aws

实施指南

开启自动安全响应 AWS

开启自动安全响应 AWS: 实施指南

Table of Contents

解决方案概述 1
功能和优势 2
使用案例 3
概念和定义 4
架构概述 6
架构图 6
AWS Well-Architected 的设计注意事项 7
卓越运营 7
安全性 8
可靠性 8
性能效率 8
成本优化 8
可持续性 8
架构详情 9
AWS Security Hub 整合 9
跨账户补救 9
剧本 9
集中式日志记录 10
通知 10
此解决方案中的 AWS 服务 10
规划您的部署 12
费用 12
费用表示例 12
定价示例（每月） 16
可选功能的额外费用 21
安全性 23
IAM 角色 23
支持 AWS 区域 23
限额 25
此解决方案中的 AWS 服务的限额 25
AWS CloudFormation 配额 25
亚马逊 EventBridge 规定配额 25
AWSSecurity Hub 部署 26
堆栈与 StackSets 部署 26

部署解决方案 27
决定将每个堆栈部署到何处 27
决定如何部署每个堆栈 28
整合的控件调查发现 28
AWS CloudFormation 模板 29
管理员账号支持 29
成员账户 30
成员角色 30
票务系统集成 30
自动部署- StackSets 31
先决条件 31
部署概述 32
（可选）步骤 0：启动工单系统集成堆栈 33
步骤 1：在委派的 Security Hub 管理员账户中启动管理堆栈 35
步骤 2：将补救角色安装到每个 Sec AWS urity Hub 成员账户中 36
步骤 3：将成员堆栈启动到每个 S AWS ecurity Hub 成员账户和区域 37
自动部署-堆栈 38
先决条件 38
部署概述 38
（可选）步骤 0：启动工单系统集成堆栈 39
步骤 1：启动管理堆栈 42
步骤 2：将补救角色安装到每个 Sec AWS urity Hub 成员账户中 45
步骤 3：启动成员堆栈 46
步骤 4：（可选）调整可用的补救措施 49
使用 Service Catalog 监控解决方案 AppRegistry 51
使用 “ CloudWatch 应用程序见解” 51
确认与此解决方案关联的成本标签 52
激活与此解决方案关联的成本分配标签 53
AWS Cost Explorer 54
使用 Amazon CloudWatch 控制面板监控解决方案的运营 55
启用 CloudWatch 指标、警报和控制面板 55
使用 CloudWatch 控制面板 55
修改警报阈值 57
订阅警报通知 59
更新此解决方案 60
从 v1.4 之前的版本升级 60

从 v1.4 及更高版本升级 60
从 v2.0.x 升级 60
故障排除 61
解决方案日志 61
已知问题解决方案 62
特定补救措施存在问题 64
Puts3 失败BucketPolicyDeny 了 64
如何禁用该解决方案 65
联系我们 Support 65
创建案例 65
我们能帮上什么忙？ 66
其他信息 66
帮助我们更快地解决您的问题 66
立即解决或联系我们 66
卸载此解决方案 67
V1.0.0-V1.2.1 67
v1.3.x 67
V1.4.0 及更高版本 68
管理员指南 69
启用和禁用解决方案的某些部分 69
SNS通知示例 70
使用解决方案 72
开启自动安全响应入门 AWS 72
准备账目 72
启用 AWS Config 72
启用AWS安全中心 73
启用整合的控制结果 73
配置跨区域查找结果聚合 74
指定 Security Hub 管理员帐户 75
为自行管理 StackSets 的权限创建角色 75
创建将生成示例结果的不安全资源 76
为相关控件创建 CloudWatch 日志组 77
将解决方案部署到教程账户 77
部署管理堆栈 77
部署成员堆栈 78
部署成员角色堆栈 79

订阅该SNS主题 79
修复示例发现 79
启动修复 80
确认补救措施解决了调查结果 80
追踪补救措施的执行情况 80
EventBridge 规则 80
Step Functions 执行 81
SSM 自动化 81
CloudWatch 日志组 81
启用全自动补救 81
确认您没有可能意外应用此发现的资源 81
启用规则 82
配置资源 82
确认补救措施解决了调查结果 80
清理 83
删除示例资源 83
删除管理堆栈 83
删除成员堆栈 83
删除成员角色堆栈 84
删除保留的角色 84
安排删除保留的KMS密钥 84
删除堆栈以获得自 StackSets 管权限 85
开发人员指南 86
源代码 86
剧本 86
添加新的补救措施 122
概述 122
第 1 步：在成员账户中创建运行手册 123
第 2 步：在成员账户中创建IAM角色 123
步骤 3：（可选）在管理员帐户中创建自动补救规则 123
添加新剧本 123
AWS Systems Manager 参数存储 124
SNS主题-修复进度 125
筛选SNS主题订阅 125
Amazon SNS 主题 — CloudWatch 警报 126
在 Config 发现结果上启动 Runbook 126

参考 128
匿名数据收集 128
相关资源 129
贡献者 129
修订 131
版权声明 135
..... cxxxvi

通过中预定义的响应和补救措施自动应对安全威胁 AWS Security Hub

发布日期：二零二零年八月（最后更新时间：二零二四年十二月）

本实施指南概述了AWS解决方案的自动安全响应、其参考架构和组件、部署规划注意事项、将 AWS 解决方案上的自动安全响应部署到 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架构资源（“堆栈”）	AWS CloudFormation 模板
访问源代码，也可以选择使用 AWS Cloud Development Kit (AWSCDK) 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。自动安全响应 AWS 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。

开启自动安全响应AWS是一种 AWS 解决方案，可以提高您的安全性，并帮助您的工作负载与 AWS Security HubWell-Architected 安全支柱最佳实践 SEC1 (0) 保持一致。该解决方案使 AWS Security Hub 客户可以更轻松地解决常见的安全发现并改善其安全状况 AWS。

您可以选择要在您的 Security Hub 主账户中部署的特定攻略手册。每本攻略手册都包含必要的自定义操作、身份和访问管理 (IAM) 角色、Amazon EventBridge 规则、S AWS ystems Manager 自动化文档、AWS Lambda函数，以及在单个AWS账户或多个账户中启动补救工作流程AWS Step Functions所

需的内容。补救措施可通过中的 “操作” 菜单进行 AWS Security Hub ，允许授权用户通过单一操作在所有 AWS Security Hub托管账户中修复发现的结果。例如，您可以应用互联网安全中心 (CIS) AWS Foundations Benchmark（一项用于保护AWS资源的合规性标准）的建议，以确保密码在 90 天内过期，并对存储在中的事件日志强制加密AWS。

> **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 规则启用自动修复时，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。

开启的自动安全响应AWS包括针对安全标准的行动手册补救措施，定义为以下内容的一部分：

- 互联网安全中心 (CIS) AWS 基础基准 v1.2.0
- CISAWS基金会基准测试 v1.4.0
- CISAWS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 Security Hub 整合控制结果功能的 “AWS安全控制 (SC) 手册”。有关更多信息，请参阅行动手册。

本实施指南讨论了在AWS云端AWS解决方案上部署自动安全响应的架构注意事项和配置步骤。它包括指向AWS CloudFormation模板的链接，这些模板使用安全性和可用性AWS的最佳实践来启动、配置和运行部署此解决方案所需的AWS计算AWS、网络、存储和其他服务。

本指南适用于具有AWS云架构实践经验的 IT 基础架构架构师、管理员和 DevOps 专业人士。

功能和优势

上的 “自动安全响应” AWS 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 Sec AWS urity 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

使用配置为组织账户和区域聚合目标的 Sec AWS urity Hub 管理员账户，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。

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。

AWSConfigRemediations 在 GovCloud 和中国分区中使用

解决方案中包含的一些补救措施是重新打包AWS自有文档，这些 AWSConfigRemediation 文档在商业分区中可用，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 S AWS ystems Manager 自动化文档和AWSIAM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：

应用程序

要作为一个单元运行的一组逻辑AWS资源。

修复，修复操作手册

实施一组解决发现的步骤。例如，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 Lambda AWS 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 Syst AWS ems Manager (SSM) 自动化文档之一，Orchestrator 使用这些文档将针对特定控件启动的补救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，分别命名为 ASR-AFSBP _Lambda.1 和-sc_2.0.0_Lambda.1。ASR每个控制运行手册都调用相同的补救运行手册，在本例中为-。ASR RemoveLambdaPublicAccess

管弦乐师

解决方案部署的 Step Functions 将来自 Sec AWS urity 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，Sec AWS urity Hub 和本解决方案支持的标准之一是AWSFSBP。

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 指出 Lambd AWS a 函数应禁止公开访问。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

S AWS ecurity 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结果。例如，控件 AWS FSBP S3.2、v1.2.0 2.3、CIS v1. CIS 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。

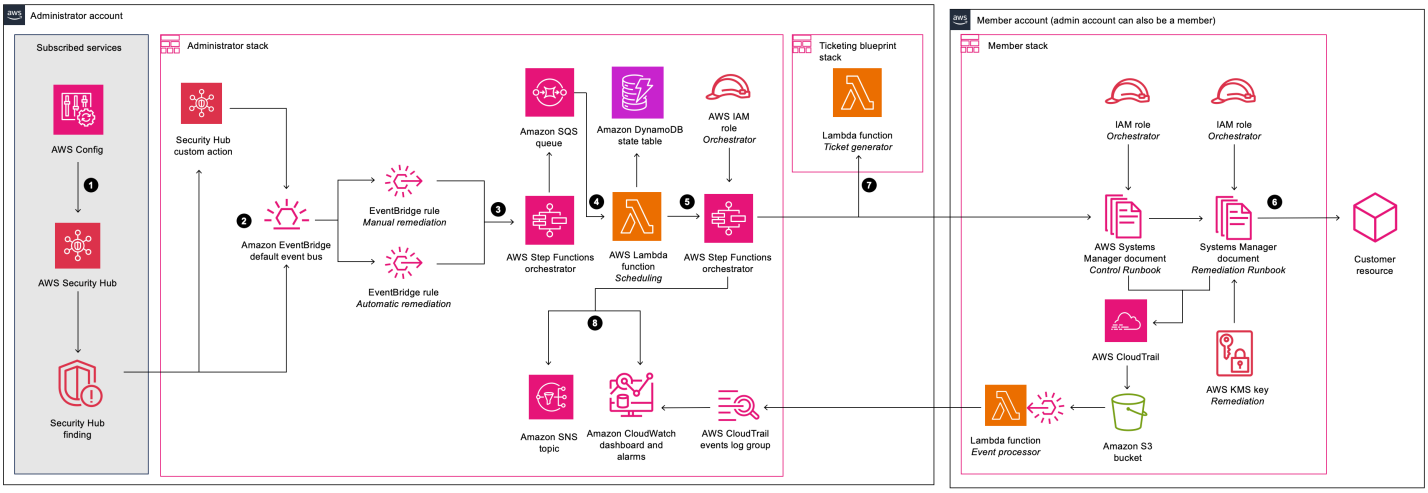
有关 AWS 术语的一般参考，请参阅AWS 词汇表。

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 资源是从 AWS Cloud Development Kit (AWSCDK) 结构中创建的。

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 Amazon Guard Duty 和 Fi AWS rewall Manager）收集事件和数据。 AWS Config这些事件和数据是根据安全标准（例如 CISAWS基金会基准测试）进行分析的。 AWS Security Hub 控制台中将异常作为发现结果进行断言。新发现将作为 Amazon EventBridge 事件发送。
2. 启动：您可以使用自定义操作根据发现启动事件，从而生成 EventBridge 事件。 AWS Security Hub自定义操作和 EventBridge规则会在 p AWS laybook 上启动自动安全响应，以解决发现的问题。该解决方案部署了：

   a. 一条与自定义操作事件相匹配的 EventBridge 规则

b. 每个支持的控件都有一个 EventBridge 事件规则（默认情况下处于停用状态），以匹配实时查找事件

您可以使用 Security Hub 控制台中的自定义操作菜单来启动自动修复。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。

3. 预修复：在管理员帐户中，AWS Step Functions处理修复事件并做好计划准备。
4. 计划：该解决方案调用计划AWS Lambda功能将修复事件放在 Amazon DynamoDB 状态表中。
5. 编排：在管理员账户中，Step Functions 使用跨账户 AWS Identity and Access Management(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。
6. 修复：成员账户中的AWS Systems Manager自动化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EnableCloudTrailForASRActionLog参数在成员堆栈中启用操作日志功能。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。
7. （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
8. 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 (AmazonSNS) 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 的设计注意事项

该解决方案是根据Well-Architecte AWS d Framework中的最佳实践设计的，该框架可帮助客户在云中设计和运行可靠、安全、高效且具有成本效益的工作负载。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。

- IAM用于身份验证和授权。

- 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。

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。
- 使用免费套餐实现每个账户的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，以及有关这些组件如何协同工作的架构详细信息。

AWS Security Hub 整合

部署aws-sharr-deploy堆栈可以与 Sec AWS urity Hub 的自定义操作功能集成。当 AWS Security Hub 控制台用户选择 Findings 进行补救时，解决方案会使用路由查找结果记录以进行修复 AWS Step Functions。

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（管理员和成员）。aws-sharr-member.template aws-sharr-member-roles.template CloudFormation有关更多信息，请参阅剧本。此模板允许对目标账户进行自动修复。

用户可以使用 Amazon CloudWatch 事件规则在每次修复的基础上自动启动自动修复。此选项将在发现报告给后立即激活对发现结果的全自动补救。 AWS Security Hub默认情况下，自动启动处于关闭状态。在安装剧本期间或之后，可以通过在 AWS Security Hub 管理员帐户中打开 CloudWatch 事件规则，随时更改此选项。

跨账户补救

Automated Security Response on AWS 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 S AWS ystems 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、更新和删除 Playbook。有关每本 playbook 中支持的补救措施的信息，请参阅开发人员指南-> Playbook。该解决方案目前支持以下攻略手册：

- 《安全控制》是一本与 Security Hub 的整合控制结果功能一致的AWS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剧本。

- 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 1.0.0，2021 年 3 月发布。
- 支付卡行业数据安全标准 (PCI-DSS) 版本 3.2.1，2018 年 5 月发布。
- 美国国家标准与技术研究院 (NIST) 版本 5.0.0，2023 年 11 月发布。

集中式日志记录

对单个AWS日志组 SO0111-的 CloudWatch 日志进行自动安全响应SHARR。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 (AmazonSNS) 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。

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。部署将在修复发现时启动协调器步骤功能的事件。
AWS IAM	核心。部署多个角色以允许对不同的资源进行修复。

AWS 服务	描述
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。
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。部署协调器，该协调器将通过 Syst AWS ems Manager 调用调用补救文档。API
AWS Systems Manager (系统管理员)	核心。部署包含将要运行的修复逻辑的系统管理器文档（链接到文档）。
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 仪表板上。
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。
AWS DynamoDB	支持。在每个账户和区域中存储上次运行的修复，以优化修正计划。
服务目录 AppRegistry	支持。为已部署的堆栈部署应用程序以跟踪成本和使用情况。
Amazon Simple Notification Service	支持。部署修复完成后会收到通知SNS的主题。
AWS SQS	支持。协助安排修复，以便解决方案可以并行运行修复。

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 AWS 区域、配额和其他注意事项。

成本

运行此解决方案所用的 AWS 服务费用由您承担。从本次修订开始，在美国东部（弗吉尼亚北部）使用默认设置运行此解决方案的成本约 AWS 区域 为 21.17 美元（每月 300 次修复），每月 3,000 次修复 134.86 美元，每月 30,000 次修复 1,281.01 美元。价格可能会发生变化。有关完整详情，请参阅此解决方案中使用的每项 AWS 服务的定价页面。

> **Note**
>
> 许多AWS服务都包括免费套餐，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。

我们建议通过创建预算AWS Cost Explorer来帮助管理成本。价格可能会发生变化。有关完整详情，请参阅此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 成员账号的数量
- 主动自动调用的修正的数量
- 补救的频率

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 [USD]
AWS Systems Manager 自动化-步数	每个账户每月 100,000 步	除免费套餐外，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，

服务	免费套餐	定价 [USD]
		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 自动化-步骤持续时间	每月 5,000 秒	除了免费套餐之外，每个 aws:executeScript action 步骤在每月 5,000 秒的免费套餐之后每秒收取 0.00003 美元的费用。
AWS Systems Manager 自动化-存储	没有免费套餐	每月每 GB 0.046 美元
AWS Systems Manager 自动化-数据传输	没有免费套餐	每 GB 转账 0.900 美元（跨账户或） out-of-Region
AWS Security Hub -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 -查找摄取事件	前 10,000 events/account/Region/month 是免费的。查找与 Security Hub 的安全检查相关的摄取事件。	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 [USD]
亚马逊 CloudWatch -指标	基本监控指标（以 5 分钟为频率）10 个详细监控指标（频率为 1 分钟）100 万个API请求（不适用于 GetMetricData和GetMetricWidgetImage）	前 10,000 个指标每月花费 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每 1,000 个请求的通话费用为 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
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

服务	免费套餐	定价 [USD]
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
亚马逊 CloudWatch -活动	包括除自定义事件之外的所有事件	自定义事件每百万事件 1.00 美元跨账户事件每百万事件 1.00 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 秒收取 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 亿个请求中有 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

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
- 每月总费用为 21.17 美元

服务	假设	月度费用 [USD]
AWS Systems Manager 自动化	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	300 次补救 * 0.000002 美元 = 0.0006 美元 0.0006 * 0.03 = 0.000018 美元	< 0.01 美元
AWS Lambda -请求	300 次补救 * 6 个请求 = 1,800 个请求 0.20 * 1,000,000 个请求 = 0.20 美元	0.20 美元
AWS Lambda -持续时间	2.56M：1.875 GB 秒 * 300 次修复 * 0.0000167 美元 = 0.009375 美元	< 0.01 美元
AWS Step Functions	17 个状态转换 * 300 次修复 = 5,100 0.025 美元 * (5,100/1,000) 状态转换 = 0.15 美元	0.15 美元

服务	假设	月度费用 [USD]
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	10.00 美元
Amazon DynamoDB	2.00 * 1,000,000 次读取和写入 = 2.00 美元	2.00 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
亚马逊 CloudWatch -指标	0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元* (300 * 3/1,000) 看跌期权指标API调用 = 0.01 美元	2.11 美元
Amazon CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
亚马逊 CloudWatch — 警报	0.10 美元 * 3 个警报 = 0.30 美元	0.30 美元
总计		21.17 美元

示例 2：每月修复 3,000 次

- 100 个账户，1 个区域
- 每次 30 次修复 account/Region/month
- 每月总花费 134.86 美元

服务	假设	月度费用 [USD]
AWS Systems Manager 自动化	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	3,000 次补救 * 0.000002 美元 = 0.006 美元 0.006 * 0.03 = 0.00018 美元	< 0.01 美元
AWS Lambda -请求	3,000 次补救 * 6 次请求 = 18,000 次请求 0.20 * 1,000,000 个请求 = 0.20 美元	0.20 美元
AWS Lambda -持续时间	2.56M：1.875 GB 秒 * 3,000 次修复 * 0.000167 美元 = 0.09375 美元	0.09 美元
AWS Step Functions	17 个状态转换 * 3,000 次修复 = 51,000 0.025 美元 * (51,000/1,000) 状态转换 = 1.275 美元	1.28 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	100 USD
Amazon DynamoDB	2.00 * 1,000,000 次读取和写入 = 2.00 美元	2.00 美元

服务	假设	月度费用 [USD]
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
亚马逊 CloudWatch -指标	0.30 美元 * 7 个自定义指标 = 2.10 美元 0.01 美元* (3000 * 3/1,000) 看跌期权指标API调用 = 0.09 美元	2.19 美元
Amazon CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
亚马逊 CloudWatch — 警报	0.10 美元 * 3 个警报 = 0.30 美元	0.30 美元
总计		134.86 美元

示例 3：每月修复 30,000 次

- 1,000 个账户，1 个区域
- 每次 30 次修复 account/Region/month
- 每月总费用为1,281.01美元

服务	假设	月度费用 [USD]
AWS Systems Manager 自动化	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	月度费用 [USD]
AWS Security Hub	未使用任何可计费的服务	$0
Amazon CloudWatch 日志	30,000 次补救 * 0.000002 美元 = 0.06 美元 0.06 * 0.03 = 0.0018 美元	< 0.01 美元
AWS Lambda -请求	30,000 次补救 * 6 次请求 = 180,000 次请求 0.20 * 1,000,000 个请求 = 0.20 美元	0.20 美元
AWS Lambda -持续时间	2.56 亿：1.875 GB 秒 * 30,000 次修复 * 0.000167 美元 = 0.9375 美元	0.94 美元
AWS Step Functions	17 个状态转换 * 30,000 次修复 = 510,000 0.025 美元 * (510,000/1,000) 状态转换 = 12.75 美元	12.75 美元
亚马逊 EventBridge 规则	规则不收费	$0
AWS Key Management Service	1 个密钥 * 1,000 个账户 * 1 个区域 * $1 = 1,000 美元	1,000 美元
Amazon DynamoDB	0.000002 * 1,000,000 次读取和写入 = 2.00 美元	2.00 美元
Amazon SQS	0.000004 * 1,000,000 个请求 = 0.40 美元	0.40 美元
Amazon SNS	0.000005 * 1,000,000 个通知 = 0.50 美元	0.50 美元

服务	假设	月度费用 [USD]
亚马逊 CloudWatch -指标	0.30 美元 * 6 个自定义指标 = 1.80 美元 0.01 美元* (30,000 * 3/1,000) 看跌期权指标看涨期权 = 0. API 90 美元	2.70 美元
Amazon CloudWatch -控制面板	3.00 美元 * 1 个仪表板 = 3.00 美元	3.00 美元
亚马逊 CloudWatch — 警报	0.10 美元 * 2 个警报 = 0.20 美元	0.20 美元
Amazon CloudWatch — 应用程序见解	0.10 美元 * 40 个警报（最大值）= 4.00 美元 0.53 美元* 10 GB 日志数据（估计值）= 5.30 美元 0.00267 * 5 OpsItems（估计值）= ~0.01 美元	9.31 美元
总计		1,281.01 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	月度费用 [USD]
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	月度费用 [USD]
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 0.0625 美元 + 0.03 美元 = Lambda 总成本 0.0952 美元	0.0925 美元

服务	假设	月度费用 [USD]
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，AWS 和您共同分担安全责任。这种共享模式减轻了您的运营负担，因为您可以AWS操作、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。

IAM 角色

AWSIdentity and Access Management (IAM) 角色允许客户为AWS云中的服务和用户分配精细的访问策略和权限。此解决方案创建的IAM角色授予解决方案的自动功能访问权限，以便在特定于每项修复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-SHARR-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。每个修正角色都允许成员角色将其传递给 S AWS ystems 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-R emoveVPCDefault SecurityGroupRules 是 ASR-R emoveVPCDefault SecurityGroupRules 修复运行手册的角色。

支持 AWS 区域

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

区域名称	区域代码
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
Asia Pacific (Seoul)	ap-northeast-2
亚太地区（新加坡）	ap-southeast-1
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 (UAE)	me-central-1

区域名称	区域代码
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-east-2
中国（北京）	cn-north-1
中国（宁夏）	cn-northwest-1

限额

服务限额（也称为限制）是 AWS 账户使用的服务资源或操作的最大数量。

此解决方案中的 AWS 服务的限额

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 service quotas。

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PDF改为查看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。

亚马逊 EventBridge 规定配额

您的AWS账户有 Amazon EventBridge 规则配额，在选择要与解决方案一起部署的行动手册时，您应该注意这些配额。每个攻略手册都将为它可以修复的每个控件创建一个 EventBridge 规则。部署多个剧本时，可以达到规则的配额。有关更多信息，请参阅《亚马逊 EventBridge 用户指南》中的亚马逊 EventBridge 配额。

AWSSecurity Hub 部署

AWSSecurity Hub 的部署和配置是此解决方案的先决条件。有关设置 Sec AWS urity Hub 的更多信息，请参阅 Sec AWSurity Hub 用户指南中的设置AWS安全中心。

至少，您的主账户中必须配置一个可以正常运行的 Security Hub。您可以在与 Security Hub 主账户相同的账户（和AWS区域）中部署此解决方案。在每个 Security Hub 主账户和辅助账户中，您还必须部署成员模板，该模板允许解决方案的 AWS Step Functions AssumeRole 权限在该账户中运行补救运行手册。

堆栈与 StackSets 部署

堆栈集允许您使用单个 AWS CloudFormation 模板在跨 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，尤其是使用多账户的客户 AWS Organizations，可以受益于使用堆栈集在多个账户中进行部署。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。

此解决方案使用 AWS CloudFormation 模板和堆栈来实现自动部署。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：用于修正的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。

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。

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。

管理员堆栈在部署成员堆栈之前必须先完成部署，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管理堆栈的 Security Hub 委托ASR管理员帐户。自动化文档必须在成员账户中执行，才能使用免费套餐进行SSM自动化。

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局资源（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发现，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《SecAWSurity 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 AWSFSBP）部署管理员或成员嵌套堆栈。

AWS CloudFormation 模板

View template

aws-sharr-deploy.template-使用此模板启动AWS解决方案的自动安全响应。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 Key Management Service、Amazon CloudWatch Logs AWS Identity and Access Management AWS Lambda AWS Step Functions、Amazon S3 和 S AWS ystems Manager。

管理员账号支持

以下模板安装在 Sec AWS urity Hub 管理员帐户中，用于启用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`aws-sharr-deploy.template`。

aws-sharr-orchestrator-log.templ ate-为 Orchestrator Step Function 创建 CloudWatch 日志组。

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

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

CIS140stack.Template-CIS 亚马逊 Web Services Foundations 基准测试，v1.4.0 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-SC v2.0.0 规则。

成员账户

aws-sharr-member.templat e-设置核心解决方案后，使用此模板在每个 Sec AWS urity Hub 成员账户（包括管理员账户）中安装 S AWS ystems 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`aws-sharr-member.template`安装以下模板：

aws-sharr-remediations.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。

PCI321MemberStack.templat DSS e PCI--v3.2.1 设置、权限和补救运行手册。

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。

成员角色

aws-sharr-member-roles.template-定义每个 AWS Security Hub 成员账户所需的修正角色。

票务系统集成

使用以下模板之一与您的票务系统集成。

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中 AWS Organizations。

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

AWSOr ganizations 可帮助您集中管理和治理您的多账户AWS环境和资源。 StackSets 最适合与 Organiz AWS ations

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 Sec AWS urity Hub 部署：

- 您的AWS组织中必须有一个委托的 Security Hub 管理员帐户。
- 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 Sec AWS ur ity Hub 用户指南中的跨区域汇总结果。
- 您应该在每个可用区域为组织激活 Security Hu AWS b。

此过程假设您有多个使用 Organizati AWS ons 的账户，并且已经委托了一个 AWS Organizations 管理员帐户和一个 S AWS ecurity Hub 管理员帐户。

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。

使用您的委托管理员账户部署 AWS Organizations。 StackSets

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）。

步骤 1：在委派的 Security Hub 管理员账户中启动管理堆栈

- 使用自我管理模式 StackSet，将`aws-sharr-deploy.template`AWS CloudFormation 模板启动到与您的 S AWS ecurity Hub 管理员位于同一区域的 Security Hub 管理员帐户。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-SHARR-Orchestrator`已经存在，请选择此选项。

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

步骤 2：将修正角色安装到每个 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`aws-sharr-member-roles.template` AWS CloudFormation 模板启动到您的 AWS Organizations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。

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

- 使用自我管理 StackSets，将`aws-sharr-member.template`AWS CloudFormation 模板启动到所有区域，在这些区域中，您的AWS组织中的每个账户都有由同一 Security Hub 管理员管理的AWS资源。

> **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。

（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。

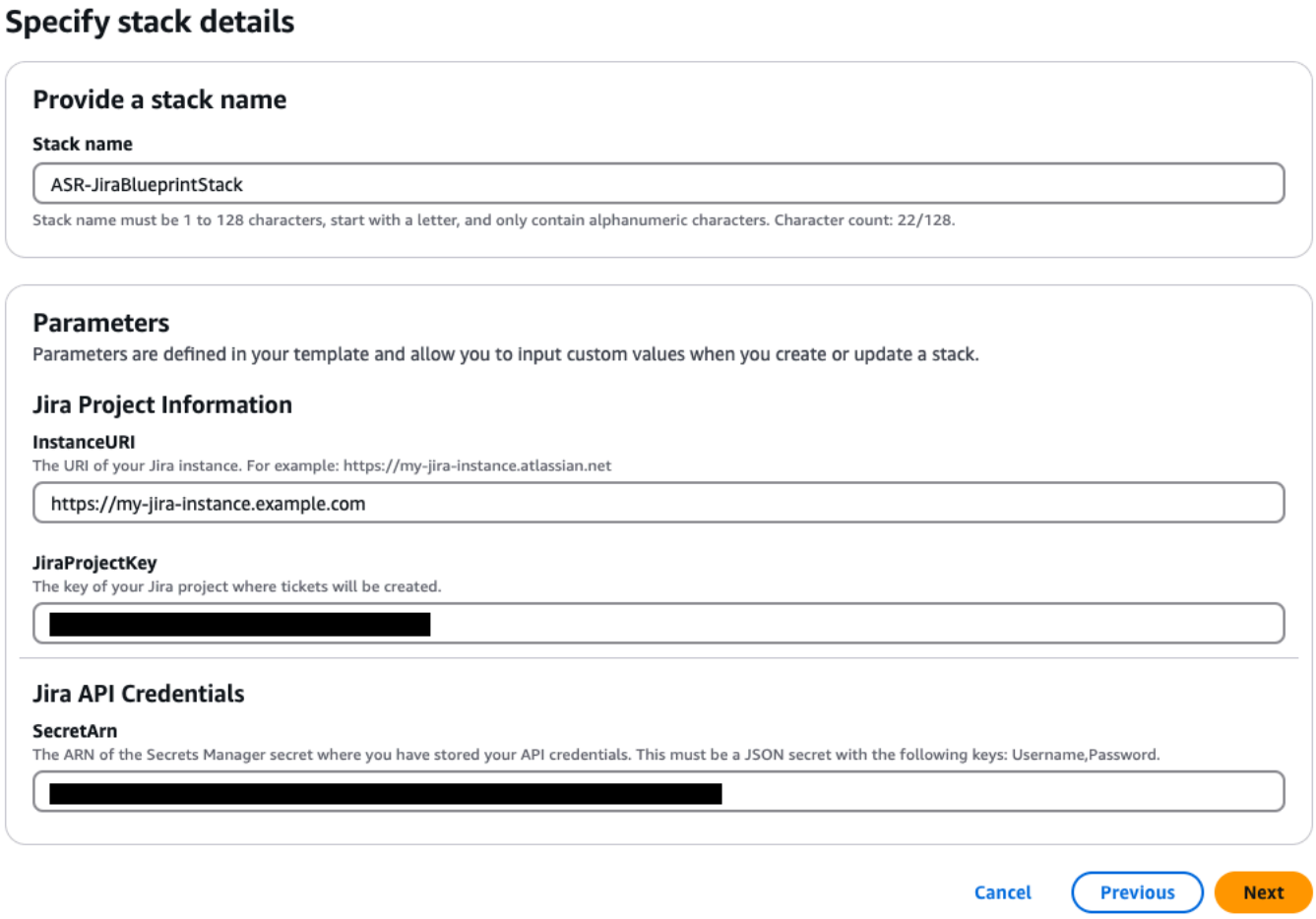
b. 将提供URI给您的 Jira 实例。

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`Password`为。

e. 将此密钥ARN的作为输入添加到堆栈中。



要部署 ServiceNow 堆栈，请执行以下操作：

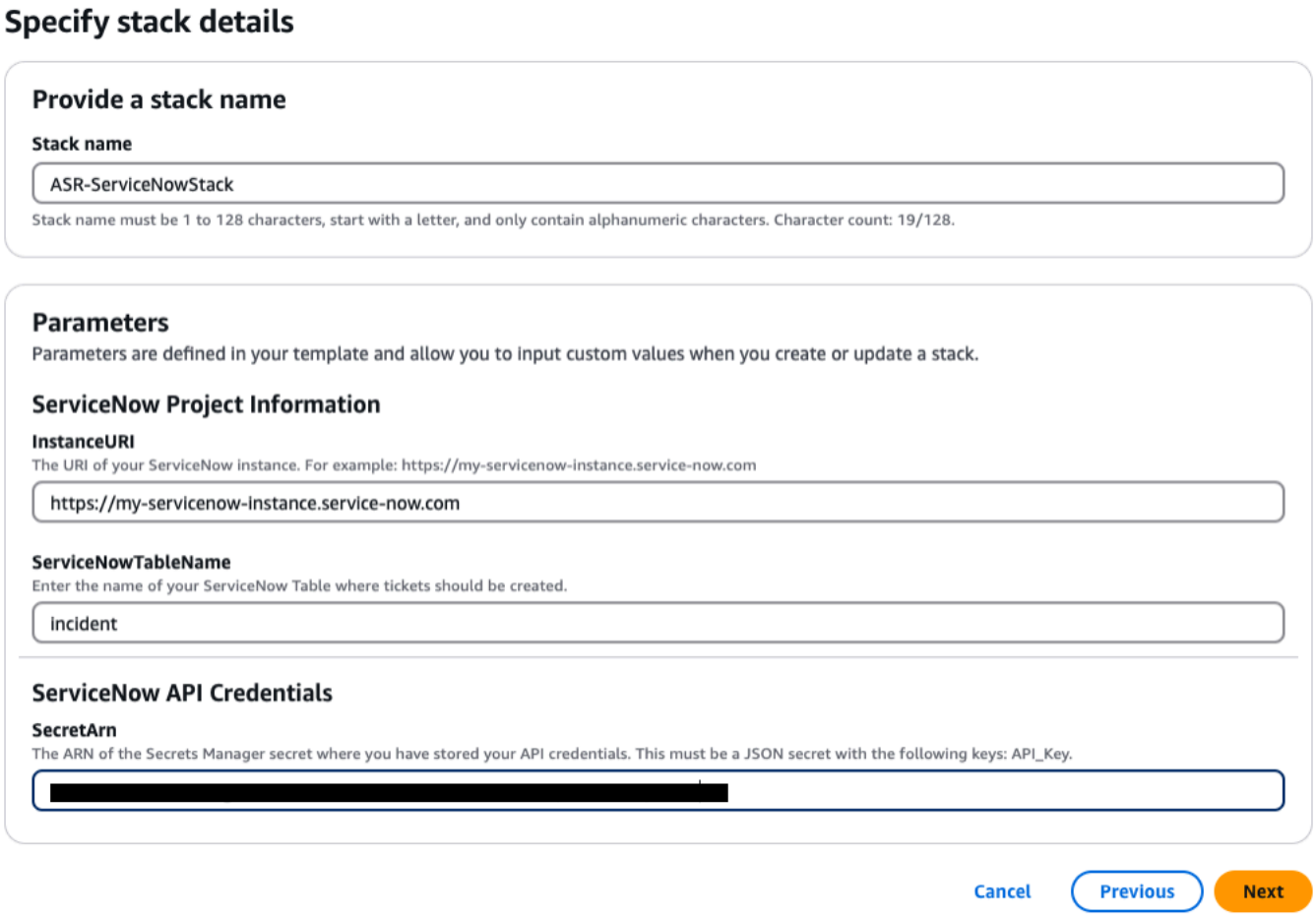
a. 输入堆栈的名称。

b. 提供您的 ServiceNow 实例的。URI

c. 提供您的 ServiceNow 表名。

d. 在中创建一个API密钥，该密钥 ServiceNow 具有修改您要写入的表的权限。

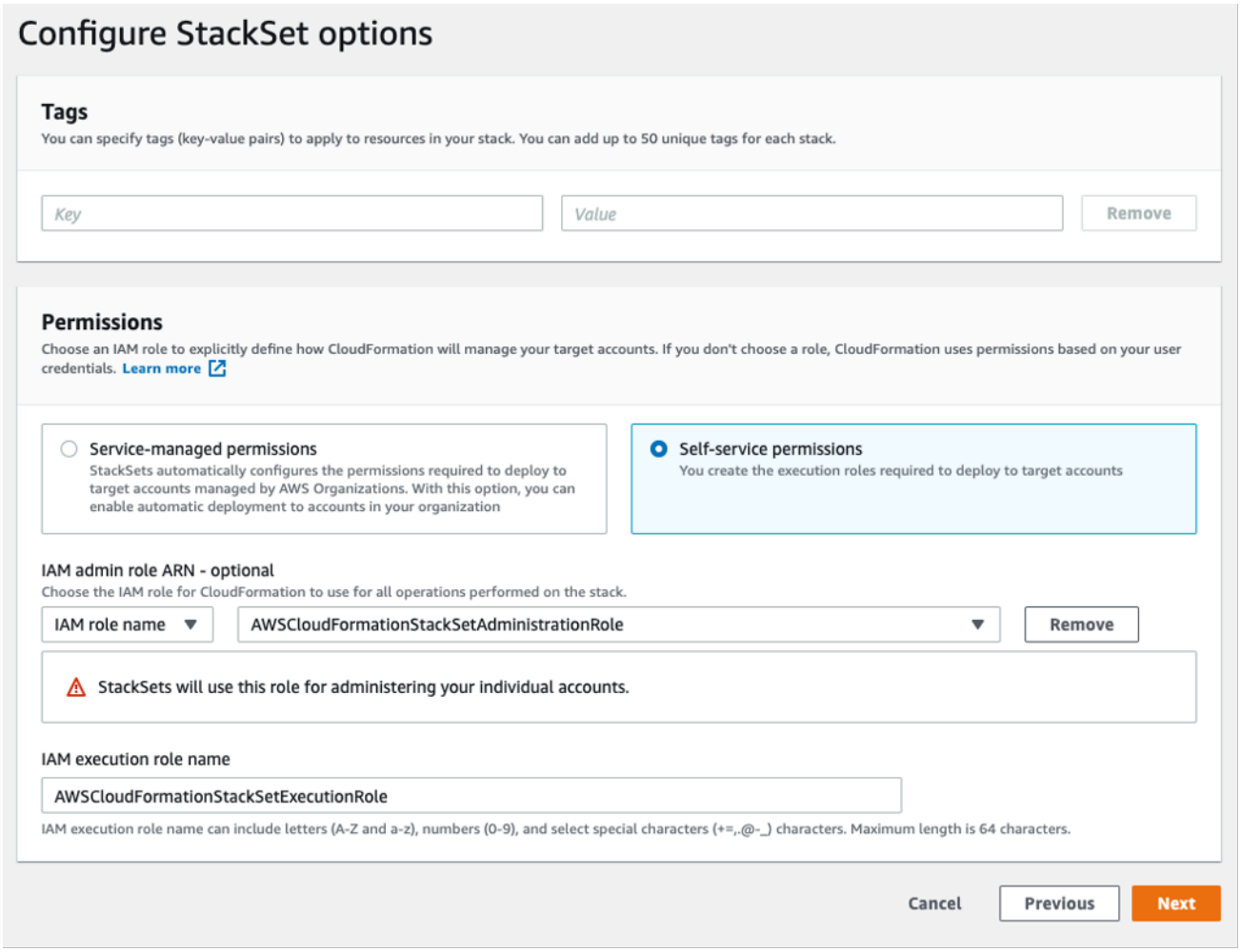
e. 在 Secrets Manager 中使用密钥创建密钥，`API_Key`并将该密钥ARN作为输入提供给堆栈。



创建自定义集成堆栈：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 `aws-sharr-deploy.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。



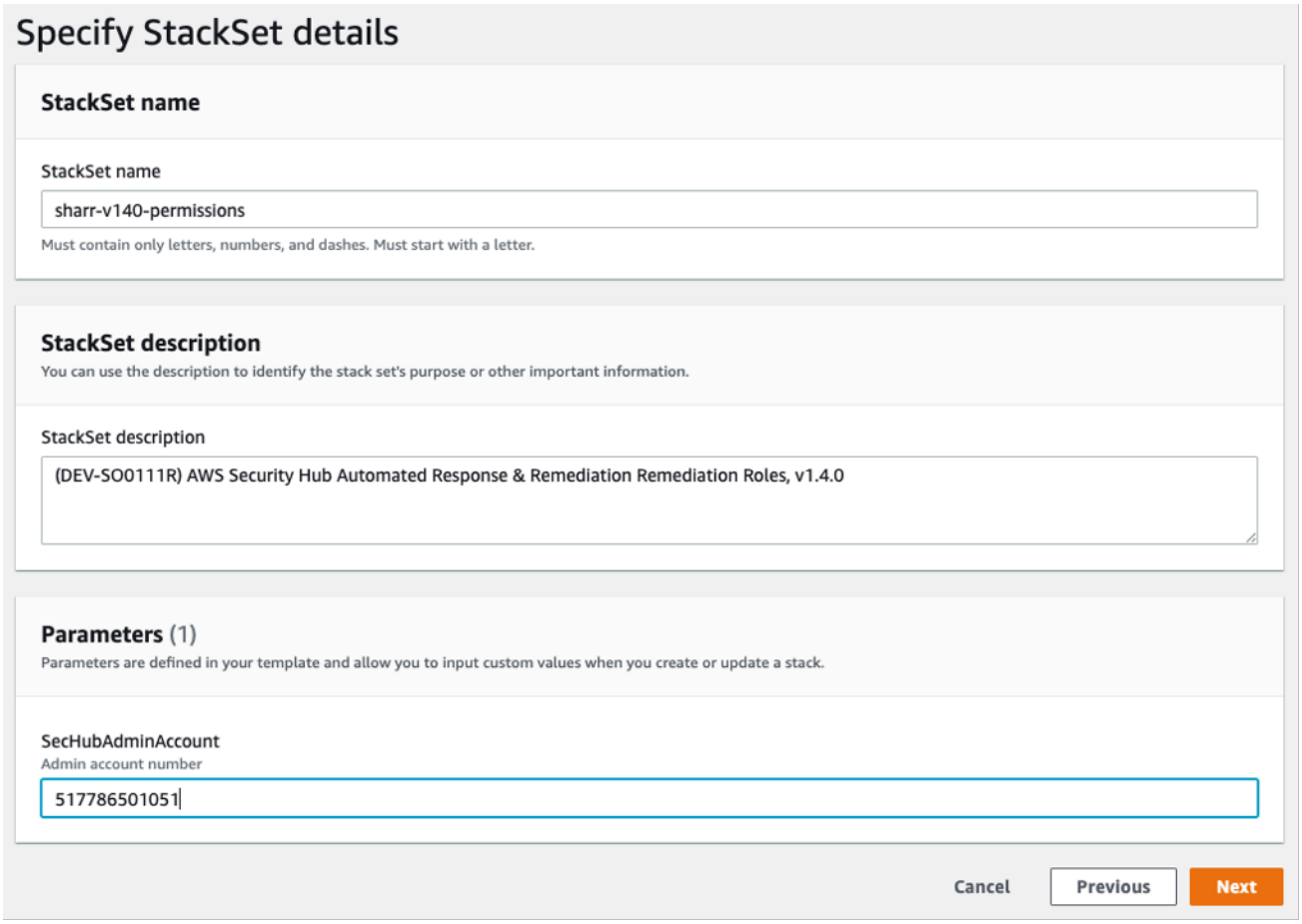
配置 StackSet 选项

2. 在账号参数中，输入 Sec AWS urity Hub 管理员账户的账户 ID。
3. 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。

步骤 2：将补救角色安装到每个 Sec AWS urity Hub 成员账户中

使用服务管理 StackSets 部署成员角色模板。`aws-sharr-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 SHARR Orchestrator 步骤函数进行跨账户API调用的全局角色。

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 Organization AWS s 中的新账户就会获得这些权限。
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

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

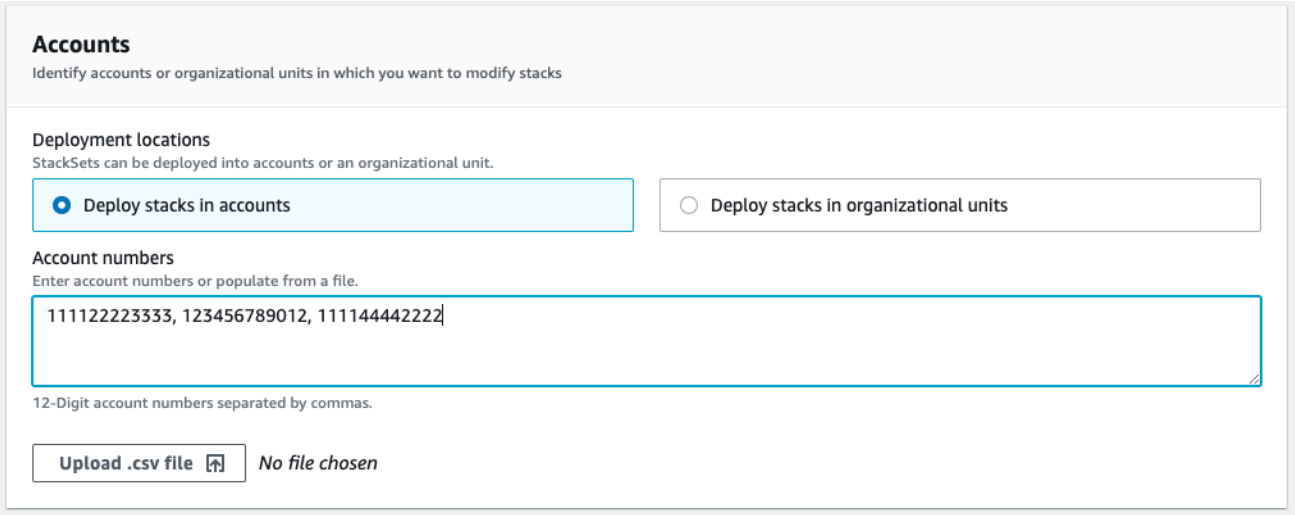
由于成员堆栈使用嵌套堆栈，因此您必须部署为自 StackSet管理堆栈。这不支持自动部署到本AWS组织的新账户。

参数

LogGroup 配置：选择接收日志的 CloudTrail 日志组。如果不存在日志组，或者每个账户的日志组不同，请选择一个方便的值。在为日志创建 CloudWatch 日志组后，账户管理员必须更新 Systems Manager — Parameter Store /Solutions/SO0111/Metrics _ LogGroupName 参数。 CloudTrail 这是为API呼叫创建指标警报的补救措施所必需的。

标准：选择要加载到成员账户的标准。这只会安装 S AWS ystems Manager 运行手册，而不会启用安全标准。

SecHubAdminAccount：输入安装解决方案管理模板的 Sec AWS urity Hub 管理员账户的账户 ID。



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 该解决方案与您的主账户和次要账户位于同一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

使用以下步骤在上部署此解决方案AWS。

（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`aws-sharr-deploy.template` AWS CloudFormation 模板启动到您的 AWS Security Hub 管理员帐户。
- 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-SHARR-Orchestrator`已存在，请选择）。

步骤 2：将修正角色安装到每个 AWS Security Hub 成员账户中

- 将`aws-sharr-member-roles.template` AWS CloudFormation 模板启动到每个成员账户的一个区域。
- 为 AWS Security Hub 管理员帐户输入 12 位数的账户 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。

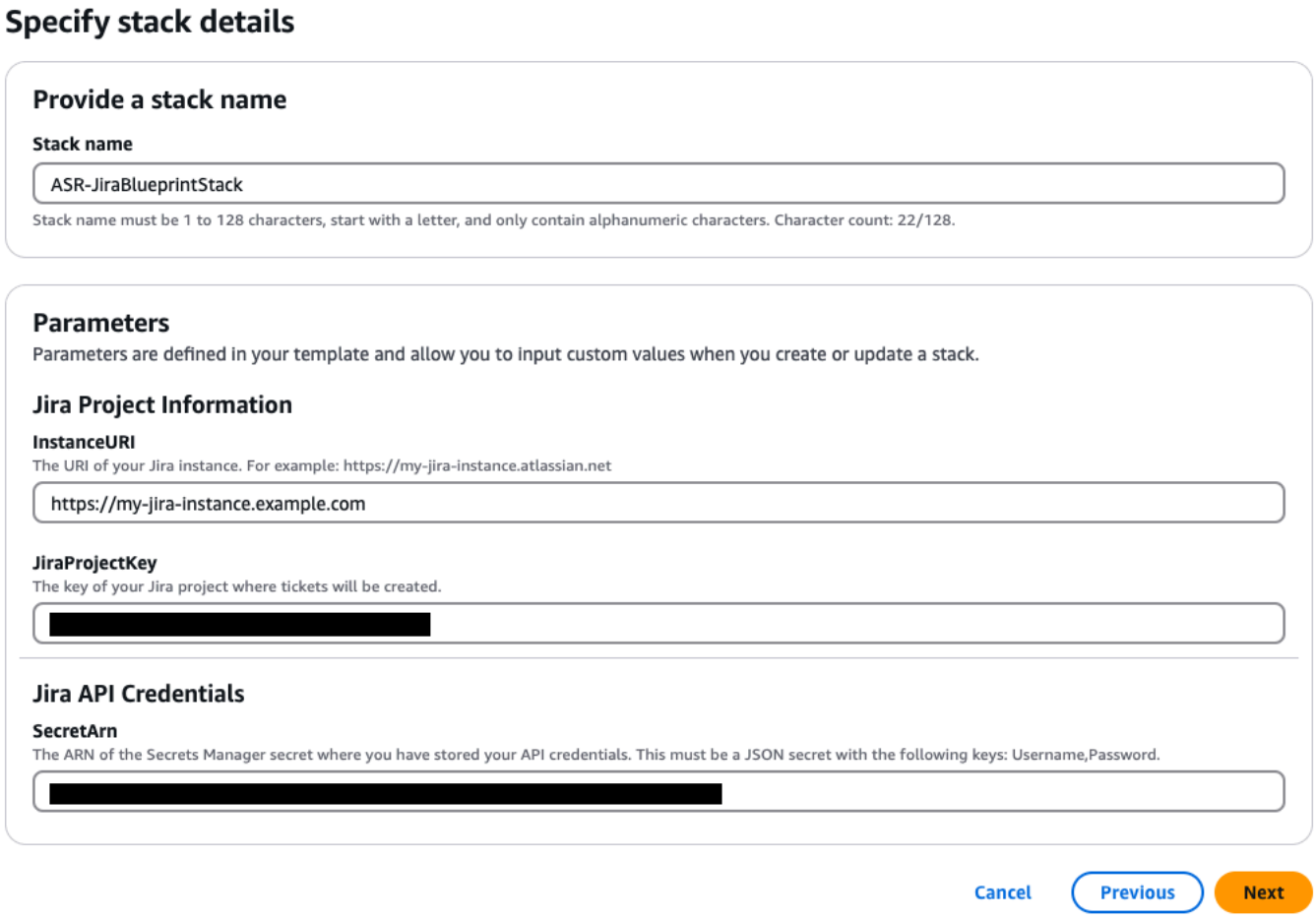
b. 将提供URI给您的 Jira 实例。

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`Password`为。

e. 将此密钥ARN的作为输入添加到堆栈中。



要部署 ServiceNow 堆栈，请执行以下操作：

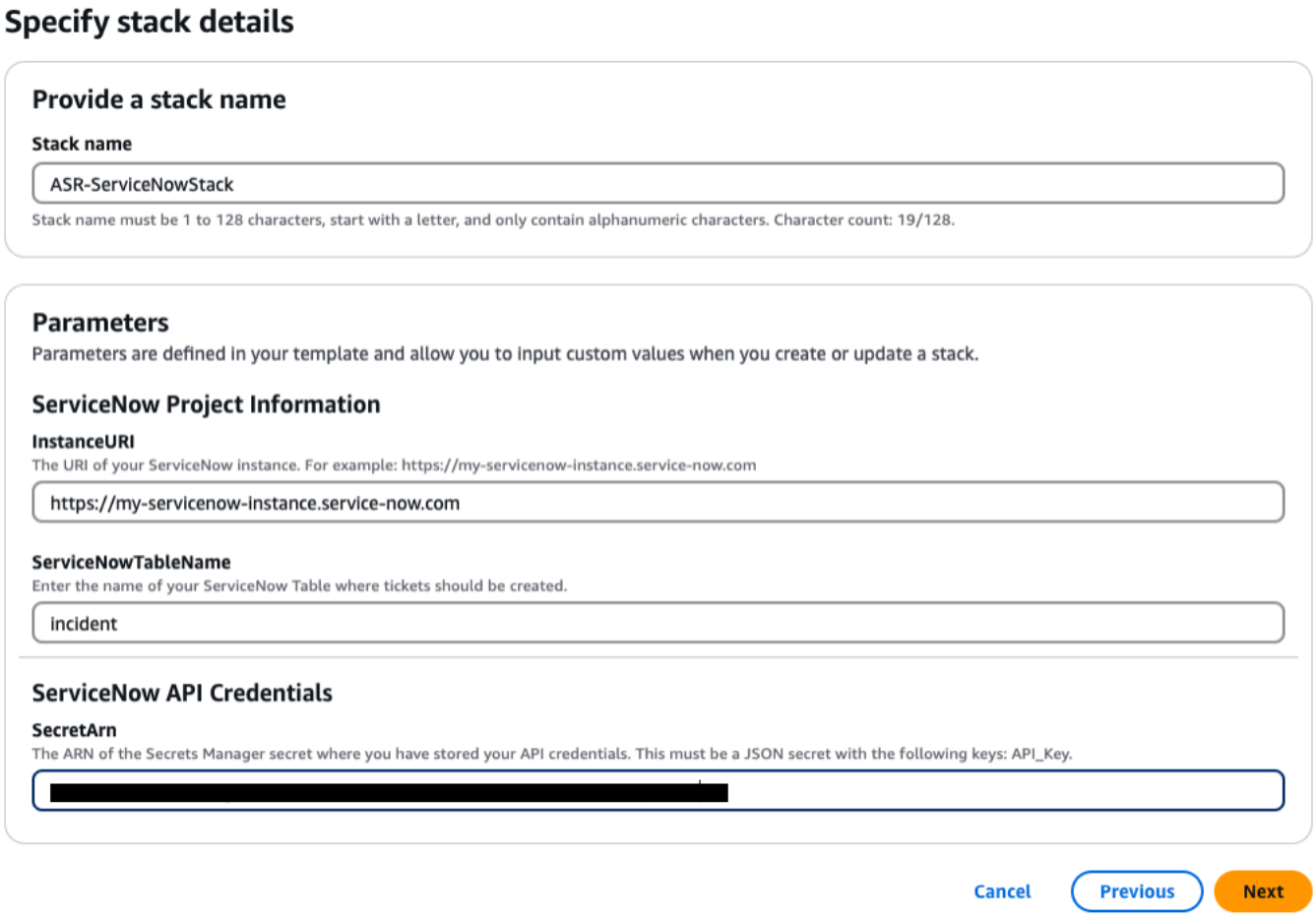
a. 输入堆栈的名称。

b. 提供您的 ServiceNow 实例的。URI

c. 提供您的 ServiceNow 表名。

d. 在中创建一个API密钥，该密钥 ServiceNow 具有修改您要写入的表的权限。

e. 在 Secrets Manager 中使用密钥创建密钥，`API_Key`并将该密钥ARN作为输入提供给堆栈。



创建自定义集成堆栈：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**
>
> 该解决方案中包含向 AWS 发送匿名运营指标的选项。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。通过这种调查收集的数据归 AWS 所有。数据收集受 AWS 隐私声明的约束。
> 要选择退出此功能，请下载模板，修改 AWS CloudFormation 映射部分，然后使用 AWS CloudFormation 控制台上传模板并部署解决方案。有关更多信息，请参阅本指南的匿名数据收集部分。

此自动 AWS CloudFormation 模板在AWS云端AWS解决方案上部署自动安全响应。在启动堆栈之前，必须启用 Security Hub 并完成先决条件。

> **Note**
>
> 您需要承担运行此解决方案时使用的 AWS 服务的费用。有关更多详细信息，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 Management Console 的 AWS Security Hub 账户登录，然后使用下面的按钮启动`aws-sharr-deploy.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。要在其他AWS地区启动此解决方案，请使用 AWS Management Console 导航栏中的区域选择器。

   > **Note**
   >
   > 此解决方案使用 AWS Systems Manager 目前仅在特定 AWS 地区可用的解决方案。该解决方案适用于所有支持该服务的地区。要了解按区域划分的最新可用情况，请参阅 AWS 区域服务列表。
3. 在创建堆栈页面上，验证 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，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	指定是否安装管理组件以自动修复FSBP控件。
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	指定是否安装管理组件以自动修复NIST控件。
重用 Orchestrator 日志组	no	选择是否重复使用现有的SO0111-SHARR-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。如果您要从 v1.2 或更高版本升级，请选择yes。
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

参数	默认值	描述
		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）。
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

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 15 分钟后收到 CREATE _ COMPLETE 状态。

步骤 2：将补救角色安装到每个 Sec AWS urity Hub 成员账户中

每个成员账户`aws-sharr-member-roles.template` StackSet 只能部署在一个区域。它定义了允许通过 SHARR 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`aws-sharr-member-roles.template` AWS CloudFormation 模板。您也可以下载模板作为自己实施的起点。

Launch solution

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。要在其他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，验证 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《Identity an IAM d Access Managem AWS ent 用户指南》中的和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。此字符串成为IAM角色名称的一部分。对成员堆栈部署和成员角色堆栈部署使用相同的值。
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

参数	默认值	描述
		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 分钟后收到 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**
>
> 该解决方案中包含向 AWS 发送匿名运营指标的选项。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。通过这种调查收集的数据归 AWS 所有。数据收集受AWS隐私政策的约束。
> 要选择退出此功能，请下载模板，修改 AWS CloudFormation 映射部分，然后使用 AWS CloudFormation 控制台上传模板并部署解决方案。有关更多信息，请参阅本指南的 “运营指标收集” 部分。

`aws-sharr-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. AWS Management Console 针对每个 AWS Security Hub 成员帐户（包括管理员帐户，该帐户也是成员）登录。选择按钮启动`aws-sharr-member.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。要在其他AWS地区启动此解决方案，请使用 AWS Management Console 导航栏中的区域选择器。

> **Note**
>
> 该解决方案使用 AWS Systems Manager，目前在大多数 AWS 地区都可用。该解决方案适用于所有支持这些服务的地区。要了解按区域划分的最新可用情况，请参阅 AWS 区域服务列表。

3. 在创建堆栈页面上，验证 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
提供用于创建指标筛选器和警报的名称 LogGroup	*<Requires input>*	指定用于 CloudWatch CloudTrail 记录API呼叫的 Logs 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	指定是否安装成员组件以自动修复FSBP控件。
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	指定是否安装成员组件以自动修复 CIS3 00 控件。
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。

参数	默认值	描述
加载NIST成员堆栈	no	指定是否安装成员组件以自动修复NIST控件。
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《用户指南》中的 Redshift.4 补救措施。AWS Security Hub
Sec Hub 管理员账户	*<Requires input>*	输入 Sec AWS urity 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。此字符串将成为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。对于一般用途 S3 存储桶，此字符串必须遵守 Amazon S3 命名规则。
EnableCloudTrailFo rASRActionLog	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。要了解由此产生的额外成本，请参阅 “成本” 部分。

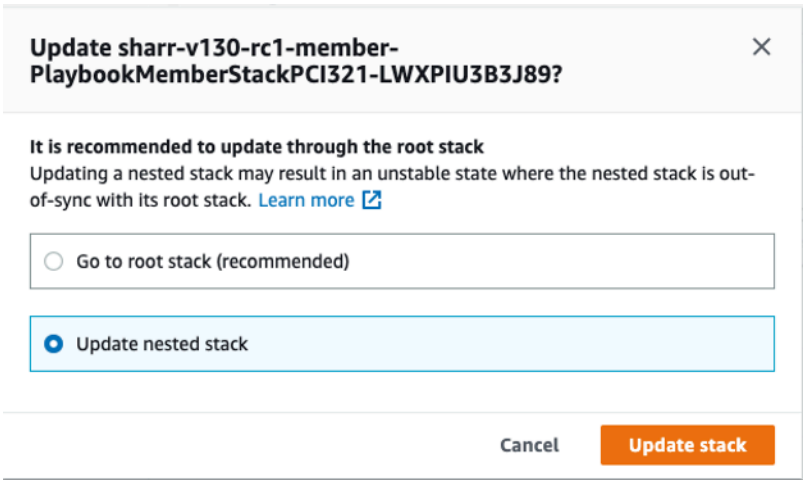
6. 在配置堆栈选项页面上，请选择下一步。
7. 在 Review 页面上，审核并确认设置。选中确认模板将创建 AWS Identity and Access Management (IAM) 资源的复选框。
8. 选择 Create stack（创建堆栈）以部署堆栈。

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 15 分钟后收到 CREATE _ COMPLETE 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AWS 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。您将在大约 15 分钟后收到 CREATE _ COMPLETE 状态。

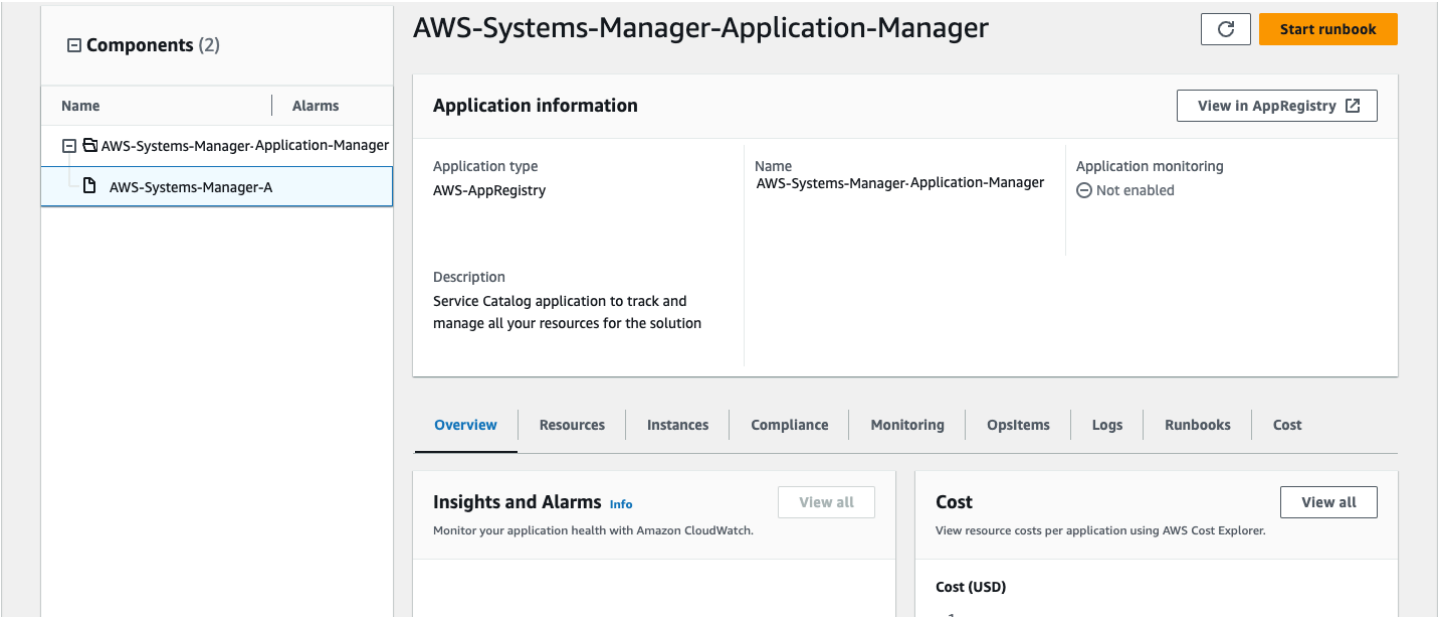
使用 Service Catalog 监控解决方案 AppRegistry

此解决方案包括服务目录 AppRegistry 资源，用于在 Service Catalog 和 S AWS ystems Manager Appl icat ion Manager 应用程序管理器中将 CloudFormation 模板 AppRegistry和底层资源注册为应用程序。

AWS Systems Manager Application Manager 为您提供了此解决方案及其资源的应用程序级视图，因此您可以：

- 从中心位置监控其资源、跨堆栈部署的资源的成本以及与此解决方案相关的日志。 AWS 账户
- 在应用程序环境中查看此解决方案资源的操作数据（例如部署状态、 CloudWatch 警报、资源配置和操作问题）。

  下图描述了 Application Manager 中解决方案堆栈的应用程序视图示例。



应用程序管理器中的解决方案堆栈

使用 “ CloudWatch 应用程序见解”

部署后，该解决方案会自动与 “ CloudWatch 应用程序见解” 集成。 CloudWatch Application Insights 通过以下方式帮助您查看和了解解决方案的运行状况和性能：

- 自动发现和监控关键应用程序资源。

- 创建自定义警报以主动识别潜在问题。
- 检测到异常或故障 OpsItems 时自动生成 Systems Manager。这些通知可 OpsItems 作为可操作的通知，及时通知您影响解决方案的问题。

按照以下步骤查看 App CloudWatch lication Insights 监控仪表板，您可以在其中查看解决方案的运行状况，并通过预先配置的仪表板和警报监控关键组件。

1. 导航至 CloudWatch 控制台。
2. 选择 “见解” 选项卡，然后选择 “应用程序见解”。
3. 选择应用程序选项卡，然后选择与解决方案关联的应用程序。

您也可以导入解决方案的 CloudWatch 控制面板，以整合对解决方案运行状况的监控。在 Application Insights 中解决方案的 “ CloudWatch 应用程序” 仪表板上，请按照以下步骤操作：

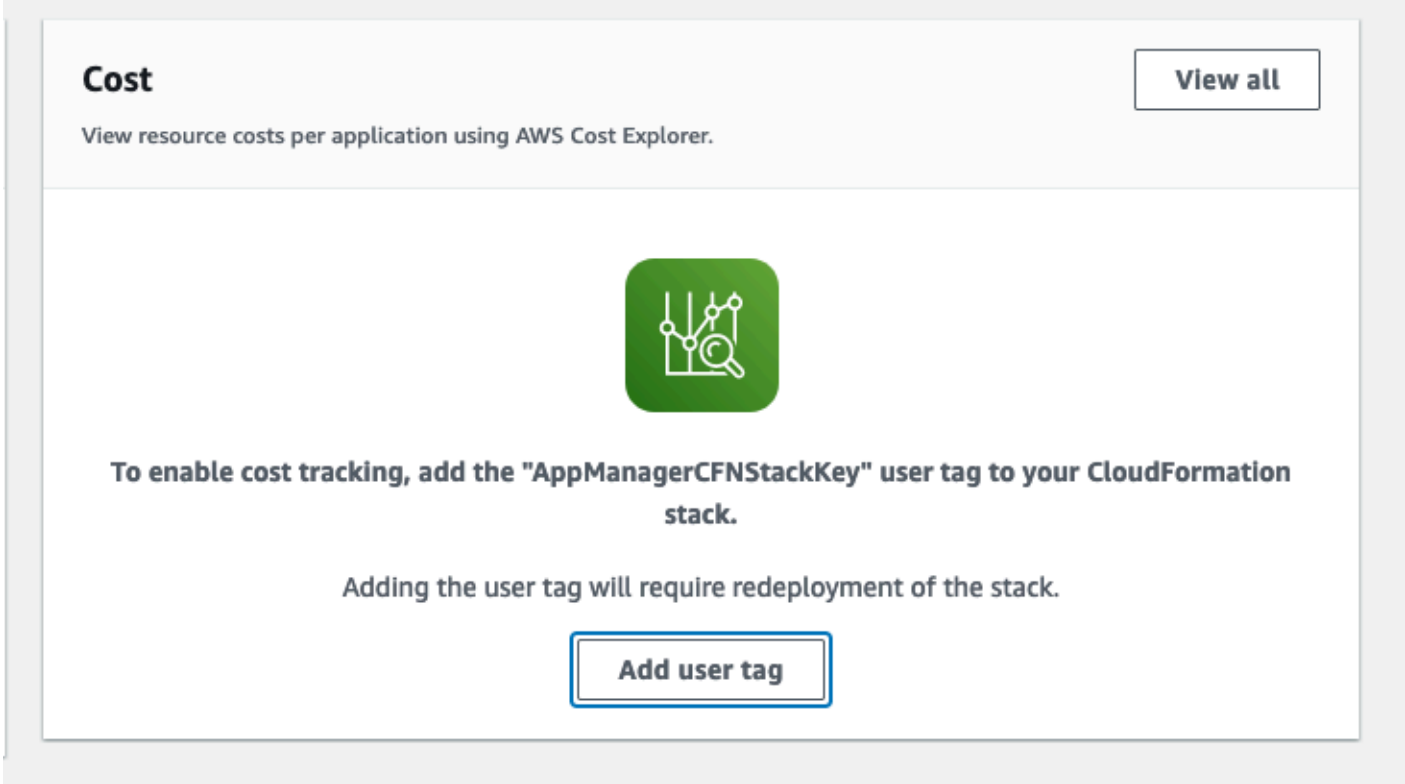
1. 选择 “自定义 CloudWatch 控制面板” 选项卡。
2. 选择 “导入 CloudWatch 控制面板”。
3. 在搜索框中`ASR-Remediation-Metrics-Dashboard`，输入并选择 AWS 仪表板上的自动安全响应。
4. 选择 Import（导入）。

现在，您可以在 App CloudWatch lication Insights 控制台中查看 App CloudWatch lication Insights 仪表板和解决方案的自定义仪表板，而无需在页面之间切换。

确认与此解决方案关联的成本标签

激活与此解决方案关联的成本分配标签后，您必须确认成本分配标签才能查看此解决方案的成本。要确认成本分配标签，请按以下步骤操作：

1. 登录 Systems Manager 控制台。
2. 在导航窗格中，选择 Application Manager。
3. 在应用程序中，选择此解决方案的应用程序名称并将其选中。
4. 在概览选项卡的成本中，选择添加用户标签。



5. 在添加用户标签页面上，输入 `confirm`，然后选择添加用户标签。

激活过程可能需要长达 24 小时才能完成，显示标签数据。

激活与此解决方案关联的成本分配标签

确认与此解决方案关联的成本标签后，必须激活成本分配标签才能查看此解决方案的成本。成本分配标签只能在组织的管理账户中激活。

要激活成本分配标签，请按以下步骤操作：

1. 登录AWS Billing and Cost Management 和成本管理控制台。
2. 在导航窗格中，选择成本分配标签。
3. 在成本分配标签页面上，筛选 `AppManagerCFNStackKey` 标签，然后从显示的结果中选择该标签。
4. 选择激活。

AWS Cost Explorer

通过与 Cost Explorer 集成，您可以在 Application Manager 控制台中查看与应用程序和应用程序组件相关AWS的成本概览。Cost Explorer 成本管理服务通过提供一段时间内的 AWS 资源成本和使用情况视图，帮助您管理成本。

1. 登录 AWS 成本管理控制台。
2. 在导航菜单中，选择 Cos t Explorer 以查看解决方案在一段时间内的成本和使用情况。

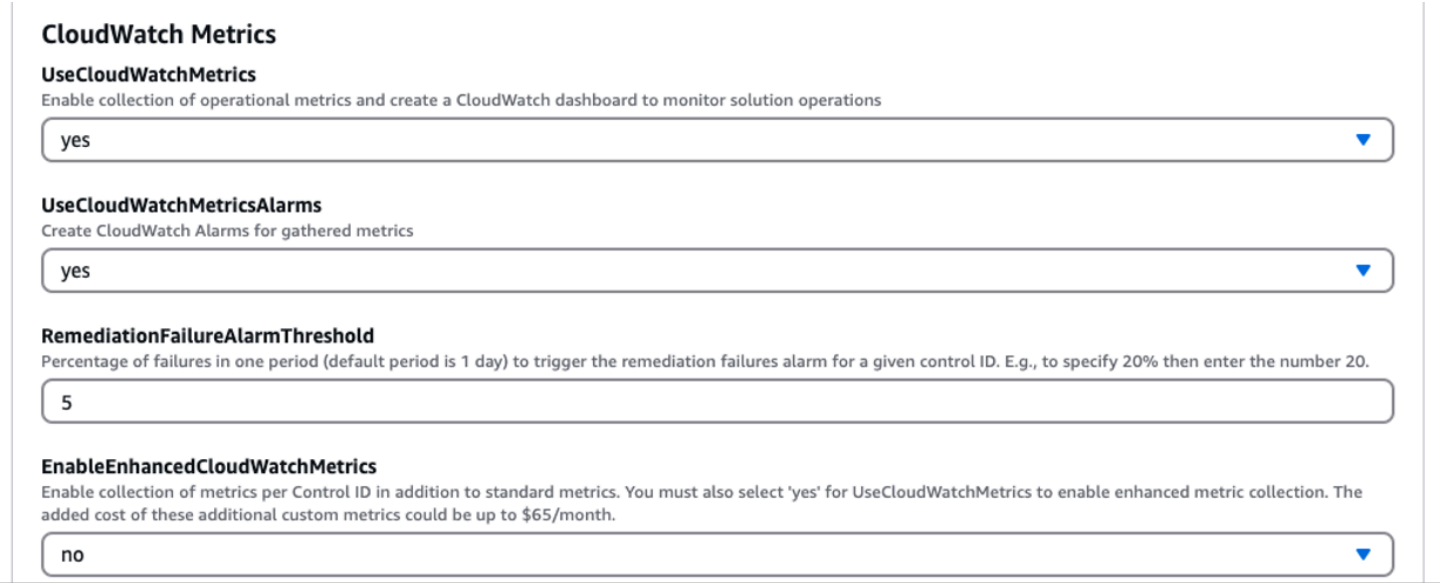
使用 Amazon CloudWatch 控制面板监控解决方案的运营

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

CloudWatch功能有四个 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。

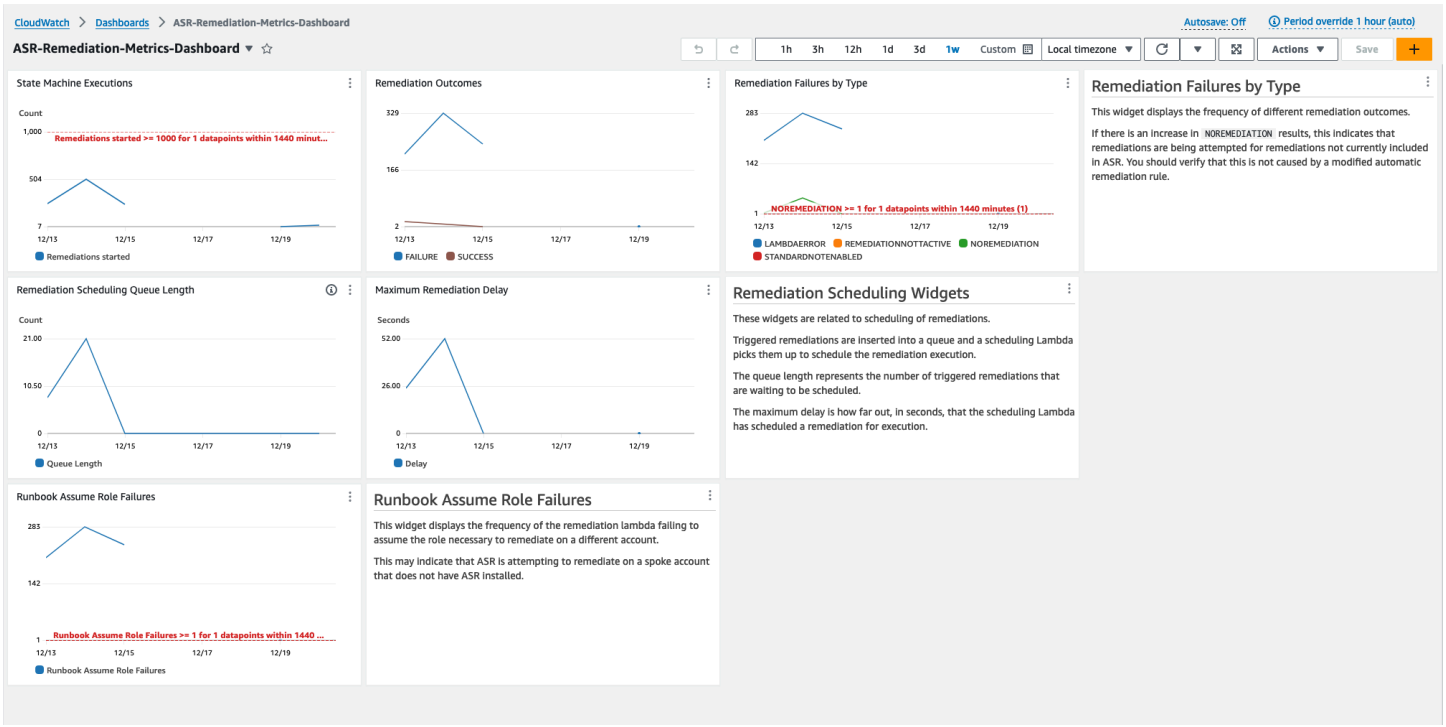
CloudWatch 仪表板包含以下部分：

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，则本节将按控件 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，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. Cloud Trail 管理操作依据 ASR-列出解决方案在部署时使用EnableCloudTrailForASRActionLog参数启用操作日志的所有成员账户的管理操作。当您观察到任何 AWS 账户中出现意外的资源变化时，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。

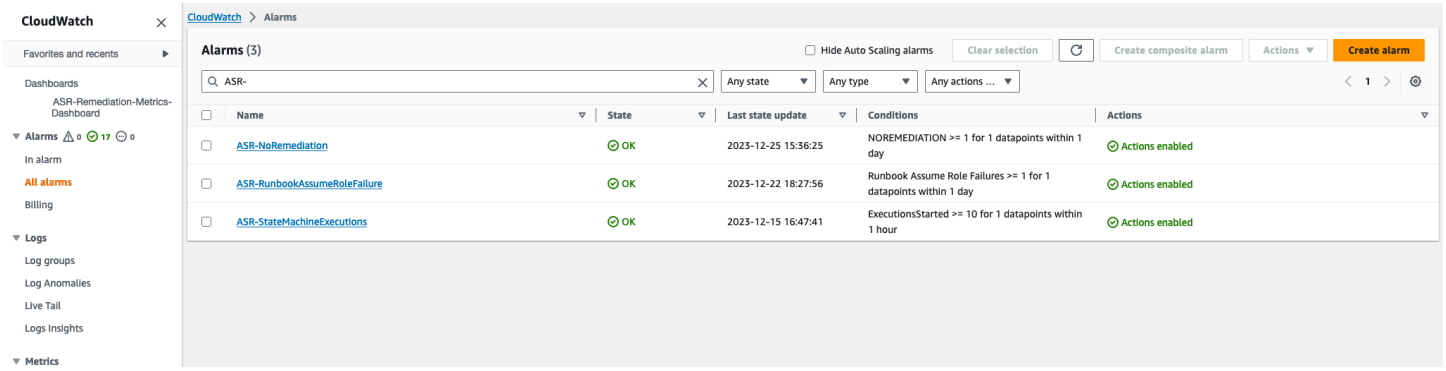
1. 在 24 小时内状态机执行次数 > 1000。
   a. 补救执行的大幅激增可能表明事件规则的启动频率高于预期。
   b. 可以使用 CloudFormation 参数更改阈值。
2. 按类型划分的修复失败 = NOREMEDIATION > 0
   a. 正在尝试对未包含在中的补救措施进行修正。ASR这可能表示事件规则已被修改，包含的补救措施超出了预期的范围。
3. 运行手册扮演角色失败 > 0
   a. 正在尝试对未正确部署解决方案的账户或区域进行补救。这可能表示已修改事件规则，使其包含的账户数量超出了预期的范围。

可以修改所有警报阈值以适应个人部署需求。

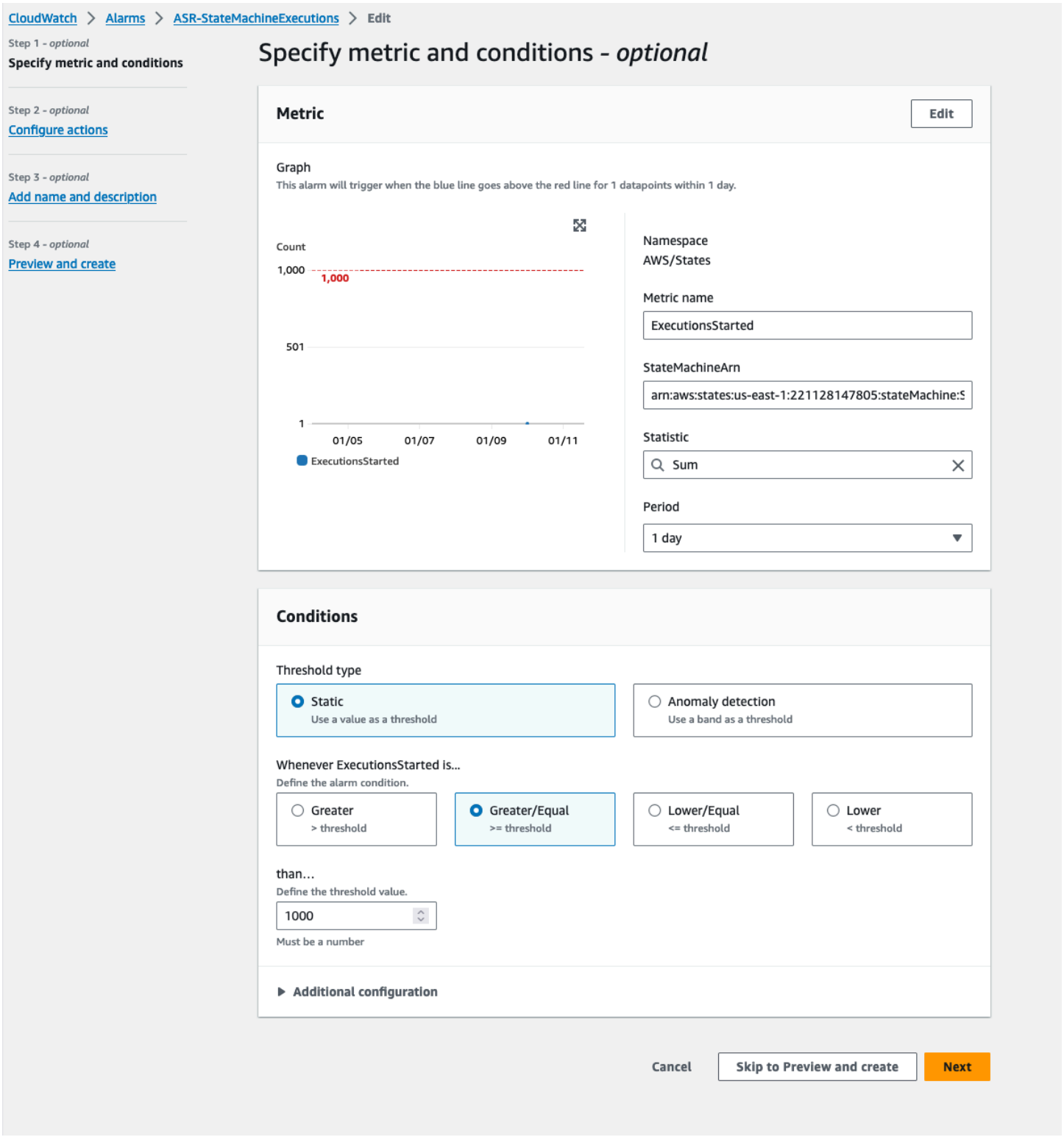


修改警报阈值

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。



3. 将阈值更改为所需的值并保存。



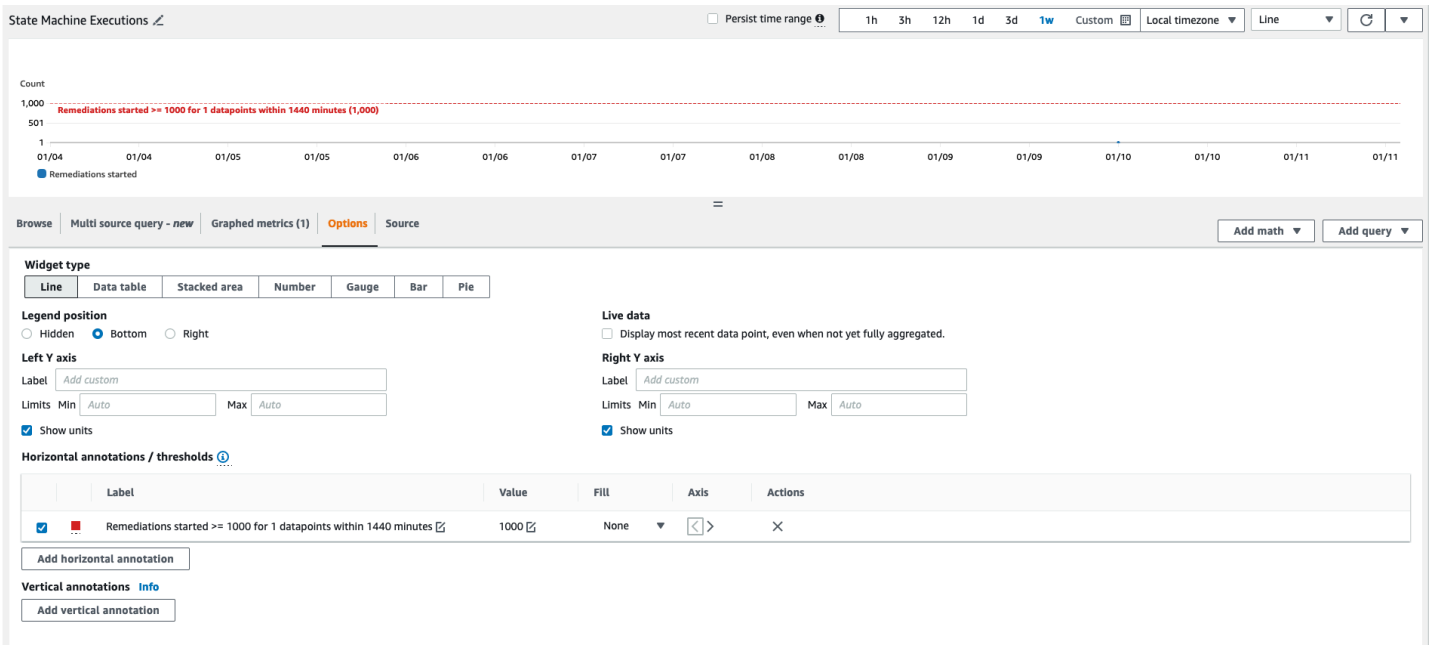
4. 导航到 CloudWatch 仪表板以修改那里的图表以匹配新设置。

   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亚马逊SNS主题 SO0111-ASR _Alarm_Topic。这将在警报进入ALARM状态时通知您。

更新此解决方案

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

故障排除

已知问题解决方案提供了缓解已知错误的说明。如果这些说明不能解决您的问题，Cont act S AWS u pport 会提供有关如何为该解决方案提交AWS支持案例的说明。

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。

此解决方案收集在下运行的修复运行手册的输出 AWS Systems Manager，并将结果记录到 AWS Security Hub 管理员帐户的 CloudWatch 日志组`SO0111-SHARR`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 Sec AWS urity Hub 管理员帐户中的`SO0111-SHARR-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AWSKMS客户经理密钥 (CMK) 进行加密。

以下疑难解答信息使用`SO0111-SHARR`日志组。使用此日志以及 S AWS ystems Manager 自动化控制台、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-SHARR`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SHARR运行手册。例如：SHARR-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，您必须登录成员帐户（来自上面的消息），转至，导航至“自动化”，然后检查执行 ID 的日志输

出eecdef79-9111-4532-921a-e098549f525。 AWS Management Console AWS Systems Manager

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。SHARR 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-SHARR-Orchestrator 立即在 “获取自动化文档” 状态下失败，并显示 502 错误：“由于访问被拒绝，Lambda 无法解密环境变量。KMS请检查该功能的KMS按键设置。KMS例外： 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-SHARR 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

Sec AWS urity 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 “我试图纠正发现但什么也没发生” 的解决方案。

- 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尝试修正发现SHARR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，因为录制器或传送渠道已经存在。

  解决方案：仔细检查您的 AWS Config 设置，确保 Config 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：

  1. 登录 Sec AWSurity 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SHARR修复”。
  5. 再次删除堆栈。

- 问题：重新部署管理堆栈后，步进功能失败。`AssumeRole`

  解决方案：重新部署管理员堆栈会中断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，CIS3.x 补救措施未显示。

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

特定补救措施存在问题

S etSSLBucket 策略因 AccessDenied 错误而失败

相关控件：AWSFSBPv1.0.0 S3.5、v3. PCI 2.1 PCI .s3.5、v1.4.0 2.1.2、SC v2.0.0 S3.5 CIS

问题：S etSSLBucket 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 （关联控件：AWSFSBPv1.0.0 S3.2、PCI v3.2.1 PCI .S3.2、v CIS 1.4.0 2.1.5.2、SC v2.0.0 S3.2）也可以将存储桶置于此状态，因为它可以在不更改存储桶策略的情况下设置公共访问阻止设置。

S etSSLBucket 策略在存储桶策略中添加了一条声明，用于拒绝不使用的请求SSL。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 FSBPv1.0.0 S3.6、 NIST.800-53.r5 CA-9 (1)、.800-53.r5 CM-2 NIST

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 SHARR _ _” CustomAction
4. 在规则上选择，然后选择 “禁用” 按钮。

联系我们 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. 附上处理请求 Support 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

使用以下步骤卸载解决方案 AWS Management Console。

V1.0.0-V1.2.1

对于 v1.0.0 到 v1.2.1 的版本，请使用 Service Catalog 卸载和/或 Playbook。CIS FSBP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. `aws-sharr-member.template`从每个成员账户中删除。
2. `aws-sharr-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 Sec AWSurity 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SHARR修复”。

5. 再次删除堆栈。

V1.4.0 及更高版本

堆栈部署

1. `aws-sharr-member.template`从每个成员账户中删除。
2. `aws-sharr-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`aws-sharr-member-roles.template`，中的IAM角色也会保留。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 日志记录或增强监控） CloudTrail 将其手动删除。RDS

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发现启动修复（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。如果你关AWSFSBP心的是 CIS v1.2.0，可以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 “NOT可用” 值以取消部署该控件运行手册。

SSM启用和禁用标准的参数：

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

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"
  }
}
```

修复成功时

```
{
  "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"
  }
}
```

使用解决方案

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：开启自动安全响应入门 AWS

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。

账户	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。此帐户还必须是您要纠正发现的所有账户的 Security Hub 委托管理员帐户，但它不必是，也不应是您的账户所属AWS组织的 Organizations 管理员帐户。AWS

启用 AWS Config

请查看以下文档：

- AWSConfig 文档
- AWSConfig 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 “包括全局资源（例如AWSIAM资源）” 选项。如果您在启用 AWS Config 时未选择此选项，则不会看到与全局资源（例如AWSIAM资源）相关的结果

账户	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：

- AWSSecurity Hub 文档
- AWSSecurity Hub 定价
- 启用 Sec AWS urity Hub

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

账户	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启用 Sec AWS urity Hub	启用 Sec AWS urity Hub
222222222222	成员	启用 Sec AWS urity Hub	启用 Sec AWS urity 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 Sec AWS urity 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行动手册而不是 SC（安全控制）。

在两个账户和两个区域中启用合并控制结果。

账户	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。

账户	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 Sec AWS urity 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 Organizations 管理 Security Hub 的委托管理AWS。

在管理员账户 (111111111111) 的 Sec AWS urity Hub 控制台中，邀请成员账户 (222222222222) 接受该管理员帐户作为 Security Hub 授权的管理员。从成员账户接受邀请。

账户	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。

账户	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
- AWSLambda 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中调URL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。

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

账户	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

AWSConfig 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`。

账户	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

aws-sharr-deploy. 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。

账户	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

aws-sharr-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。

账户	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

View template

aws-sharr-member-roles. 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。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。

账户	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。

订阅该SNS主题

补救更新

话题- SO0111-SHARR _ 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- 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

在管理员帐户中，导航到 Security Hub 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 “修复ASR”。您将看到一条通知，告知调查结果已发送至 Amazon EventBridge。

账户	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

您应该会收到两条SNS通知。第一个将表示补救已启动，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。

账户	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

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 R emediate_ SHARR with_ _ 的 EventBridge 规则。CustomAction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

在管理员帐户中，找到名为 “SO0111-SHARR-Orchestrator” 的 Ste AWS p 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 的执行历史中追踪修正的执行情况。

SSM 自动化

在成员账户中，导航到SSM自动化控制台。您将发现名为 “ASR-sc_2.0.0_Lambda.1” 的文档执行了两次，名为 “-” 的文档执行了一次。ASR 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-SHARR” 的日志组。此日志组是来自 Orchestrator Step Functions 的高级日志的目标。

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。

确认您没有可能意外应用此发现的资源

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。

账户	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

账户	用途	us-east-1 中的行动	us-west-2 中的行动
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

启用规则

在管理员账户中，找到名为 sc_2.0.0_ AutoTrigger Lambda.1_ 的 EventBridge 规则并将其启用。

账户	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启用自动修复规则	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。

账户	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。您应该会收到两条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。

账户	用途	us-east-1 中的行动	us-west-2 中的行动
111111111111	Admin	启用自动修复规则	无

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

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。

账户	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。

账户	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。

账户	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

账户	用途	us-east-1 中的行动	us-west-2 中的行动
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。

账户	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。

账户	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

管理员和成员堆栈都创建和保留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。

账户	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

账户	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

开发人员指南

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

该解决方案包括互联网安全中心 () 基金会基准 v1.2.0、基金会基准 v1.4.0、基金会基准测试 v3.4.0、AWS基金会基准 v3.0.0、CISAWS基础安全最佳实践 (CIS) v.1.0.0、CISAWS支付卡行业数据安全标准 (-FSBP) v3. 2.1 和美国AWS国家标准研究院的一部分定义的安全标准的剧本补救措施 PCI DSS和技术 (NIST)。

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 AWSSystems Manager 控制台，然后在导航窗格中选择 “文档”。

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
补救总数	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupELBHealthCheck	自动扩展。1		自动扩展。1		自动扩展。1		自动扩展。1

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 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-CreateMultiRegionTrail 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.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnableLogFileValidation 确保已激活 CloudTrail 日志文件验证	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.
ASR-EnableCloudTrailToCloudWatchLogging 确保 CloudTrail 跟踪与 Amazon CloudWatch 日志集成	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
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.
ASR-EnableAWSConfig 确保 AWS Config 已激活	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-M 私 akeEBSSnapshots 人 Amazon EBS 快照不应公开恢复	EC21.		EC21.		EC21.		EC21.
ASR-RemoveVPCefault 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.
ASR-E 日志 nableVPCFlow VPC应全部启用流日志 VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnablEbsEncryptionByDefault EBS应激活默认加密	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7
ASR-RevokeUnrotatedKeys 用户的访问密钥应每 90 天或更短时间轮换一次	IAM3.	1.4		1.14	IAM3.	1.14	IAM3.
ASR-S 政策etIAMPassword IAM默认密码策略	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-RevokeUnusedIAMUserCredentials 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
ASR-RevokeUnusedIAMUserCredentials 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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-RemoveLambdaPublicAccess Lambda函数应禁止公众访问	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-M私akeRDSSnapshot人 RDS快照应禁止公众访问	RDS1.		RDS1.		RDS1.		RDS1.
ASR-DisablePublicAccessToRDSInstance RDS数据库实例应禁止公共访问	RDS2.		RDS2.		RDS2.	2.3.3	RDS2.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EncryptRDSSnapshot RDS集群快照和数据库快照应进行静态加密	RDS4.				RDS4.		RDS4.
ASR-EnableMultiAZOnRDSInstance RDS数据库实例应配置多个可用区	RDS5.				RDS5.		RDS5.
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnableRDSCluster DeletionProtection RDS群集应激活删除保护	RDS.7				RDS.7		RDS.7
ASR-EnableRDSInstance DeletionProtection RDS数据库实例应激活删除保护	RDS.8				RDS.8		RDS.8
ASR-EnableMinorVersionUpgradeOnRDSDInstance RDS应激活自动次要版本升级	RDS.13				RDS.13	2.3.2	RDS.13

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDS应将数据库集群配置为将标签复制到快照	RDS.16				RDS.16		RDS.16
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift集群应禁止公共访问	Redshift.1		Redshift.1		Redshift.1		Redshift.1

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnableAutomaticSnapshotsOnRedshiftCluster 亚马逊 Redshift 集群应激活自动快照	Redshift.3				Redshift.3		Redshift.3
ASR-EnableRedshiftClusterAuditLogging 亚马逊 Redshift 集群应激活审核日志	Redshift.4				Redshift.4		Redshift.4

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-配置 3 BucketPublicAccessBlock S3 存储桶应禁止公开写入访问		S3.3					S3.3
ASR-EnableDefaultEncryptionS3 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-S 政策 etSSLBucket S3 存储桶应要求请求才能使用 SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-S3 BlockDenylist 应限制授予其他存储桶 AWS 账户 内策略的 Amazon S3 权限	S3.6				S3.6		S3.6
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
ASR-EnableKeyRotation 确保已激活客户创建CMKs的轮换		2.8	KMS1.	3.8	KMS4.	3.6	KMS4.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在针对未经授权的API呼叫的日志指标筛选器和警报		3.1		4.1			云监视.1
ASR-CreateLogMetricFilterAndAlarm 确保存在日志指标筛选器和警报，以便在没有 AWS Management Console 登录的情况下登录 MFA		3.2		4.2			云监视2

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在针对“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
ASR-CreateLogMetricFilterAndAlarm 确保存在针对IAM策略变更的日志指标筛选器和警报		3.4		4.4			Cloudwatch.4

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
ASR-CreateLogMetricFilterAndAlarm 确保存在针对 AWS Management Console 身份验证失败的日志指标筛选器和警报		3.6		4.6			Cloudwatch.6

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在 AWS Config 配置更改的日志指标筛选器和警报		3.9		4.9			Cloudwatch.9
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 确保存在针对网络访问控制列表更改的日志指标筛选器和警报 (NACL)		3.11		4.11			Cloudwatch.11
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
ASR-CreateLogMetricFilterAndAlarm 确保存在日志指标筛选器和VPC变更警报		3.14		4.14			Cloudwatch.14

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
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-ConfigureSNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-C 角色 reateIAMSupport		1.20		1.17		1.17	IAM.18
ASR-DisablePublicIPAutoAssign Amazon EC2 子网不应自动分配公有 IP 地址	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionForSNSTopic	SNS1.				SNS1.		SNS1.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnableDeliveryStatusLoggingForSNSTopic 应为发送到主题的通知消息启用传输状态记录	SNS2.				SNS2.		SNS2.
ASR-EnableEncryptionForSQSQueue	SQS1.				SQS1.		SQS1.
ASR-M 私akeRDSSnapshot人 RDS快照应该是私有的	RDS1.		RDS1.				RDS1.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-BlockSSMDocumentPublicAccess SSM文件不应公开	SSM4.				SSM4.		SSM4.
ASR-EnableCloudFrontDefaultRootObject CloudFront 发行版应该配置一个默认的根对象	CloudFront1.				CloudFront1.		CloudFront1.
ASR-SetCloudFrontOriginDomain CloudFront 发行版不应指向不存在的 S3 来源	CloudFront.12				CloudFront.12		CloudFront.12

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-RemoveCodeBuildPrivilegedMode CodeBuild项目环境应该有一个日志持续 AWS Config时间	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.
ASR-终止EC2Instance 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	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-启用 IMDSV2Onnstance 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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-DisableUnrestrictedAccessToHighRiskPorts 安全组不应允许无限制地访问高风险端口	EC2.19				EC2.19		EC2.19
ASR-DisableTGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways不应自动接受VPC附件请求	EC2.23				EC2.23		EC2.23

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnablePrivateRepositoryScanning ECR私有存储库应配置图像扫描	ECR1.				ECR1.		ECR1.
ASR-EnableGuardDuty GuardDuty应该启用	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
ASR-EnableAutoSecretRotation Secrets Manager 密钥应启用自动轮换	SecretsManager1.				SecretsManager1.		SecretsManager1.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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.
ASR-EnableAPIGatewayCacheDataEncryption API网关 RESTAPI 缓存数据应进行静态加密					APIGateway5.		APIGateway5.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-SetLogGroupRetentionDays CloudWatch 日志组应在指定的时间段内保留					CloudWatch.16		CloudWatch.16
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

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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.
ASR-A 收ttachSSMPermissions件人 EC2 亚马逊 EC2实例应由 Systems Manager 管理	SSM1.		SSM3.				SSM1.

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
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
ASR-EnableAPIGatewayExecutionLogs	APIGateway1.						APIGateway1.
ASR-EnableMacie 应启用 Amazon Macie	Macie.1				Macie.1		Macie.1

描述	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	安全控制 ID
ASR-EnablAthenaWorkGroupLogging Athena 工作组应启用日志记录	Athena.4						Athena.4

添加新的补救措施

向现有攻略手册添加新的补救措施不需要修改解决方案本身。

> **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SHARR和/或 SO0111，以便于查找和识别。

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。这必须符合支持的标准SHARR。它必须是 “”、“CIS”、“AFSBPPCI”、“” 或 NIST “SC” 之一。

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

控制：要修复的控件的控件 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 控制台并获取调查结果的示例JSON。
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. 管理员帐户 AWS Step Functions 中的将运行您的运行手册。您的运行手册必须指定修正角色，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 Management 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-<standard>-<version>-<control>` 开头。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 Sec AWS urity Hub 中的SHARR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 Sec AWS urity 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`值以匹配您的调查结果`GeneratorId`中的值JSON。
4. 保存并激活规则。

添加新剧本

从GitHub 存储库下载AWS解决方案手册和部署源代码中的自动安全响应。

AWS CloudFormation 资源由AWS CDK组件创建，资源包含可用于创建和配置新 playbook 的 playbook 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.md 文件。GitHub

AWS Systems Manager 参数存储

“自动安全响应” AWS 使用 S AWS ystems Manager 参数存储来存储操作数据。以下参数存储在参数存储中：

名称	值	使用
/Solutions/SO0111/CMK_REMEDIATION_ARN	AWS KMS 用于加密数据以进行FSBP补救的密钥	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	AWS KMS 用于加密数据的密钥 SHARR	加密解决方案数据
/Solutions/SO0111/SNS_Topic_ARN	ARN该解决方案的 Amazon SNS 主题	补救事件通知
/Solutions/SO0111/SNS_Topic_Config.1	SNS AWS Config 更新主题	配置.1 修复
/Solutions/SO0111/sendAnonymousMetrics	Yes	匿名指标收集
/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

名称	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

Amazon SNS 主题-修复进度

上的自动安全响应AWS会创建亚马逊SNS主题 SO0111-SHARR _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 <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in
 account <account_ID>
```

这是完成消息。它表示补救已完成，没有错误；但是，成功修复的最终测试标准是 AWS Config 检查和/或手动验证。

筛选SNS主题订阅

Amazon SNS 订阅筛选政策：

1. 导航到该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"]
      }
   }
```

Amazon SNS 主题 — CloudWatch 警报

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。

任何进入该ALARM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 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 Security Hub 为此规则生成的调查结果中找到，AWS Config 也可以在 Security Hub 生成的调查结果中找到。
2. 导航到 AWS Systems Manager 参数存储区，然后选择创建参数。
3. 您的规则名称应为 `/Solutions/SO0111/`*`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"

}
```

5. 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。
6. 完成后，您可以使用 Security Hub 上的 “修复方式ASR” 自定义操作来修复您的配置规则。

参考

本节包含有关用于收集该解决方案的独特指标的可选功能的信息、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。

匿名数据收集

该解决方案中包含向 AWS 发送匿名运营指标的选项。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。启用后，将收集以下信息并将其发送至AWS：

- 解决方案 ID-AWS 解决方案标识符
- 唯一 ID (UUID)-为每个 AWS Security Hub 响应和修复部署随机生成的唯一标识符
- 时间戳-数据收集时间戳
- 实例数据-有关此堆栈部署的信息
- CloudWatchMetricsDashboardEnabled-"Yes" 如果在部署期间启用了 CloudWatch 指标和控制面板
- 状态-部署状态（通过或失败的解决方案）或（通过或失败的修复）
- 错误消息-状态字段中的通用错误消息
- Generator_ID-Security Hub 规则信息
- 类型-修复类型和名称
- productArn-部署 Security Hub 的区域
- finding_trigge d _ by-所执行的补救类型（自定义操作或自动触发器）

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。要选择退出此功能，请在启动 AWS CloudFormation 模板之前完成以下步骤。

1. 将 AWS CloudFormation 模板下载到本地硬盘。
2. 使用文本编辑器打开 AWS CloudFormation 模板。
3. 从以下位置修改 AWS CloudFormation 模板映射部分：

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'Yes'
```

更改为：

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'No'
```

4. 登录 AWS CloudFormation 控制台。
5. 选择创建堆栈。
6. 在创建堆栈页面的指定模板部分，选择上传模板文件。
7. 在上传模板文件下，选择选择文件，然后从本地驱动器中选择编辑过的模板。
8. 选择下一步，然后按照本指南“自动化部署”部分的启动堆栈中的步骤操作。

相关资源

- 自动响应和补救 AWS Security Hub
- CIS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 (PCIDSS)
- 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

修订

Date	更改
2020 年 8 月	初始版本
2020 年 10 月	在附录 C 中添加了其他疑难解答信息。
2020 年 11 月	增加了中国区域的部署说明；更新了 Security Hub 管理员账户的解决方案部署说明；有关更多信息，请参阅存储CHANGELOG库中的 GitHub .md 文件。
2021 年 4 月	版本 v1.2.0：添加了新的剧本架构和新的补救措施。FSBP有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2021 年 5 月	版本 v1.2.1：修复了影响 EC2 .2 和 EC2 .7 的问题的错误。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2021 年 8 月	版本 v1.3.0：添加了 PCI DSS v3.2.1 剧本。在 CIS v1.2.0 中添加了 17 个新的补救措施。向中添加了四种新的补救措施FSBP。已CIS转换为使用基于SSM运行手册的新剧本架构。添加了使用客户定义的补救措施扩展现有 Playbook 的说明。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2021 年 9 月	版本 v1.3.1：`CreateLogMetricFilterAndAlarm.py` 已更改为激活操作，并在中添加SNS通知。`SO0111-SHARR-LocalAlarmNotification` 已更改 CIS 2.8 修正以匹配新的查找数据格式。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

Date	更改
2021 年 11 月	版本 1.3.2：修复了 CIS v1.2.0 控件 3.1-3.14 的错误。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2021 年 12 月	版本 v1.4.0：现在可以使用部署解决方案。StackSets除了跨账户之外，现在还支持跨区域修复。现在，移除堆栈后，成员账户IAM角色将保留。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 1 月	版本 v1.4.1：错误修复。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 1 月	版本 v1.4.2：错误修复。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 6 月	版本 v1.5.0：其他补救措施。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 12 月	1.5.1 版本进行了更改，将SSM文档创建从自定义资源 Lambda `CfnDocument` 切换到。SSM文档名称的前缀更新为以开头，ASR而不是SHARR。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 3 月	版本 2.0.0：增加了对安全控制和 CIS v1.4.0 标准的支持、对标准的五项新补救措施、对 CIS v1.2.0 FSBP 标准的一项新补救措施、服务目录 AppRegistry 集成以及用于避免因文档限制而导致部署失败的额外保护措施。SSM有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

Date	更改
2023 年 4 月	版本 2.0.1：缓解了所有新 S3 存储桶的 S3 对象所有权（ACLs已禁用）的新默认设置所造成的影响。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 5 月	文档更新：更新了 Well-Architected 定义，添加了有关在何处部署每个堆栈的指南，增加了带有特定补救措施的问题疑难解答版本，并在通知中更新了代码示例。SNS
2023 年 7 月	文档更新：更新了架构图和工作流程中的解决方案组件。
2023 年 10 月	版本 2.0.2：更新了软件包版本以解决安全漏洞。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 11 月	文档更新：在 “使用 S AWS ervice Catalog 监控解决方案” AppRegistry 部分添加了确认与解决方案关联的成本标签。
2024 年 3 月	版本 2.1.0：增加了对标准的支持，为NIST标准添加了 17 个新的补救措施，添加了用于监控解决方案的 CloudWatch 控制面板，为架构添加了限制处理程序，增加了对 Security Hub 可自定义输入参数的支持，并增加了对修复 Config 发现的支持。FSBP有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2024 年 4 月	版本 2.1.1：更新为 CloudFormation 参数顺序和默认值文档更新。添加了对NIST标准的引用。添加了有关 EventBridge 规则服务配额的信息。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

Date	更改
2024 年 6 月	版本 2.1.2： AppRegistry 为避免更新解决方案时出错，某些剧本已禁用。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2024 年 9 月	版本 2.1.3：解决了 EC2 .18 和 EC2 .19 的修复脚本中的一个问题，即 IpProtocol 设置为 -1 的安全组规则被错误忽略。将修复SSM文档中的所有 Python 运行时从 Python 3.8 升级到 Python 3.11。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2024 年 11 月	版本 2.1.4：将所有控制运行手册中的 Python 运行时从 Python 3.8 升级到 Python 3.11。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2024 年 12 月	版本 2.2.0：添加了票务系统集成、 CloudTrail 操作日志和 CIS 3.0.0 Playbook。增强的仪表板和通知。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

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。