實作指南

上的自動化安全回應 AWS

上的自動化安全回應 AWS: 實作指南

Table of Contents

解決方案概觀 1
功能和優勢 2
使用案例 3
概念和定義 4
架構概觀 6
架構圖 6
AWS Well-Architected 設計考量事項 7
卓越營運 7
安全 8
可靠性 8
效能效率 8
成本最佳化 8
永續性 9
架構詳細資訊 10
AWS Security Hub 整合 10
跨帳戶修復 10
手冊 10
集中式記錄 11
通知 11
AWS 此解決方案中的 服務 11
規劃您的部署 13
成本 13
成本表範例 13
定價範例 （每月） 17
選用功能的額外費用 22
安全 23
IAM 角色 23
支援的 AWS 區域 24
配額 25
此解決方案中 AWS服務的配額 25
AWS CloudFormation 配額 26
Amazon EventBridge 規則配額 26
AWS Security Hub 部署 26
堆疊與 StackSets 部署 26

部署解決方案 27
決定部署每個堆疊的位置 27
決定如何部署每個堆疊 28
合併的控制問題清單 28
AWS CloudFormation 範本 29
管理員帳戶支援 29
成員帳戶 30
成員角色 30
票證系統整合 30
自動化部署 - StackSets 31
必要條件 31
部署概觀 32
（選用） 步驟 0：啟動票證系統整合堆疊 33
步驟 1：在委派的 Security Hub Admin 帳戶中啟動 Admin 堆疊 35
步驟 2：在每個 AWS Security Hub 成員帳戶中安裝修補角色 36
步驟 3：在每個 AWS Security Hub 成員帳戶和區域中啟動成員堆疊 37
自動化部署 - Stacks 38
必要條件 38
部署概觀 38
（選用） 步驟 0：啟動票證系統整合堆疊 39
步驟 1：啟動管理員堆疊 41
步驟 2：在每個 AWS Security Hub 成員帳戶中安裝修補角色 45
步驟 3：啟動成員堆疊 46
步驟 4：（選用） 調整可用的補救措施 49
使用 Service Catalog 監控解決方案 AppRegistry 51
使用 CloudWatch Application Insights 51
確認與解決方案相關聯的成本標籤 52
啟用與解決方案相關聯的成本分配標籤 53
AWS Cost Explorer 54
使用 Amazon CloudWatch 儀表板監控解決方案的操作 55
啟用 CloudWatch 指標、警示和儀表板 55
使用 CloudWatch 儀表板 55
修改警示閾值 57
訂閱警示通知 59
更新解決方案 60
從 v1.4 之前的版本升級 60

從 v1.4 和更新版本升級 60
從 v2.0.x 升級 60
疑難排解 61
解決方案日誌 61
已知問題解決方案 62
特定修復的問題 64
PutS3BucketPolicyDeny fails 64
如何停用解決方案 65
聯絡人 Support 65
建立案例 65
如何提供協助？ 66
其他資訊 66
協助我們更快解決您的案例 66
立即解決或聯絡我們 66
解除安裝解決方案 67
V1.0.0-V1.2.1 67
V1.3.x 67
V1及更新版本 68
管理員指南 69
啟用和停用 解決方案的部分 69
SNS 通知範例 70
使用解決方案 72
上的自動安全回應入門 AWS 72
準備帳戶 72
啟用AWS組態 72
啟用AWS安全中樞 73
啟用合併控制問題清單 73
設定跨區域調查結果彙總 74
指定 Security Hub 管理員帳戶 75
建立自我管理 StackSets 許可的角色 75
建立會產生範例問題清單的不安全資源 76
建立相關控制項的 CloudWatch 日誌群組 77
將解決方案部署到教學帳戶 77
部署管理員堆疊 77
部署成員堆疊 78
部署成員角色堆疊 79

訂閱 SNS 主題 79
修復範例問題清單 79
啟動修復 80
確認修復已解決問題清單 80
追蹤修復的執行 80
EventBridge 規則 80
Step Functions 執行 81
SSM 自動化 81
CloudWatch 日誌群組 81
啟用全自動化修復 81
確認您沒有可能不小心套用此調查結果的資源 81
啟用規則 82
設定 資源 82
確認修復已解決問題清單 80
清除 83
刪除範例資源 83
刪除管理員堆疊 83
刪除成員堆疊 83
刪除成員角色堆疊 84
刪除保留的角色 84
排程保留的KMS金鑰以進行刪除 84
刪除自我管理 StackSets 許可的堆疊 85
開發人員指南 86
來源碼 86
手冊 86
新增新的修補 124
概觀 125
步驟 1. 在成員帳戶中建立 Runbook (s) 125
步驟 2. 在成員帳戶中建立IAM角色 （多個） 125
步驟 3：（選用） 在管理員帳戶中建立自動修復規則 126
新增手冊 126
AWS Systems Manager 參數存放區 126
SNS 主題 - 修復進度 127
篩選SNS主題訂閱 128
Amazon SNS主題 – CloudWatch Alarms 129
在 Config 調查結果上啟動 Runbook 129

參考資料 130
匿名資料收集 130
相關資源 131
貢獻者 131
修訂 133
注意 137
..... cxxxviii

使用 中的預先定義回應和修補動作，自動處理安全威脅 AWS Security Hub

發佈日期：2020 年 8 月 (上次更新日期：2024 年 12 月)

此實作指南提供AWS解決方案的自動化安全回應概觀、其參考架構和元件、規劃部署的考量事項、在 Amazon Web Services (AWS) 雲端部署 AWS 解決方案上的自動化安全回應的組態步驟。

使用此導覽表快速尋找這些問題的答案：

如果您想要 . . .	讀取 . . .
了解執行此解決方案的成本	成本
了解此解決方案的安全考量	安全性
了解如何規劃此解決方案的配額	配額
了解此解決方案支援哪些AWS區域	支援AWS的區域
檢視或下載此解決方案中包含的AWS CloudFormation 範本，以自動部署此解決方案的基礎設施資源 (「堆疊」)	AWS CloudFormation 範本
存取原始程式碼，並選擇性地使用AWS雲端開發套件 (AWSCDK) 來部署解決方案。	GitHub 儲存庫

安全性的持續演變需要主動步驟來保護資料，這可能會讓安全團隊難以、昂貴且耗時地做出反應。自動化安全回應 AWS 解決方案可協助您快速回應安全問題，方法是根據產業合規標準和最佳實務提供預先定義的回應和修補動作。

上的自動安全回應AWS是 AWS 解決方案，可搭配 AWS Security Hub 來改善您的安全性，並協助讓您的工作負載符合 Well-Architected 安全支柱最佳實務 (SEC10)。此解決方案可讓 AWS Security Hub 客戶更輕鬆地解決常見的安全問題清單，並改善其安全狀態 AWS。

您可以選擇要在 Security Hub 主要帳戶中部署的特定手冊。每個手冊都包含必要的自訂動作、 Identity and Access Management (IAM) 角色、Amazon EventBridge 規則、AWS Systems Manager 自動化文件、AWS Lambda函數，以及在單一AWS帳戶內或跨多個帳戶啟動修補工作流程AWS Step

Functions所需的 。補救措施可從 中的動作選單中運作， AWS Security Hub 並允許授權使用者使用單一動作來修復其所有 AWS Security Hub受管帳戶的調查結果。例如，您可以套用 Center for Internet Security (CIS) AWS Foundations Benchmark 的建議，這是保護AWS資源的合規標準，可確保密碼在 90 天內過期，並強制加密存放在 的事件日誌AWS。

> **Note**
>
> 補救措施適用於需要立即採取行動的緊急情況。此解決方案只會在您透過 AWS Security Hub 管理主控台啟動，或使用 Amazon EventBridge 規則啟用特定控制項的自動修復時，對修復問題清單進行變更。若要還原這些變更，您必須手動將資源放回其原始狀態。
> 修復作為 CloudFormation 堆疊一部分部署 AWS 的資源時，請注意這可能會導致偏離。盡可能修改定義堆疊資源和更新堆疊的程式碼，以修復堆疊資源。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是偏離？。

上的自動安全回應AWS包括安全標準的手冊修復，定義如下：

- 網際網路安全中心 (CIS) AWS Foundations Benchmark 1.2.0 版
- CIS AWS Foundations Benchmark 1.4.0 版
- CIS AWS Foundations Benchmark 3.0.0 版
- AWS 基礎安全最佳實務 (FSBP) 1.0.0 版
- 支付卡產業資料安全標準 (PCI-DSS) 3.2.1 版
- 國家標準技術研究所 (NIST) SP 800-53 修訂版 5

解決方案也包含 Security Hub 合併控制問題清單功能AWS的安全控制 (SC) 手冊。如需詳細資訊，請參閱 手冊。

本實作指南討論在 AWS 雲端部署自動化安全回應AWS解決方案的架構考量和組態步驟。其中包含範本的連結，這些AWS CloudFormation範本會使用安全性和可用性的AWS最佳實務，在 上啟動、設定和執行部署此解決方案所需的AWS運算、網路AWS、儲存和其他服務。

本指南適用於在 AWS 雲端中具有實際架構經驗的 IT 基礎設施架構師、管理員和 DevOps 專業人員。

功能和優勢

上的自動安全回應AWS提供下列功能：

自動修復特定控制項的問題清單

為控制項啟用 Amazon EventBridge 規則，以便在問題清單出現在 AWS Security Hub 中後立即自動修復該控制項的問題清單。

從單一位置管理多個帳戶和區域的修復

從設定為組織帳戶和區域的彙總目的地的 AWS Security Hub 管理員帳戶，針對部署解決方案的任何帳戶和區域中的調查結果啟動修復。

收到修復動作和結果的通知

訂閱解決方案所部署的 Amazon SNS主題，以便在啟動修復時收到通知，以及修復是否成功。

與 Jira 或 等票證系統整合 ServiceNow

為了協助您的組織回應修補（例如，更新您的基礎設施程式碼），此解決方案可以將票證推送到您的外部票證系統。

在 GovCloud 和中國分割區 AWSConfigRemediations 中使用

解決方案中包含的一些補救措施是 AWS擁有的文件的重新封裝，這些 AWSConfigRemediation 文件可在商業分割區中使用，但不適用於 GovCloud 或 中國。部署此解決方案，在這些分割區中使用這些文件。

透過自訂修復和 Playbook 實作擴展解決方案

解決方案的設計是可擴展且可自訂。若要指定替代修復實作，請部署自訂 AWS Systems Manager 自動化文件和AWSIAM角色。若要支援解決方案未實作的整組新控制項，請部署自訂 Playbook。

使用案例

在組織的帳戶和區域中強制遵循標準

部署標準（例如AWS基礎安全最佳實務）的手冊，以便能夠使用提供的修補。在部署解決方案的任何帳戶和區域中，自動或手動啟動資源的修復，以修正不合規的資源。

部署自訂修補或手冊，以滿足組織的合規需求

使用提供的 Orchestrator 元件做為架構。建置自訂修補，以根據組織的特定需求處理 out-of-compliance資源。

概念和定義

本節說明關鍵概念並定義此解決方案特有的術語：

應用程式

您想要作為單位運作的邏輯AWS資源群組。

修補、修補 Runbook

一組解決問題清單的步驟實作。例如，控制項安全控制 (SC) Lambda.1「Lambda 函數政策應禁止公開存取」的修復會修改相關 AWS Lambda 函數的政策，以移除允許公開存取的陳述式。

Control Runbook

Orchestrator 用來將特定控制項的起始修復路由至正確修復 Runbook 的一組 AWS Systems Manager (SSM) 自動化文件之一。例如，SC Lambda.1 和AWS基礎安全最佳實務 (FSBP) Lambda.1 的修復會使用相同的修復 Runbook 實作。Orchestrator 會叫用每個控制項的控制項 Runbook，分別名為 ASR-AFSBP_Lambda.1 和 ASR-SC_2.0.0_Lambda.1。每個控制項 Runbook 都會叫用相同的修復 Runbook，在這種情況下，該修復 Runbook 會是 ASR-RemoveLambdaPublicAccess。

協調程式

解決方案所部署的步驟函數，會做為來自 AWS Security Hub 的調查結果物件的輸入，並在目標帳戶和區域中叫用正確的控制 Runbook。Orchestrator 也會在修補啟動和修補成功或失敗時通知解決方案SNS主題。

標準

組織定義為合規架構一部分的一組控制項。例如，AWSSecurity Hub 和此解決方案支援的其中一項標準是 AWS FSBP。

控制

資源為了符合規範而應該或不應該擁有的屬性描述。例如，控制項 AWS FSBP Lambda.1 指出 AWS Lambda Functions 應該禁止公開存取。允許公開存取的 函數會失敗此控制。

合併控制問題清單、安全控制、安全控制檢視

AWS Security Hub 的一項功能，在啟用時，會以其合併控制項顯示問題清單IDs，IDs而不是對應至特定標準。例如，控制項 AWS FSBP S3.2、CISv1.2.0 2.3、CISv1.4.0 2.1.5.2 和 PCI-DSS v3.2.1 S3.1

所有映射到合併 (SC) 控制項 S3.2 “S3 儲存貯體應禁止公開讀取存取。” 開啟此功能時，會使用 SC Runbook。

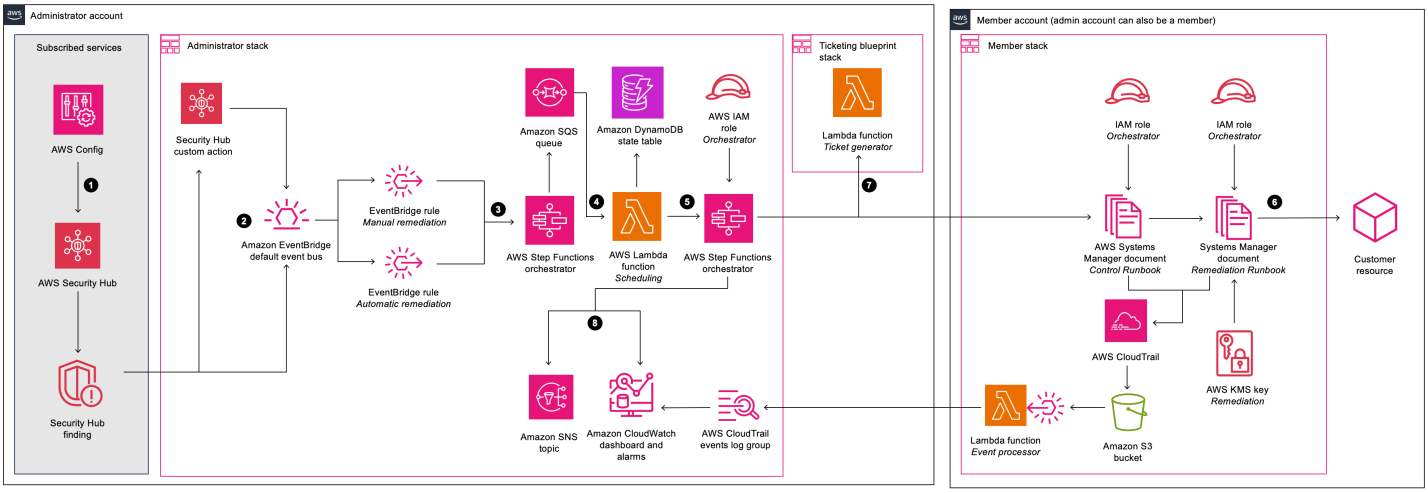
如需 AWS 術語的一般參考，請參閱AWS 詞彙表。

架構概觀

本節提供使用此解決方案部署元件的參考實作架構圖。

架構圖

使用預設參數部署此解決方案會在 AWS 雲端中建置下列環境。



AWS 架構上的自動化安全回應

> **Note**
>
> AWS CloudFormation 資源是從AWS雲端開發套件 (AWSCDK) 建構模組建立。

搭配 AWS CloudFormation 範本部署之解決方案元件的高階程序流程如下：

1. Detect： AWS Security Hub 為客戶提供其AWS安全狀態的全面檢視。它有助於他們根據安全產業標準和最佳實務來衡量其環境。其運作方式是從其他 AWS服務收集事件和資料，例如 AWS Config、Amazon Guard Duty 和 AWS Firewall Manager。這些事件和資料會根據安全標準進行分析，例如 CIS AWS Foundations Benchmark。例外狀況會在 AWS Security Hub 主控台中宣告為問題清單。新的問題清單會以 Amazon EventBridge 事件的形式傳送。
2. 啟動：您可以使用自訂動作針對問題清單啟動事件，這會導致 EventBridge 事件。 AWS Security Hub 自訂動作和 EventBridge規則會在AWS手冊上啟動自動安全回應，以解決問題清單。解決方案部署：

   a. 符合自訂動作事件的 EventBridge 規則

b. 每個支援的控制項有一個 EventBridge 事件規則（預設為停用），以符合即時調查結果事件

您可以使用 Security Hub 主控台中的自訂動作選單來啟動自動修復。在非生產環境中仔細測試之後，您也可以啟用自動修復。您可以針對個別修補啟用自動化，您不需要在所有修補上啟用自動啟動。

3. 預先修復：在管理員帳戶中， 會AWS Step Functions處理修復事件，並準備排程。
4. 排程：解決方案會叫用排程AWS Lambda函數，將修復事件放置在 Amazon DynamoDB 狀態資料表中。
5. Orchestrate：在管理員帳戶中，Step Functions 使用跨帳戶 AWS Identity and Access Management(IAM) 角色。Step Functions 會叫用成員帳戶中的修復，其中包含產生安全問題清單的資源。
6. 修復：成員帳戶中的AWS Systems Manager自動化文件會執行修復目標資源上的問題清單所需的動作，例如停用 Lambda 公有存取。

   或者，您可以使用 EnableCloudTrailForASRActionLog 參數在成員堆疊中啟用動作日誌功能。此功能會擷取成員帳戶中解決方案採取的動作，並在解決方案的 Amazon CloudWatch 儀表板中顯示這些動作。
7. （選用）建立票證：如果您使用 TicketGenFunctionName 參數在 Admin 堆疊中啟用票證，解決方案會叫用提供的票證產生器 Lambda 函數。此 Lambda 函數會在成員帳戶中成功執行修復之後，在您的票務服務中建立票證。我們提供堆疊以與 Jira 和 整合 ServiceNow。
8. 通知和日誌： 手冊會將結果記錄到 CloudWatch 日誌群組，將通知傳送到 Amazon Simple Notification Service (AmazonSNS) 主題，並更新 Security Hub 問題清單。解決方案會在問題清單備註中維護動作的稽核線索。

AWS Well-Architected 設計考量事項

此解決方案的設計採用 AWS Well-Architected Framework 的最佳實務，可協助客戶在雲端設計及操作可靠、安全、高效且符合成本效益的工作負載。本節說明如何在建置此解決方案時套用 Well-Architected Framework 的設計原則和最佳實務。

卓越營運

本節說明如何使用卓越營運支柱的原則和最佳實務來建構此解決方案。

- 定義為 IaC 使用的資源 CloudFormation。
- 可能的話，以下列特性實作的補救措施：

- 冪等性
- 錯誤處理和報告
- 日誌
- 在失敗時將資源還原至已知狀態

安全

本節說明如何使用安全支柱的原則和最佳實務來建構此解決方案。

- IAM 用於身分驗證和授權。
- 角色許可的範圍越窄越好，雖然在許多情況下，此獨佔需要萬用字元許可才能對任何資源採取行動。

可靠性

本節說明如何使用可靠性支柱的原則和最佳實務來建構此解決方案。

- 如果修復無法解決問題清單的根本原因，Security Hub 會繼續建立問題清單。
- 無伺服器服務可讓解決方案視需要擴展。

效能效率

本節說明如何使用效能效率支柱的原則和最佳實務來建構此解決方案。

- 此解決方案旨在成為您擴展的平台，而不必自行實作協調和許可。

成本最佳化

本節說明如何使用成本最佳化支柱的原則和最佳實務來建構此解決方案。

- 無伺服器服務只允許您支付使用的項目。
- 在每個帳戶中使用免費方案進行SSM自動化

永續性

本節說明如何使用永續性支柱的原則和最佳實務來建構此解決方案。

- 無伺服器服務可讓您視需要擴展或縮減規模。

架構詳細資訊

本節說明構成此解決方案的元件AWS和服務，以及這些元件如何一起運作的架構詳細資訊。

AWS Security Hub 整合

部署aws-sharr-deploy堆疊會與 AWS Security Hub 的自訂動作功能整合。當 AWS Security Hub 主控台使用者選取問題清單進行修復時，解決方案會使用 路由問題清單記錄以進行修復 AWS Step Functions。

跨帳戶許可和 AWS Systems Manager Runbook 必須使用 aws-sharr-member.template和 aws-sharr-member-roles.template CloudFormation 範本部署到所有 AWS Security Hub 帳戶 （管理員和成員）。如需詳細資訊，請參閱 手冊。此範本允許在目標帳戶中自動修復。

使用者可以使用 Amazon CloudWatch 事件規則，根據每個修復自動啟動自動修復。此選項會在問題清單回報時，立即啟用問題清單的全自動修復 AWS Security Hub。根據預設，自動啟動會關閉。此選項可在安裝手冊期間或之後隨時變更，方法是開啟 AWS Security Hub 管理員帳戶中 CloudWatch 的事件規則。

跨帳戶修復

上的自動安全回應AWS使用跨帳戶角色，使用跨帳戶角色跨主要和次要帳戶運作。這些角色會在解決方案安裝期間部署到成員帳戶。每個修補都會指派個別角色。主要帳戶中的修復程序已獲得許可，以擔任需要修復之帳戶中的修復角色。修復是由在 帳戶中執行且需要修復的 AWS Systems Manager Runbook 執行。

手冊

一組修復會分組到稱為手冊的套件。使用這個解決方案的範本安裝、更新和移除手冊。如需每個手冊中支援的補救措施的相關資訊，請參閱 開發人員指南 -> 手冊。此解決方案目前支援下列手冊：

- Security Control，與 AWS Security Hub 的合併控制調查結果功能一致的手冊，發佈於 2023 年 2 月 23 日。

> **Important**
>
> 在 Security Hub 中啟用合併控制問題清單時，這是解決方案中唯一應該啟用的手冊。

- 網際網路安全中心 (CIS) Amazon Web Services Foundations 基準，1.2.0 版，2018 年 5 月 18 日發佈。
- 網際網路安全中心 (CIS) Amazon Web Services Foundations 基準，1.4.0 版，2022 年 11 月 9 日發佈。
- 網際網路安全中心 (CIS) Amazon Web Services Foundations 基準，3.0.0 版，2024 年 5 月 13 日發佈。
- AWS 基礎安全最佳實務 (FSBP) 1.0.0 版，2021 年 3 月發佈。
- 支付卡產業資料安全標準 (PCI-DSS) 3.2.1 版，2018 年 5 月發佈。
- 國家標準技術研究所 (NIST) 5.0.0 版，2023 年 11 月發佈。

集中式記錄

單一 CloudWatch 日誌群組 SO0111- AWS日誌上的自動安全回應SHARR。這些日誌包含解決方案的詳細記錄，用於解決方案的故障診斷和管理。

通知

此解決方案使用 Amazon Simple Notification Service (Amazon SNS) 主題來發佈修復結果。您可以使用此主題的訂閱來擴展解決方案的功能。例如，您可以傳送電子郵件通知和更新故障票證。

AWS 此解決方案中的 服務

解決方案使用下列 服務。核心服務需要使用 解決方案，而支援服務則連接核心服務。

AWS 服務	描述
Amazon EventBridge	核心。部署將在問題清單修復時啟動協調器步驟函數的事件。
AWS IAM	核心。部署許多角色，以允許對不同資源進行修復。
AWS Lambda	核心。部署多個 lambda 函數，由步驟函數協調器用來修復問題。

AWS 服務	描述
AWS Security Hub	核心。為客戶提供其 AWS 安全狀態的全面檢視。
AWS Step Functions	核心。部署 協調程式，以使用 AWS Systems Manager API呼叫呼叫修復文件。
AWS Systems Manager	核心。部署包含將執行之修復邏輯的系統管理員文件（文件連結）。
AWS CloudTrail	支援。記錄解決方案對您的 AWS 資源所做的變更，並在 CloudWatch 儀表板上顯示這些變更。
Amazon CloudWatch	支援。部署日誌群組，讓不同的手冊用來記錄結果。收集指標，以在具有警示的自訂儀表板上顯示。
AWS DynamoDB	支援。將上次執行的修補儲存在每個帳戶和區域中，以最佳化修補的排程。
Service Catalog AppRegistry	支援。部署已部署堆疊的應用程式，以追蹤成本和用量。
Amazon Simple Notification Service	支援。部署在完成修復後收到通知SNS的主題。
AWS SQS	支援。協助排程修復，讓解決方案可以平行執行修復。

規劃您的部署

本節說明部署解決方案之前的成本、網路安全 AWS 區域、支援、配額和其他考量事項。

成本

您需負擔執行此解決方案所使用的 AWS 服務成本。截至此修訂為止，以美國東部（維吉尼亞北部）預設設定執行此解決方案的成本 AWS 區域 ，每月 300 個修補大約為 21.17 美元，每月 3，000 個修補大約為 134.86 美元，每月 30，000 個修補大約為 1，281.01 美元。價格可能變動。如需完整詳細資訊，請參閱此解決方案中使用的每個 AWS 服務定價頁面。

> **Note**
>
> 許多 AWS 服務包含免費方案 – 客戶可免費使用的基準服務數量。實際成本可能高於或低於提供的定價範例。

我們建議您建立預算，AWS Cost Explorer以協助管理成本。價格可能變動。如需完整詳細資訊，請參閱此解決方案中使用的每個 AWS 服務的定價網頁。

成本表範例

執行此解決方案的總成本取決於下列因素：

- AWS Security Hub 成員帳戶的數量
- 自動調用的作用中修復數量
- 修復的頻率

此解決方案使用下列 AWS 元件，這會根據您的組態產生成本。為小型、中型和大型組織提供定價範例。

服務	免費方案	定價 【USD】
AWS Systems Manager 自動化 - 步驟計數	每月每個帳戶 100，000 個步驟	除了免費方案之外，每個基本步驟都會收取每個步驟 0.002 美元的費用。對於多帳戶自

服務	免費方案	定價 【USD】
		動化，包含在任何子帳戶中執行的所有步驟只會計入原始帳戶。
AWS Systems Manager 自動化 - 步驟持續時間	每月 5，000 秒	除了免費方案之外，在每月 5，000 秒的免費方案之後，每個 aws：executeScript action 步驟每秒都會收費 0.00003 美元。
AWS Systems Manager 自動化 - 儲存	無免費方案	每月每 GB 0.046 美元
AWS Systems Manager 自動化 - 資料傳輸	無免費方案	每轉移 GB 0.900 美元 （ 跨帳戶或 out-of-Region)
AWS Security Hub - 安全檢查	無免費方案	前 100，000 次檢查checks/account/Region/month費用 0.0010 美元 接下來的 400，000 每筆檢查checks/account/Region/month成本為 0.0008 美元 每次檢查費用超過 500，000 checks/account/Region/month 美元
AWS Security Hub - 尋找擷取事件	前 10，000 個events/account/Region/month是免費的。尋找與 Security Hub 安全檢查相關聯的擷取事件。	每個事件超過 10，000 筆 events/account/Region/month 費用 0.00003

服務	免費方案	定價 【USD】
Amazon CloudWatch - 指標	基本監控指標 (5 分鐘頻率） 10 個詳細監控指標 (1 分鐘頻率） 1 百萬個API請求 （不適用於 GetMetricData 和 GetMetricWidgetImage)	前 10，000 個指標每月花費 0.30 美元 接下來的 240，000 個指標每月花費 0.10 美元 接下來的 750，000 個指標每月花費 0.05 美元 超過 1，000，000 個指標每月花費 0.02 美元 API 每 1，000 個請求的呼叫成本為 0.01 美元
Amazon CloudWatch - 儀表板	3 個儀表板，每月最多 50 個指標	每月每個儀表板 3.00 美元
Amazon CloudWatch - 警示	10 警示指標 （不適用於高解析度警示）	標準解析度 (60 秒） 每個警示指標的成本為 0.10 美元 高解析度 (10 秒） 每個警示指標的成本為 0.30 美元 標準解析異常偵測每個警示 0.30 美元 高解析度異常偵測每個警示的成本為 0.90 美元 每個警示的複合成本為 0.50 美元
Amazon CloudWatch - Logs 集合	5GB 資料 （擷取、封存儲存和由 Logs Insights 查詢掃描的資料）	每 GB 0.50 美元

服務	免費方案	定價 【USD】
Amazon CloudWatch - Logs Storage	5GB 資料 （擷取、封存儲存和由 Logs Insights 查詢掃描的資料）	掃描的資料每 GB 0.005 美元
Amazon CloudWatch - 事件	包含自訂事件以外的所有事件	自訂事件每百萬美元 1.00 美元 跨帳戶事件每百萬美元 1.00 美元
AWS Lambda - 請求	每月 1M次免費請求	每 1M00 萬筆請求 0.20 美元
AWS Lambda - 持續時間	每月 400，000 GB 的運算時間	每 GB-秒 $0.0000166667。持續時間的價格取決於您配置給函數的記憶體量。您可以將任何數量的記憶體配置到 128MB 到 10，240MB 之間的函數，以 1MB 為增量。
AWS Step Functions - 狀態轉換	每月 4，000 次免費狀態轉換	之後每 1，000 個州轉換 $0.025
Amazon EventBridge	AWS 服務發佈的所有狀態變更事件都是免費的	發佈的自訂事件費用為 100 萬美元 第三方 (SaaS) 事件每發佈一百萬美元的事件 跨帳戶事件的傳送成本為 100 萬美元
Amazon SNS	每月前 100 萬次 Amazon SNS 請求免費	之後每 100 萬個請求 0.50 美元
Amazon SQS	每月前 100 萬次 Amazon SQS 請求免費	之後每 100 萬到 1，000 億個請求 0.40 美元
Amazon DynamoDB	前 25GB 的儲存空間是免費的	之後每 100 萬次一致讀取和寫入 200 美元

定價範例（每月）

範例 1：每月 300 個修補

- 10 個帳戶，1 個區域
- 每個 30 個修復 account/Region/month
- 每月總成本 21.17 美元

服務	假設	每月費用 【USD】
AWS Systems Manager 自動化	步驟：~4 個步驟 * 300 個修補 * $0.002 = $2.40 持續時間：10 秒 * 300 個修補 * $0.00003 = $0.09	2.49 美元
AWS Security Hub	未使用計費服務	0 USD
Amazon CloudWatch Logs	300 個修補 * $0.000002 = $0.0006 $0.0006 * 0.03 = $0.000018	< 0.01 美元
AWS Lambda - 請求	300 個修復 * 6 個請求 = 1，800 個請求 $0.20 * 1，000，000 個請求 = $0.20	0.20 美元
AWS Lambda - 持續時間	256M：1.875 GB 秒 * 300 個修復 * $0.0000167 = $0.009375	< 0.01 美元
AWS Step Functions	17 個狀態轉換 * 300 個修復 = 5，100 $0.025 * (5，100/1，000) 州轉換 = $0.15	0.15 美元

服務	假設	每月費用 【USD】
Amazon EventBridge 規則	規則不收費	0 USD
AWS Key Management Service	1 個金鑰 * 10 個帳戶 * 1 個區域 * $1 = $10	10.00 美元
Amazon DynamoDB	$2.00 * 1，000，000 讀取和寫入 = $2.00	2.00 美元
Amazon SQS	$0.40 * 1，000，000 個請求 = $0.40	0.40 美元
Amazon SNS	0.50 美元 * 1，000，000 個通知 = 0.50 美元	0.50 美元
Amazon CloudWatch - 指標	$0.30 * 7 個自訂指標 = $2.10 $0.01 * (300 * 3 / 1，000) 提出指標API呼叫 = $0.01	2.11 美元
Amazon CloudWatch - 儀表板	$3.00 * 1 個儀表板 = $3.00	3.00 美元
Amazon CloudWatch – 警示	$0.10 * 3 個警示 = $0.30	0.30 美元
總計		21.17 美元

範例 2：每月 3，000 個修補

- 100 個帳戶，1 個區域
- 每個 30 個修復 account/Region/month
- 每月總成本 134.86 美元

服務	假設	每月費用 【USD】
AWS Systems Manager 自動化	步驟：~4 個步驟 * 3，000 個修補 * $0.002 = $24.00	24.90 美元

服務	假設	每月費用 【USD】
	持續時間：10 秒 * 3，000 個修補 * 0.0000 美元3 = 0.90 美元	
AWS Security Hub	未使用計費服務	0 USD
Amazon CloudWatch Logs	3，000 個修補 * $0.00002 = $0.006 $0.006 * 0.03 = $0.00018	< 0.01 美元
AWS Lambda - 請求	3，000 個修復 * 6 個請求 = 18，000 個請求 $0.20 * 1，000，000 個請求 = $0.20	0.20 美元
AWS Lambda - 持續時間	256M：1.875 GB 秒 * 3，000 個修補 * 0.000167 美元 = 0.09375 美元	0.09 美元
AWS Step Functions	17 個狀態轉換 * 3，000 個修復 = 51，000 個 $0.025 * (51，000/1，000) 州轉換 = $1.275	1.28 美元
Amazon EventBridge 規則	規則不收費	0 USD
AWS Key Management Service	1 個金鑰 * 100 個帳戶 * 1 個區域 * $1 = $100	100 美元
Amazon DynamoDB	$2.00 * 1，000，000 讀取和寫入 = $2.00	2.00 美元
Amazon SQS	$0.40 * 1，000，000 個請求 = $0.40	0.40 美元

服務	假設	每月費用 【USD】
Amazon SNS	0.50 美元 * 1，000，000 個通知 = 0.50 美元	0.50 美元
Amazon CloudWatch - 指標	$0.30 * 7 個自訂指標 = $2.10 $0.01 * (3000 * 3 / 1，000) 下調指標API呼叫 = $0.09	2.19 美元
Amazon CloudWatch - 儀表板	$3.00 * 1 個儀表板 = $3.00	3.00 美元
Amazon CloudWatch – 警示	$0.10 * 3 個警示 = $0.30	0.30 美元
總計		134.86 美元

範例 3：每月 30，000 個修補

- 1，000 個帳戶，1 個區域
- 每個 30 個修復 account/Region/month
- 每月總成本 1，281.01 美元

服務	假設	每月費用 【USD】
AWS Systems Manager 自動化	步驟：~4 個步驟 * 30，000 個修補 * $0.002 = $240.00 持續時間：10 秒 * 30，000 個修補 * 0.0000 美元3 = 9.00 美元	249.00 美元
AWS Security Hub	未使用計費服務	0 USD
Amazon CloudWatch Logs	30，000 個修補 * $0.00002 = $0.06 $0.06 * 0.03 = $0.0018	< 0.01 美元

服務	假設	每月費用 【USD】
AWS Lambda - 請求	30，000 個修補 * 6 個請求 = 180，000 個請求 $0.20 * 1，000，000 個請求 = $0.20	0.20 美元
AWS Lambda - 持續時間	256M：1.875 GB 秒 * 30，000 個修補 * 0.000167 美元 = 0.9375 美元	0.94 美元
AWS Step Functions	17 個狀態轉換 * 30，000 個修復 = 510，000 個 $0.025 * (510，000/1，000) 州轉換 = $12.75	12.75 美元
Amazon EventBridge 規則	規則不收費	0 USD
AWS Key Management Service	1 個金鑰 * 1，000 個帳戶 * 1 個區域 * $1 = $1，000	1，000 美元
Amazon DynamoDB	$0.000002 * 1，000，000 讀取和寫入 = $2.00	2.00 美元
Amazon SQS	$0.00004 * 1，000，000 個請求 = $0.40	0.40 美元
Amazon SNS	$0.000005 * 1，000，000 個通知 = $0.50	0.50 美元
Amazon CloudWatch - 指標	$0.30 * 6 個自訂指標 = $1.80 $0.01 * (30，000 * 3 / 1，000) 下調指標API呼叫 = $0.90	2.70 美元
Amazon CloudWatch - 儀表板	$3.00 * 1 個儀表板 = $3.00	3.00 美元
Amazon CloudWatch – 警示	$0.10 * 2 個警示 = $0.20	0.20 美元

服務	假設	每月費用 【USD】
Amazon CloudWatch – Application Insights	$0.10 * 40 個警示 （ 上限 ） = $4.00 $0.53 * 10 GB 日誌資料 （ 預估 ） = 5.30 美元 $0.00267 * 5 OpsItems (est.) = ~$0.01	9.31 美元
總計		1，281.01 美元

選用功能的額外費用

本節識別與此解決方案的選用功能相關的額外費用。

增強 CloudWatch 型指標

如果您在部署管理員堆疊時yes為 EnableEnhancedCloudWatchMetrics 參數選取 ，解決方案會為每個控制項 ID 建立兩個自訂指標和一個警示。成本取決於您要修復IDs的控制數目。在下表中，我們假設您IDs每月修復所有 96 種不同的控制，以判斷成本上限。

服務	假設 96 控制項 IDs * 2 = 192 個自訂指標	每月費用 【USD】
Amazon CloudWatch - 指標	$0.30 * 192 個自訂指標 = $57.60	57.60 美元
Amazon CloudWatch - 警示	$0.10 * 96 個警示 = $9.60	9.60 美元
總計		67.20 美元

CloudTrail 動作日誌

在您啟用動作日誌功能的每個成員帳戶中，解決方案會建立 CloudTrail 追蹤記錄所有寫入管理事件。Lambda 函數會篩選出與解決方案無關的事件。這表示成本與您帳戶中的管理事件總數有關，因為與解決方案無關的事件仍由追蹤擷取並由 Lambda 函數處理。

對於下表，我們假設帳戶中每月有 150，000 個管理事件。實際成本取決於您帳戶中的實際管理事件活動。

服務	假設	每月費用 【USD】
AWS CloudTrail	150，000 * $2.00/100，000 = $3.00	3.00 美元
Lambda	150，000 * 0.2 * 0.125 = 3，750 GB-秒 3，750 * $0.0000166667 = $0.0625 運算時間成本 0.15 * $0.20 = $0.03 請求成本 $0.0625 + $0.03 = $0.0952 總 Lambda 成本	0.0925 美元
總計		每個成員帳戶 3.09 美元

安全

當您在AWS基礎設施上建置系統時，安全責任會由您和 共同承擔AWS。此共用模型可減輕您的操作負擔，因為 會AWS操作、管理和控制元件，包括主機作業系統、虛擬化層，以及服務操作所在設施的實體安全性。如需AWS安全性的詳細資訊，請造訪 AWS 雲端安全性。

IAM 角色

AWS Identity and Access Management (IAM) 角色可讓客戶將精細存取政策和許可指派給 AWS 雲端中的服務和使用者。此解決方案會建立IAM角色，授予解決方案的自動化函數存取權，以在每個修補的特定許可集中執行修補動作。

管理員帳戶的 Step Function 會指派給 SO0111-SHARR-Orchestrator-Admin role。只有此角色才允許在每個成員帳戶中擔任 SO0111-Orchestrator-Member。每個修復角色都允許成員角色將其傳遞給 AWS Systems Manager 服務，以執行特定的修復 Runbook。修復角色名稱以 SO0111 開頭，後面接著符合修復 Runbook 名稱的描述。例如，SO0111-RemoveVPCDefaultSecurityGroupRules 是 ASR-R emoveVPCDefaultSecurityGroupRules 修復 Runbook 的角色。

支援的 AWS 區域

區域名稱	區域代碼
美國東部 (俄亥俄)	us-east-2
美國東部 (維吉尼亞北部)	us-east-1
美國西部 (加利佛尼亞北部)	us-west-1
美國西部 (奧勒岡)	us-west-2
非洲 (開普敦)	af-south-1
亞太區域 (香港)	ap-east-1
亞太區域 (海德拉巴)	ap-south-2
亞太區域 (雅加達)	ap-southeast-3
亞太區域 (墨爾本)	ap-southeast-4
亞太區域 (孟買)	ap-south-1
亞太區域 (大阪)	ap-northeast-3
亞太區域 (首爾)	ap-northeast-2
亞太區域 (新加坡)	ap-southeast-1
亞太區域 (雪梨)	ap-southeast-2
亞太區域 (東京)	ap-northeast-1
加拿大 (中部)	ca-central-1

區域名稱	區域代碼
歐洲 (法蘭克福)	eu-central-1
歐洲 (愛爾蘭)	eu-west-1
歐洲 (倫敦)	eu-west-2
歐洲 (米蘭)	eu-south-1
歐洲 (巴黎)	eu-west-3
歐洲 (西班牙)	eu-south-2
歐洲 (斯德哥爾摩)	eu-north-1
歐洲 (蘇黎世)	eu-central-2
中東 (巴林)	me-south-1
中東 (UAE)	me-central-1
南美洲 (聖保羅)	sa-east-1
AWS GovCloud （美國東部）	us-gov-east-1
AWS GovCloud （美國西部）	us-gov-east-2
中國 (北京)	cn-north-1
中國 (寧夏)	cn-northwest-1

配額

服務配額也稱為限制，是AWS您的帳戶的服務資源或操作數量上限。

此解決方案中 AWS服務的配額

請確定您有足夠的配額，可用於此解決方案中實作的每個 服務。如需詳細資訊，請參閱 AWS 服務配額。

使用以下連結前往該服務的 頁面。若要檢視文件中所有 AWS 服務的 Service Quotas 而不切換頁面，PDF請改為檢視 中的服務端點和配額頁面中的資訊。

AWS CloudFormation 配額

在此解決方案中啟動堆疊時AWS CloudFormation ，您應該注意AWS您的帳戶配額。透過了解這些配額，您可以避免限制會讓您無法成功部署此解決方案的錯誤。如需詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的AWS CloudFormation 配額。

Amazon EventBridge 規則配額

AWS 您的帳戶具有 Amazon EventBridge 規則配額，您在選擇要使用 解決方案部署的手冊時應注意這些配額。每個手冊都會為可以修復的每個控制項建立 EventBridge 規則。部署多個手冊時，可以達到規則的配額。如需詳細資訊，請參閱《Amazon 使用者指南》中的 Amazon EventBridge 配額。EventBridge

AWS Security Hub 部署

AWS Security Hub 部署和組態是此解決方案的先決條件。如需設定 AWS Security Hub 的詳細資訊，請參閱 AWS Security Hub 使用者指南中的設定 AWS Security Hub。

您至少必須在主要帳戶中設定有效的 Security Hub。您可以在與 Security Hub 主要帳戶相同的 帳戶（和AWS區域）中部署此解決方案。在每個 Security Hub 主要和次要帳戶中，您還必須部署成員範本， AssumeRole 允許解決方案的 AWS Step Functions 在該帳戶中執行修復 Runbook。

堆疊與 StackSets 部署

堆疊集可讓您使用單一 AWS CloudFormation 範本，在跨 AWS 區域的 AWS 帳戶中建立堆疊。從 1.4 版開始，此解決方案會根據資源部署的位置和方式來分割資源，以支援堆疊集部署。多帳戶客戶，特別是使用 的客戶 AWS Organizations，可以受益於使用堆疊集在多個帳戶中部署。它減少了安裝和維護解決方案所需的工作量。如需詳細資訊 StackSets，請參閱使用 AWS CloudFormation StackSets。

部署解決方案

> **Important**
>
> 如果在 Security Hub 中開啟合併控制問題清單功能 (這是新部署中的預設值)，則只有在部署此解決方案時啟用安全控制 (CS) 手冊。如果功能未開啟，請僅針對 Security Hub 中啟用的安全標準啟用手冊。啟用其他手冊可能會導致達到 EventBridge 規則的配額。

此解決方案使用AWS CloudFormation 範本和堆疊來自動化其部署。 CloudFormation 範本會指定此解決方案中包含AWS的資源及其屬性。 CloudFormation 堆疊會佈建範本中描述的資源。

若要讓解決方案運作，必須部署三個範本。首先，決定部署範本的位置，然後決定如何部署範本。

此概觀將描述範本，以及如何決定部署它們的位置和方式。下一節將更詳細說明如何將每個堆疊部署為 Stack 或 StackSet。

決定部署每個堆疊的位置

這三個範本將由下列名稱參考，並包含下列資源：

- 管理員堆疊：協調器步驟函數、事件規則和 Security Hub 自訂動作。
- 成員堆疊：修復SSM自動化文件。
- 成員角色堆疊：用於修復IAM的角色。

管理員堆疊必須部署在單一帳戶和單一區域中一次。它必須部署到您已設定為組織 Security Hub 調查結果彙總目的地的帳戶和區域中。

解決方案在 Security Hub 調查結果上運作，因此如果該帳戶或區域尚未設定為彙總 Security Hub 管理員帳戶和區域中的調查結果，則無法對特定帳戶和區域的調查結果進行操作。

例如，組織在區域 `us-east-1`和 中擁有操作帳戶`us-west-2`，而 帳戶`111111111111`是區域 中 Security Hub 委派的管理員`us-east-1`。帳戶 `222222222222`和 `333333333333` 必須是委派管理員帳戶 的 Security Hub 成員帳戶`111111111111`。所有三個帳戶都必須設定為將調查結果從 彙總`us-west-2`到 `us-east-1`。管理員堆疊必須部署到 `111111111111`中的帳戶`us-east-1`。

如需尋找彙總的詳細資訊，請參閱 Security Hub 委派管理員帳戶和跨區域彙總的文件。

管理員堆疊必須先完成部署，才能部署成員堆疊，以便從成員帳戶到中樞帳戶建立信任關係。

成員堆疊必須部署到您想要修復問題清單的每個帳戶和區域。這可能包括您先前部署 ASR Admin 堆疊的 Security Hub 委派管理員帳戶。自動化文件必須在成員帳戶中執行，才能使用自動化的免費方案 SSM。

使用先前的範例，如果您想要從所有帳戶和區域修復問題清單，成員堆疊必須部署到所有三個帳戶 (111111111111、 222222222222和 333333333333) 和兩個區域 (us-east-1 和 us-west-2)。

成員角色堆疊必須部署到每個帳戶，但它包含每個帳戶只能部署一次的全域資源 (IAM 角色）。您部署成員角色堆疊的區域並不重要，因此為了簡單起見，我們建議部署到部署管理員堆疊的相同區域。

使用上一個範例，我們建議將成員角色堆疊部署到 中的所有三個帳戶 (111111111111、222222222222和 333333333333)us-east-1。

決定如何部署每個堆疊

部署堆疊的選項為

- CloudFormation StackSet （自我管理許可）
- CloudFormation StackSet （服務受管許可）
- CloudFormation 堆疊

StackSets 使用服務管理許可是最方便的，因為它們不需要部署您自己的角色，並且可以自動部署到組織中的新帳戶。遺憾的是，此方法不支援巢狀堆疊，我們在 Admin 堆疊和成員堆疊中使用。可以用這種方式部署的唯一堆疊是成員角色堆疊。

請注意，部署到整個組織時，組織管理帳戶不會包含在內，因此如果您想要修復組織管理帳戶中的問題清單，您必須分別部署到此帳戶。

成員堆疊必須部署到每個帳戶和區域，但不能使用 StackSets 搭配服務管理許可部署，因為它包含巢狀堆疊。因此，我們建議您 StackSets 使用具有自我管理許可的 來部署此堆疊。

管理員堆疊只會部署一次，因此可以部署為純 CloudFormation堆疊，或做為單一帳戶和區域中 StackSet 具有自我管理許可的 。

合併的控制問題清單

您可以在 Security Hub 的合併控制問題清單功能開啟或關閉時，設定組織中的帳戶。請參閱 AWS Security Hub 使用者指南中的合併控制問題清單。

> **Important**
>
> 如果啟用，您必須使用解決方案的 v2.0.0 或更新版本。此外，您必須為「SC」或「安全控制」標準部署管理員和成員巢狀堆疊。這會部署自動化文件和 EventBridge 規則，以與開啟此功能時IDs產生的合併控制項搭配使用。使用此功能時，不需要為特定標準 （ 例如 AWS FSBP) 部署管理員或成員巢狀堆疊。

AWS CloudFormation 範本

View template

aws-sharr-deploy.template - 使用此範本啟動 AWS解決方案上的自動安全回應。範本會安裝解決方案的核心元件、 AWS Step Functions 日誌的巢狀堆疊，以及您選擇的每個安全標準的巢狀堆疊。

使用的服務包括 Amazon Simple Notification Service AWS Key Management Service、 AWS Identity and Access Management AWS Lambda、、 AWS Step Functions、Amazon CloudWatch Logs、Amazon S3 和 AWS Systems Manager。

管理員帳戶支援

下列範本會安裝在 AWS Security Hub 管理員帳戶中，以開啟您要支援的安全標準。您可以在安裝 時選擇要安裝的下列哪些範本`aws-sharr-deploy.template`。

aws-sharr-orchestrator-log.template - 建立 Orchestrator Step Function 的 CloudWatch 日誌群組。

AFSBPStack.template - AWS 基礎安全最佳實務 1.0.0 版規則。

CIS120Stack.template - CIS Amazon Web Services Foundations 基準，1.2.0 版規則。

CIS140Stack.template - CIS Amazon Web Services Foundations 基準，1.4.0 版規則。

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

NISTStack.template - 國家標準技術研究所 (NIST)，5.0.0 版規則。

SCStack.template - SC 2.0.0 版規則。

成員帳戶

aws-sharr-member.template - 在您設定核心解決方案後使用此範本，在每個 AWS Security Hub 成員帳戶（包括管理員帳戶）中安裝 AWS Systems Manager 自動化 Runbook 和許可。此範本可讓您選擇要安裝的安全標準手冊。

會根據您的選擇`aws-sharr-member.template`安裝下列範本：

aws-sharr-remediations.template - 一或多個安全標準所使用的常見修補程式碼。

AFSBPMemberStack.template - AWS 基礎安全最佳實務 1.0.0 版的設定、許可和修復 Runbook。

CIS120MemberStack.template - CIS Amazon Web Services Foundations 基準測試，1.2.0 版設定、許可和修復 Runbook。

CIS140MemberStack.template - CIS Amazon Web Services Foundations 基準測試，1.4.0 版設定、許可和修復 Runbook。

PCI321MemberStack.template - PCI-DSS v3.2.1 設定、許可和修復 Runbook。

NISTMemberStack.template - 國家標準技術研究所 (NIST)、5.0.0 版設定、許可和修復執行手冊。

SCMemberStack.template - 安全控制設定、許可和修復 Runbook。

成員角色

aws-sharr-member-roles.template - 定義每個 AWS Security Hub 成員帳戶中所需的修復角色。

票證系統整合

使用下列其中一個範本與您的票務系統整合。

JiraBlueprintStack.template - 如果您使用 Jira 做為您的票務系統，請部署 。

View template

ServiceNowBlueprintStack.template - 如果您使用 ServiceNow 做為您的票務系統，請部署 。

如果您想要整合不同的外部票證系統，您可以使用其中一個堆疊做為藍圖，了解如何實作自己的自訂整合。

自動化部署 - StackSets

> **Note**
>
> 建議您使用 部署 StackSets。不過，對於單一帳戶部署或測試或評估目的，請考慮堆疊部署選項。

啟動解決方案之前，請檢閱本指南中討論的架構、解決方案元件、安全性和設計考量事項。遵循 step-by-step本節中的指示，設定解決方案並將其部署到您的 AWS Organizations。

部署時間：每個帳戶約 30 分鐘，取決於 StackSet 參數。

必要條件

AWS Organizations 可協助您集中管理多帳戶AWS環境和資源。與 AWS Organizations StackSets 合作。

如果您先前已部署此解決方案的 v1.3.x 或更早版本，則必須解除安裝現有的解決方案。如需詳細資訊，請參閱更新解決方案。

在部署此解決方案之前，請檢閱您的 AWS Security Hub 部署：

- 您的AWS組織中必須有委派的 Security Hub 管理員帳戶。
- Security Hub 應設定為跨區域彙總問題清單。如需詳細資訊，請參閱 AWS Security Hub 使用者指南中的跨區域彙總問題清單。
- 您應該在有 AWS 使用量的每個區域中，為您的組織啟用 Security Hub。

此程序假設您有多個使用 AWS Organizations 的帳戶，並已委派 AWS Organizations 管理員帳戶和 AWS Security Hub 管理員帳戶。

部署概觀

> **Note**
>
> StackSets 此解決方案的 部署使用服務受管和自我管理的組合 StackSets。目前 StackSets 必須使用自我管理，因為它們使用巢狀 StackSets，服務管理尚不支援 StackSets。

StackSets 從 中的委派管理員帳戶部署 AWS Organizations。

規劃

使用下列表單來協助 StackSets 部署。準備您的資料，然後在部署期間複製並貼上這些值。

```
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):
____________________,
____________________,
____________________,
____________________,
____________________
```

（選用）步驟 0：部署票證整合堆疊

- 如果您想要使用票證功能，請先將票證整合堆疊部署到您的 Security Hub 管理員帳戶。
- 從此堆疊複製 Lambda 函數名稱，並提供它做為管理堆疊的輸入（請參閱步驟 1)。

步驟 1：在委派的 Security Hub 管理員帳戶中啟動管理員堆疊

- 使用自我管理 StackSet，在與 AWS Security Hub 管理員位於相同區域的 Security Hub 管理員帳戶中啟動`aws-sharr-deploy.template`AWS CloudFormation 範本。此範本使用巢狀堆疊。
- 選擇要安裝的安全標準。根據預設，只會選取 SC（建議）。

- 選擇要使用的現有 Orchestrator 日誌群組。Yes 如果先前安裝SO0111-SHARR- Orchestrator已存在，請選取 。

如需自我管理的詳細資訊 StackSets，請參閱AWS CloudFormation 《 使用者指南》中的授予自我管理許可。

步驟 2：在每個成員帳戶中安裝修補角色 AWS Security Hub

等待步驟 1 完成部署，因為步驟 2 中的範本參考步驟 1 建立IAM的角色。

- 使用服務受管 StackSet，在 中每個帳戶中的單一區域中啟動aws-sharr-member-roles.template AWS CloudFormation 範本 AWS Organizations。
- 選擇在新帳戶加入組織時自動安裝此範本。
- 輸入 AWS Security Hub 管理員帳戶的帳戶 ID。

步驟 3：在每個 AWS Security Hub 成員帳戶和區域中啟動成員堆疊

- 使用自我管理 StackSets，將aws-sharr-member.templateAWS CloudFormation 範本啟動到組織內每個帳戶中都有AWS資源的所有區域，這些資源由相同的 Security Hub 管理員AWS管理。

> **Note**
>
> 在服務受管 StackSets 支援巢狀堆疊之前，您必須為加入組織的任何新帳戶執行此步驟。

- 選擇要安裝的 Security Standard 手冊。
- 提供 CloudTrail 日誌群組的名稱（某些修復所使用的名稱）。
- 輸入 AWS Security Hub 管理員帳戶的帳戶 ID。

（選用）步驟 0：啟動票證系統整合堆疊

1. 如果您想要使用票證功能，請先啟動個別的整合堆疊。
2. 選擇 Jira 或 提供的整合堆疊 ServiceNow，或使用它們做為藍圖，以實作您自己的自訂整合。

   若要部署 Jira 堆疊：

   a. 輸入堆疊的名稱。

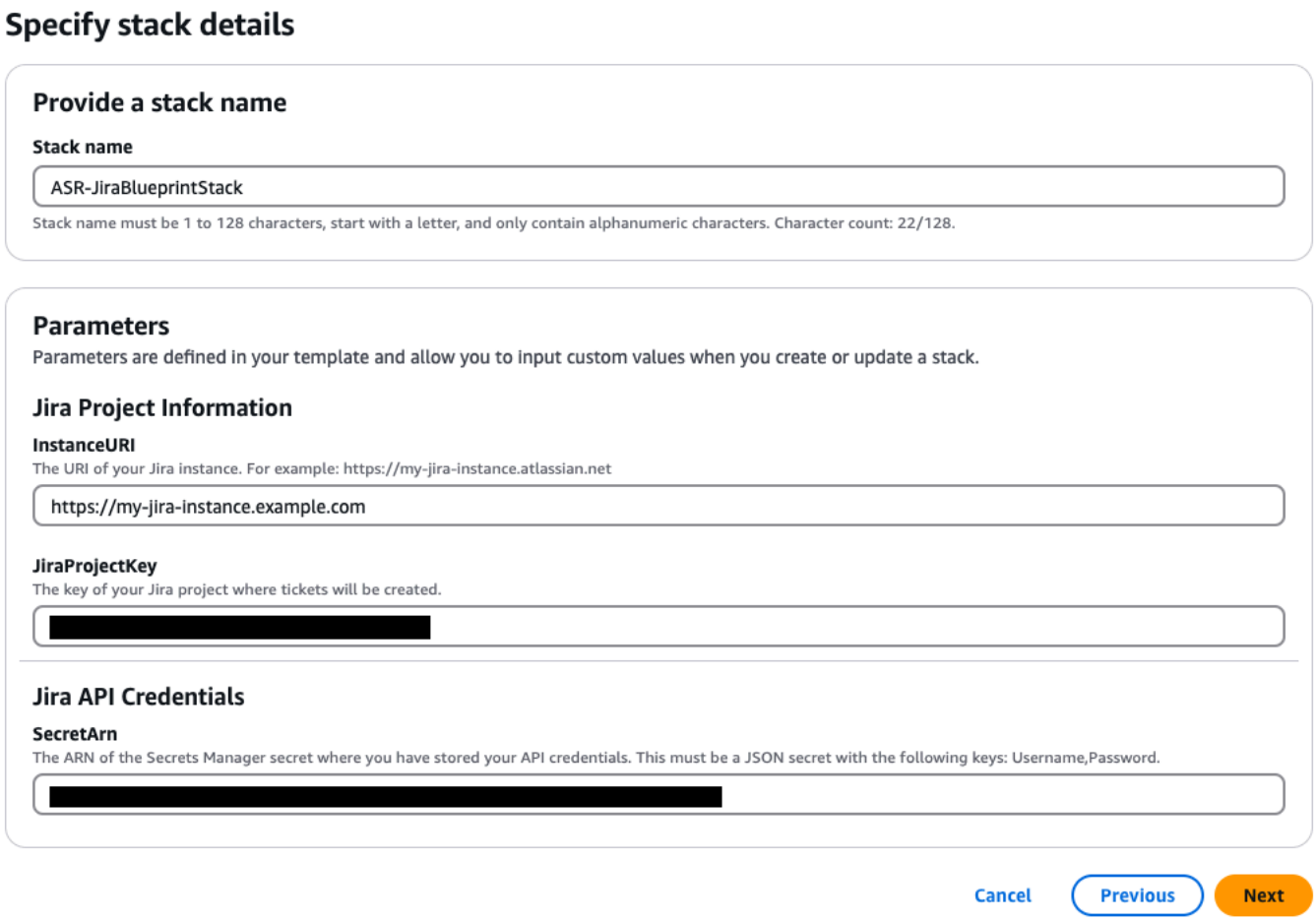
   b. 將 URI提供給 Jira 執行個體。

c. 為您要傳送票證的 Jira 專案提供專案金鑰。

d. 在 Secrets Manager 中建立新的金鑰/值秘密，該秘密會保存您的 Jira `Username`和 `Password`。

> **Note**
>
> 您可以選擇使用 Jira API金鑰來取代密碼，方法是提供使用者名稱做為 `Username`，而API金鑰做為 `Password`。

e. 新增此秘密ARN的 做為堆疊的輸入。



若要部署 ServiceNow 堆疊：

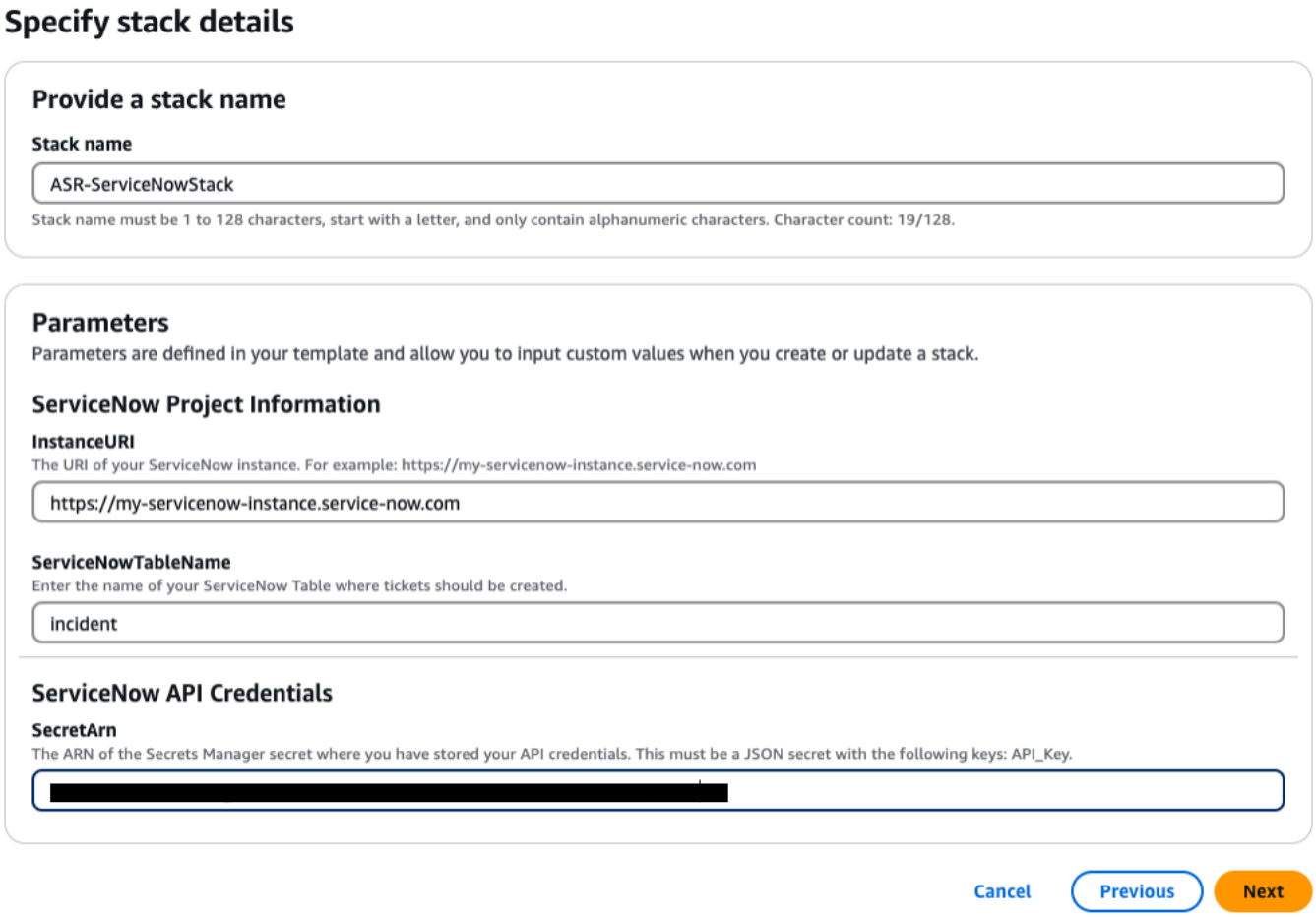
a. 輸入堆疊的名稱。

b. 提供 ServiceNow 執行個體URI的 。

c. 提供您的 ServiceNow 資料表名稱。

d. 在 中建立API金鑰， ServiceNow 並具有修改您要寫入之資料表的許可。

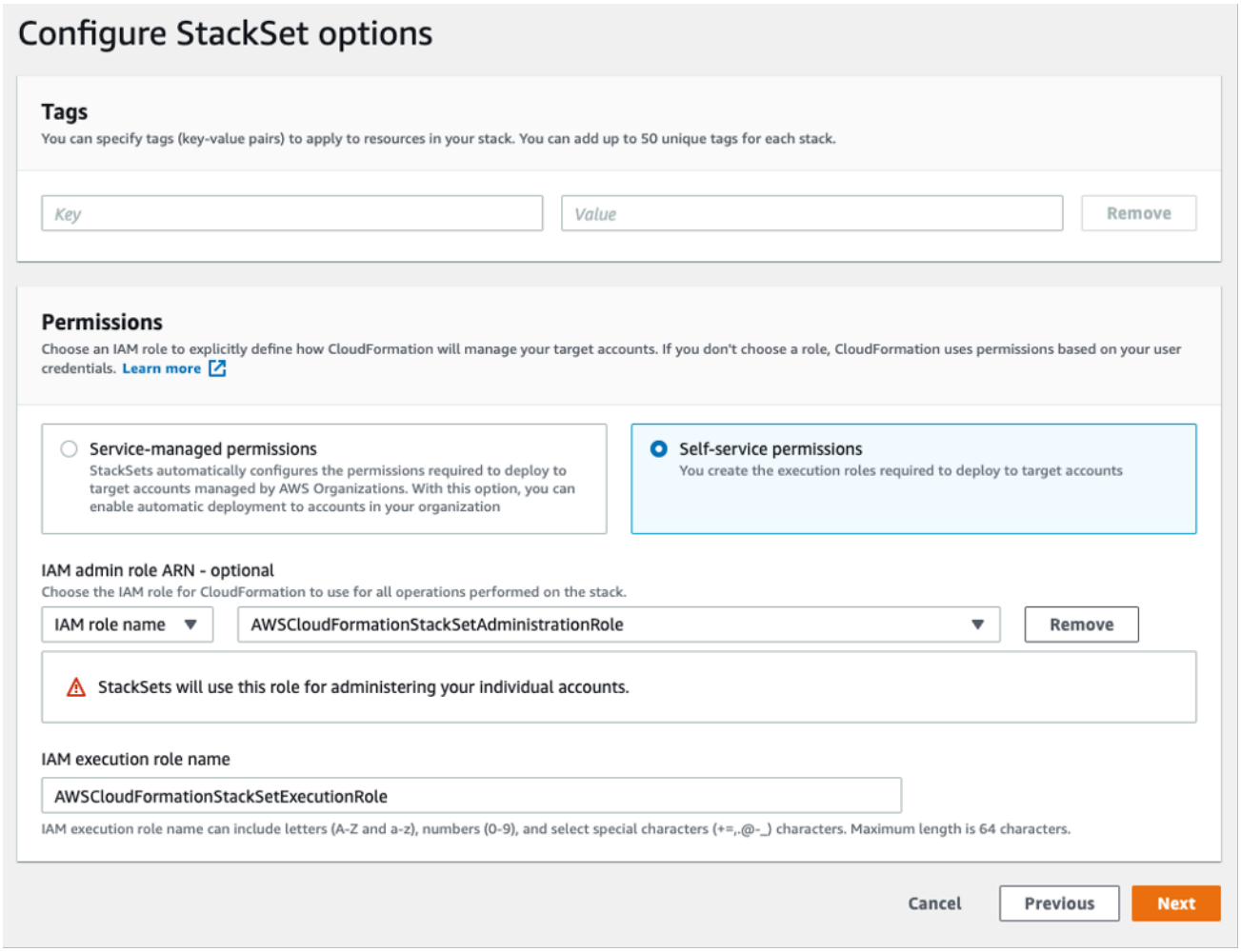
e. 使用 金鑰在 Secrets Manager 中建立秘密，API_Key並提供秘密ARN做為堆疊的輸入。



若要建立自訂整合堆疊：包含解決方案協調器 Step Functions 可以針對每個修復呼叫的 Lambda 函數。Lambda 函數應採用 Step Functions 提供的輸入，根據您的票證系統需求建構承載，並向您的系統提出建立票證的請求。

步驟 1：在委派的 Security Hub 管理員帳戶中啟動管理員堆疊

1. aws-sharr-deploy.template使用您的 Security Hub 管理員帳戶啟動管理員堆疊 。一般而言，單一區域中每個組織一個。由於此堆疊使用巢狀堆疊，您必須將此範本部署為自我管理 StackSet。



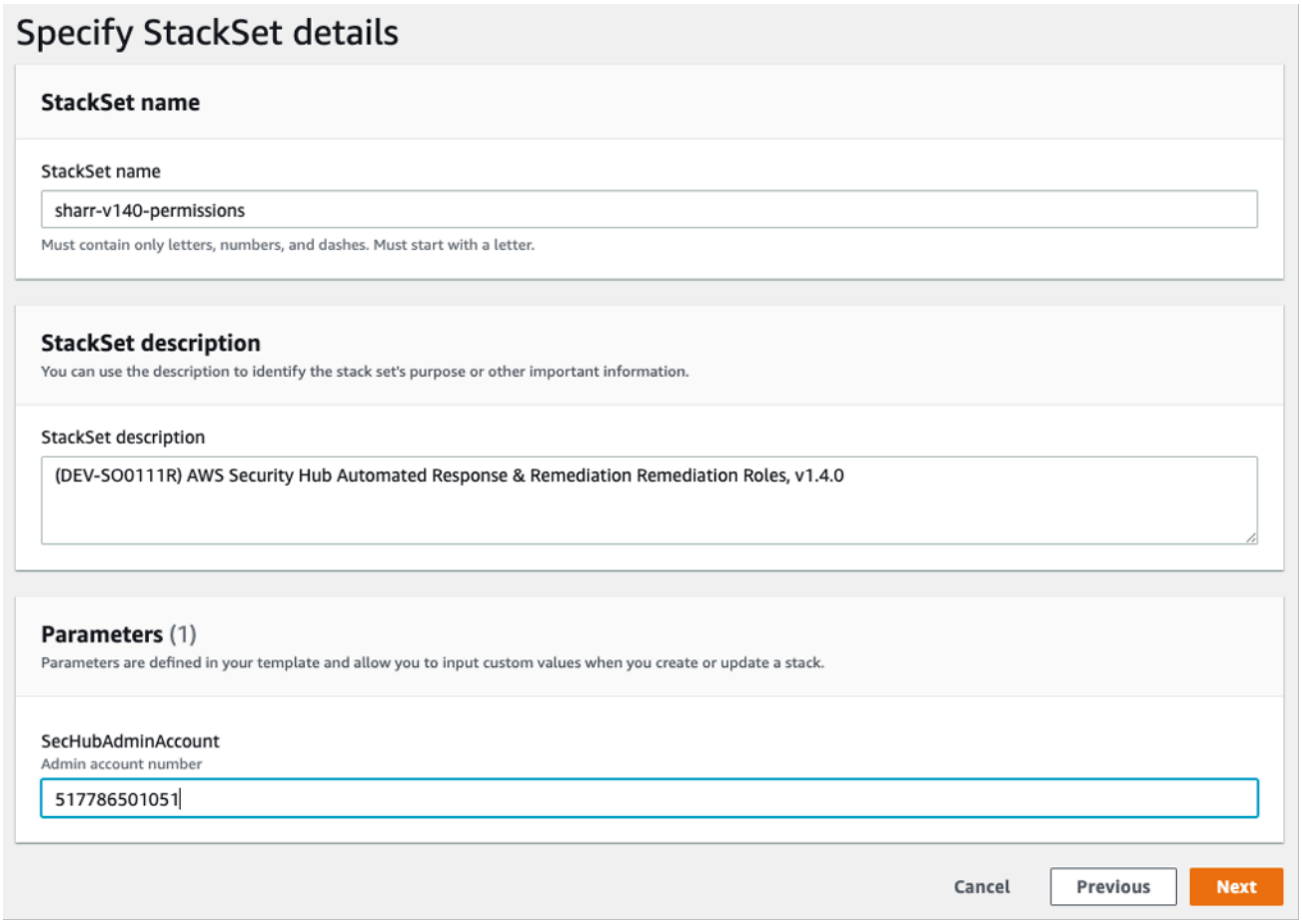
設定 StackSet 選項

2. 針對帳戶號碼參數，輸入 AWS Security Hub 管理員帳戶的帳戶 ID。
3. 對於指定區域參數，請僅選取開啟 Security Hub 管理員的區域。請等待此步驟完成，再繼續步驟 2。

步驟 2：在每個 AWS Security Hub 成員帳戶中安裝修補角色

使用受管服務 StackSets 來部署成員角色範本 `aws-sharr-member-roles.template`。這 StackSet 必須部署在每個成員帳戶的一個區域中。它定義了允許來自 SHARR Orchestrator 步驟函數的跨帳戶API呼叫的全域角色。

1. 根據您的組織政策，部署到整個組織（典型）或組織單位。
2. 開啟自動部署，讓 AWS Organizations 中的新帳戶收到這些許可。
3. 針對指定區域參數，選取單一區域。 IAM角色是全域的。您可以在部署 StackSet時繼續執行步驟 3。



指定 StackSet 詳細資訊

步驟 3：在每個 AWS Security Hub 成員帳戶和區域中啟動成員堆疊

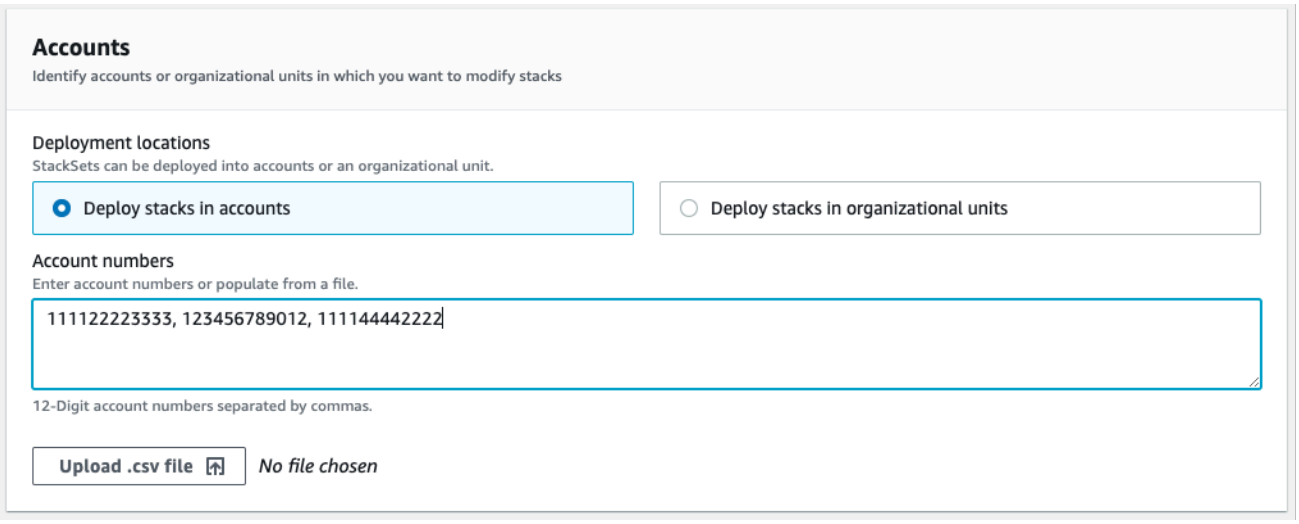
由於成員堆疊使用巢狀堆疊，您必須以自我管理的方式部署 StackSet。這不支援自動部署到 AWS Organization 中的新帳戶。

參數

LogGroup 組態：選擇接收日誌的 CloudTrail 日誌群組。如果不存在，或如果每個帳戶的日誌群組不同，請選擇方便的值。帳戶管理員在建立 CloudTrail 日誌的 CloudWatch 日誌群組之後，必須更新 Systems Manager – 參數 Store /Solutions/SO0111/Metrics_LogGroupName parameter。這對於在API呼叫時建立指標警示的修復是必要的。

標準：選擇要載入成員帳戶的標準。這只會安裝 AWS Systems Manager Runbook，不會啟用安全標準。

SecHubAdminAccount：輸入安裝解決方案管理員範本的 AWS Security Hub Admin 帳戶的帳戶 ID。



帳戶

部署位置：您可以指定帳戶號碼或組織單位的清單。

指定區域：選取您要修復問題清單的所有區域。您可以根據帳戶和區域的數目，適當調整部署選項。區域並行可以是平行的。

自動化部署 - Stacks

> **Note**
>
> 對於多帳戶客戶，我們強烈建議使用 部署 StackSets。

啟動解決方案之前，請檢閱本指南中討論的架構、解決方案元件、安全性和設計考量事項。遵循 step-by-step本節中的指示，設定解決方案並將其部署到您的帳戶。

部署時間：約 30 分鐘

必要條件

部署此解決方案之前，請確定 與您的主要和次要帳戶 AWS Security Hub 位於相同的 AWS 區域。如果您先前已部署此解決方案，則必須解除安裝現有的解決方案。如需詳細資訊，請參閱更新解決方案。

部署概觀

使用下列步驟在 上部署此解決方案AWS。

（選用）步驟 0：啟動票證系統整合堆疊

- 如果您想要使用票證功能，請先將票證整合堆疊部署到您的 Security Hub 管理員帳戶。
- 從此堆疊複製 Lambda 函數名稱，並提供它做為管理堆疊的輸入（請參閱步驟 1)。

步驟 1：啟動管理員堆疊

- 在您的 AWS Security Hub 管理員帳戶中啟動`aws-sharr-deploy.template` AWS CloudFormation 範本。
- 選擇要安裝的安全標準。
- 選擇要使用的現有 Orchestrator 日誌群組（如果先前安裝`SO0111-SHARR-Orchestrator`已存在，請選擇`Yes`此選項）。

步驟 2：在每個成員帳戶中安裝修補角色 AWS Security Hub

- 在每個成員帳戶的一個區域中啟動`aws-sharr-member-roles.template` AWS CloudFormation 範本。
- 輸入 AWS Security Hub 管理員帳戶的 12 位數帳戶 IG。

步驟 3：啟動成員堆疊

- 指定要與 3.1-3.14 CIS 修復搭配使用的 CloudWatch Logs 群組名稱。它必須是接收日誌的 CloudWatch Logs CloudTrail 日誌群組的名稱。
- 選擇是否要安裝修復角色。每個帳戶只能安裝這些角色一次。
- 選取要安裝的手冊。
- 輸入 AWS Security Hub 管理員帳戶的帳戶 ID。

步驟 4：（選用）調整可用的補救措施

- 移除以每個成員帳戶為基礎的任何修復。此為選擇性步驟。

（選用）步驟 0：啟動票證系統整合堆疊

1. 如果您想要使用票證功能，請先啟動個別的整合堆疊。
2. 選擇 Jira 或 提供的整合堆疊 ServiceNow，或使用它們做為藍圖，以實作您自己的自訂整合。

   若要部署 Jira 堆疊：

a. 輸入堆疊的名稱。

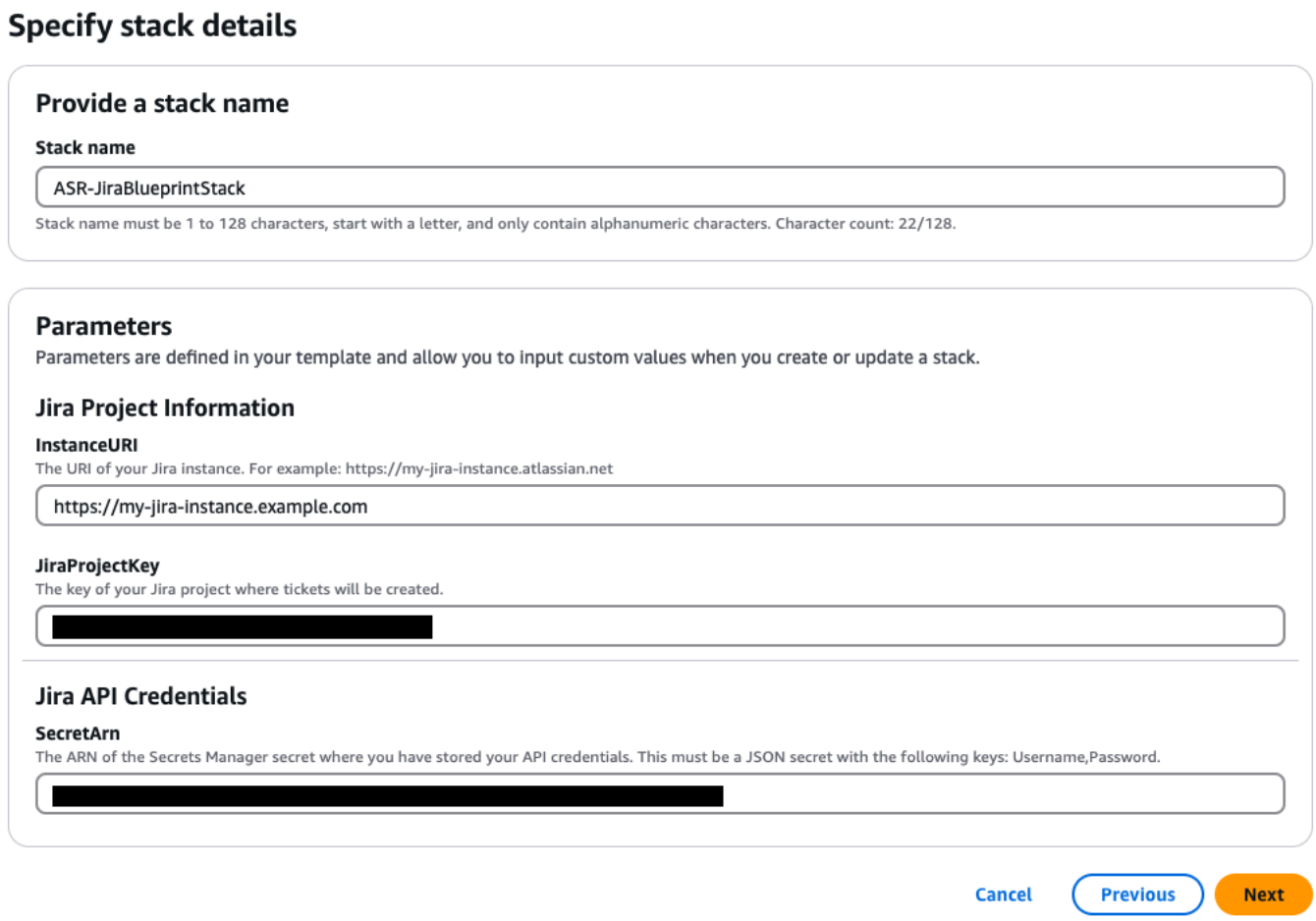
b. 將 URI提供給 Jira 執行個體。

c. 為您要傳送票證的 Jira 專案提供專案金鑰。

d. 在 Secrets Manager 中建立新的金鑰/值秘密，該秘密會保存您的 Jira `Username`和 `Password`。

> **Note**
>
> 您可以選擇使用 Jira API金鑰取代您的密碼，方法是將使用者名稱做為 ，`Username`並將API金鑰做為 `Password`。

e. 新增此秘密ARN的 做為堆疊的輸入。



若要部署 ServiceNow 堆疊：

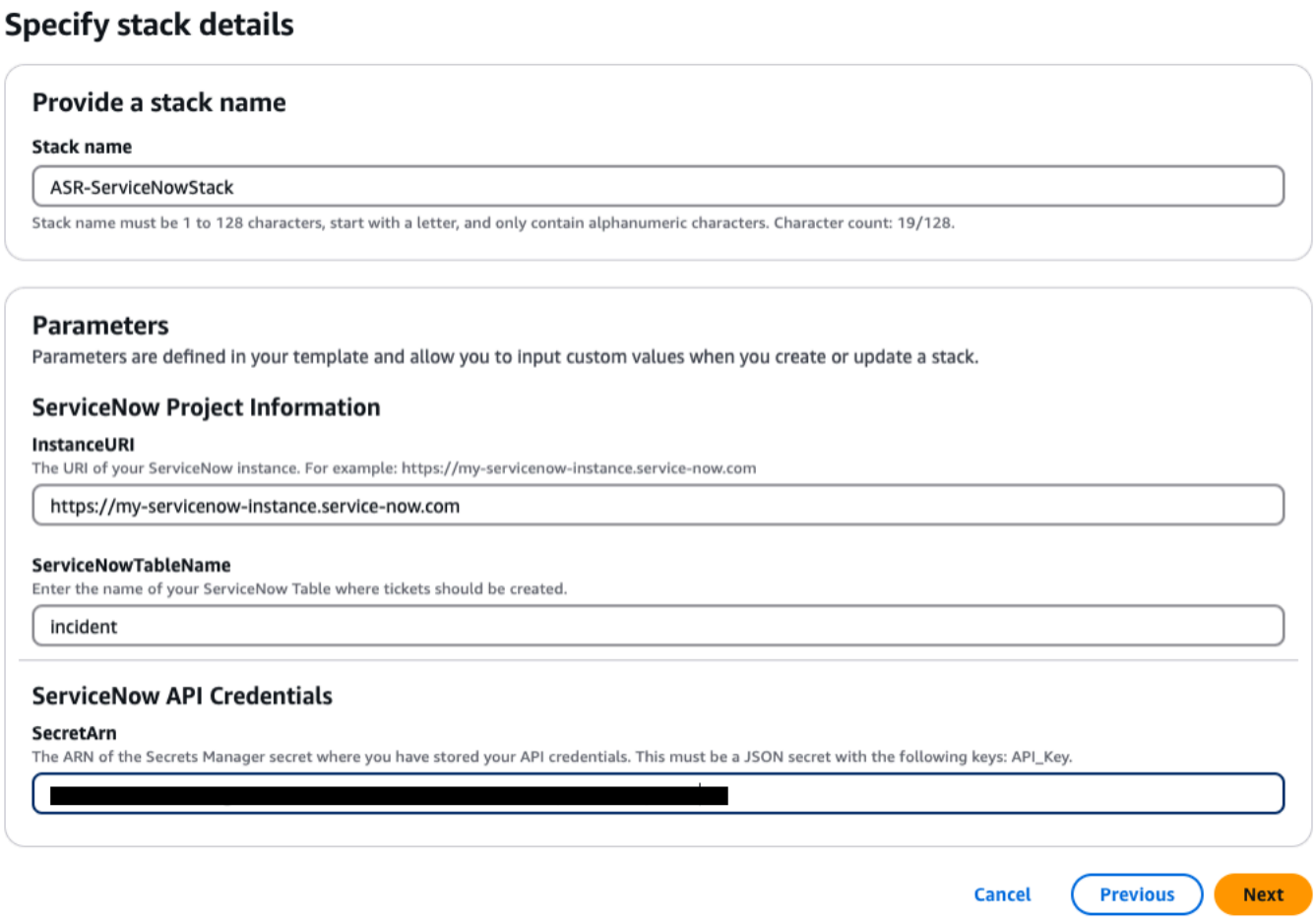
a. 輸入堆疊的名稱。

b. 提供 ServiceNow 執行個體URI的 。

c. 提供您的 ServiceNow 資料表名稱。

d. 在 中建立API金鑰， ServiceNow 並具有修改您要寫入之資料表的許可。

e. 使用 金鑰在 Secrets Manager 中建立秘密，`API_Key`並提供秘密ARN做為堆疊的輸入。



若要建立自訂整合堆疊：包含解決方案協調器 Step Functions 可以針對每個修復呼叫的 Lambda 函數。Lambda 函數應採用 Step Functions 提供的輸入，根據您的票證系統需求建構承載，並向您的系統提出建立票證的請求。

步驟 1：啟動管理員堆疊

> **Important**
>
> 此解決方案包含將匿名操作指標傳送至 的選項AWS。我們使用這些資料來更好地了解客戶如何使用此解決方案和相關的服務和產品。 AWS擁有透過此調查所收集的資料。資料收集受 AWS 隱私權通知的約束。

若要選擇退出此功能，請下載範本、修改AWS CloudFormation映射區段，然後使用 AWS CloudFormation 主控台上傳範本並部署解決方案。如需詳細資訊，請參閱本指南的匿名資料收集一節。

此自動化 AWS CloudFormation 範本會在 AWS 雲端部署AWS自動化安全回應解決方案。啟動堆疊之前，您必須啟用 Security Hub 並完成先決條件。

> **Note**
>
> 您需負責支付執行此解決方案時所使用的AWS服務成本。如需詳細資訊，請參閱本指南中的成本區段，並參考此解決方案中每個AWS服務的定價網頁。

1. AWS Management Console 從目前設定 的 帳戶登入 AWS Security Hub ，然後使用下面的按鈕來啟動`aws-sharr-deploy.template` AWS CloudFormation 範本。

   Launch solution

   您也可以將下載範本作爲自有實作的起點。
2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動此解決方案 AWS，請使用導覽列中的 AWS Management Console 區域選擇器。

   > **Note**
   >
   > 此解決方案使用目前僅在特定 AWS 區域中可用的 AWS Systems Manager 。解決方案適用於支援此服務的所有 區域。如需依區域分類的最新可用性，請參閱AWS 區域服務清單。
3. 在建立堆疊頁面上，驗證 Amazon S3 URL文字方塊中URL是否有正確的範本，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱 AWS Identity and Access Management 使用者指南中的 IAM和 STS限制。
5. 在參數頁面上，選擇下一步。

參數	預設	描述
Load SC Admin Stack	yes	指定是否要安裝管理員元件，以自動修復 SC 控制項。
負載AFSBP管理堆疊	no	指定是否安裝 管理元件以自動修復FSBP控制項。
載入 CIS120 Admin Stack	no	指定是否要安裝管理員元件，以自動修復 CIS120 個控制項。
載入 CIS140 Admin Stack	no	指定是否要安裝 管理員元件以自動修復 CIS140 個控制項。
載入 CIS300 Admin Stack	no	指定是否要安裝 管理元件以自動修復 CIS300 個控制項。
載入PC1321管理員堆疊	no	指定是否要安裝 管理員元件，以自動修復PC1321控制項。
載入NIST管理員堆疊	no	指定是否要安裝 管理員元件，以自動修復NIST控制項。
重複使用 Orchestrator Log Group	no	選取是否要重複使用現有的 SO0111-SHARR-Orchestrator CloudWatch Logs 群組。這可簡化重新安裝和升級，而不會遺失先前版本的日誌資料。如果您要從 v1.2 或更高版本升級，請選取 。yes

參數	預設	描述
使用 CloudWatch 指標	yes	指定是否要啟用 CloudWatch 指標來監控解決方案。這會建立 CloudWatch 儀表板來檢視指標。
使用 CloudWatch 指標警示	yes	指定是否啟用解決方案的 CloudWatch 指標警示。這將為解決方案收集的特定指標建立警示。
RemediationFailure AlarmThreshold	5	指定每個控制項 ID 修復失敗百分比的閾值。例如，如果您輸入 5，如果控制 ID 在指定日期失敗超過 5% 的修復，則會收到警示。 此參數僅在建立警示時才運作（請參閱使用 CloudWatch 指標警示參數）。
EnableEnhancedCloudWatchMetrics	no	如果 yes， 會建立其他 CloudWatch 指標，以IDs 個別追蹤 CloudWatch 儀表板上的所有控制項，並以 CloudWatch 警示的形式追蹤。 請參閱 成本 區段，以了解此產生的額外費用。
TicketGenFunctionName	（選用輸入）	選用。如果您不想整合票證系統，請保留空白。否則，請提供步驟 0 堆疊輸出的 Lambda 函數名稱，例如：SO0111-ASR-ServiceNow-TicketGenerator 。

6. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
7. 在檢視 頁面上，檢視和確認的設定。勾選確認範本將建立 AWS Identity and Access Management (IAM) 資源的方塊。
8. 選擇 Create stack (建立堆疊) 以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內收到 CREATE_COMPLETE 狀態。

步驟 2：在每個 AWS Security Hub 成員帳戶中安裝修補角色

每個成員帳戶只能在一個區域中`aws-sharr-member-roles.template` StackSet 部署 。它定義了允許來自 SHARR Orchestrator 步驟函數的跨帳戶API呼叫的全域角色。

1. 登入每個 AWS Security Hub 成員帳戶的 AWS 管理主控台 （包括管理員帳戶，這也是成員）。選取按鈕以啟動`aws-sharr-member-roles.template` AWS CloudFormation 範本。您也可以將下載範本作爲自有實作的起點。

Launch solution

2. 根據預設，範本會在美國東部 （維吉尼亞北部） 區域啟動。若要在不同區域中啟動此解決方案 AWS，請使用 AWS 管理主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，驗證 Amazon S3 URL文字方塊中URL是否有正確的範本，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱 AWS Identity and Access Management 使用者指南中的 IAM和 STS限制。
5. 在參數頁面上，指定下列參數，然後選擇下一步。

參數	預設	描述
命名空間	*<Requires input>*	輸入最多 9 個小寫英數字元的字串。此字串會成為IAM角色名稱的一部分。針對成員堆疊部署和成員角色堆疊部署使用相同的值。
Sec Hub 帳戶管理員	*<Requires input>*	輸入 AWS Security Hub 管理員帳戶的 12 位數帳戶 ID。此

參數	預設	描述
		值會將許可授予管理員帳戶的解決方案角色。

6. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
7. 在檢視 頁面上，檢視和確認的設定。勾選確認範本將建立 AWS Identity and Access Management (IAM) 資源的方塊。
8. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 5 分鐘內收到 CREATE_COMPLETE 狀態。您可以在此堆疊載入時繼續下一個步驟。

步驟 3：啟動成員堆疊

> **Important**
>
> 此解決方案包含將匿名操作指標傳送至 的選項AWS。我們使用這些資料來更好地了解客戶如何使用此解決方案和相關的服務和產品。 AWS擁有透過此調查所收集的資料。資料收集受 AWS 隱私權政策約束。
> 若要選擇退出此功能，請下載範本、修改AWS CloudFormation映射區段，然後使用AWS CloudFormation 主控台上傳範本並部署解決方案。如需詳細資訊，請參閱本指南的操作指標集合一節。

`aws-sharr-member` 堆疊必須安裝在每個 Security Hub 成員帳戶中。此堆疊會定義自動修復的 Runbook。每個成員帳戶的管理員可以控制可透過此堆疊取得哪些修補。

1. 登入 AWS Management Console 每個 AWS Security Hub 成員帳戶的 （包括管理員帳戶，其也是成員）。選取按鈕以啟動`aws-sharr-member.template` AWS CloudFormation 範本。

   Launch solution

   您也可以將下載範本作爲自有實作的起點。
2. 根據預設，範本會在美國東部 （維吉尼亞北部） 區域啟動。若要在不同區域中啟動此解決方案 AWS，請使用導覽列中的 AWS Management Console 區域選擇器。

> **Note**
>
> 此解決方案使用 AWS Systems Manager，目前可在大多數 AWS 區域使用。解決方案可在支援這些服務的所有 區域中運作。如需依區域分類的最新可用性，請參閱AWS 區域服務清單。

3. 在建立堆疊頁面上，驗證 Amazon S3 URL文字方塊中URL是否有正確的範本，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱 AWS Identity and Access Management 使用者指南中的 IAM和 STS限制。
5. 在參數頁面上，指定下列參數，然後選擇下一步。

參數	預設	描述
提供 LogGroup 用於建立指標篩選條件和警示的 名稱	*<Requires input>*	指定 CloudTrail 記錄API呼叫的 CloudWatch Logs 群組名稱。這用於 CIS 3.1-3.14 修復。
載入 SC 成員堆疊	yes	指定是否要安裝成員元件以自動修復 SC 控制項。
載入AFSBP成員堆疊	no	指定是否要安裝成員元件以自動修復FSBP控制項。
載入 CIS120 成員堆疊	no	指定是否要安裝成員元件以自動修復 CIS120 個控制項。
載入 CIS140 成員堆疊	no	指定是否要安裝成員元件以自動修復 CIS140 個控制項。
載入 CIS300 成員堆疊	no	指定是否要安裝成員元件以自動修復 CIS300 個控制項。
載入PC1321成員堆疊	no	指定是否要安裝成員元件以自動修復PC1321控制項。

參數	預設	描述
載入NIST成員堆疊	no	指定是否要安裝成員元件以自動修復NIST控制項。
為 Redshift 稽核記錄建立 S3 儲存貯體	no	選取yes是否應該為 RedShift.4 修復建立 S3 FSBP 儲存貯體。如需 S3 儲存貯體和修復的詳細資訊，請參閱 AWS Security Hub 使用者指南中的 Redshift.4 修復。
Sec Hub 管理員帳戶	*<Requires input>*	輸入 AWS Security Hub 管理員帳戶的 12 位數帳戶 ID。
命名空間	*<Requires input>*	輸入最多 9 個小寫英數字元的字串。此字串會成為IAM角色名稱和動作日誌 S3 儲存貯體的一部分。針對成員堆疊部署和成員角色堆疊部署使用相同的值。此字串必須遵循一般用途 Amazon S3 S3 命名規則。
EnableCloudTrailForASRActionLog	no	yes 如果您想要監控 CloudWatch 儀表板上解決方案執行的管理事件，請選取 。解決方案會在您選取 的每個成員帳戶中建立 CloudTrail 線索yes。請參閱成本 區段，以了解此產生的額外費用。

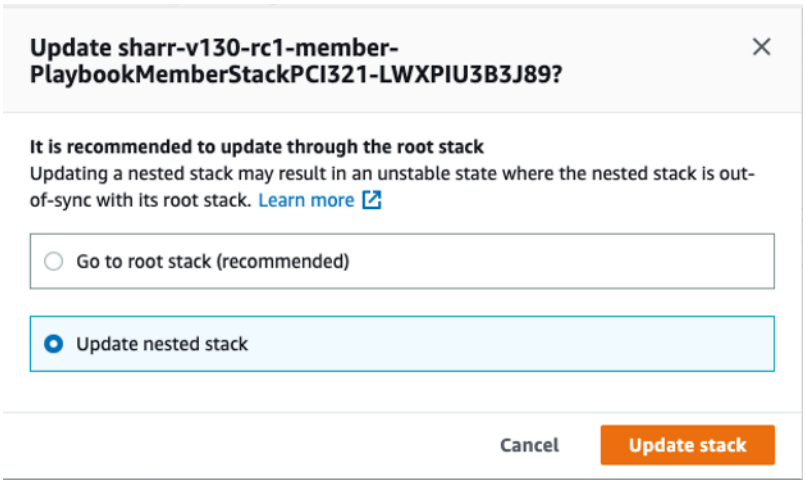
6. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
7. 在檢視 頁面上，檢視和確認的設定。勾選確認範本將建立 AWS Identity and Access Management (IAM) 資源的方塊。
8. 選擇 Create stack (建立堆疊) 以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內收到 CREATE_COMPLETE 狀態。

步驟 4：（選用）調整可用的補救措施

如果您想要從成員帳戶移除特定修復，您可以更新安全標準的巢狀堆疊來執行此操作。為了簡化，巢狀堆疊選項不會傳播到根堆疊。

1. 登入 AWS CloudFormation 主控台，然後選取巢狀堆疊。
2. 選擇更新。
3. 選取更新巢狀堆疊，然後選擇更新堆疊。



更新巢狀堆疊

4. 選取使用目前範本，然後選擇下一步。
5. 調整可用的修補。將所需控制項的值變更為 `Available`，並將不需要的控制項變更為 `Not available`。

> **Note**
>
> 關閉修補會移除安全標準和控制項的解決方案修補 Runbook。

6. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
7. 在檢視 頁面上，檢視和確認的設定。勾選確認範本將建立 AWS Identity and Access Management (IAM) 資源的方塊。
8. 請選擇更新堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內收到 CREATE_COMPLETE 狀態。

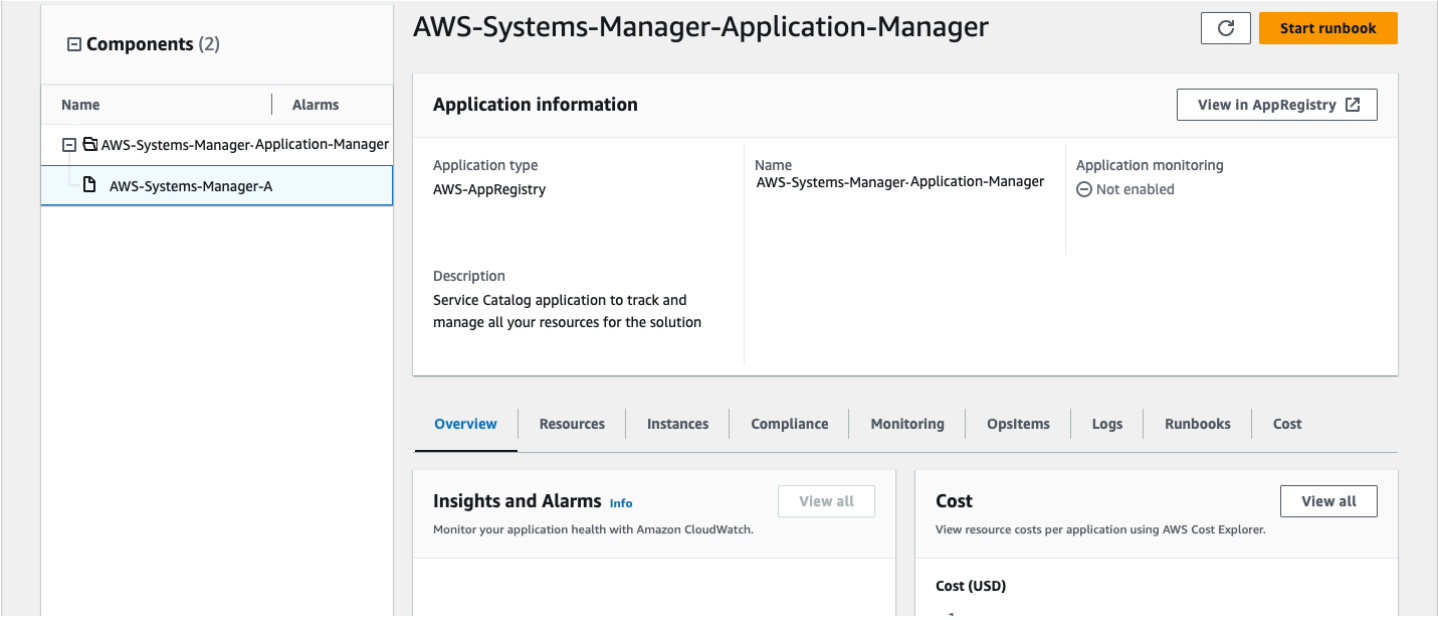
使用 Service Catalog 監控解決方案 AppRegistry

此解決方案包含 Service Catalog AppRegistry 資源，可將 CloudFormation 範本和基礎資源註冊為 Service Catalog AppRegistry 和 AWS Systems Manager Application Manager 中的應用程式。

AWS Systems Manager Application Manager 提供您此解決方案及其資源的應用程式層級檢視，讓您可以：

- 從中央位置監控其資源、跨堆疊和與此解決方案相關聯的已部署資源成本 AWS 帳戶，以及日誌。
- 檢視應用程式內容中此解決方案資源的操作資料（例如部署狀態、 CloudWatch 警示、資源組態和操作問題）。

  下圖描述 Application Manager 中解決方案堆疊的應用程式檢視範例。



Application Manager 中的解決方案堆疊

使用 CloudWatch Application Insights

此解決方案會在部署時自動與 CloudWatch Application Insights 整合。 CloudWatch Application Insights 可協助您查看並了解解決方案的運作狀態和效能，方法如下：

- 自動探索和監控金鑰應用程式資源。

- 建立自訂警示以主動識別潛在問題。
- 偵測到異常或失敗 OpsItems 時自動產生 Systems Manager。這些 OpsItems 通知可做為可行的通知，即時通知您影響解決方案的問題。

請依照下列步驟檢視 CloudWatch Application Insights 監控儀表板，您可以在其中檢視解決方案的運作狀態，並透過預先設定的儀表板和警示監控關鍵元件。

1. 導覽至 CloudWatch 主控台。
2. 選擇洞見索引標籤，然後選擇 Application Insights。
3. 選擇應用程式索引標籤，然後選擇與解決方案相關聯的應用程式。

您也可以匯入解決方案的 CloudWatch 儀表板，以整合對解決方案運作狀態的監控。在 Application CloudWatch Insights 中解決方案的應用程式儀表板上，請遵循下列步驟：

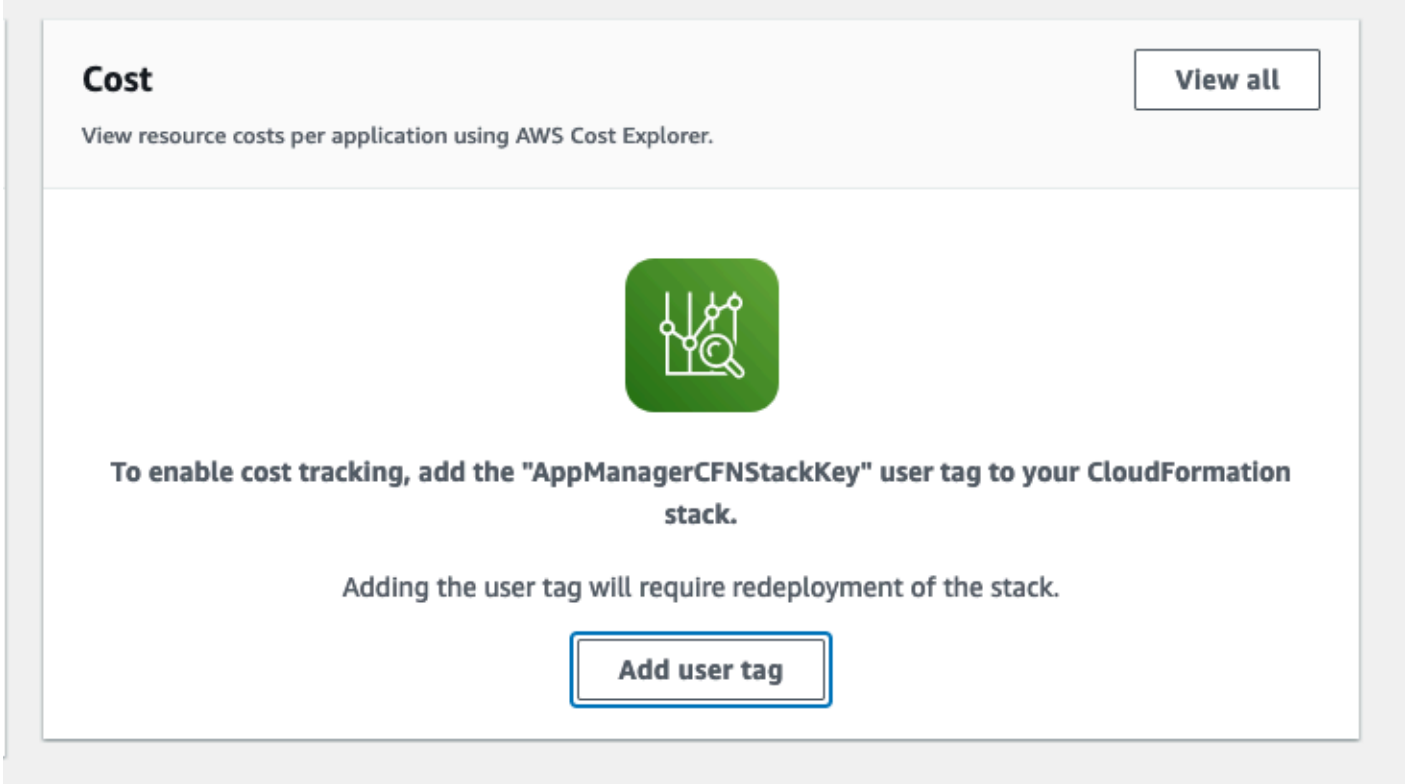
1. 選擇自訂 CloudWatch 儀表板索引標籤。
2. 選擇匯入 CloudWatch 儀表板。
3. 在搜尋方塊中，輸入 `ASR-Remediation-Metrics-Dashboard`，然後選取 AWS 儀表板上的自動安全回應。
4. 選擇匯入。

現在您可以在 CloudWatch Application Insights 主控台中檢視 CloudWatch Application Insights 儀表板和解決方案的自訂儀表板，而不必在頁面之間切換。

確認與解決方案相關聯的成本標籤

啟用與解決方案相關聯的成本分配標籤後，您必須確認成本分配標籤，才能查看此解決方案的成本。若要確認成本分配標籤：

1. 登入 Systems Manager 主控台。
2. 在導覽窗格中，選擇 Application Manager。
3. 在應用程式中，選擇此解決方案的應用程式名稱，然後選取它。
4. 在概觀索引標籤中，在成本中，選取新增使用者標籤。



5. 在新增使用者標籤頁面上，輸入 `confirm`，然後選取新增使用者標籤。

啟用程序最多可能需要 24 小時才能完成，並顯示標籤資料。

啟用與解決方案相關聯的成本分配標籤

確認與此解決方案相關聯的成本標籤後，您必須啟用成本分配標籤，以查看此解決方案的成本。成本分配標籤只能從組織的管理帳戶啟用。

若要啟用成本分配標籤：

1. 登入 AWS Billing and Cost Management 和 Cost Management 主控台。
2. 在導覽窗格中，選取成本分配標籤。
3. 在成本分配標籤頁面上，篩選`AppManagerCFNStackKey`標籤，然後從顯示的結果中選取標籤。
4. 選擇 Activate (啟用)。

AWS Cost Explorer

您可以透過與 AWS Cost Explorer 整合，在 Application Manager 主控台中查看與應用程式和應用程式元件相關聯的成本概觀。Cost Explorer 透過提供一段時間AWS的資源成本和用量的檢視，協助您管理成本。

1. 登入 AWS Cost Management 主控台。
2. 在導覽功能表中，選取 Cost Explorer 以檢視解決方案隨時間的成本和用量。

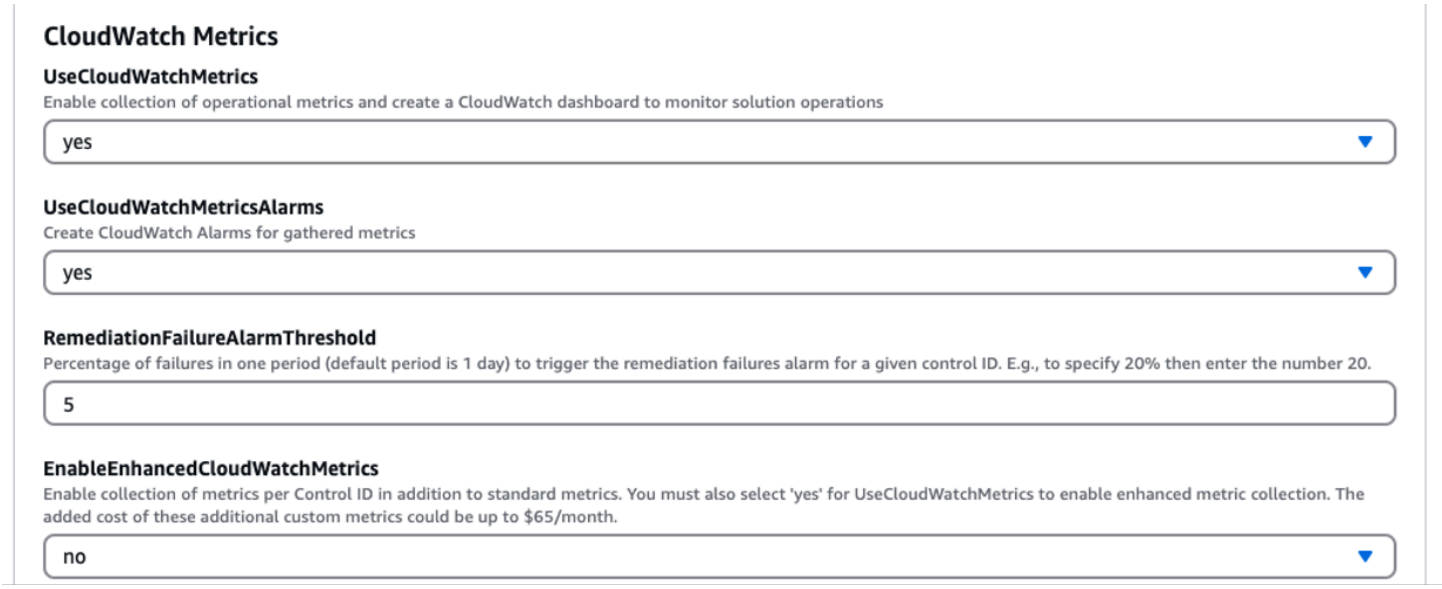
使用 Amazon CloudWatch 儀表板監控解決方案的操作

此解決方案包含顯示在 Amazon CloudWatch 儀表板上的自訂指標和警示。

CloudWatch 儀表板和警示會監控解決方案的操作，並在發生潛在問題時發出警示。

啟用 CloudWatch 指標、警示和儀表板

功能有四個 CloudFormation 範本參數 CloudWatch。



1. UseCloudWatchMetrics – 將此設定為yes啟用操作指標的集合，並建立 CloudWatch 儀表板來檢視這些指標。
2. UseCloudWatchAlarms – 將此設定為yes啟用解決方案的預設警示。
3. RemediationFailureAlarmThreshold – 一段時間內無法修補以引發警示的百分比。
4. EnableEnhancedCloudWatchMetrics – 將此參數設定為 yes，以收集每個控制項 ID 的個別指標。根據預設，此參數會設為 no，因此只會IDs收集所有控制項中修復總數的指標。每個控制 ID 的個別指標和警示會產生額外費用。

使用 CloudWatch 儀表板

若要檢視儀表板：

1. 導覽至 Amazon， CloudWatch 然後導覽至 Dashboards。
2. 選取名為 "ASR-Remediation-Metrics-Dashboard" 的儀表板。

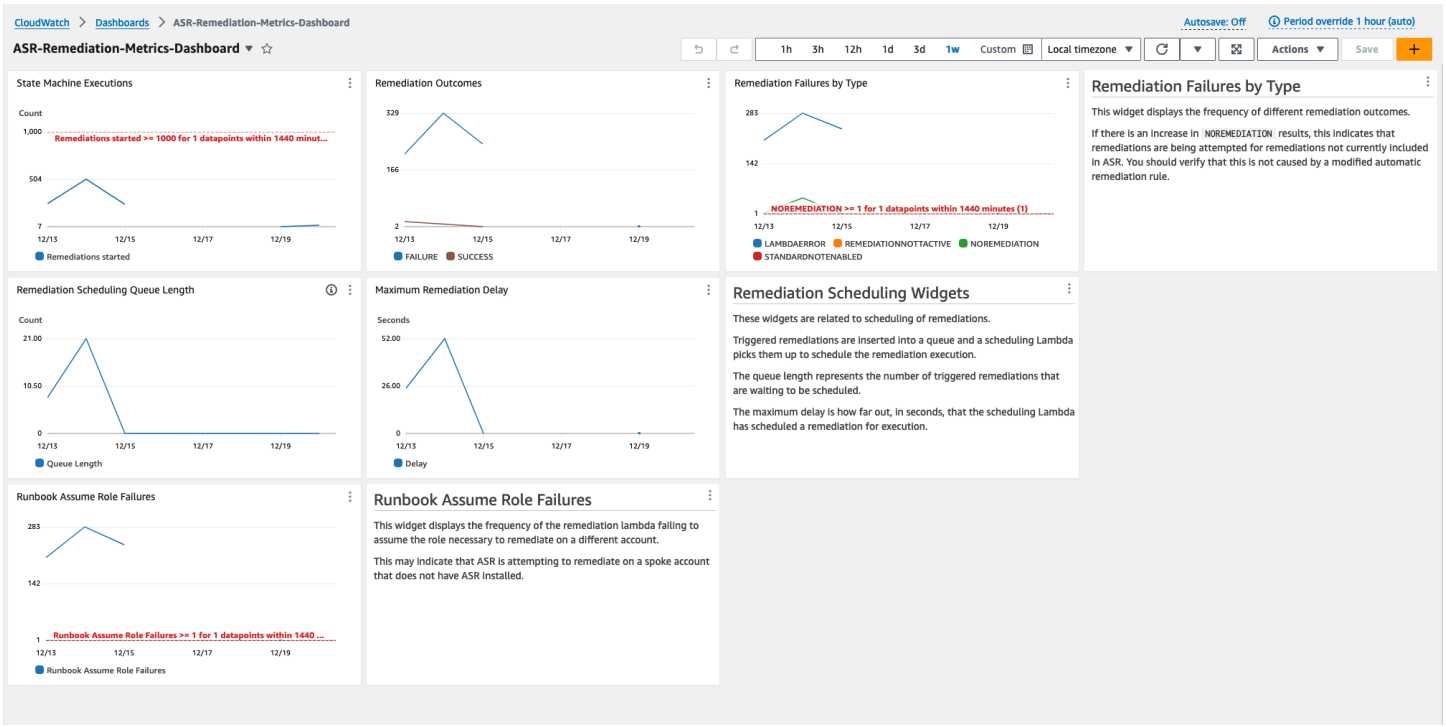
CloudWatch 儀表板包含下列區段：

1. 成功修復總數 – 可讓您深入了解解決方案已成功修復的 Security Hub 問題清單數量。
2. 修復失敗 – 顯示失敗的修復總數和百分比，以及失敗原因。大量故障可能會暗示您可能需要更詳細調查的解決方案發生技術問題。
3. 依控制項 ID 修正成功/失敗 – 如果您在部署時間啟用增強型指標，本節會依控制項 ID 列出修補結果。當修復失敗區段顯示高故障率時，本節會顯示故障是分散到許多控制項 IDs，還是只有特定控制項IDs失敗。
4. Runbook 假設角色失敗 – 顯示由於未安裝解決方案成員角色的帳戶嘗試修復而發生的失敗次數。由於缺少角色而導致自動修復嘗試重複失敗，會導致不必要的成本。在相關帳戶中安裝成員角色堆疊、停用解決方案建立的所有 EventBridge 規則，或在 Security Hub 中取消帳戶關聯，以緩解此問題。
5. Cloud Trail Management Actions by ASR – 列出您在部署時間使用 EnableCloudTrailForASRActionLog 參數啟用動作日誌的所有成員帳戶中解決方案的管理動作。當您發現任何 AWS 帳戶的意外資源變更時，此小工具可協助您了解 解決方案是否修改了資源。

CloudWatch 儀表板也隨附預先定義的警示，提醒常見的操作錯誤。

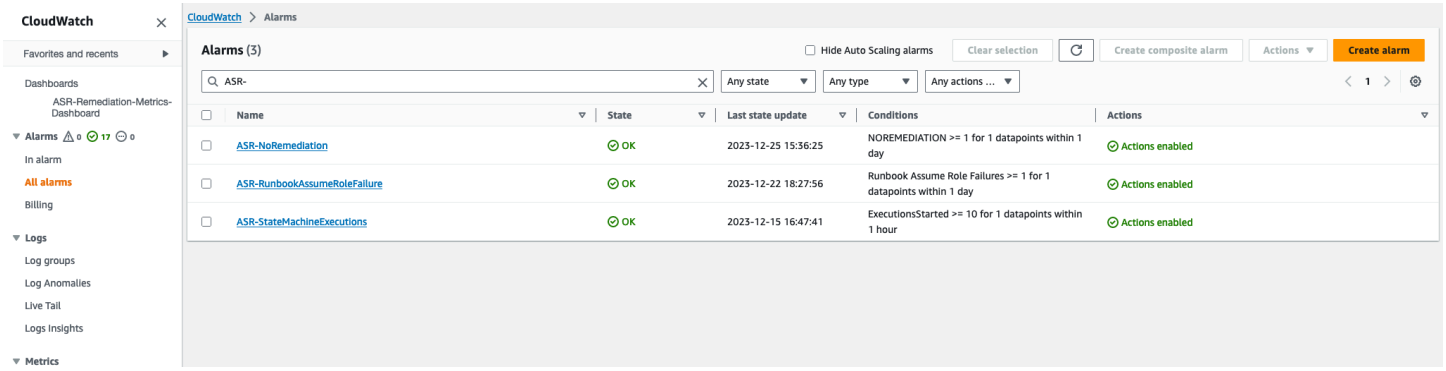
1. 狀態機器在 24 小時內執行 > 1000。
   a. 修復執行的大幅激增可能表示事件規則啟動的頻率高於預期。
   b. 您可以使用 CloudFormation 參數變更閾值。
2. 依類型 = NOREMEDIATION > 0 的修復失敗
   a. 正在嘗試修復未包含在 中的修復ASR。這可能表示已修改事件規則，以包含超過預期的修補。
3. Runbook 假設角色失敗 > 0
   a. 嘗試對未正確部署解決方案的帳戶或區域進行修復。這可能表示已修改事件規則，以包含比預期更多的帳戶。

您可以修改所有警示閾值，以符合個別部署需求。

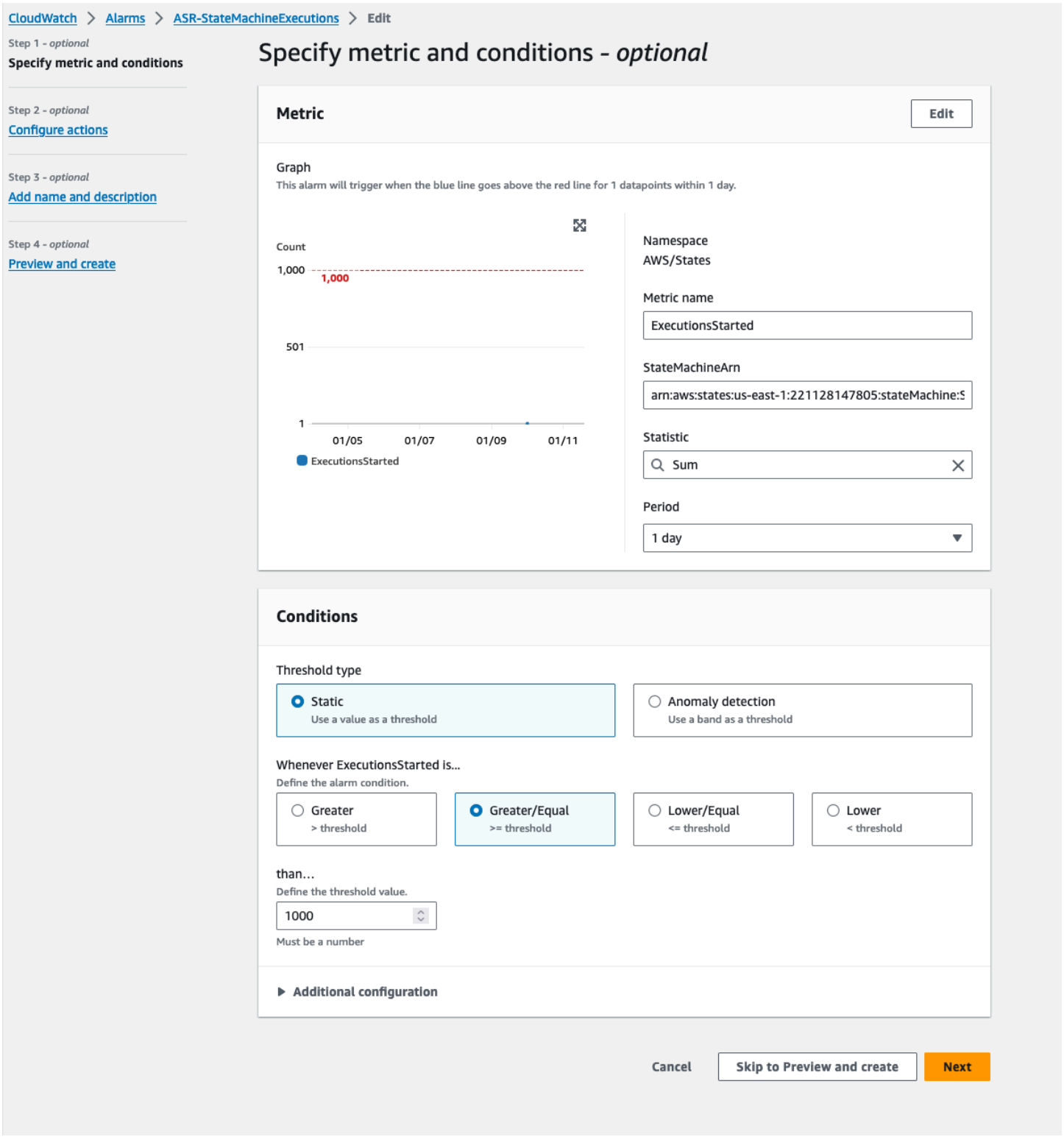


修改警示閾值

1. 導覽至 Amazon CloudWatch -> 警示 -> 所有警示。
2. 選擇您要修改的警示，然後選擇動作 -> 編輯。



3. 將閾值變更為所需的值並儲存。



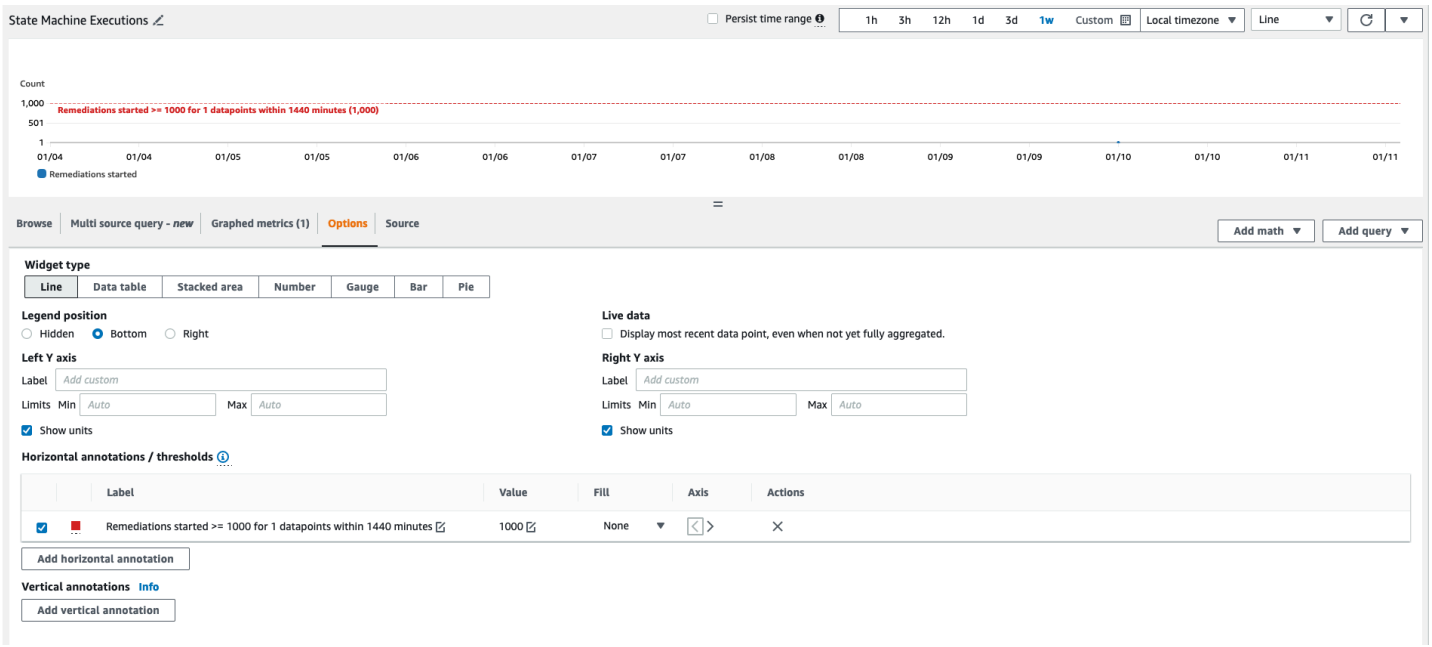
4. 導覽至 CloudWatch 儀表板以修改其中的圖表，以符合新設定。

   a. 選取對應小工具右上角的省略符號。

   b. 選擇 Edit (編輯)。

c. 變更為選項索引標籤。

d. 修改警示註釋以符合新設定。



訂閱警示通知

在管理員帳戶中，訂閱管理員堆疊 SO0111-ASR_Alarm_Topic 建立的 Amazon SNS主題。這會在警示進入 ALARM 狀態時通知您。

更新解決方案

從 v1.4 之前的版本升級

如果您先前已部署 v1.4.x 之前的 解決方案，請解除安裝 ，然後安裝最新版本：

1. 解除安裝先前部署的解決方案。請參閱解除安裝解決方案。
2. 啟動最新的範本。請參閱部署解決方案。

> **Note**
>
> 如果您要從 v1.2.1 或更早版本升級至 v1.3.0 或更新版本，請將使用現有的 Orchestrator Log Group 設定為 No。如果您要重新安裝 v1.3.0 或更新版本，您可以Yes針對此選項選取 。此選項可讓您繼續記錄 Orchestrator Step Functions 的相同日誌群組。

從 v1.4 和更新版本升級

如果您要從 v1.4.x 升級，請更新所有堆疊，或 StackSets 如下所示：

1. 使用最新的範本更新 Security Hub 管理員帳戶中的堆疊。
2. 在每個成員帳戶中，更新最新範本的許可。
3. 在目前部署的所有區域中的每個成員帳戶中，從最新的範本更新成員堆疊。

從 v2.0.x 升級

如果您要從 v2.0.x 升級，請升級至 v2.1.2 或更新版本。更新至 v2.1.0 - v2.1.1 將失敗 CloudFormation。

疑難排解

已知問題解決提供減輕已知錯誤的指示。如果這些指示無法解決您的問題，請聯絡 AWS Support 提供為此解決方案開啟AWS支援案例的說明。

解決方案日誌

本節包含此解決方案的疑難排解資訊，請參閱左側導覽以取得主題。

此解決方案會從執行於 的修復 Runbook 收集輸出 AWS Systems Manager，並將結果記錄到管理員帳戶中SO0111-SHARR的 CloudWatch Logs AWS Security Hub 群組。每個控制項每天有一個串流。

Orchestrator Step Functions 會記錄 Security AWS Hub 管理帳戶中所有轉換為 SO0111-SHARR-Orchestrator CloudWatch Logs 群組的步驟。此日誌是稽核追蹤，用於記錄 Step Functions 每個執行個體的狀態轉換。每個 Step Functions 執行有一個日誌串流。

兩個日誌群組都是使用 AWS KMS Customer-Manager 金鑰 (CMK) 加密。

下列疑難排解資訊使用 SO0111-SHARR 日誌群組。使用此日誌，以及 AWS Systems Manager Automation 主控台、Automation Executions 日誌、Step Function 主控台和 Lambda 日誌來故障診斷問題。

如果修復失敗，類似下列的訊息將記錄到日誌串流SO0111-SHARR中的標準、控制項和日期。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)
```

下列訊息提供其他詳細資訊。此輸出來自安全標準和控制的 SHARR Runbook。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.
```

此資訊會指向失敗，在這種情況下，這是在成員帳戶中執行的子自動化。若要對此問題進行故障診斷，您必須登入成員帳戶中 AWS Management Console 的 （從上述訊息），前往 AWS

Systems Manager，導覽至自動化，並檢查執行 ID 的日誌輸出eecdef79-9111-4532-921a-e098549f525。

已知問題解決方案

- 問題：解決方案部署失敗，並出現錯誤，指出 Amazon 中已有資源可用 CloudWatch。

  解決方法：檢查 CloudFormation 資源/事件區段中指出日誌群組已存在的錯誤訊息。SHARR 部署範本允許重複使用現有的日誌群組。確認您已選取重複使用。

- 問題： 解決方案無法在 EventBridge 規則無法建立的手冊巢狀堆疊中部署錯誤

  解決方法：您可能已達到 EventBridge 規則的配額，其中包含部署的手冊數量。您可以在 Security Hub 中使用與本解決方案中的 SC 手冊配對的合併控制問題清單、僅部署所用標準的手冊，或請求增加 EventBridge 規則配額，以避免這種情況。

- 問題：我在同一帳戶中的多個區域中執行 Security Hub。我想要在多個區域中部署此解決方案。

  解決方案：將管理員堆疊部署在與 Security Hub 管理員相同的帳戶和區域中。在已設定 Security Hub 成員的每個帳戶和區域中安裝成員範本。在 Security Hub 中啟用彙總。

- 問題：部署後，SO0111SHARR--Orchestrator 在取得自動化文件狀態中立即失敗，錯誤為 502：「Lambda 無法解密環境變數，因為KMS存取遭拒。請檢查函數的KMS金鑰設定。 KMS 例外狀況： UnrecognizedClientExceptionKMS訊息：請求中包含的安全字符無效。（服務：AWSLambda；狀態碼：502；錯誤碼：KMSAccessDeniedException；請求 ID：...”

  解決方法：在執行修復之前，讓解決方案穩定約 10 分鐘。如果問題仍然存在，請開啟支援票證或 GitHub 問題。

- 問題：我嘗試修復問題清單，但未發生任何情況。

  解決方法：檢查調查結果的備註，了解未修正的原因。常見的原因是調查結果沒有自動修復。目前，如果沒有透過備註以外的修復，則無法直接提供意見回饋給使用者。檢閱解決方案日誌。在 主控台中開啟 CloudWatch日誌。尋找 SO0111-SHARR CloudWatch Logs 群組。排序清單，讓最新更新的串流首先出現。選取您嘗試執行之問題清單的日誌串流。您應該會在該處發現任何錯誤。故障的一些原因可能是：問題清單控制和修復控制之間不相符、跨帳戶修復（尚未支援），或問題清單已修復。如果 無法判斷失敗的原因，請收集日誌並開啟支援票證。

- 問題：開始修復後，Security Hub 主控台中的狀態尚未更新。

  解決方案：Security Hub 主控台不會自動更新。重新整理目前的檢視。調查結果的狀態應更新。問題清單可能需要數小時才能從失敗轉換為通過。調查結果是從其他 服務傳送至 AWS Security Hub

的事件資料建立，例如 AWS Config。重新評估規則之前的時間取決於基礎服務。如果這無法解決問題，請參閱上述解決方法「我嘗試修復問題清單，但沒有發生。」

- 問題：協調器步驟函數在取得自動化文件狀態中失敗：呼叫 AssumeRole 操作時發生錯誤 (AccessDenied)。

  解決方法：成員範本尚未安裝在SHARR正在嘗試修復問題清單的成員帳戶中。遵循成員範本的部署說明。

- 問題：Config.1 Runbook 失敗，因為錄製器或交付管道已存在。

  解決方法：仔細檢查您的 AWS Config 設定，以確保 Config 已正確設定。在某些情況下，自動化修復無法修正現有的 Config AWS 設定。

- 問題：修復成功，但傳回訊息 `"No output available yet because the step is not successfully executed."`

  解決方法：這是此版本中已知的問題，其中某些修復 Runbook 不會傳回回應。修復 Runbook 將正常失敗，並在解決方案無法運作時發出訊號。

- 問題：解決方案失敗並傳送堆疊追蹤。

  解決方案：我們偶爾會錯失處理錯誤條件的機會，導致堆疊追蹤而非錯誤訊息。嘗試從追蹤資料對問題進行故障診斷。如果您需要協助，請開啟支援票證。

- 問題：移除自訂動作資源上的 v1.3.0 堆疊失敗。

  解決方案：移除管理員範本可能會在移除自訂動作時失敗。這是將在下一個版本中修正的已知問題。如果發生這種情況：

  1. 登入 AWS Security Hub 管理主控台。
  2. 在管理員帳戶中，前往設定。
  3. 選取自訂動作索引標籤
  4. 使用 手動刪除項目修復SHARR。
  5. 再次刪除堆疊。

- 問題：重新部署管理員堆疊後，步驟函數在 上失敗`AssumeRole`。

  解決方案：重新部署管理員堆疊會中斷管理員帳戶中管理員角色與成員帳戶中成員角色之間的信任連線。您必須重新部署所有成員帳戶中的成員角色堆疊。

- 問題：CIS3.x 修復在超過 24 小時`PASSED`後仍未顯示。

解決方法：如果您在成員帳戶中沒有 SO0111-SHARR_LocalAlarmNotificationSNS主題的訂閱，這是常見的情況。

特定修復的問題

S etSSLBucket政策失敗並發生錯誤 AccessDenied

相關聯的控制項：AWSFSBPv1.0.0 S3.5、PCIv3.2.1 PCI.S3.5、CISv1.4.0 2.1.2、SC v2.0.0 S3.5

問題：S etSSLBucket政策失敗並 AccessDenied發生錯誤：

呼叫 PutBucketPolicy操作時發生錯誤 (AccessDenied)：存取遭拒

如果已啟用儲存貯體的封鎖公開存取設定， 會嘗試放置儲存貯體政策，其中包含允許公開存取的陳述式，但此錯誤會失敗。您可以透過放置包含此類陳述式的儲存貯體政策，然後啟用該儲存貯體的公有存取區塊來達到此狀態。

修復 ConfigureS3BucketPublicAccessBlock （ 相關控制項：v1AWSFSBP.0.0 S3.2、PCIv3.2.1 PCI.S3.2、CISv1.4.0 2.1.5.2、SC v2.0.0 S3.2) 也可以將儲存貯體置於此狀態，因為它在不變更儲存貯體政策的情況下設定公有存取區塊設定。

S etSSLBucket政策會將陳述式新增至儲存貯體政策，以拒絕不使用 的請求SSL。它不會修改政策中的其他陳述式，因此，如果有允許公開存取的陳述式，則修復會嘗試放置仍包含這些陳述式的修改後儲存貯體政策失敗。

解決方法：修改儲存貯體政策，以移除允許公開存取與儲存貯體上區塊公開存取設定衝突的陳述式。

PutS3BucketPolicyDeny fails

相關聯的控制項： AWS FSBPv1.0.0 S3.6、 NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

問題：PutS3BucketPolicyDeny 出現下列錯誤：

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

如果目標儲存貯體上所有政策的主體為「*」，解決方案就無法將拒絕政策新增至目標儲存貯體，因為它會封鎖所有主體的所有儲存貯體動作。

解決方法：修改儲存貯體政策，允許對特定帳戶執行動作，而不是使用「*」主體，並限制拒絕的動作。

如何停用解決方案

發生事件時，您可能會發現需要停用解決方案，而不移除任何基礎設施。這些案例詳細說明如何在解決方案中停用不同的元件。

案例 1：停用單一控制項的自動修復。

1. 在 AWS CloudFormation 主控台 EventBridge 中導覽至 。
2. 在側邊欄中選取規則。
3. 選取預設事件匯流排，並搜尋您要停用的控制項。
4. 選取規則上的 ，然後選取停用按鈕。

案例 2：停用所有控制項的自動修復。

1. 在 主控台 EventBridge 中導覽至 。
2. 在側邊欄中選取規則。
3. 選取「預設」事件匯流排，然後選取以下所有規則。
4. 選取「停用」按鈕上的 。請注意，您可能需要為多頁規則執行此操作。

案例 3：停用帳戶的手動修復

1. 在 主控台 EventBridge 中導覽至 。
2. 在側邊欄中選取規則。
3. 選取「預設」事件匯流排，並搜尋「Remediate_with_SHARR_CustomAction」
4. 在規則上選取 ，然後選取「停用」按鈕。

聯絡人 Support

如果您有AWS開發人員支援、AWS商業支援或AWS企業支援，您可以使用支援中心來取得此解決方案的專家協助。以下章節將提供說明。

建立案例

1. 登入支援中心。

2. 選擇建立案例。

如何提供協助？

1. 選擇技術。
2. 針對服務，選取解決方案。
3. 針對類別，選取其他解決方案。
4. 針對嚴重性，選取最符合您使用案例的選項。
5. 當您輸入服務、類別和嚴重性時，介面會填入常見故障診斷問題的連結。如果您無法使用這些連結來解決問題，請選擇下一步：其他資訊。

其他資訊

1. 針對主旨，輸入摘要您的問題的文字。
2. 針對描述，請詳細說明問題。
3. 選擇連接檔案。
4. 連接處理請求 Support 所需的資訊。

協助我們更快解決您的案例

1. 輸入請求的資訊。
2. 選擇下一步驟：立即解決或聯絡我們。

立即解決或聯絡我們

1. 檢閱立即解決解決方案。
2. 如果您無法解決這些解決方案的問題，請選擇聯絡我們，輸入請求的資訊，然後選擇提交。

解除安裝解決方案

使用下列程序來解除安裝 解決方案 AWS Management Console。

V1.0.0-V1.2.1

對於 1.0.0 版到 1.2.1 版，請使用 Service Catalog 解除安裝 CIS和/或 FSBP Playbook。已不再使用 v1.3.0 Service Catalog。

1. 登入AWS CloudFormation 主控台並導覽至 Security Hub 主要帳戶。
2. 選擇服務目錄以終止任何佈建的手冊、移除任何安全群組、角色或使用者。
3. 從 Security Hub 成員帳戶移除發言`CISPermissions.template`範本。
4. 移除 Security Hub 管理員和成員帳戶的發言`AFSBPMemberStack.template`範本。
5. 導覽至 Security Hub 主要帳戶，選取解決方案的安裝堆疊，然後選擇刪除。

> **Note**
>
> CloudWatch 日誌群組日誌會保留。我們建議您根據組織的日誌保留政策的要求保留這些日誌。

V1.3.x

1. `aws-sharr-member.template` 從每個成員帳戶移除 。
2. `aws-sharr-admin.template` 從管理員帳戶移除 。

> **Note**
>
> 移除 v1.3.0 中的管理員範本可能會在移除自訂動作時失敗。這是將在下一個版本中修正的已知問題。請使用下列指示來修正此問題：
>
> 1. 登入 AWS Security Hub 管理主控台。
> 2. 在管理員帳戶中，前往設定。
> 3. 選取自訂動作索引標籤。
> 4. 使用 手動刪除項目修復SHARR。

5. 再次刪除堆疊。

V1及更新版本

堆疊部署

1. `aws-sharr-member.template` 從每個成員帳戶移除 。
2. `aws-sharr-admin.template` 從管理員帳戶移除 。

StackSet 部署

對於每個 StackSet，移除堆疊，然後 StackSet 以部署的相反順序移除 。

請注意，即使移除範本， 中IAM的角色`aws-sharr-member-roles.template`仍會保留。如此一來，使用這些角色的修復才能繼續運作。在驗證 SO0111-* 角色不再由主動修復使用後，例如 CloudTrail CloudWatch 記錄或RDS增強型監控，即可手動移除這些 SO0111-* 角色。

管理員指南

啟用和停用 解決方案的部分

身為解決方案管理員，您可以控制啟用解決方案的功能。

部署成員和成員角色堆疊的位置：

- 管理員堆疊將只能啟動修復（透過自訂動作或全自動 EventBridge 規則），其中成員和成員角色堆疊已部署為參數值的管理員帳戶號碼。
- 若要完全免除帳戶或區域控制解決方案，請勿將成員或成員角色堆疊部署到這些帳戶或區域。

Security Hub 中的帳戶和區域問題清單彙總組態：

- 管理員堆疊只能針對抵達管理員帳戶和區域的調查結果啟動修復（透過自訂動作或全自動 EventBridge 規則）。
- 若要完全免除帳戶或區域控制解決方案，請勿包含這些帳戶或區域，以將問題清單傳送到部署管理員堆疊的相同管理員帳戶和區域。

部署了哪些標準巢狀堆疊：

- 管理員堆疊只能針對在目標成員帳戶和區域中部署控制項 Runbook 的控制項啟動修復（透過自訂動作或全自動 EventBridge 規則）。這些由每個標準的成員堆疊部署。
- 管理員堆疊只能使用具有由管理員堆疊針對該標準部署規則的控制項 EventBridge 規則來啟動全自動修復。這些會部署到管理員帳戶。
- 為了簡化，我們建議您在管理員和成員帳戶中一致地部署標準。如果您關心 AWSFSBP和 CIS v1.2.0，請將這兩個巢狀管理堆疊部署到管理員帳戶，並將這兩個巢狀成員堆疊部署到每個成員帳戶和區域。

在每個巢狀成員堆疊中部署了哪些控制 Runbook：

- 管理員堆疊只能針對由成員堆疊針對每個標準在目標成員帳戶和區域中部署控制項 Runbook 的控制項啟動修復（透過自訂動作或全自動 EventBridge 規則）。
- 若要對針對特定標準啟用哪些控制項執行更精細的控制，標準的每個巢狀堆疊都有部署控制 Runbook 的參數。將控制項的 參數設定為「NOT可用」值，以取消部署該控制項 Runbook。

SSM 啟用和停用標準的參數：

- 管理員堆疊只能針對透過標準管理員堆疊部署的 SSM 參數啟用的標準啟動修復（透過自訂動作或全自動 EventBridge 規則）。
- 若要停用標準，請將路徑為 "/Solutions/SO0111/<standard_name>/<standard_version>/status" 的 SSM 參數值設為 "No"。

SNS 通知範例

啟動修復時

```
{
  "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"
  }
}
```

修復成功時

```
{
  "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"
  }
}
```

當修復失敗時

```
{
  "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"
  }
}
```

使用解決方案

這是教學課程，將引導您完成第一次部署 ASR。它將以部署解決方案的先決條件開頭，並以您在成員帳戶中修復範例問題清單結尾。

教學課程： 上的自動化安全回應入門 AWS

這是教學課程，將引導您完成第一次部署。它將以部署解決方案的先決條件開頭，並以您在成員帳戶中修復範例問題清單結尾。

準備帳戶

為了示範解決方案的跨帳戶和跨區域修補功能，本教學課程將使用兩個帳戶。您也可以將解決方案部署到單一 帳戶。

下列範例使用 帳戶111111111111和 222222222222 來示範解決方案。 111111111111將是 管理帳戶，而 222222222222 將是 成員帳戶。我們將設定解決方案來修復區域 us-east-1和 中資源的調查結果us-west-2。

下表範例說明我們將針對每個帳戶和區域中的每個步驟採取的動作。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	無	無
222222222222	成員	無	無

管理員帳戶是將執行解決方案管理動作的帳戶，也就是手動啟動修復，或使用 EventBridge 規則啟用全自動修復。此帳戶也必須是您希望修復問題清單的所有帳戶的 Security Hub 委派管理員帳戶，但它不需要也不應該是您AWS帳戶所屬AWS組織的組織管理員帳戶。

啟用AWS組態

檢閱下列文件：

- AWS 組態文件
- AWS 組態定價
- 啟用AWS組態

在帳戶和兩個區域中啟用 AWS Config。這會產生費用。

> **Important**
>
> 請確定您選取「包含全域資源 （例如AWSIAM資源）」的選項。如果您在啟用 Config AWS 時未選取此選項，則不會看到與全域資源 （例如AWSIAM資源） 相關的問題清單

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	啟用AWS組態	啟用AWS組態
222222222222	成員	啟用AWS組態	啟用AWS組態

啟用AWS安全中樞

檢閱下列文件：

- AWS Security Hub 文件
- AWS Security Hub 定價
- 啟用 AWS Security Hub

在帳戶和兩個區域中啟用 AWS Security Hub。這會產生費用。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	啟用 AWS Security Hub	啟用 AWS Security Hub
222222222222	成員	啟用 AWS Security Hub	啟用 AWS Security Hub

啟用合併控制問題清單

檢閱下列文件：

- 產生和更新控制問題清單

在本教學課程中，我們將示範 解決方案的使用方式，並啟用 AWS Security Hub 的合併控制問題清單功能，這是建議的組態。在寫入時不支援此功能的分割區中，您將需要部署標準特定的手冊，而不是 SC （安全控制）。

在帳戶和兩個區域中啟用合併的控制問題清單。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	啟用合併控制問題清單	啟用合併控制問題清單
222222222222	成員	啟用合併控制問題清單	啟用合併控制問題清單

使用新功能產生問題清單可能需要一些時間。您可以繼續教學課程，但如果沒有新功能，將無法修復產生的問題清單。使用新功能產生的調查結果可以透過`GeneratorId`欄位值 來識別`security-control/<control_id>`。

設定跨區域調查結果彙總

檢閱下列文件：

- 跨區域彙總
- 啟用跨區域彙總

在兩個帳戶中設定從 us-west-2 到 us-east-1 的調查結果彙總。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	從 us-west-2 設定彙總	無
222222222222	成員	從 us-west-2 設定彙總	無

問題清單可能需要一些時間才能傳播到彙總區域。您可以繼續教學課程，但您將無法從其他區域修復問題清單，直到問題清單開始出現在彙總區域中為止。

指定 Security Hub 管理員帳戶

檢閱下列文件：

- 在 AWS Security Hub 中管理帳戶
- 管理組織成員帳戶
- 依邀請管理成員帳戶

在繼續範例中，我們將使用手動邀請方法。對於一組生產帳戶，我們建議透過 AWS Organizations 管理 Security Hub 委派的管理。

從管理員帳戶 (111111111111) 中的 AWS Security Hub 主控台，邀請成員帳戶 (222222222222) 接受管理員帳戶做為 Security Hub 委派管理員。從成員帳戶接受邀請。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	邀請成員帳戶	無
222222222222	成員	接受邀請	無

問題清單可能需要一些時間才能傳播到管理員帳戶。您可以繼續教學課程，但您將無法從成員帳戶修復問題清單，直到問題清單開始出現在管理員帳戶中為止。

建立自我管理 StackSets 許可的角色

檢閱下列文件：

- AWS CloudFormation StackSets
- 授予自我管理許可

我們會將 CloudFormation 堆疊部署到多個帳戶，因此我們將使用 StackSets。我們無法使用服務受管許可，因為管理員堆疊和成員堆疊具有服務不支援的巢狀堆疊，因此我們必須使用自我管理許可。

部署堆疊以取得 StackSet 操作的基本許可。對於生產帳戶，您可能想要根據「進階許可選項」文件來縮小許可範圍。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	部署 StackSet 管理員角色堆疊 部署 StackSet 執行角色堆疊	無
222222222222	成員	部署 StackSet 執行角色堆疊	無

建立會產生範例問題清單的不安全資源

檢閱下列文件：

- Security Hub 控制項參考
- AWS Lambda 控制項

下列範例資源具有不安全組態，以示範修復。控制範例為 Lambda.1：Lambda 函數政策應禁止公開存取。

> **Important**
>
> 我們將刻意建立具有不安全組態的資源。請檢閱控制項的性質，並評估在環境中為自己建立此類資源的風險。請注意您的組織在偵測和報告此類資源時可能擁有的任何工具，並在適當時請求例外狀況。如果您選擇的範例控制項不適合您，請選取解決方案支援的另一個控制項。

在成員帳戶的第二個區域中，導覽至 AWS Lambda 主控台，並在最新的 Python 執行時間建立函數。在組態 -> 許可下，新增政策陳述式，以允許在沒有身分驗證URL的情況下從 叫用函數。

在主控台頁面上確認 函數允許公開存取。解決方案修復此問題後，請比較許可以確認公有存取已撤銷。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	無	無

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
222222222222	成員	無	使用不安全的組態建立 Lambda 函數

Config AWS 可能需要一些時間來偵測不安全的組態。您可以繼續教學課程，但在 Config 偵測到問題清單之前，您將無法修復問題清單。

建立相關控制項的 CloudWatch 日誌群組

檢閱下列文件：

- 使用 Amazon CloudTrail Logs 監控 CloudWatch 日誌檔案
- CloudTrail 控制項

解決方案支援的各種 CloudTrail 控制項需要一個 CloudWatch日誌群組，而該群組是多區域的目標 CloudTrail。在下列範例中，我們將建立預留位置日誌群組。對於生產帳戶，您應該正確設定與 CloudWatch Logs 的 CloudTrail 整合。

在每個帳戶和區域中建立具有相同名稱的日誌群組，例如：`asr-log-group`。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	建立日誌群組	建立日誌群組
222222222222	成員	建立日誌群組	建立日誌群組

將解決方案部署到教學帳戶

URLs 為管理員、成員和成員角色堆疊收集三個 Amazon S3。

部署管理員堆疊

View template

aws-sharr-deploy.template

在管理員帳戶中，導覽至 CloudFormation 主控台，並將管理員堆疊部署到 Security Hub 問題清單彙總區域。

No 為載入巢狀管理堆疊的所有參數值選擇 ，但「SC」或「安全控制」堆疊除外。此堆疊包含我們在帳戶中設定的合併控制問題清單資源。

選擇 No以重複使用協調器日誌群組，除非您之前已在此帳戶和區域中部署此解決方案。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	部署管理員堆疊	無
222222222222	成員	無	無

等待管理員堆疊完成部署後再繼續，以便從成員帳戶到管理員帳戶建立信任關係。

部署成員堆疊

View template

aws-sharr-member.template

在管理員帳戶中，導覽至 CloudFormation StackSets 主控台，並將成員堆疊部署到每個帳戶和區域。使用此教學課程中建立的 StackSets 管理員和執行角色。

輸入您建立的日誌群組名稱，做為日誌群組名稱的 參數值。

No 為載入巢狀成員堆疊的所有參數值選擇 ，但「SC」或「安全控制」堆疊除外。此堆疊包含我們在帳戶中設定的合併控制問題清單資源。

輸入管理員帳戶的 ID 做為管理員帳戶號碼參數的值。在我們的範例中，這是 111111111111。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	部署成員 StackSet /確認成員堆疊已部署	確認成員堆疊已部署
222222222222	成員	確認成員堆疊已部署	確認成員堆疊已部署

部署成員角色堆疊

aws-sharr-member-roles.template

在管理員帳戶中，導覽至 CloudFormation StackSets 主控台，並將成員堆疊部署至每個帳戶。使用此教學課程中建立的 StackSets 管理員和執行角色。輸入管理員帳戶的 ID 做為管理員帳戶號碼參數的值。在我們的範例中，這是 111111111111。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	部署成員 StackSet /確認成員堆疊已部署	無
222222222222	成員	確認成員堆疊已部署	無

您可以繼續，但在完成 CloudFormation StackSets 部署之前將無法修復問題清單。

訂閱 SNS 主題

修復更新

主題 - SO0111-SHARR_Topic

在管理員帳戶中，訂閱管理員堆疊建立的 Amazon SNS主題。這將通知您何時啟動修復，以及何時成功或失敗。

警示

主題 - SO0111-ASR_Alarm_Topic

在管理員帳戶中，訂閱管理員堆疊建立的 Amazon SNS主題。這將在指標警示啟動時通知您。

修復範例問題清單

在管理員帳戶中，導覽至 Security Hub 主控台，並尋找資源的調查結果，其中包含您在本教學課程中建立的不安全組態。

這可以透過幾種方式完成：

1. 在支援合併控制問題清單功能的分割區中，標記為「控制項」的頁面可讓您依合併控制 ID 找到問題清單。
2. 在「安全標準」頁面中，您可以根據其所屬的標準找到控制項。
3. 您可以在「調查結果」頁面上檢視所有調查結果，並依屬性搜尋。

我們建立的公有 Lambda 函數合併控制 ID 為 Lambda.1。

啟動修復

選取與我們所建立資源相關的調查結果左側的核取方塊。在「動作」下拉式功能表中，選取「使用 ASR「修復」。您將看到問題清單已傳送至 Amazon 的通知 EventBridge。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	啟動修復	無
222222222222	成員	無	無

確認修復已解決問題清單

您應該會收到兩個SNS通知。第一個 表示已啟動修復，第二個 表示修復成功。收到第二個通知後，導覽至成員帳戶中的 Lambda 主控台，並確認公有存取權已撤銷。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	無	無
222222222222	成員	無	確認修復成功

追蹤修復的執行

若要進一步了解解決方案的運作方式，您可以追蹤修復的執行。

EventBridge 規則

在管理員帳戶中，找到名為 Remediate_with_SHARR_ CustomAction的 EventBridge 規則。此規則符合您從 Security Hub 傳送的調查結果，並將其傳送至 Orchestrator Step Functions。

Step Functions 執行

在管理員帳戶中，找到名為 "SO0111-SHARR-Orchestrator" 的 AWS Step Functions。此步驟函數會呼叫目標帳戶和區域中的SSM自動化文件。您可以在此步驟AWS函數的執行歷史記錄中追蹤修復的執行。

SSM 自動化

在成員帳戶中，導覽至SSM自動化主控台。您會發現兩個名為 "ASR-SC_2.0.0_Lambda.1" 的文件執行，以及一個名為 "ASR-RemoveLambdaPublicAccess" 的文件執行。

第一個執行來自目標帳戶中的協調器步驟函數。第二個執行發生在目標區域中，可能不是調查結果的來源區域。最終執行是從 Lambda 函數撤銷公有存取政策的修復。

CloudWatch 日誌群組

在管理員帳戶中，導覽至 CloudWatch Logs 主控台並尋找名為 "SO0111-SHARR" 的日誌群組。此日誌群組是 Orchestrator Step Functions 中高階日誌的目的地。

啟用全自動化修復

解決方案的另一種操作模式是在問題清單抵達 Security Hub 時自動修復問題清單。

確認您沒有可能不小心套用此調查結果的資源

啟用自動修復會在符合您啟用之控制項 (Lambda.1) 的所有資源上啟動修復。

> **Important**
>
> 確認您希望解決方案範圍內的所有公有 Lambda 函數撤銷此許可。完全自動化的修補不會限制在您建立的 函數範圍內。如果在安裝此解決方案的任何帳戶和區域中偵測到此控制項，解決方案將會修復此控制項。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	確認沒有所需的公有函數	確認沒有所需的公有函數

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
222222222222	成員	確認沒有所需的公有函數	確認沒有所需的公有函數

啟用規則

在 Admin 帳戶中，找到名為 SC_2.0.0_Lambda.1_AutoTrigger 的 EventBridge 規則並啟用它。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	啟用自動修復規則	無
222222222222	成員	無	無

設定 資源

在成員帳戶中，重新設定 Lambda 函數以允許公開存取。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	無	無
222222222222	成員	無	設定 Lambda 函數以允許公開存取

確認修復已解決問題清單

Config 可能需要一些時間才能再次偵測不安全的組態。您應該會收到兩個SNS通知。第一個 表示已啟動修復。第二個表示修復成功。收到第二個通知後，導覽至成員帳戶中的 Lambda 主控台，並確認公有存取權已撤銷。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	啟用自動修復規則	無

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
222222222222	成員	無	確認修復成功

清除

刪除範例資源

在成員帳戶中，刪除您建立的範例 Lambda 函數。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	無	無
222222222222	成員	無	刪除範例 Lambda 函數

刪除管理員堆疊

在管理員帳戶中，刪除管理員堆疊。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	刪除管理員堆疊	無
222222222222	成員	無	無

刪除成員堆疊

在管理員帳戶中，刪除成員 StackSet。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	刪除成員 StackSet 確認成員堆疊已刪除	確認成員堆疊已刪除

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
222222222222	成員	確認成員堆疊已刪除	確認成員堆疊已刪除

刪除成員角色堆疊

在管理員帳戶中，刪除成員角色 StackSet。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	刪除成員角色 StackSet 確認已刪除 rmember 角色堆疊	無
222222222222	成員	確認成員角色堆疊已刪除	無

刪除保留的角色

在每個帳戶中，刪除保留IAM的角色。

重要：這些角色會保留給需要 角色的修復，才能繼續運作 （例如VPC流程記錄）。在刪除任何這些角色之前，請確認您不需要繼續執行這些角色。

刪除任何字首為 SO0111- 的角色。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	刪除保留的角色	無
222222222222	成員	刪除保留的角色	無

排程保留的KMS金鑰以進行刪除

管理員和成員會同時建立和保留KMS金鑰。如果您保留這些金鑰，將產生費用。

這些金鑰會保留，以便讓您存取解決方案加密的任何資源。在排定刪除之前，請確認您不需要它們。

使用解決方案或歷史記錄中建立的別名來識別解決方案部署的金鑰 CloudFormation 。排定刪除它們。

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	識別和排程要刪除的管理員金鑰 識別並排程要刪除的成員金鑰	識別並排程要刪除的成員金鑰
222222222222	成員	識別並排程要刪除的成員金鑰	識別並排程要刪除的成員金鑰

刪除自我管理 StackSets 許可的堆疊

刪除為允許自我管理 StackSets 許可而建立的堆疊

帳戶	用途	us-east-1 中的動作	us-west-2 中的動作
111111111111	管理員	刪除 StackSet 管理員角色堆疊	無
222222222222	成員	刪除 StackSet 執行角色堆疊	無

開發人員指南

本節提供解決方案的原始程式碼和其他自訂項目。

來源碼

請造訪我們的GitHub 儲存庫，下載此解決方案的範本和指令碼，並與他人共用您的自訂。

手冊

此解決方案包含網際網路安全中心 (CIS) AWS Foundations Benchmark 1.2.0 版、 CIS AWS Foundations Benchmark 1.4.0 版、 CIS AWS Foundations Benchmark 3.0.0 版、AWS基礎安全最佳實務 (FSBP) 1.0.0 版、支付卡產業資料安全標準 (PCI-DSS) 3.2.1 版和國家標準技術研究所 (NIST) 中所定義安全標準的手冊修復。

如果您已啟用合併控制問題清單，則所有標準都支援這些控制項。如果啟用此功能，則只需要部署 SC 手冊。如果沒有，則先前列出的標準支援手冊。

> **Important**
>
> 僅部署已啟用標準的手冊，以避免達到服務配額。

如需特定修復的詳細資訊，請參閱 Systems Manager 自動化文件，其中包含您帳戶中解決方案所部署的名稱。前往 AWS Systems Manager 主控台，然後在導覽窗格中選擇文件。

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
總計補救措施	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupE	Autoscaling.1		Autoscaling.1		Autoscaling.1		Autoscaling.1

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
LBHealthCheck 與負載平衡器相關聯的 Auto Scaling 群組應使用負載平衡器運作狀態檢查							
ASR-CreateMultiRegionTrail CloudTrail 應該啟用並設定至少一個多區域追蹤	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail 應該啟用靜態加密	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableLogFileValidation 確保 CloudTrail 日誌檔案驗證已啟用	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.
ASR-EnableCloudTrailToCloudWatchLogging 確保 CloudTrail 追蹤與 Amazon CloudWatch Logs 整合	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-ConfigureS3BucketLogging 確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取記錄		2.6		3.6		3.4	CloudTrail.7
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild 專案環境變數不應包含純文字登入資料	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableAWSConfig 確保 AWS Config 已啟用	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1
ASR-MakeEBSSnapshotsPrivate Amazon EBS快照不應可公開還原	EC21.		EC21.		EC21.		EC21.
ASR-RemoveVPCDefaultSecurityGroupRules VPC 預設安全群組應禁止傳入和傳出流量	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableVPCFlow日誌 VPC 流程記錄應該在所有中啟用 VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-EnablEeEbsEncryptionByDefault EBS 應啟用預設加密	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7
ASR-RevokeUnrotatedKeys 使用者存取金鑰應每 90 天或更短時間輪換一次	IAM3.	1.4		1.14	IAM3.	1.14	IAM3.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-SetIAMPassword政策 IAM 預設密碼政策	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7
ASR-RevokeUnusedIAMUserCredentials 如果未在 90 天內使用使用者登入資料，則應關閉	IAM.8	1.3	IAM.7		IAM.8		IAM.8
ASR-RevokeUnusedIAMUserCredentials 如果未在 45 天內使用使用者登入資料，則應關閉				1.12		1.12	IAM.22

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-RemoveLambdaPublicAccess Lambda 函數應該禁止公開存取	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshot私有 RDS 快照應禁止公開存取	RDS1.		RDS1.		RDS1.		RDS1.
ASR-DisablePublicAccessToRDSInstance RDS 資料庫執行個體應禁止公開存取	RDS2.		RDS2.		RDS2.	2.3.3	RDS2.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EncryptRDSSnapshot RDS 叢集快照和資料庫快照應靜態加密	RDS4.				RDS4.		RDS4.
ASR-EnableMultiAZOnRDSInstance RDS 資料庫執行個體應該設定多個可用區域	RDS5.				RDS5.		RDS5.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableEnhancedMonitoringOnRDSInstance 應為RDS資料庫執行個體和叢集設定增強型監控	RDS.6				RDS.6		RDS.6
ASR-EnableRDSClusterDeletionProtection RDS 叢集應該已啟用刪除保護	RDS.7				RDS.7		RDS.7

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableRDSInstanceDeletionProtection RDS 資料庫執行個體應該已啟用刪除保護	RDS.8				RDS.8		RDS.8
ASR-EnableMinorVersionUpgradeOnRDSDBInstance RDS 應啟用自動次要版本升級	RDS.13				RDS.13	2.3.2	RDS.13

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDS 資料庫叢集應設定為將標籤複製到快照	RDS.16				RDS.16		RDS.16
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift 叢集應禁止公開存取	Redshift.1		Redshift.1		Redshift.1		Redshift.1

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift 叢集應該啟用自動快照	Redshift.3				Redshift.3		Redshift.3
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift 叢集應該啟用稽核記錄	Redshift.4				Redshift.4		Redshift.4

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift 應該已啟動主要版本的自動升級	Redshift.6				Redshift.6		Redshift.6
ASR-ConfigureS3PublicAccessBlock 應啟用 S3 Block Public Access 設定	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-ConfigureS3BucketPublicAccessBlock S3 儲存貯體應禁止公開讀取存取	S3.2		S3.2	2.1.5.2	S3.2		S3.2
ASR-ConfigureS3BucketPublicAccessBlock S3 儲存貯體應禁止公有寫入存取		S3.3					S3.3
ASR-EnableDefaultEncryptionS3 S3 儲存貯體應啟用伺服器端加密	S3.4		S3.4	2.1.1	S3.4		S3.4

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-SetSSLBucket政策 S3 儲存貯體應要求使用 的請求 SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3BlockDenylist 應限制授予其他儲存貯 AWS 帳戶 體政策的 Amazon S3 許可	S3.6				S3.6		S3.6
應在儲存貯體層級啟用 S3 封鎖公開存取設定	S3.8				S3.8		S3.8

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-ConfigureS3BucketPublicAccessBlock 確保 的 S3 儲存貯體 CloudTrail 日誌不可公開存取		2.3					CloudTrail.6
ASR-CreateAccessLoggingBucket 確保已在 S3 儲存貯體上啟用 CloudTrail S3 儲存貯體存取記錄		2.6					CloudTrail.7

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableKeyRotation 確保CMKs已啟用客戶建立的輪換		2.8	KMS1.	3.8	KMS4.	3.6	KMS4.
ASR-CreateLogMetricFilterAndAlarm 確保日誌指標篩選條件和警示對未經授權的API呼叫存在		3.1		4.1			Cloudwatch.1

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保沒有的 AWS Management Console 登入存在日誌指標篩選條件和警示 MFA		3.2		4.2			Cloudwatch.2
ASR-CreateLogMetricFilterAndAlarm 確保存在日誌指標篩選條件和警示以使用「根」使用者		3.3	CW.1	4.3			Cloudwatch.3

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保IAM政策變更存在日誌指標篩選條件和警示		3.4		4.4			Cloudwatch.4
ASR-CreateLogMetricFilterAndAlarm 確保CloudTrail 組態變更存在日誌指標篩選條件和警示		3.5		4.5			Cloudwatch.5

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保 AWS Management Console 驗證失敗時存在日誌指標篩選條件和警示		3.6		4.6			Cloudwatch.6
ASR-CreateLogMetricFilterAndAlarm 確保日誌指標篩選條件和警示存在，以停用或排程刪除已建立的客戶 CMKs		3.7		4.7			Cloudwatch.7

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示		3.8		4.8			Cloudwatch.8
ASR-CreateLogMetricFilterAndAlarm 確保 AWS Config 組態變更存在日誌指標篩選條件和警示		3.9		4.9			Cloudwatch.9

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保安全群組變更存在日誌指標篩選條件和警示		3.10		4.10			Cloudwatch.10
ASR-CreateLogMetricFilterAndAlarm 確保網路存取控制清單 (NACL) 的變更存在日誌指標篩選條件和警示		3.11		4.11			Cloudwatch.11

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保網路閘道變更存在日誌指標篩選條件和警示		3.12		4.12			Cloudwatch.12
ASR-CreateLogMetricFilterAndAlarm 確保路由表變更存在日誌指標篩選條件和警示		3.13		4.13			Cloudwatch.13

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保VPC變更存在日誌指標篩選條件和警示		3.14		4.14			Cloudwatch.14
AWS-DisablePublicAccessForSecurityGroup 確保沒有任何安全群組允許從 0.0.0.0/0 傳入連接埠 22		4.1	EC25.		EC2.13		EC2.13

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
AWS-DisablePublicAccessForSecurityGroup 確保沒有任何安全群組允許從 0.0.0.0/0 傳入連接埠 3389		4.2			EC2.14		EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASR-CreateIAMSupport角色		1.20		1.17		1.17	IAM.18

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-DisablePublicIPAutoAssign Amazon EC2子網路不應自動指派公有 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	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableDeliveryStatusLoggingForSNSTopic 應針對傳送至主題的通知訊息啟用交付狀態記錄	SNS2.				SNS2.		SNS2.
ASR-EnableEncryptionForSQSQueue	SQS1.				SQS1.		SQS1.
ASR-MakeRDSSnapshot私有 RDS 快照應為私有	RDS1.		RDS1.				RDS1.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-BlockSSMDocumentPublicAccess SSM 文件不應公開	SSM4.				SSM4.		SSM4.
ASR-EnableCloudFrontDefaultRootObject CloudFront 分佈應該設定預設根物件	CloudFront1.				CloudFront1.		CloudFront1.
ASR-SetCloudFrontOriginDomain CloudFront 分佈不應指向不存在的 S3 原始伺服器	CloudFront.12				CloudFront.12		CloudFront.12

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-RemoveCodeBuildPrivilegedMode CodeBuild專案環境應具有記錄 AWS Configuration	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.
ASR-終止EC2 Instance 停止的EC2執行個體應該在指定的期間之後移除	EC24.				EC24.		EC24.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-啟用IMDSV2OnInstance EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2)	EC2.8				EC2.8	5.6	EC2.8
ASR-RevokeUnauthorizedInboundRules 安全群組應只允許授權連接埠無限制的傳入流量	EC2.18				EC2.18		EC2.18

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-DisableUnrestrictedToHighRiskPorts 安全群組不應允許無限制存取高風險的連接埠	EC2.19				EC2.19		EC2.19
ASR-DisableTGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways 不應自動接受VPC附件請求	EC2.23				EC2.23		EC2.23

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnablePrivateRepositoryScanning ECR 私有儲存庫應設定映像掃描	ECR1.				ECR1.		ECR1.
ASR-EnableGuardDuty GuardDuty 應該啟用	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.
ASR-ConfigureS3BucketLogging 應啟用 S3 儲存貯體伺服器存取記錄	S3.9				S3.9		S3.9

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableBucketEventNotifications S3 儲存貯體應該啟用事件通知	S3.11				S3.11		S3.11
ASR-SetS3LifecyclePolicy S3 儲存貯體應該已設定生命週期政策	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation Secrets Manager 秘密應該啟用自動輪換	SecretsManager1.				SecretsManager1.		SecretsManager1.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-RemoveUnusedSecret 移除未使用的 Secrets Manager 秘密	SecretsManager3.				SecretsManager3.		SecretsManager3.
ASR-UpdateSecretRotationPeriod Secrets Manager 秘密應該在指定的天數內輪換	SecretsManager4.				SecretsManager4.		SecretsManager4.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnableAPIGatewayCacheDataEncryption API 閘道 RESTAPI 快取資料應靜態加密					APIGateway5.		APIGateway5.
ASR-SetLogGroupRetentionDays CloudWatch 日誌群組應保留一段指定的時間					CloudWatch.16		CloudWatch.16

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-AttachServiceVPCEndpoint Amazon EC2應設定為使用為Amazon EC2服務建立的VPC端點	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty篩選條件應加上標籤							GuardDuty 2.
ASR-TagGuardDutyResource GuardDuty偵測器應加上標籤							GuardDuty 4.

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-ttachSSMPermissions收件人EC2 Amazon EC2執行個體應該由 Systems Manager 管理	SSM1.		SSM3.				SSM1.
ASR-ConfigureLaunchConfigNoPublicIPDocument 使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2執行個體不應具有公有 IP 地址					Autoscaling.5		Autoscaling.5

描述	AWS FSBP	CIS 1.2.0 版	PCI v3.2.1	CIS 1.4.0 版	NIST	CIS v3.0.0	安全控制 ID
ASR-EnablAPIGatewayExecutionLogs	APIGateway1.						APIGateway1.
ASR-EnablMacie 應啟用 Amazon Macie	Macie.1				Macie.1		Macie.1
ASR-EnablAthenaWorkGroupLogging Athena 工作群組應該已啟用記錄	Athena.4						Athena.4

新增新的修補

將新的修補新增至現有的手冊，不需要修改解決方案本身。

> **Note**
>
> 以下指示會利用解決方案安裝的資源做為起點。根據慣例，大多數解決方案資源名稱都包含 SHARR和/或 SO0111，以便輕鬆找到和識別它們。

概觀

AWS Runbook 上的自動安全回應必須遵循下列標準命名：

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

標準：安全標準的縮寫。這必須符合 支援的標準SHARR。它必須是「CIS」、「AFSBP」、「PCI」、「NIST」或「SC」之一。

版本：標準的版本。同樣地，這必須符合調查結果資料中 支援的版本SHARR和版本。

控制項：要修復之控制項的控制項 ID。這必須符合調查結果資料。

1. 在成員帳戶中建立 Runbook （成員帳戶）。
2. 在成員帳戶中建立 IAM 角色 ()。
3. （選用）在管理員帳戶中建立自動修復規則。

步驟 1. 在成員帳戶中建立 Runbook (s)

1. 登入 AWS Systems Manager 主控台並取得問題清單 的範例JSON。
2. 建立可修復問題清單的自動化 Runbook。在我擁有索引標籤中，使用ASR-文件索引標籤下的任何文件作為起點。
3. 管理員帳戶中 AWS Step Functions 的 會執行您的 Runbook。您的 Runbook 必須指定修補角色，才能在呼叫 Runbook 時傳遞。

步驟 2. 在成員帳戶中建立IAM角色 （多個）

1. 登入 AWS Identity and Access Management 主控台。
2. 從 IAM SO0111 角色取得範例並建立新的角色。角色名稱必須以 `SO0111-Remediate-`*`<standard>`*`-`*`<version>`*`-`*`<control>` 開頭。例如，如果新增 CIS v1.2.0 控制 5.6，則角色必須為 `SO0111-Remediate-CIS-1.2.0-5.6`。
3. 使用 範例，建立適當範圍的角色，只允許必要的API呼叫執行修復。

此時，您的修復處於作用中狀態，並可從 AWS Security Hub 中的SHARR自訂動作自動修復。

步驟 3：（選用）在管理員帳戶中建立自動修復規則

自動（非「自動」）修補是指在 AWS Security Hub 收到調查結果後立即執行修補。使用此選項之前，請仔細考慮風險。

1. 在 CloudWatch Events 中檢視相同安全標準的範例規則。規則的命名標準為 `standard_control_`**`AutoTrigger`**。
2. 從要使用的範例複製事件模式。
3. 變更 `GeneratorId`值，以符合您的問題清單 `GeneratorId`中的 JSON。
4. 儲存並啟用規則。

新增手冊

從 GitHub 儲存庫下載AWS解決方案手冊和部署原始程式碼上的自動安全回應。

這些 AWS CloudFormation 資源是從 AWS CDK元件建立的，而資源包含的手冊範本程式碼可用來建立和設定新的手冊。如需設定專案和自訂手冊的詳細資訊，請參閱 中的 README.md 檔案 GitHub。

AWS Systems Manager 參數存放區

上的自動安全回應AWS使用 AWS Systems Manager 參數存放區來儲存操作資料。下列參數會存放在參數存放區中：

名稱	Value	使用
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS KMS 金鑰，用於加密資料以進行FSBP修復	客戶資料加密，例如 CloudTrail 日誌，做為修復的一部分
`/Solutions/SO0111/CMK_ARN`	AWS KMS SHARR用來加密資料的金鑰	解決方案資料的加密
`/Solutions/SO0111/SNS_Topic_ARN`	ARN 解決方案的 Amazon SNS 主題	修補事件的通知
`/Solutions/SO0111/SNS_Topic_Config.1`	SNS AWS Config 更新主題	Config.1 修復

名稱	Value	使用
/Solutions/SO0111/sendAnonymousMetrics	Yes	匿名指標集合
/Solutions/SO0111/version	解決方案版本	
/Solutions/SO0111/ *<security standard long name>*/*<version>* /status	enabled	指出 標準是否在解決方案中處於作用中狀態。您可以將此標準變更為 以停用自動修復 disabled
/Solutions/SO0111/ *<security standard long name>*/shortname	String	安全標準的簡短名稱。例如：'CIS'、'AFSBP'、'PCI'
/Solutions/SO0111/ *<security standard long name>*/*<version>* /*<control>* /remap	String	當一個控制項使用與另一個控制項相同的修復時，這些參數會完成重新映射

Amazon SNS主題 - 修復進度

上的自動安全回應AWS會建立 Amazon SNS主題 SO0111-SHARR_Topic。本主題用於發佈有關修復進度的更新。以下是傳送至此主題的三個可能通知。

```
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>
```

這是完成訊息。它表示修復已完成，沒有錯誤；但是，成功修復的確定性測試是 Config AWS 檢查和/或手動驗證。

篩選SNS主題訂閱

Amazon SNS訂閱篩選條件政策：

1. 導覽至 SNS主題的訂閱。
2. 在訂閱篩選條件政策下，選取「編輯」。
3. 展開「訂閱篩選條件政策」，並切換「訂閱篩選條件政策」選項以啟用篩選條件。
4. 選取「訊息內文」範圍。
5. 將政策新增至JSON編輯器。
6. 儲存變更。

範例政策：

依帳戶篩選

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

篩選錯誤

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

依控制項篩選

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

Amazon SNS主題 – CloudWatch Alarms

此解決方案會建立 Amazon SNS主題 SO0111-ASR_Alarm_Topic。此主題用於發佈警示提醒。

任何進入 ALARM 狀態的警示的詳細資訊都會傳送至此主題。

在 Config 調查結果上啟動 Runbook

此解決方案可以根據自訂 AWS Config 問題清單啟動 Runbook。若要這樣做，您需要：

1. 尋找您要修復的 AWS Config 規則名稱。這可以在 Security Hub 為此規則產生的調查結果 AWS Config 中找到。
2. 導覽至 AWS Systems Manager 參數存放區，然後選取建立參數。
3. 規則的名稱應該是 /Solutions/SO0111/*Rule name from Step 1*
4. 值的格式應該如下：

```
{
"RunbookName":"Name of SSM runbook",
"RunbookRole": "Role that Orchestrator will assume"
}
```

5. RunbookName 是必要欄位，且將是修復此 Config 規則時執行的 Runbook。 RunbookRole 是協調程式在執行此角色時將擔任的角色。這不是必要欄位，如果不填寫，協調程式會預設為使用帳戶的成員角色。
6. 設定完成後，您可以使用 Security Hub 上的「Remediate withASR」自訂動作來修復 Config 規則。

參考資料

本節包含收集此解決方案唯一指標的選用功能、相關資源的指標，以及有助於此解決方案的建置器清單的相關資訊。

匿名資料收集

此解決方案包含將匿名操作指標傳送至 的選項AWS。我們使用這些資料更好地了解客戶使用此解決方案、相關服務和產品的方式。啟用時，會收集以下資訊並傳送至 AWS：

- 解決方案 ID - AWS解決方案識別符
- 唯一 ID (UUID) - 隨機產生、每個 AWS Security Hub 回應和修復部署的唯一識別符
- 時間戳記 - 資料收集時間戳記
- 執行個體資料 - 此堆疊部署的相關資訊
- CloudWatchMetricsDashboardEnabled - "Yes" 如果在部署期間啟用 CloudWatch 指標和儀表板
- 狀態 - 部署狀態（傳遞或失敗的解決方案）或（傳遞或失敗的修補）
- 錯誤訊息 - 狀態欄位中的一般錯誤訊息
- Generator_id - Security Hub 規則資訊
- 類型 - 修復類型和名稱
- productArn - 部署 Security Hub 的區域
- finding_triggered_by - 執行的修復類型（自訂動作或自動觸發）

AWS 擁有透過此調查收集的資料。資料收集受 AWS隱私權通知的約束。若要選擇退出此功能，請在啟動 AWS CloudFormation 範本之前完成下列步驟。

1. 將AWS CloudFormation 範本下載至本機硬碟。
2. 使用文字編輯器開啟 AWS CloudFormation 範本。
3. 從以下位置修改 AWS CloudFormation 範本映射區段：

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

至:

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

4. 登入 AWS CloudFormation 主控台。
5. 選取建立堆疊。
6. 在建立堆疊頁面上，指定範本區段，選取上傳範本檔案。
7. 在上傳範本檔案下，選擇選擇檔案，然後從本機磁碟機中選取編輯的範本。
8. 選擇下一步，並遵循本指南自動部署區段中啟動堆疊的步驟。

相關資源

- 使用 自動回應和修復 AWS Security Hub
- CIS Amazon Web Services Foundations 基準測試，1.2.0 版
- AWS 基礎安全最佳實務標準
- 支付卡產業資料安全標準 (PCIDSS)
- 國家標準技術研究所 (NIST) SP 800-53 修訂版 5

貢獻者

下列個人對本文件有所貢獻：

- Mike O’Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- 最大格蘭納特
- Tim Mekari
- Aaron Schuetter

- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega

修訂

日期	變更
2020 年 8 月	初始版本
2020 年 10 月	新增其他故障診斷資訊至附錄 C。
2020 年 11 月	新增中國區域的部署說明；更新 Security Hub 管理員帳戶的解決方案部署說明；如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2021 年 4 月	1.2.0 版：新增了新的手冊架構和新的FSBP修補。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2021 年 5 月	1.2.1 版：針對影響 EC2.2 和 .EC27 的問題進行錯誤修正。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2021 年 8 月	1.3.0 版：新增 3.2PCIDSS.1 版手冊。已新增 17 個新的修補至 CIS v1.2.0。已新增四個新的修補至 FSBP。根據 SSM Runbook CIS轉換為使用新的 Playbook 架構。新增了透過客戶定義的修復擴展現有手冊的說明。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2021 年 9 月	1.3.1 版：`CreateLogMetricFilterAndAlarm.py` 變更為啟用動作，將SNS通知新增至 `SO0111-SHARR-LocalAlarmNotification` 。變更 CIS 2.8 修復以符合新的調查結果資料格式。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

日期	變更
2021 年 11 月	1.3.2 版：1.2.0 CIS版的錯誤修正控制 3.1 - 3.14。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2021 年 12 月	1.4.0 版：現在可以使用 部署解決方案。StackSets除了跨帳戶之外，現在還支援跨區域修復。現在移除堆疊時，會保留成員帳戶IAM角色。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2022 年 1 月	1.4.1 版：錯誤修正。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2022 年 1 月	1.4.2 版：錯誤修正。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2022 年 6 月	1.5.0 版：其他修補。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2022 年 12 月	1.5.1 版 將SSM文件建立從自訂資源 Lambda 切換到 的變更。 `CfnDocument` SSM 文件名稱的字首會更新為以 開頭，ASR而非 SHARR。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2023 年 3 月	2.0.0 版：新增了對安全控制和 v1CIS.4.0 標準的支援、五項新的FSBP標準修補、一項新的 CIS v1.2.0 標準修補、服務目錄 AppRegistry 整合，以及額外的保護，以避免因SSM文件限流而發生部署失敗。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2023 年 4 月	2.0.1 版：已緩解所有新 S3 儲存貯體的 S3 物件擁有權 (ACLs 已停用） S3新預設設定所造成的影響。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

日期	變更
2023 年 5 月	文件更新：更新 Well-Architected 定義、新增了有關在何處部署每個堆疊的指導、針對特定修復問題的其他故障診斷版本，以及更新SNS通知中的程式碼範例。
2023 年 7 月	文件更新：更新了工作流程中的架構圖表和解決方案元件。
2023 年 10 月	2.0.2 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2023 年 11 月	文件更新：將與解決方案相關聯的確認成本標籤新增至使用 AWS Service Catalog 監控解決方案 AppRegistry 一節。
2024 年 3 月	2.1.0 版：新增NIST標準支援、新增 17 個新的FSBP標準修補、新增監控解決方案 CloudWatch 儀表板、新增架構調節處理常式、新增 Security Hub 可自訂輸入參數的支援，以及新增 Config 問題清單的修補支援。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 4 月	2.1.1 版：更新至 CloudFormation 參數順序和預設值 文件更新。新增對 NIST 標準的參考。新增 EventBridge 規則服務配額的相關資訊。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 6 月	2.1.2 版： AppRegistry 針對特定手冊停用，以避免更新解決方案時發生錯誤。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

日期	變更
2024 年 9 月	2.1.3 版：已解決 EC2.18 和 EC2.19 修復指令碼中的問題，其中將 IpProtocol 設為 -1 的安全群組規則被錯誤地忽略。將修復SSM文件中的所有 Python 執行時間從 Python 3.8 升級到 Python 3.11。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 11 月	2.1.4 版：從 Python 3.8 升級至 Python 3.11 的所有控制執行手冊中的升級 Python 執行時間。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 12 月	2.2.0 版：新增票務系統整合、 CloudTrail 動作日誌和 CIS 3.0.0 手冊。增強型儀表板和通知。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件： (a) 僅供參考， (b) 代表 AWS 目前的產品產品和實務， 可能隨時變更，恕不另行通知。 和 (c) 不會從 AWS 及其附屬公司建立任何承諾或保證， 供應商或 licensors. AWS products 或服務是以「原樣」方式提供，不做任何保證， 表示法、 或任何類型的條件， 無論明示或暗示。 對客戶 AWS 的責任和責任受 AWS 協議控制， 本文件不屬於 也不會修改 AWS 與其客戶之間的任何協議。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。