允许在不进行身份验证的情况下从 URL 调用该函数。

在控制台页面确认该功能允许公共访问。解决方案修复此问题后，比较权限以确认公共访问权限已被撤销。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	无	无

Account	用途	us-east-1 中的行动	us-west-2 中的行动
222222222222	成员	无	使用不安全的配置创建 Lambda 函数

AWS Config 可能需要一些时间才能检测到不安全的配置。您可以继续本教程，但在 Config 检测到发现之前，您将无法对其进行补救。

为相关控件创建 CloudWatch 日志组

请查看以下文档：

- 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件
- CloudTrail 控件

该解决方案支持的各种 CloudTrail 控件要求有一个作为多区域 CloudTrail目标的 CloudWatch 日志组。在以下示例中，我们将创建一个占位符日志组。对于生产帐户，您应该正确配置与 CloudWatch 日志的 CloudTrail 集成。

在每个账户和区域中创建一个同名的日志组，例如：`asr-log-group`。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	创建日志组	创建日志组
222222222222	成员	创建日志组	创建日志组

将解决方案部署到教程账户

收集管理员、成员和成员角色堆栈 URLs 的三个 Amazon S3。

部署管理堆栈

View template

automa

security-response-admin。模板

在管理员帐户中，导航到 CloudFormation 控制台并将管理堆栈部署到 Security Hub 查找聚合区域。

选择No用于加载嵌套管理堆栈的所有参数的值，“SC” 或 “安全控制” 堆栈除外。此堆栈包含我们在账户中配置的合并控制结果的资源。

除非您No之前已在此账户和区域中部署过此解决方案，否则请选择重复使用 Orchestrator 日志组。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	部署管理堆栈	无
222222222222	成员	无	无

等到管理员堆栈完成部署后再继续，这样就可以创建从成员账户到管理员账户的信任关系。

部署成员堆栈

automa
security-response-member。模板

在管理员帐户中，导航到 CloudFormation StackSets 控制台并将成员堆栈部署到每个账户和区域。使用在本教程中创建的 StackSets 管理员和执行角色。

输入您创建的日志组的名称作为日志组名称的参数值。

选择No用于加载嵌套成员堆栈的所有参数的值，“SC” 或 “安全控制” 堆栈除外。此堆栈包含我们在账户中配置的合并控制结果的资源。

输入管理员帐户的 ID 作为管理员账号参数的值。在我们的示例中，这是111111111111。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	部署成员 StackSet /确认成员堆栈已部署	确认成员堆栈已部署
222222222222	成员	确认成员堆栈已部署	确认成员堆栈已部署

部署成员角色堆栈

automated-security-response-member-roles.template 模板按钮-roles.temp automated-security-response-member

在管理员帐户中，导航到 CloudFormation StackSets 控制台并将成员堆栈部署到每个账户。使用在本教程中创建的 StackSets 管理员和执行角色。输入管理员帐户的 ID 作为管理员账号参数的值。在我们的示例中，这是111111111111。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	部署成员 StackSet /确认成员堆栈已部署	无
222222222222	成员	确认成员堆栈已部署	无

您可以继续，但在 CloudFormation StackSets 完成部署之前，您将无法修复发现的结果。

订阅 SNS 主题

补救更新

话题-{https---us-east-1-console-aws-amazon-com-sns-v3-- home-region-us-east 1 —-topic-arn-aws-sns us-east-1-221128147805-so0111-asr-Topic} [so0111-asr_Topic] [so0111-asr_Topic]

在管理员账户中，订阅由管理堆栈创建的 Amazon SNS 主题。这将在启动修复以及修正成功或失败时通知您。

警报

话题-{https---us-east-1-console-aws-amazon-com-sns-v3-- home-region-us-east 1 —-topic-arn-aws-sns us-east-1-221128147805-so0111-asr-alarm-Topic} [so0111-asr_alarm_Topic]

在管理员账户中，订阅由管理堆栈创建的 Amazon SNS 主题。这将在指标警报启动时通知您。

修复示例发现

> **Important**
>
> 此示例需要使用 Security Hub CSPM 控制台。Security Hub（非 cSPM）控制台目前不支持通过自定义操作进行手动修复。要在不使用 Security Hub CSPM 控制台的情况下修复发现的问题，请参阅使用 Web 用户界面修复部分。

在管理员帐户中，导航到 Security Hub CSPM 控制台，找到您在本教程中创建的配置不安全的资源。

这可以通过几种方式来实现：

1. 在支持合并控制结果功能的分区中，标有 “控件” 的页面允许您通过合并的控件 ID 来查找查找结果。
2. 在 “安全标准” 页面中，您可以根据控件所属的标准找到该控件。
3. 您可以在 “调查结果” 页面上查看所有发现结果并按属性进行搜索。

我们创建的公共 Lambda 函数的统一控制 ID 是 Lambda.1。

启动修复

选中与我们创建的资源相关的查找结果左侧的复选框。在 “操作” 下拉菜单中，选择 “使用 ASR 修复”。您将看到一条通知，告知调查结果已发送至 Amazon EventBridge。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启动修复	无
222222222222	成员	无	无

确认补救措施解决了调查结果

您应该会收到两个 SNS 通知。第一个将表示已启动补救，第二个将表示补救成功。收到第二条通知后，导航到成员账户中的 Lambda 控制台并确认已撤销公开访问权限。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	无	无
222222222222	成员	无	确认修复成功

使用 Web 用户界面进行修复

或者，您可以使用解决方案的 Web 用户界面来修复 AWS Security Hub 的发现并查看过去的补救措施。

> **Note**
>
> 部署管理堆栈时，必须将`ShouldDeployWebUI`参数设置为 “是”，才能使用解决方案的 Web UI。

登录 Web 用户界面

部署解决方案后，您将收到一封电子邮件，其中包含临时凭证和来自 no-reply@verificationemail.com 的解决方案 Web UI 链接。这将发送到您在部署管理堆栈时提供的电子邮件地址。

找到电子邮件，复制临时凭证，然后单击 Web UI 链接。此链接将直接带您进入登录页面，您将在其中输入临时凭证并设置新密码。

找到 Lambda.1 的调查结果

登录后，您将看到 “调查结果” 页面。此页面显示您的 Security Hub 管理员账户中所有支持补救的 Security Hub 发现，包括已登录 AWS Security Hub 的成员账户的调查结果。

在调查结果页面上，使用搜索栏筛选资源 ID，方法是输入您在本教程中创建的 Lambda 函数的 ARN，然后使用 “=” 运算符执行搜索。这将显示您创建的 Lambda 函数的解决方案所支持的所有 AWS Security Hub 调查结果。

要查找本教程中生成的`Lambda.1`查找结果，请在 “查找类型” 上应用另一个过滤器。单击搜索栏，选择 “查找类型”，然后选择 “=” 运算符。如果您的环境中启用了整合控制结果，请输入`security-control/Lambda.1`。否则，请选择支持 Lambda.1 控件的安全标准并输入生成器 ID；例如。`aws-foundational-security-best-practices/v/1.0.0/Lambda.1`

应用资源 ID 和查找结果类型筛选条件后，您只能看到 AWS Security Hub 为表中列出的测试资源生成的 Lambda.1 调查结果。

> **Note**
>
> AWS Security Hub 可能需要一些时间才能为您创建的资源生成 Lambda.1 调查结果。如果在应用两个筛选器后都看不到搜索结果，请等待 5-10 分钟，然后再次搜索搜索结果。

启动修复

选择您在上一步中找到的结果，然后单击 “操作” > “修复”。这将开始对您选择的发现进行修正。

您可以在 “执行历史记录” 页面上查看此修复的进度。等待几分钟后，单击右上角的刷新图标刷新 “执行历史记录” 页面，您应该会看到状态已从变`In progress`为`Success`。

确认补救措施解决了调查结果

当 AWS Securit `Resolved` y Hub 将发现标记为时，它将自动从 Web 用户界面的调查结果页面中删除。

要验证补救措施是否解决了调查结果，请导航到成员账户中的 Lambda 控制台并确认已撤销公开访问权限。

> **Note**
>
> 即使修正状态为，某些发现仍可能显示在 “调查结果” 页面上`Success`。这是因为资源更新后，AWS Security Hub 最多需要 24 小时才能将发现标记为已解决。通过选择查找结果并单击 “操作” > “隐藏”，可以隐藏您不想在 “查找结果” 页面上看到的查找结果。

追踪补救措施的执行情况

为了更好地了解解决方案的工作原理，您可以跟踪修复的执行情况。

EventBridge 规则

在管理员帐户中，找到名为 rem ediat CustomAction e_with EventBridge _asr_ 的规则。此规则与你从 Security Hub 发送的调查结果相匹配，并将其发送到 Orchestrator Step Functions。

Step Functions 执行

在管理员账户中，找到名为 “so0111-asr-Orchestrato r” 的 AWS Step Functions。此步骤函数调用目标账户和区域中的 SSM 自动化文档。您可以在此 AWS Step Functions 的执行历史中追踪补救措施的执行情况。

SSM 自动化

在成员帐户中，导航到 SSM 自动化控制台。你会发现一个名为 “asr-sc_2.0.0_Lambda.1” 的文档被执行了两次，一个名为 “ASR-” 的文档被执行了一次。RemoveLambdaPublicAccess

第一次执行来自目标账户中的 Orchestrator 步骤函数。第二次执行发生在目标区域，该区域可能不是发现的起源区域。最后一次执行是撤销 Lambda 函数的公共访问策略的补救措施。

CloudWatch 日志组

在管理员帐户中，导航到 CloudWatch 日志控制台并找到名为 “SO0111-ASR” 的日志组。此日志组是 Orchestrator Step Functions 中高级日志的目标。

启用全自动补救

该解决方案的另一种操作模式是在发现结果送达 Security Hub 时自动对其进行修复。

> **Important**
>
> 在启用全自动修复之前，请确保在您符合解决方案进行自动更改的账户和区域配置解决方案。如果您想缩小解决方案自动修复的范围，请参阅以下有关筛选全自动修复的部分。

示例：为 Lambda.1 启用全自动补救措施

启用自动修复将启动对与您启用的控件相匹配的所有资源的补救措施 (Lambda.1)。

> **Important**
>
> 确认您希望撤销解决方案范围内的所有公共 Lambda 函数的此权限。全自动修复的范围将不限于您创建的函数。如果在安装该控制的任何账户和区域中检测到此控件，则该解决方案将对其进行修复。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	确认没有需要的公共函数	确认没有需要的公共函数
222222222222	成员	确认没有需要的公共函数	确认没有需要的公共函数

找到修复配置 DynamoDB 表

在管理员帐户中，在Outputs CloudFormation 控制台中查看管理员堆栈的。您将看到标题为的输出RemediationConfigurationDynamoDBTable。

这是修复配置 DynamoDB 表的名称，该表控制解决方案的自动修复配置。复制此输出的值，然后在 DynamoDB 控制台中找到相应的 DynamoDB 表。

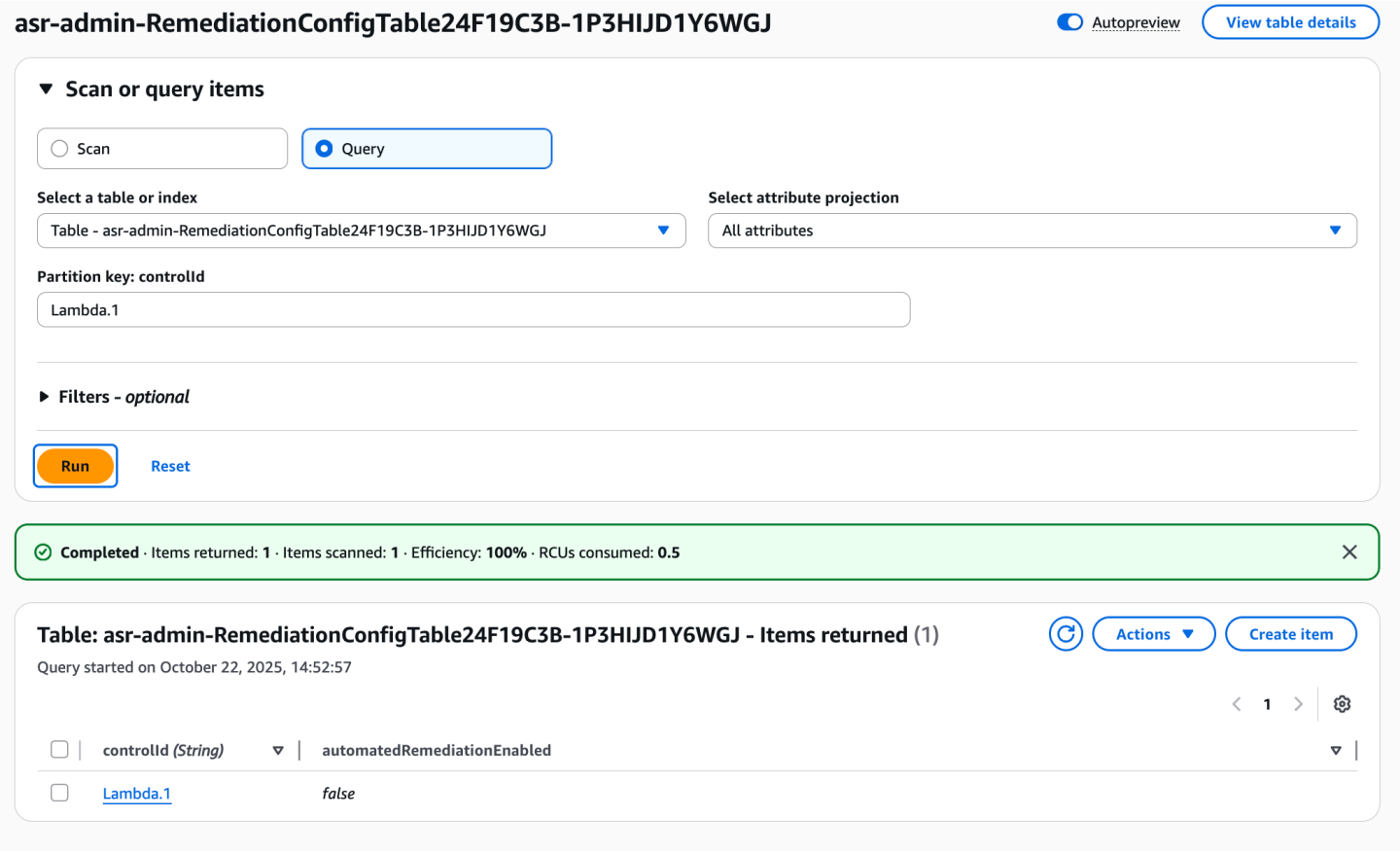
Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	找到 “修复配置 DynamoDB” 表。	无
222222222222	成员	无	无

修改修正配置表

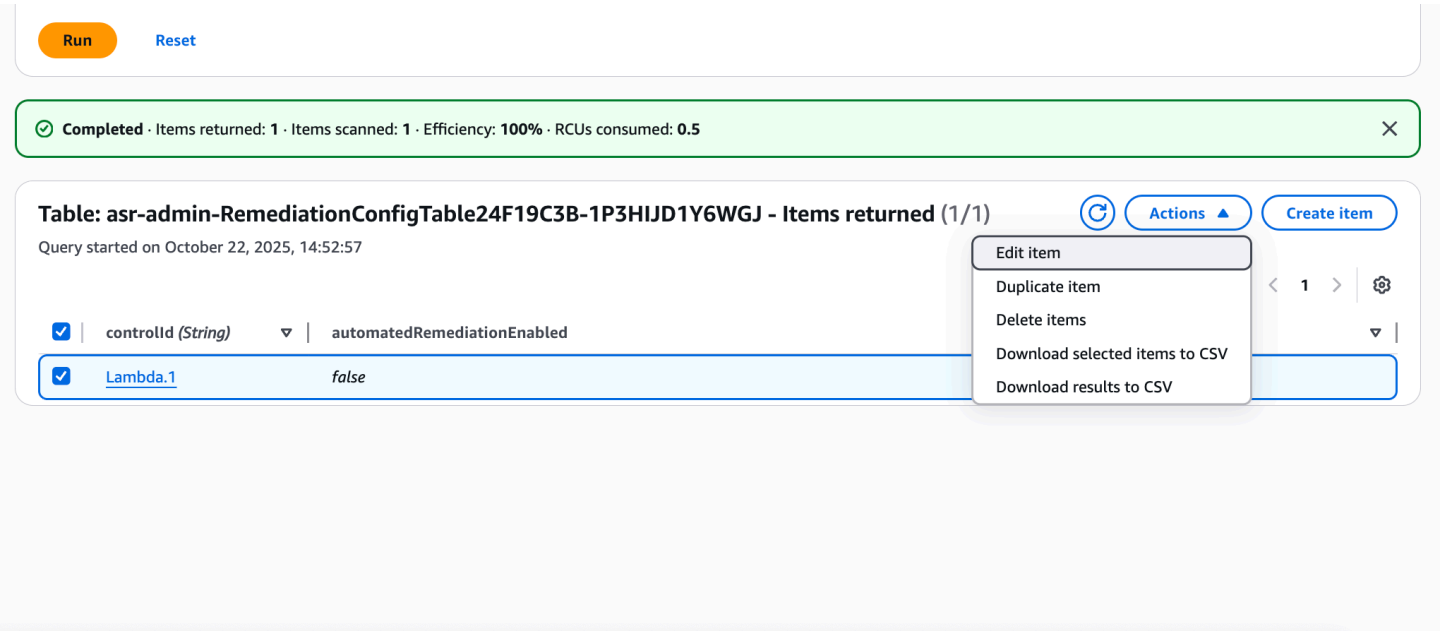
在您找到 “修复配置” 表的 DynamoDB 控制台中，选择 “浏览表项目”。

表中的每一项都对应于解决方案支持的 Security Hub 控件。每个项目都有一个automatedRemediationEnabled属性，可以对其进行修改以启用对关联控件的全自动修正。

要启用 Lambda.1，请在扫描或查询项目下选择查询。在 “分区键：controlID” 下输入Lambda.1并单击 “运行”。您将看到返回的与 Lambda.1 控件相对应的单个项目。



现在，选择该Lambda.1项目，然后单击 “操作” > “编辑项目”。



最后，将automatedRemediationEnabled属性值更改为 True。单击 “保存并关闭”。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	修改修复配置 DynamoDB 表。	无
222222222222	成员	无	无

配置资源

在成员账户中，重新配置 Lambda 函数以允许公开访问。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	无	无
222222222222	成员	无	将 Lambda 函数配置为允许公开访问

确认补救措施解决了调查结果

Config 可能需要一些时间才能再次检测到不安全的配置。您应该会收到两个 SNS 通知。第一个将表示补救措施已启动。第二个将表示修复成功。收到第二条通知后，导航到成员账户中的 Lambda 控制台并确认已撤销公开访问权限。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	无	无
222222222222	成员	无	确认修复成功

（可选）为全自动修复配置筛选

如果您想限制解决方案运行修正的范围，则可以应用筛选器。这些筛选器仅适用于全自动修复，不会影响手动调用的修正。

该解决方案提供以下维度的筛选：

1. 账户编号
2. 组织单位 (OUs)
3. 资源标签

每个维度都可以通过修改解决方案部署的与给定维度相对应的 Systems Manager 参数来配置。Parameter Store 中的所有筛选参数都可以在/ASR/Filters/路径下的管理员帐户中找到。

每个维度都有两个配置参数，一个用于筛选值，另一个用于过滤器模式。例如，“账户 ID” 维度有两个名为/ASR/Filters/AccountFilters和的参数/ASR/Filters/AccountFilterMode。必须对两者进行修改才能配置对账户 ID 的筛选。

例如，要将全自动修正限制为仅在账户111111111111和中运行222222222222，可以将的值更改为 “111111111111、2222 /ASR/Filters/AccountFilters 22222222”。然后，将的值更改/ASR/Filters/AccountFilterMode为 “包含”。然后，该解决方案将忽略为除111111111111或2222222222之外的账户生成的任何调查结果。

每个过滤器参数都采用以逗号分隔的值列表进行筛选，并且每个 “模式” 参数可以设置为 “包含”、“排除” 或 “禁用”。

清理

删除示例资源

在成员账户中，删除您创建的示例 Lambda 函数。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	无	无
222222222222	成员	无	删除示例 Lambda 函数

删除管理堆栈

在管理员帐户中，删除管理员堆栈。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	删除管理堆栈	无
222222222222	成员	无	无

删除成员堆栈

在管理员帐户中，删除该成员 StackSet。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	删除成员 StackSet 确认成员堆栈已删除	确认成员堆栈已删除
222222222222	成员	确认成员堆栈已删除	确认成员堆栈已删除

删除成员角色堆栈

在管理员帐户中，删除成员角色 StackSet。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	删除成员角色 StackSet 确认已删除记住角色堆栈	无
222222222222	成员	确认已删除成员角色堆栈	无

删除保留的角色

在每个账户中，删除保留的 IAM 角色。

重要：保留这些角色用于需要角色才能使补救措施继续发挥作用的修复（例如 VPC 流日志）。在删除这些角色之前，请确认您不需要继续使用这些角色。

删除所有以 SO0111- 为前缀的角色。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	删除保留的角色	无
222222222222	成员	删除保留的角色	无

安排删除保留的 KMS 密钥

管理员和成员堆栈同时创建和保留 KMS 密钥。如果您保留这些钥匙，则需要支付费用。

保留这些密钥是为了让您可以访问解决方案加密的任何资源。在安排删除它们之前，请确认您不需要它们。

使用解决方案或 CloudFormation 历史记录中创建的别名识别解决方案部署的密钥。安排将其删除。

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	确定并安排删除管理员密钥 识别并安排要删除的成员密钥	识别并安排要删除的成员密钥
222222222222	成员	识别并安排要删除的成员密钥	识别并安排要删除的成员密钥

删除堆栈以获得自 StackSets 管权限

删除为允许自行 StackSets 管理权限而创建的堆栈

Account	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	删除 StackSet 管理员角色堆栈	无
222222222222	成员	删除 StackSet 执行角色堆栈	无

开发者指南

本节提供解决方案的源代码和其他自定义设置。

源代码

访问我们的GitHub 存储库，下载此解决方案的模板和脚本，并与其他人共享您的自定义设置。

剧本

该解决方案包括针对互联网安全中心 (CIS) AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1.2.0、CIS AWS 基金会基准 v1.4.0、CIS AWS 基金会基准测试 v3.0.0、AWS 基础安全最佳实践 (FSBP) v.1.0.0、支付卡行业数据安全标准 (PCI-DSS) v3.2. 1 和美国国家标准与技术研究院 (NSBP) v.1.0.0、支付卡行业数据安全标准 (PCI-DSS)v3.2.1 和美国国家标准与技术研究院 (NSBP) IST)。

如果您启用了合并控制结果，则所有标准都支持这些控件。如果启用此功能，则只需要部署 SC 剧本。如果不是，则前面列出的标准支持这些剧本。

> **Important**
>
> 仅部署已启用标准的行动手册，以避免达到服务配额。

有关特定补救措施的详细信息，请参阅 Systems Manager 自动化文档，其中包含解决方案在您的账户中部署的名称。前往 AWS Systems Manager 控制台，然后在导航窗格中选择 “文档”。

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
补救总数	63	34	29	33	65	19	90
ASR-Check EnableAutoScalingGroup ELBHealth	自动扩展。1		自动扩展。1		自动扩展。1		自动扩展。1

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
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							
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 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)					自动扩展。3		自动扩展。3

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateCloudTrailMultiRegionTrail CloudTrail 应激活并配置至少一条多区域跟踪	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail 应该激活静态加密	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.
ASR-EnableLogFileValidation 确保已激活 CloudTrail 日志文件验证	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableCloudTrailToCloudWatchLogging 确保 CloudTrail 跟踪与 Amazon CloudWatch 日志集成	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.
ASR 配置 3 BucketLogging 确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录		2.6		3.6		3.4	CloudTrail.7

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild 项目环境变量不应包含明文凭证	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.
启用 ASR AWSConfig 确保 AWS Config 已激活	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1
ASR 设为私有 EBSSnapshots Amazon EBS 快照不应公开恢复	EC21.		EC21.		EC21.		EC21.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR 移除 VPCDefault SecurityGroupRules VPC 默认安全组应禁止入站和出站流量	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.
启用 ASR 的日志 VPCFlow 应全部启用 VPC 流量记录 VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-EnableEbsEncryptionByDefault 应激活 EBS 默认加密	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-RevokeUnrotatedKeys 用户的访问密钥应每 90 天或更短时间轮换一次	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
ASR 设置政策 IAMPassword IAM 默认密码策略	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7
ASR-证书 RevokeUnused IAMUser 如果在 90 天内未使用用户凭证，则应将其关闭	IAM.8	1.3	IAM.7		IAM.8		IAM.8

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-证书 RevokeUnused IAMUser 如果在 45 天内未使用用户凭证，则应将其关闭				1.12		1.12	IAM.22
ASR-RemoveLambdaPublicAccess Lambda 函数应禁止公众访问	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR 设为私有 RDSSnapshot RDS 快照应禁止公共访问	RDS.1		RDS.1		RDS.1		RDS.1

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-DisablePublicAccessToRDSInstance RDS 数据库实例应禁止公共访问	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2
ASR 加密 RDSSnapshot RDS 集群快照和数据库快照应进行静态加密	RDS.4				RDS.4		RDS.4
ASR-EnableMultiAZOnRDSInstance RDS 数据库实例应配置多个可用区	RDS.5				RDS.5		RDS.5

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableEnhancedMonitoringOnRDSInstance 应为 RDS 数据库实例和集群配置增强监控	RDS.6				RDS.6		RDS.6
启用 ASR RDSClusterDeletionProtection RDS 集群应激活删除保护	RDS.7				RDS.7		RDS.7
启用 ASR RDSInstanceDeletionProtection RDS 数据库实例应激活删除保护	RDS.8				RDS.8		RDS.8

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableMinorVersionUpgradeOnRDSDBInstance 应激活 RDS 自动次要版本升级	RDS.13				RDS.13	2.3.2	RDS.13
ASR-EnableCopyTagsToSnapshotOnRDSCluster 应将 RDS 数据库集群配置为将标签复制到快照	RDS.16				RDS.16		RDS.16

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift 集群应禁止公共访问	Redshift.1		Redshift.1		Redshift.1		Redshift.1
ASR-EnableAutomaticSnapshotsOnRedshiftCluster 亚马逊 Redshift 集群应激活自动快照	Redshift.3				Redshift.3		Redshift.3

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableRedshiftClusterAuditLogging 亚马逊 Redshift 集群应激活审核日志	Redshift.4				Redshift.4		Redshift.4
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster 亚马逊 Redshift 应该激活主要版本的自动升级	Redshift.6				Redshift.6		Redshift.6

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR 配置 3 PublicAccessBlock 应激活 S3 阻止公共访问设置	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR 配置 3 BucketPublicAccessBlock S3 存储桶应禁止公开读取访问	S3.2		S3.2	2.1.5.2	S3.2		S3.2
ASR 配置 3 BucketPublicAccessBlock S3 存储桶应禁止公开写入访问		S3.3					S3.3

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-S3 EnableDefaultEncryption S3 存储桶应激活服务器端加密	S3.4		S3.4	2.1.1	S3.4		S3.4
ASR 设置政策 SSLBucket S3 存储桶应要求请求使用 SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3 BlockDenylist 应限制存储桶策略中授予其他 AWS 账户的 Amazon S3 权限	S3.6				S3.6		S3.6

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
应在存储桶级别激活 S3 阻止公共访问设置	S3.8				S3.8		S3.8
ASR 配置 3 BucketPublicAccessBlock 确保不可公开访问的 S3 存储桶 CloudTrail 日志		2.3					CloudTrail.6
ASR-CreateAccessLoggingBucket 确保在 S3 存储桶上激活 CloudTrail S3 存储桶访问日志记录		2.6					CloudTrail.7

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableKeyRotation 确保已激活客户创建 CMKs 的轮换		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4
ASR-CreateLogMetricFilterAndAlarm 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		3.1		4.1			云监视.1

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 确保在没有 MFA 的情况下登录 AWS 管理控制台时存在日志指标筛选器和警报		3.2		4.2			云监视2
ASR-CreateLogMetricFilterAndAlarm 确保存在“root” 用户使用的日志指标筛选器和警报		3.3	CW.1	4.3			云监视3

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在关于 IAM 策略更改的日志指标筛选条件和警报		3.4		4.4			Cloudwatch.4
ASR-CreateLogMetricFilterAndAlarm 确保存在 CloudTrail 配置更改的日志指标筛选器和警报		3.5		4.5			Cloudwatch.5

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在针对 AWS 管理控制台身份验证失败的日志指标筛选器和警报		3.6		4.6			Cloudwatch.6
ASR-CreateLogMetricFilterAndAlarm 确保存在日志指标筛选器和警报，用于禁用或计划删除已创建的客户 CMKs		3.7		4.7			Cloudwatch.7

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 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		3.8		4.8			Cloudwatch.8
ASR-CreateLogMetricFilterAndAlarm 确保存在针对 AWS Config 配置更改的日志指标筛选器和警报		3.9		4.9			Cloudwatch.9

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在关于安全组更改的日志指标筛选条件和警报		3.10		4.10			Cloudwatch.10
ASR-CreateLogMetricFilterAndAlarm 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		3.11		4.11			Cloudwatch.11

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在关于网络网关更改的日志指标筛选条件和警报		3.12		4.12			Cloudwatch.12
ASR-CreateLogMetricFilterAndAlarm 确保存在关于路由表更改的日志指标筛选条件和警报		3.13		4.13			Cloudwatch.13

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在关于 VPC 更改的日志指标筛选条件和警报		3.14		4.14			Cloudwatch.14
AWS-DisablePublicAccessForSecurityGroup 确保没有安全组允许从 0.0.0.0/0 到端口 22 的入站流量		4.1	EC25.		EC2.13		EC2.13

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
AWS-DisablePublicAccessForSecurityGroup 确保没有安全组允许从 0.0.0.0/0 到端口 3389 的入站流量		4.2			EC2.14		EC2.14
ASR 配置 SNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASR 创建角色 IAMSupport		1.20		1.17		1.17	IAM.18
ASR-DisablePublic IPAuto 分配 Amazon EC2 子网不应自动分配公有 IP 地址	EC2.15				EC2.15		EC2.15

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableCloudTrailLogFileValidation	CloudTrail.4.	2.2	CloudTrail.3.	3.2			CloudTrail.4.
ASR-EnableEncryptionForSNSTopic	SNS.1				SNS.1		SNS.1
ASR-EnableDeliveryStatusLoggingForSNSTopic 应为发送到主题的通知消息启用传输状态记录	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionForSQSQueue	SQS.1				SQS.1		SQS.1

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-makeRDSSnapshot 私有 RDS 快照应该是私有的	RDS.1		RDS.1				RDS.1
ASR 屏蔽 SSMDocument PublicAccess SSM 文档不应公开	SSM.4				SSM.4		SSM.4
ASR-EnableCloudFrontDefaultRootObject CloudFront 发行版应该配置一个默认的根对象	CloudFront1.				CloudFront1.		CloudFront1.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-SetCloudFrontOriginDomain CloudFront 发行版不应指向不存在的 S3 来源	CloudFront.12				CloudFront.12		CloudFront.12
ASR-RemoveCodeBuildPrivilegedMode CodeBuild 项目环境应该有日志 AWS 配置	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.
ASR 终止实例 EC2 应在指定的时间段后移除已停止的 EC2 实例	EC24.				EC24.		EC24.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
启用 ASR IMDSV2 OnInstance EC2 实例应使用实例元数据服务版本 2 (IMDSv2)	EC2.8				EC2.8	5.6	EC2.8
ASR-RevokeUnauthorizedInboundRules 安全组应仅允许授权端口不受限制的传入流量	EC2.18				EC2.18		EC2.18
在此处插入标题 安全组不应允许无限制地访问高风险端口	EC2.19				EC2.19		EC2.19

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
禁用 ASR TGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateway 不应自动接受 VPC 连接请求	EC2.23				EC2.23		EC2.23
ASR-EnablePrivateRepositoryScanning ECR 私有存储库应配置图像扫描	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty 应该启用	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR 配置 3 BucketLogging 应启用 S3 存储桶服务器访问日志记录	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications S3 存储桶应启用事件通知	S3.11				S3.11		S3.11
ASR-sets3LifecyclePolicy S3 存储桶应配置生命周期策略	S3.13				S3.13		S3.13

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableAutoSecretRotation Secrets Manager 密钥应启用自动轮换	SecretsManager1.				SecretsManager1.		SecretsManager1.
ASR-RemoveUnusedSecret 移除未使用 Secrets Manager 密钥	SecretsManager3.				SecretsManager3.		SecretsManager3.
ASR-UpdateSecretRotationPeriod Secrets Manager 密钥应在指定的天数内轮换	SecretsManager4.				SecretsManager4.		SecretsManager4.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
启用 ASR APIGateway CacheDataEncryption API Gateway REST API 缓存数据应静态加密					APIGateway5.		APIGateway5.
ASR-SetLogGroupRetentionDays CloudWatch 日志组应在指定的时间段内保留					CloudWatch.16		CloudWatch.16

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-AttachServiceVPCEndpoint EC2 应将亚马逊配置为使用为亚马逊 EC2 服务创建的 VPC 终端节点	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty 应该给过滤器加标签							GuardDuty 2.
ASR-TagGuardDutyResource GuardDuty 应给探测器加标签							GuardDuty 4.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR 连接到 SSMPermissions EC2 亚马逊 EC2 实例应由 Systems Manager 管理	SSM.1		SSM.3				SSM.1
ASR-ConfigureLaunchConfigNoPublicIPDocument 使用 Auto Scaling 群组启动配置启动的亚马逊 EC2 实例不应具有公有 IP 地址					Autoscaling.5		Autoscaling.5

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
启用 ASR APIGatewa y Execution Logs	APIGatewa y1.						APIGatewa y1.
ASR-Enabl eMacie 应启用 Amazon Macie	Macie.1				Macie.1		Macie.1
ASR-Enabl eAthenaWo rkGroupLo gging Athena 工作组应启用日志记录	Athena.4						Athena.4

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR 强制执行 ALB HTTPSFor 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		ELB.1		ELB.1		ELB.1
ASR 限制 ECSRoot Filesyste mAccess ECS 容器应限制为仅对根文件系统具有只读访问权限。	ECS.5				ECS.5		ECS.5

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableElastiCacheBackups ElastiCache (Redis OSS) 集群应启用自动备份	ElastiCache1.				ElastiCache1.		ElastiCache1.
ASR-EnableElastiCacheVersionUpgrades ElastiCache 集群应启用自动次要版本升级	ElastiCache2.				ElastiCache2.		ElastiCache2.

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache 复制组应启用自动故障切换	ElastiCache3.				ElastiCache3.		ElastiCache3.
ASR-缩放 ConfigureDynamoDBAuto DynamoDB 表应根据需求自动扩展容量	DynamoDB1				DynamoDB1		DynamoDB.1
ASR-资源 TagDynamoDBTable 应标记 DynamoDB 表							DynamoDB.5

描述	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	安全控件 ID
ASR-保护 EnableDynamo DBDeletion DynamoDB 表应启用删除保护					DynamodB 6		DynamodB. 6

添加新的补救措施

补救措施可以通过更新相应的 playbook 文件手动添加，也可以通过编程方式通过 CDK 构造扩展解决方案，具体取决于您的首选工作流程。

> **Note**
>
> 随后的说明利用解决方案安装的资源作为起点。按照惯例，大多数解决方案资源名称都包含 ASR and/or SO0111，以便于查找和识别它们。

手动工作流程概述

AWS 运行手册上的自动安全响应必须遵循以下标准命名：

ASR-*<standard>*--*<version>* *<control>*

标准：安全标准的缩写。这必须符合 ASR 支持的标准。它必须是 “CIS”、“AFSBP”、“PCI”、“NIST” 或 “SC” 之一。

版本：标准的版本。同样，这必须与 ASR 支持的版本和查找数据中的版本相匹配。

控制：要修复的控件的控制 ID。这必须与发现数据相匹配。

1. 在成员账户中创建运行手册。

2. 在成员账户中创建 IAM 角色。
3. （可选）在管理员帐户中创建自动修复规则。

第 1 步：在成员账户中创建运行手册

1. 登录 AWS Systems Manager 控制台并获取查找结果的 JSON 示例。
2. 创建修复发现的自动化操作手册。在 Ow ned by me 选项卡中，使用 “ASR-文档” 选项卡下的任何文档作为起点。
3. 管理员账户中的 AWS Step Functions 将运行你的运行手册。您的 runbook 必须指定修正角色，以便在调用 runbook 时传递。

第 2 步：在成员账户中创建 IAM 角色

1. 登录 AWS Identity and Access 管理控制台。
2. 从 IAM SO0111 角色中获取示例并创建一个新角色。角色名称必须以 so0111-remediate---开头。*<standard> <version> <control>*例如，如果添加 CIS v1.2.0 控件 5.6，则角色必须是。`SO0111-Remediate-CIS-1.2.0-5.6`
3. 使用该示例，创建一个范围适当的角色，该角色仅允许必要的 API 调用来执行修复。

此时，您的补救处于活动状态，可以通过 AWS Security Hub 中的 ASR 自定义操作进行自动修复。

步骤 3：（可选）在管理员帐户中创建自动补救规则

自动（不是 “自动”）补救是指在 AWS Security Hub 收到结果后立即执行补救。在使用此选项之前，请仔细考虑风险。

1. 在 “ CloudWatch 事件” 中查看相同安全标准的示例规则。规则的命名标准是`standard_control_*AutoTrigger*`。
2. 复制示例中的事件模式以供使用。
3. 更改该`GeneratorId`值以匹配您的查找 JSON `GeneratorId` 中的值。
4. 保存并激活规则。

CDK 工作流程概述

总而言之，将修改或添加 ASR 存储库中的以下文件。在此示例中，在 SC 和 AFSBP 剧本中添加了针对 ElastiCache .2 的新补救措施。

> **Note**
>
> 所有新的补救措施都应添加到 SC 行动手册中，因为它整合了 ASR 中可用的所有补救措施。如果您只打算部署一组特定的攻略手册（例如 AFSBP），则可以：(1) 将补救措施仅添加到预期的剧本中，或者 (2) 将补救措施添加到相应 Security Hub 标准中存在的所有 playbook 中，以及 SC 剧本。为了灵活起见，建议使用第二种选择。

在此示例中， ElastiCache.2 包含在以下 Security Hub 标准中：

- AFSBP
- nist.800-53.r5 SI-2
- nist.800-53.r5 SI-2 (2)
- nist.800-53.r5 SI-2 (4)
- nist.800-53.r5 SI-2 (5)
- PCI DSS v4.0.1/6.3.3

由于默认情况下，ASR 仅为 AFSBP 和 NIST.800-53 实现剧本，因此除了 SC 之外，我们还将在这些剧本中添加这个新的补救措施。

Modify

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[标准名称] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.
- source/playbooks/NIST80053/lib/[标准名称] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.
- source/playbooks/SC/lib/sc_remediations.t
- source/test/regex_registry.t

Add

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> 为运行手册选择的名称可以是任何字符串，只要它与所做的其余更改一致。

- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2. ElastiCache ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

开发步骤

1. 创建《修复运行手册》。
2. 创建控制运行手册。
3. 将每个控制运行手册与行动手册集成。
4. 创建修复 IAM 角色并集成修复运行手册
5. 更新单元测试

步骤 1：创建修复运行手册

这是用于修复资源的 SSM 文档。它必须包含`AutomationAssumeRole`参数，即有权执行修复的 IAM 角色。创建新的修复运行手册时，请查看现有文件`source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml`作为参考。

所有新的运行手册都应添加到该`source/remediation_runbooks/`目录中。

步骤 2：创建控制运行手册

控制运行手册是特定于剧本的运行手册，它解析给定标准中的发现数据并执行相应的修复运行手册。由于我们要在 SC、AFSBP 和 NIST8 0053 剧本中添加 ElastiCache .2 补救措施，因此我们必须为每个剧本创建一个新的控制运行手册。创建了以下文件：

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2. ElastiCache ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

这些文件的命名很重要，必须遵循格式 <PLAYBOOK_NAME>_ <CONTROL.ID>.ts/yaml

ASR 中的某些 playbook 支持 IaC 控制运行手册 TypeScript，而另一些则必须使用原始 YAML 编写。以相应行动手册中的现有补救措施为例。在本示例中，我们将介绍使用 IaC 的 SC 剧本。

在 SC 剧本中，您的新控制运行手册应导出一个扩展 ControlRunbookDocument 并与修复运行手册名称相匹配的类。看看下面的例子：

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`是您要添加的补救措施的控件 ID，正如在 Sec urity Hub 的合并控制视图中定义的那样。
- `remediationName`是您为补救运行手册选择的名称。
- `scope`是您正在修复的资源的范围，表示该资源是全球存在还是存在于特定区域。
- `resourceIdRegex`是用于捕获要作为参数传递给修复运行手册的资源 ID 的正则表达式。只应捕获一个群组，所有其他群组都应处于非捕获状态。如果您想传递整个 ARN，请省略此字段。
- `resourceIdName`是您要为使用捕获的资源 ID 设置的名称`resourceIdRegex`，它应与修复运行手册中的资源 ID 参数名称相匹配。

- updateDescription是您希望在修复成功后分配给 Security Hub 中调查结果的 “注释” 部分的字符串。

您还必须导出一个名为的函数createControlRunbook，该函数会返回您的类的新实例。对于 ElastiCache .2，这看起来像：

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

其中，controlId是安全标准中定义的与操作手册相关的控件 ID。

如果 Security Hub 控件包含要传递给修复运行手册的参数，则可以通过向以下方法添加替代来传递这些参数：-getExtraSteps: 定义在 Security Hub 中为控件实现的每个参数的默认值

> **Note**
>
> 必须为 Security Hub 中的每个参数指定一个默认值

- getInputParamsStepOutput: 定义控制运行手 GetInputParams 册步骤的输出
- 每个输出都有nameoutputType、和selector。selector应与getExtraSteps方法重写中使用的选择器相同。
- getRemediationParams：定义传递给修复运行手册的参数，这些参数从 GetInputParams 步骤输出中获取。

要查看示例，请导航到该source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts文件。

第 3 步：将每个控制运行手册与攻略手册集成

对于在上一步中创建的每个控制运行手册，您现在必须将其与相关行动手册中的基础架构定义集成。针对每个控制运行手册，请按照以下步骤操作。

> **Important**
>
> 如果您使用原始 YAML 而不是 typescript IaC 创建控制运行手册，请跳到下一节。

在“*/<playbook_name>*/control_runbooks-construct.ts导入”新创建的控制运行手册文件中，例如：

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

接下来，转到阵列中查看

```
const controlRunbooksRecord: Record<string, any>
```

并添加一个将控件 ID（特定于剧本）映射到您创建的createControlRunbook方法的新条目：

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

将剧本特定的控件 ID 添加到补救措施列表中，如下所示：*<playbook_name>*_remediations.ts

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

该versionAdded字段应为解决方案的最新版本。如果添加补救措施违反了模板大小限制，请增加versionAdded。您可以调整中每个 playbook 成员堆栈中包含的修正次数。solution_env.sh

步骤 4：创建修复 IAM 角色并集成修复运行手册

每个补救措施都有自己的 IAM 角色，该角色具有执行修复运行手册所需的自定义权限。此外，需要调用该RunbookFactory.createRemediationRunbook方法，将您在步骤 1 中创建的修复运行手册添加到解决方案的 CloudFormation 模板中。

在中remediation-runook-stack.ts，每个补救措施在RemediationRunbookStack类中都有自己的代码块。以下代码块显示了为 ElastiCache .2 修正创建新的 IAM 角色和补救运行手册集成的过程：

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);
```

```
      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

步骤 5：更新单元测试

我们建议在添加新的补救措施后更新并运行单元测试。

首先，必须向source/test/regex_registry.ts文件中添加任何新的正则表达式（尚未添加）。此文件强制对解决方案运行手册中包含的每个新正则表达式进行测试。以该addElastiCacheClusterTestCases函数为例，该函数用于测试 ElastiCache 修正中使用的正则表达式。

最后，你需要更新每个堆栈的快照。快照是版本控制的 CloudFormation 模板定义，用于跟踪对 ASR 基础架构所做的更改。您可以通过在deployment目录中运行以下命令来更新这些快照文件：

```
./run-unit-tests.sh update
```

现在，您已准备好部署新的补救措施了！导航到下面的 “生成和部署” 部分，获取有关使用新更改构建和部署解决方案的说明。

添加新剧本

从GitHub 存储库中下载 AWS 上的自动安全响应解决方案手册和部署源代码。

AWS CloudFormation 资源由 AWS CDK 组件创建，资源包含可用于创建和配置新剧本的剧本模板代码。有关设置项目和自定义 playbook 的更多信息，请参阅中的 README.m d 文件。 GitHub

AWS Systems Manager Parameter Store

AWS 上的自动安全响应使用 AWS Systems Manager Parameter Store 来存储操作数据。以下参数存储在参数存储中：

Name	值	使用
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS KMS 密钥将加密数据以进行 FSBP 补救	作为补救措施的一部分，对客户数据（例如 CloudTrail 日志）进行加密
`/Solutions/SO0111/CMK_ARN`	ASR 将用来加密数据的 AWS KMS 密钥	加密解决方案数据
`/Solutions/SO0111/SNS_Topic_ARN`	该解决方案的 Amazon SNS 主题的 ARN	补救事件通知
`/Solutions/SO0111/SNS_Topic_Config.1`	AWS Config 更新的 SNS 主题	配置.1 修复
`/Solutions/SO0111/version`	解决方案版本	
`/Solutions/SO0111/<security standard long name>/<version>` /status	`enabled`	表示该标准在解决方案中是否处于活动状态。通过将标准更改为，可以禁用标准以进行自动修复 `disabled`

Name	值	使用
/Solutions/SO0111/*<security standard long name>*/shortname	String	安全标准的简称。例如：CIS、AFSBP、PCI
/Solutions/SO0111//*<security standard long name><version>* /*<control>* /remap	String	当一个控件使用与另一个控件相同的补救措施时，这些参数会完成重映射
/ASR/Filters/AccountFilterMode	包括、排除或禁用	控制账户 ID 筛选行为，以实现全自动修复
/ASR/Filters/AccountFilters	以逗号分隔的 AWS 账户列表 IDs	解决方案应筛选自动补救措施的 AWS 账户 IDs 列表。
/ASR/Filters/OUFilterMode	包括、排除或禁用	控制组织单位 (OUs) 筛选行为，以实现全自动修复
/ASR/Filters/OUFilters	以逗号分隔的组织单位 ID 列表	解决方案应筛选自动补救措施的列表。 OUs
/ASR/Filters/TagFilterMode	包括、排除或禁用	控制资源标签筛选行为，以实现全自动修复
/ASR/Filters/TagFilters	以逗号分隔的资源标签密钥列表	解决方案应筛选自动修复的资源标签密钥列表。

Amazon SNS 主题-修复进度

AWS 上的自动安全响应会创建一个 Amazon SNS 主题 so0111-asr_Topic。本主题用于发布有关修复进度的最新信息。以下是向该主题发送的三种可能的通知。

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

这是完成消息。它表示补救已完成，没有错误；但是，成功修复的权威测试是 AWS Config 检查 and/or 手动验证。

筛选 SNS 主题订阅

亚马逊 SNS 订阅筛选政策：

1. 导航到 SNS 主题的订阅。
2. 在 “订阅筛选策略” 下，选择 “编辑”。
3. 展开 “订阅筛选器策略”，然后切换 “订阅筛选器策略” 选项以启用过滤器。
4. 选择 “邮件正文” 范围。
5. 将您的政策添加到 JSON 编辑器中。
6. 保存更改。

策略示例：

按账户筛选

```
{
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
```

筛选错误

```
{
"severity": ["ERROR"]
```

```
}
```

按控件筛选

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

亚马逊 SNS 主题-警报 CloudWatch

此解决方案创建了一个 Amazon SNS 主题。SO0111-ASR_Alarm_Topic本主题用于发布警报警报。

任何进入警报状态的警报的详细信息都将发送到此主题。

在 Config 发现结果上启动 Runbook

此解决方案可以根据自定义 AWS Config 发现结果启动运行手册。为此，你需要：

1. 找到您要修复的 AWS Config 规则名称。这可以在 AWS Config 中找到，也可以在 Security Hub 为此规则生成的调查结果中找到。
2. 导航到 AWS Systems Manager Parameter Systems Store，然后选择创建参数。
3. 您的规则名称应为 /Solutions/SO0111/ [.replacable] Rule name from Step 1
4. 该值的格式应如下所示：

```
{

"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

1. RunbookName 是必填字段，将是修复此 Config 规则时运行的运行手册。 RunbookRole 是协调员在运行此角色时将扮演的角色。这不是必填字段，如果省略，协调器将默认使用账户的成员角色。
2. 完成此操作后，您可以使用 Security Hub 上的 “使用 ASR 修复” 自定义操作来修复您的 Config 规则。

网页用户界面

该解决方案的 Web 用户界面允许用户一键修复 AWS Security Hub 的调查结果，查看和下载过去的补救措施，以及委派对解决方案的访问权限。

使用该解决方案不需要 Web UI；您也可以配置全自动修复以避免手动执行，或者利用 AWS Security Hub CSPM 控制台使用 “使用 ASR 修复” 自定义操作启动补救。

> **Note**
>
> 部署管理堆栈时，必须将`ShouldDeployWebUI`参数设置为 “是”，才能使用解决方案的 Web UI。

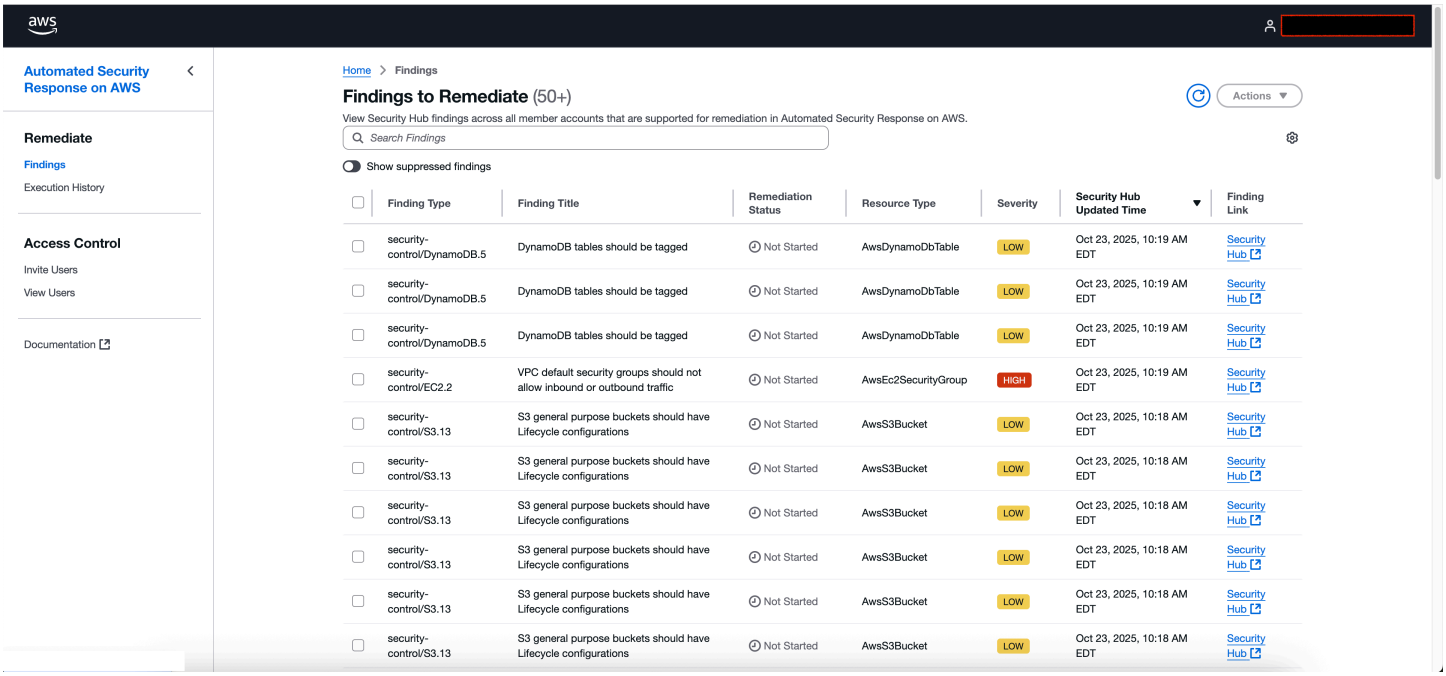
工作方式

该解决方案的 Web 用户界面是一个单页 Web 应用程序，由 Amazon S3 托管在您的账户中，并由亚马逊 CloudFront分发。该解决方案还使用 API Gateway 部署 REST API 来支持 Web 用户界面中的操作。

部署管理堆栈后，解决方案的 Lambda 函数开始将您的管理员账户中存在的该解决方案支持的所有 AWS Security Hub 发现加载到 DynamoDB 中。完成此操作后，由于解决方案部署的 EventBridge 规则，Web UI 中显示的发现结果将与 Security Hub 近乎实时地保持同步。

每周都会触发该解决方案的 Lambda 函数，以刷新存储 Web 用户界面中显示的 AWS Security Hub 发现结果的 DynamoDB 表。这样可以确保清理陈旧的数据并保留我们的 DynamoDB 表。 up-to-date如果要将此基准配置为更高或更少的运行频率，请修改`SO0111-ASR-SynchronizationFindingsLambdaWeeklyRule`位于部署解决方案的同一区域的管理员帐户中名为的 EventBridge 规则。

直接在 Web 用户界面中运行修复



在调查结果页面上，管理员或委托管理员用户可以查看该解决方案支持的所有 AWS Security Hub 调查结果以进行补救。这包括在 Security Hub 主账户中注册的 Security Hub 成员账户的调查结果。如果解决方案也部署在聚合区域，则还会显示任何已上线区域的调查结果。要查看该解决方案支持的结果列表，请参阅 playbook 部分。

账户操作员用户只能查看来自他们有权访问的 AWS 账户的调查结果，如邀请中所述。此外，他们只能对与其关联的账户中的资源进行修复。

要运行修复，请在表格中选择任意数量的项目，然后单击 “操作” > “修复”。也可以通过单击 “操作” > “隐藏” 来隐藏查找结果，这会在默认视图中隐藏选定的查找结果。通过单击 “显示隐藏的查找结果” 开关，您可以随时查看隐藏的查找结果。

开始对发现进行补救后，可以单击 “修正状态” 列，同时补救处于`In Progress`或将直接`Failed`进入该修正的 “执行历史记录” 页面上。

筛选可用的发现和补救措施

在 “调查结果” 和 “执行历史记录” 页面上，您可以按每个表格中显示的任意列筛选表格中显示的数据。

例如，在 “调查结果” 页面上，您可以在 “查找类型” 上进行筛选，通过单击搜索栏并选择 “查找类型” 来搜索特定类型的 AWS Security Hub 调查结果（例如 Lambda.1 或 Athena.4）。

> **Note**
>
> 在搜索栏中自动填充的值并不代表可用数据的完整列表。每个搜索条件的建议值仅代表当前获取并显示在用户界面中的数据。

您也可以在一次搜索中合并多个属性。例如，您可以在搜索中同时应用查找类型和资源 ID 来执行逻辑AND查询。此外，您可以应用多个相同的筛选条件来执行逻辑OR搜索，例如查找类型 = Lambda.1 和查找类型 = Athena. 4。同样的原则适用于 “执行历史记录” 页面

Web UI 中的身份验证和授权

该解决方案的 Web 用户界面受 Amazon Cognito 提供的身份验证保护。部署解决方案后，将在 Web 用户界面旁边配置和配置 Cognito 用户池、Cognito 应用程序客户端和 Cognito 用户池域。作为管理员堆栈参数提供的电子邮件地址被分配了临时凭证，并被授予对 Web UI 的管理员访问权限。

有三种权限类型可以定义用户对 Web UI 的访问权限：

权限类型	访问级别	使用场景
Admin	在 Web UI 中完全控制；可以查看所有发现和补救措施、运行任何补救措施以及 invite/view 任何用户。	仅分配给部署管理堆栈的用户，前提是他们在 CloudFormation 部署期间提供电子邮件地址。
委派管理员	Web UI 中的控制权得到提升；可以查看所有发现和补救措施、运行任何补救措施以及 invite/view 账户操作员用户。无法在 Web UI 中邀请或查看管理员和委派管理员。	管理员用户可以通过邀请委派管理员用户来委派解决方案的访问权限，委托管理员用户将能够运行和管理任何补救措施。
账户操作员	Web UI 中的控制有限；仅限于在应邀与之关联的账户中查看和修正调查结果。无法邀请或查看其他用户。	Day-to-day 本应具有有限访问权限才能在已注册帐户子集中运行修正的用户。管理员或授权管理员负责邀请这些用户并定义其范围。

所有用户必须先获得管理员或委托管理员的邀请，然后才能登录 Web UI。要邀请其他用户，管理员或授权管理员可以在 Web UI 的 “邀请用户” 页面上输入他们的电子邮件地址和权限级别。

管理员和授权管理员还可以查看、管理和删除现有用户。要查看所有用户的列表，请导航至查看用户页面。

要管理现有用户，请从表格中选择该用户，然后单击 “管理用户”。然后，您可以通过单击 “删除用户” 来删除该用户。如果用户是账户操作员，则可以在解决方案的背景下修改 IDs 他们有权访问的 AWS 账户列表。目前不支持更改现有用户的权限类型。

请注意，授权管理员只能查看和管理账户操作员用户。

与外部集成 IdPs

您可以自定义该解决方案提供的身份验证机制，以允许用户使用您自己的 OIDC 或 SAML 身份提供商（例如 Okta 或 Microsoft Entra ID）进行登录。以下与外部集成的步骤 IdPs 需要访问部署管理堆栈的 AWS 账户。

> **Important**
>
> 在使用解决方案配置的任何外部 IdP 登录之前，仍必须邀请用户。此外，链接到其 IdP 个人资料的电子邮件地址必须与邀请函中提供的电子邮件地址一致。

步骤 1-找到解决方案的用户池

在 Amazon Cognito 控制台中，找到名为 SO0111-ASR-的解决方案用户池。UserPool

单击用户池名称 SO0111-ASR-UserPool，进入概述页面。从那里，从导航栏中选择 “社交和外部提供商”。

第 2 步-添加您的身份提供商

在 “社交和外部提供商” 页面上，单击右上角的 “添加身份提供商” 按钮。

根据您的身份提供商选择 OIDC 或 SAML。

选择提供商类型后，系统将提示您输入有关您的身份提供商的信息。

为 SAML 提供商填写以下字段：

1. 提供商名称：您的提供商的友好名称
2. IDP 发起的 SAML 登录：选择 `Require SP-initiated SAML assertions - Recommended`
3. 元数据文档来源：选择 `Upload metadata document`
4. 元数据文档：上传您的 IdP 提供的 SAML 元数据文档。
5. 在 SAML 提供商和用户池之间的 “映射属性” 下，单击 “添加其他属性”。对于用户池属性，请`email`从下拉列表中选择。在 S AML 属性中，输入您的 SAML 身份提供商中存储用户电子邮件地址的属性的全名。例如 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` 。
6. 单击 “添加身份提供商” 以保存您的更改。

为 OIDC 提供商填写以下字段：

1. 提供商名称：您的提供商的友好名称
2. 客户端 ID：输入您的 OpenID Connect 身份提供商提供的客户端 ID。
3. 客户机密钥：输入 OpenID Connect 身份提供商提供的客户机密钥。
4. 授权范围：输入 `openid profile email`
5. 属性请求方法：`POST`根据您的身份提供商的配置选择`GET`或。
6. 设置方法：选择`Auto fill through issuer URL`并输入 OIDC 提供商提供的发行人 URL。或者，也可以手动输入值。
7. 在 OpenID Connect 提供商和用户池之间的 “映射属性” 下，单击 “添加其他属性”。对于用户池属性，请`email`从下拉列表中选择。在 O penID Connect 属性中，输入 OIDC 身份提供商中存储用户电子邮件地址的属性的全名。例如 `email`。
8. 单击 “添加身份提供商” 以保存您的更改。

> **Important**
>
> 即使您的身份提供商的属性名称也是，您也必须为`email`用户池属性添加属性映射`email`。

第 3 步-将您的提供商添加到解决方案的应用程序客户端

导航到 “应用程序客户端” 页面，然后选择名为 so011 1-asr-webui-的客户端。UserPoolClient

单击 “登录页面” 选项卡，在 “托管登录页面配置” 下单击 “编辑”。

在身份提供者字段中，添加您在上一步中创建的身份提供商。单击 Save Changes（保存更改）。

第 4 步-配置您的身份提供商

要允许您的身份提供者在登录后重定向到解决方案的 Web UI，您必须在 IdP 配置 URLs 中将以下内容列入许可名单。

根据您的提供商类型，将以下回拨 URLs之一列入白名单：

1. SAML 回调网址：https://so0111-asr-*<your-aws-account-id>* .auth。 *<aws-region>*.amazoncognito。 com/saml2/idpresponse
2. OIDC 回调网址：https://so0111-asr-*<your-aws-account-id>* .auth。 *<aws-region>*.amazoncognito。 com/oauth2/idpresponse

您应<your-aws-account-id>替换为部署管理堆栈的 AWS 账户 ID<aws-region>，以及部署管理堆栈的区域。

第 4 步-验证您的集成

导航到 Web UI 登录页面。确认您的自定义身份提供者在登录页面上可见。

要测试集成，请使用邀请用户页面邀请新用户。然后，在 Web UI 登录页面上单击您的自定义身份提供商，确保用户可以进行身份验证。

请注意，您的自定义 IdP 中用户的个人资料必须链接到其邀请中提供的相同电子邮件地址。换句话说，您的提供商声明中的电子邮件地址必须与邀请相匹配。

参考

本节包括有关数据收集的可选功能的信息、相关资源的指针以及为该解决方案做出贡献的构建者列表。

数据收集

此解决方案向 AWS 发送有关该解决方案使用情况的运营指标（“数据”）。我们使用这些数据来更好地了解客户如何使用此解决方案以及相关服务和产品。AWS 对这些数据的收集受 AWS 隐私声明的约束。

相关资源

- 使用 AWS Security Hub 进行自动响应和补救
- 独联体亚马逊 Web Services 基金会基准测试，版本 1.2.0
- AWS 基础安全最佳实践标准
- 支付卡行业数据安全标准 (PCI DSS)
- 美国国家标准与技术研究所 (NIST) SP 800-53 Rev. 5

贡献者

以下个人参与了本文档的编撰：

- 迈克·奥布莱恩
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schuetter
- 安德鲁·扬科夫斯基
- 乔什·莫斯
- Ryan Garay
- Thiemo Belmega

- Mykhailo Markhain
- Manish Jangid
- 安德鲁·斯蒂芬
- 彼得 DeVries
- Mukta Dadariya

修订

发布日期：2020 年 8 月（最后更新时间：2025 年 1 月）

访问我们 GitHub 存储库中的 Changelog.md，跟踪特定版本的改进和修复。

版权声明

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。