實作指南

AWS 上的自動化安全回應

AWS 上的自動化安全回應: 實作指南

Table of Contents

在 AWS Security Hub 中使用預先定義的回應和修補動作自動解決安全威脅

此實作指南提供 AWS 解決方案上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、將 AWS 解決方案上的自動化安全回應部署至 Amazon Web Services (AWS) 雲端的組態步驟。

使用此導覽表快速找到這些問題的答案：

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	支援的 AWS 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 (AWS CDK) 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。AWS 自動化安全回應解決方案可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，協助您快速回應安全問題。

AWS 上的自動化安全回應是 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調查結果，並改善 AWS 中的安全狀態。

您可以選擇要在 Security Hub 主要帳戶中部署的特定手冊。每個程序手冊都包含啟動單一 AWS 帳戶或跨多個帳戶內修補工作流程所需的必要自訂動作、 Identity and Access Management (IAM) 角色、Amazon EventBridge 規則、AWS Systems Manager 自動化文件、AWS Lambda 函數和 AWS Step Functions。修復可從 AWS Security Hub 中的動作功能表運作，並允許授權使用者透過單一動作

來修復其所有 AWS Security Hub 受管帳戶的問題清單。例如，您可以從 Center for Internet Security (CIS) AWS Foundations Benchmark 套用建議，這是保護 AWS 資源的合規標準，以確保密碼在 90 天內過期，並強制加密存放在 AWS 中的事件日誌。

> **Note**
>
> 修補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 Management 主控台啟動，或使用 Amazon EventBridge 規則針對特定控制項啟用自動修復時，對修復的問題清單進行變更。若要還原這些變更，您必須手動將資源放回其原始狀態。修復部署為 CloudFormation 堆疊一部分的 AWS 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？。

AWS 上的自動化安全回應包含安全標準的手冊修補，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 Foundational Security Best Practices (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 AWS Security Hub 合併控制調查結果功能的安全控制 (SC) 手冊。如需詳細資訊，請參閱 手冊。

本實作指南討論在 AWS 雲端中部署自動化安全回應的架構考量和組態步驟。它包含 AWS CloudFormation 範本的連結，這些範本會使用 AWS 最佳實務在 AWS 上啟動、設定和執行部署此解決方案所需的 AWS 運算、網路、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

AWS 上的自動化安全回應提供下列功能：

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問題清單啟動修復。

收到修復動作和結果的通知

訂閱解決方案部署的 Amazon SNS 主題，以便在修復啟動時收到通知，以及修復是否成功。

與 Jira 或 ServiceNow 等票證系統整合

為了協助您的組織對修復做出反應（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 和中國分割區中使用 AWSConfigRemediations

解決方案中包含的一些補救措施是 AWS 擁有的 AWSConfigRemediation 文件的重新封裝，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

解決方案設計為可擴展且可自訂。若要指定替代修復實作，請部署自訂的 AWS Systems Manager 自動化文件和 AWS IAM 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 Foundational Security Best Practices) 的 手冊，以使用提供的修補。針對部署解決方案的任何帳戶和區域中的資源，自動或手動啟動修補，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解決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：

修補、修補 Runbook

一組解決問題清單之步驟的實作。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。

控制 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 Foundational Security Best Practices (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，在此情況下，它會是 ASR-RemoveLambdaPublicAccess。

協調器

解決方案所部署的 Step Functions，其會從 AWS Security Hub 做為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，AWS Security Hub 和此解決方案支援的其中一個標準是 AWS FSBP。

控制項

為了符合規範，資源應擁有或不應擁有的屬性描述。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。

合併控制調查結果、安全控制、安全控制檢視

AWS Security Hub 的一項功能，啟用時會顯示具有合併控制項 IDs的問題清單，而不是對應至特定標準的 IDs。例如，控制項 AWS FSBP S3.2、CIS v1.2.0 2.3、CIS v1.4.0 2.1.5.2 和 PCI-DSS v3.2.1 S3.1 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。

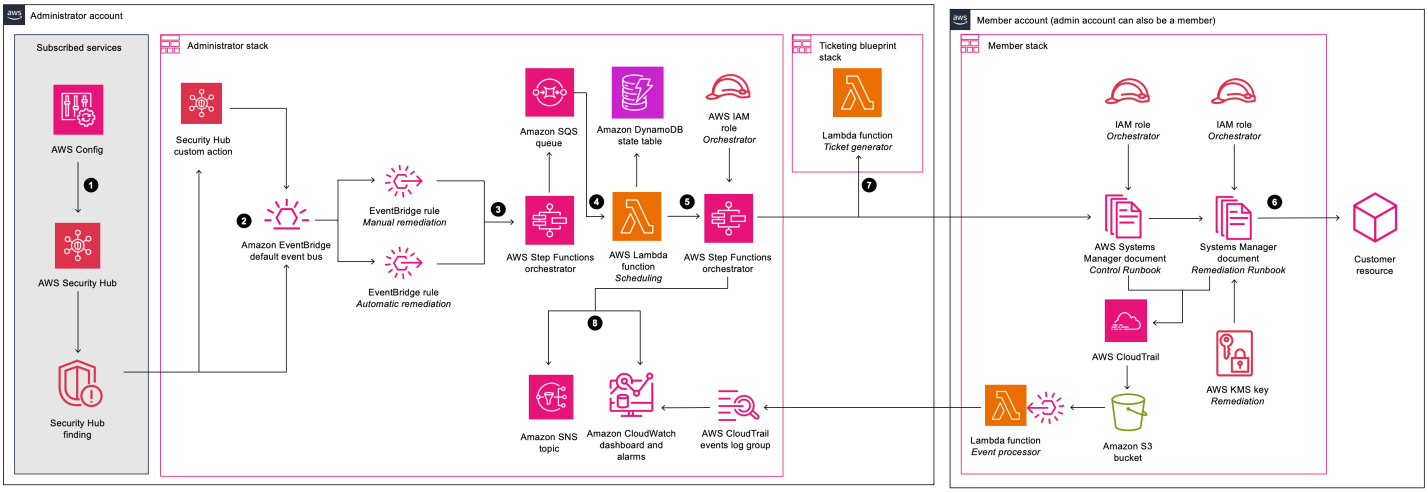
架構概觀

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 (AWS CDK) 建構模組建立。

使用 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 可為客戶提供 AWS 安全狀態的完整檢視。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。它的運作方式是從其他 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根據調查結果啟動事件，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. 一個 EventBridge 規則，以符合自訂動作事件

b. 每個支援的控制項（預設為停用）一個 EventBridge 事件規則，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，您也可以啟用自動化修復。您可以啟用個別修補的自動化，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，AWS Step Functions 會處理修復事件，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 會在成員帳戶中叫用修復，其中包含產生安全調查結果的資源。
6. 修復：成員帳戶中的 AWS Systems Manager Automation 文件會執行修復目標資源問題清單所需的動作，例如停用 Lambda 公開存取。

   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，在您的票證服務中建立票證。我們提供與 Jira 和 ServiceNow 整合的堆疊。
8. 通知和日誌：程序手冊會將結果記錄到 CloudWatch 日誌群組、傳送通知至 Amazon Simple Notification Service (Amazon SNS) 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、有效率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。

- 使用 CloudFormation 定義為 IaC 的資源。
- 盡可能使用下列特性實作的修補：
  - 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。

- 用於身分驗證和授權的 IAM。
- 角色許可的範圍盡可能縮小，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一個平台，讓您無需自行實作協同運作和許可即可擴展。

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量的費用。
- 在每個帳戶中使用 SSM 自動化的免費方案

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縱向擴展或縮減規模。**

架構詳細資訊

本節說明構成此解決方案的元件和 AWS 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automated-security-response-admin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 AWS Step Functions 路由問題清單記錄進行修復。

跨帳戶許可和 AWS Systems Manager Runbook 必須使用 automated-security-response-member.template和 automated-security-response-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給 AWS Security Hub 時，立即啟用問題清單的全自動修復。根據預設，自動啟動會關閉。此選項可在安裝程序手冊期間或之後隨時變更，方法是在 AWS Security Hub 管理員帳戶中開啟 CloudWatch Events 規則。

跨帳戶修復

AWS 上的自動化安全回應使用跨帳戶角色，以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會獲得許可，以擔任帳戶中需要修復的修復角色。修復是由帳戶內執行且需要修復的 AWS Systems Manager Runbook 執行。

手冊

一組修復會分組到稱為程序手冊的套件中。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修復的資訊，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，已於 2023 年 2 月 23 日發佈。

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

- Center for Internet Security (CIS) Amazon Web Services Foundations 基準測試，版本 1.2.0，2018 年 5 月 18 日發佈。
- Center for Internet Security (CIS) Amazon Web Services Foundations 基準測試，1.4.0 版，2022 年 11 月 9 日發佈。
- Center for Internet Security (CIS) Amazon Web Services Foundations 基準測試，3.0.0 版，2024 年 5 月 13 日發佈。
- AWS Foundational Security Best Practices (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

AWS 日誌上自動安全回應至單一 CloudWatch Logs 群組 SO0111-ASR。這些日誌包含解決方案的詳細記錄，用於疑難排解和管理解決方案。

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。

- SO0111-ASR_Topic – 用於傳送與已執行修復相關的一般資訊和錯誤訊息。
- SO0111-ASR_Alarm_Topic – 用於在觸發其中一個解決方案的警示時發出通知，表示解決方案未如預期般運作。

此解決方案中的 AWS 服務

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

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 安全中樞	核心。為客戶提供 AWS 安全狀態的完整檢視。
AWS Step Functions	核心。部署協調器，以使用 AWS Systems Manager API 呼叫來調用修復文件。
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 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。部署不同手冊將用於記錄結果的日誌群組。收集要在具有警示的自訂儀表板上顯示的指標。
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。
Amazon Simple Notification Service	支援。部署修復完成後收到通知的 SNS 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。
AWS Key Management Service	支援。用來加密資料以進行修復。
AWS Config	支援。記錄與 AWS Security Hub 搭配使用的所有資源。

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、支援的 AWS 區域、配額和其他考量事項。

成本

您必須負責用來執行此解決方案的 AWS 服務成本。

截至此修訂，估計每月成本為：

- 小型部署 (10 個帳戶，1 個區域 - 美國東部/北部。 維吉尼亞州）：每月 300 個修補約 21.17 美元
- 中型部署 (100 個帳戶，1 個區域 - 美國東部/北部。 維吉尼亞州）：每月 3，000 個修補約 134.86 USD
- 大型部署 (1，000 個帳戶，10 個區域）：每月大約 10，271.70 USD 進行 30，000 次修補

> **Important**
>
> 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。

我們建議您透過 AWS Cost Explorer 建立預算，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
- 作用中自動調用修復的數量
- 修復的頻率

此解決方案使用以下 AWS 元件，這會根據您的組態產生成本。定價範例適用於小型、中型和大型組織。

服務	免費方案	定價 【美元】
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，每個基本步驟都會按每個步驟收取 0.002 USD。對於多帳戶自動化，包括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 動作步驟每秒都會收費 0.00003 USD。
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 張checks/account/Region/每月每張支票 0.0010 美元 接下來 400，000 張checks/account/Region/每月每張支票 0.0008 USD 超過 500，000 張checks/account/Region/每月每張支票 0.0005 美元
AWS Security Hub - 尋找擷取事件	前 10，000 個events/account/Region/月是免費的。尋找與	超過 10，000 個events/account/Region/每月每個事件 0.00003 美元

服務	免費方案	定價 【美元】
	Security Hub 安全檢查相關聯的擷取事件。	
Amazon CloudWatch - 指標	基本監控指標 （頻率為 5 分鐘） 10 個詳細監控指標 （頻率為 1 分鐘） 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 個指標費用為每月 0.10 USD 接下來的 750，000 個指標費用為每月 0.05 USD 指標 每月超過 1，000，000 個指標成本 0.02 USD API 呼叫每 1，000 個請求 0.01 美元
Amazon CloudWatch - 儀表板	3 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 個警示指標 （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 標準解決異常偵測每個警示 0.30 USD 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 - 日誌集合	5GB 資料 （由 Logs Insights 查詢掃描的擷取、封存儲存和資料）	每 GB 0.50 美元

服務	免費方案	定價 【美元】
Amazon CloudWatch - 日誌儲存	5GB 資料 （由 Logs Insights 查詢掃描的擷取、封存儲存和資料）	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	自訂事件的每百萬事件 1.00 美元跨帳戶事件的每百萬事件 1.00 美元
AWS Lambda - 請求	每月 1M個免費請求	每 1M00 萬個請求 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 USD。持續時間的價格取決於您配置給函數的記憶體數量。您可以將任意數量的記憶體配置到 128MB 到 10，240MB 之間的函數，以 1MB 為單位遞增。
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	自訂事件每發佈一百萬美元的自訂事件 第三方 (SaaS) 事件每發佈一百萬美元的事件 跨帳戶事件每傳送 100 萬美金的跨帳戶事件
Amazon SNS	每月前 100 萬個 Amazon SNS 請求是免費的	之後每 100 萬個請求 0.50 美元
Amazon SQS	每月前 100 萬個 Amazon SQS 請求是免費的	之後每 100 萬到 1，000 億個請求 0.40 美元

服務	免費方案	定價 【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 2.00 美元
AWS Key Management Service 定價	每月 20，000 個請求	每 1 個 KMS 金鑰 1.00 美元。對於您自動或隨需輪換的 KMS 金鑰，金鑰的第一次和第二次輪換會增加每月 1 USD （按比例分配的每小時） 的成本。

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account/Region/month 30 個修補
- 每月總成本 21.17 美元

服務	前提	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 * $0.00002 = $0.0006 $0.0006 * 0.03 = $0.000018	< 0.01 美元
AWS Lambda - 請求	300 個修補 * 6 個請求 = 1，800 個請求	0.20 美元

服務	前提	每月費用 【USD】
	$0.20 * 1，000，000 個請求 = $0.20	
AWS Lambda - 持續時間	256M：1.875 GB 秒 * 300 個修補 * $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
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 * 1，000，000 個通知 = $0.50	0.50 美元
Amazon CloudWatch - 指標	$0.30 * 7 個自訂指標 = $2.10 $0.01 * (300 * 3 / 1，000) 放置指標 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account/Region/month 30 個修補
- 每月總成本 134.86 美元

服務	前提	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 持續時間：10 秒 * 3，000 個修補 * 0.0000 美元3 = 0.90 美元	24.90 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 個修補 * 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 = $0.09375	0.09 美元
AWS Step Functions	17 個狀態轉換 * 3，000 個修補 = 51，000 個 $0.025 * (51，000/1，000) 州轉換 = $1.275	1.28 美元

服務	前提	每月費用 【USD】
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
Amazon SNS	$0.50 * 1，000，000 個通知 = $0.50	0.50 美元
Amazon CloudWatch - 指標	$0.30 * 7 個自訂指標 = $2.10 $0.01 * (3000 * 3 / 1，000) 放置指標 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、10 個區域
- 每個account/Region/month 30 個修補
- 每月總成本 $1，271.70

服務	前提	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	249.00 美元

服務	前提	每月費用 【USD】
	持續時間：10 秒 * 30，000 個修補 * 0.0000 美元3 = 9.00 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
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 個修補 = 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 * 1，000 個帳戶 * 10 個區域 = $10，000	10，000 美元
Amazon DynamoDB	$0.00002 * 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

服務	前提	每月費用 【USD】
Amazon SNS	$0.00005 * 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) 放置指標 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
總計		10，271.70 美元

Important

啟用輪換時，KMS Key Rotation Costs AWS Key Management Service (KMS) 每年會自動輪換一次客戶受管金鑰。每次輪換都會產生每個金鑰每年 1.00 USD 的成本。例如，在單一區域中擁有 1000 個帳戶，這會產生額外的每年 1000 美元 (1 個輪換 × 1000 個金鑰 × 1.00 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。

增強型 CloudWatch 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 數目。在下表中，我們假設您每月修復全部 96 個不同的控制 IDs，以判斷成本上限。

服務	假設 96 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，我們假設帳戶中每個月有 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	前提	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，安全責任將由您與 AWS 共同承擔。此共用模型可減少您的操作負擔，因為 AWS 會操作、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的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-ASR-Orchestrator-Admin 角色。只有此角色才能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至 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-RemoveVPCDefaultSecurityGroupRules 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
Africa (Cape Town)	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

區域名稱	區域代碼
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
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
Europe (Paris)	eu-west-3
歐洲 (西班牙)	eu-south-2
Europe (Stockholm)	eu-north-1
歐洲 (蘇黎世)	eu-central-2
Middle East (Bahrain)	me-south-1
中東 (阿拉伯聯合大公國)	me-central-1
南美洲 (聖保羅)	sa-east-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

區域名稱	區域代碼
中國 (北京)	cn-north-1
中國 (寧夏)	cn-northwest-1
以色列 (特拉維夫)	il-central-1
加拿大西部 (卡加利)	ca-west-1
墨西哥 （墨西哥市）	mx-central-1
亞太區域 （泰國）	ap-southeast-7

> **Note**
>
> 任何未列出的新 AWS 區域都可以透過本機部署支援，但無法一鍵式部署。

配額

服務配額 (也稱為限制) 是您 AWS 帳戶的服務資源或操作數目最大值。

此解決方案中 AWS 服務的配額

請確定您為此解決方案中實作的每個服務有足夠的配額。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。若要在不切換頁面的情況下檢視文件中所有 AWS 服務的 Service Quotas，請改為檢視 PDF 中服務端點和配額頁面中的資訊。

AWS CloudFormation 配額

您的 AWS 帳戶具有在此解決方案中啟動堆疊時應注意的 AWS CloudFormation 配額。透過了解這些配額，您可以避免限制會阻止您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。 AWS CloudFormation

AWS CloudWatch 配額

您的 AWS 帳戶具有與 CloudWatch 資源政策繫結的 AWS CloudWatch 配額，每個帳戶每個區域僅允許 10 個資源政策，因此無法請求增加配額，請參閱《AWS CloudWatch 使用者指南》中的 AWS

CloudWatch Logs Quotas。 CloudWatch 在部署之前，請檢查您目前的用量，以確保您在部署解決方案時不會超過此閾值。

Amazon EventBridge 規則配額

您的 AWS 帳戶具有 Amazon EventBridge 規則配額，您在選擇使用 解決方案部署的手冊時應注意這些配額。每個程序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 EventBridge 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運作中的 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，允許 AssumeRole 許可給解決方案的 AWS Step Functions，以在帳戶中執行修復 Runbook。

Stack 與 StackSets 部署

堆疊集可讓您使用單一 AWS CloudFormation 範本，跨 AWS 區域在 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 AWS Organizations 的客戶，可以受益於使用堆疊集在多個帳戶中進行部署。它減少了安裝和維護解決方案所需的工作量。如需 StackSets 的詳細資訊，請參閱使用 AWS CloudFormation StackSets。

部署解決方案

> **Important**
>
> 如果在 Security Hub 中開啟合併控制調查結果功能 (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。如果未開啟此功能，請僅針對 Security Hub 中啟用的安全標準啟用程序手冊。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的 AWS 資源及其屬性。CloudFormation 堆疊會佈建範本中所述的資源。

為了讓解決方案運作，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：用於修復的 IAM 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。如果您想要使用動作日誌功能來監控管理事件，您必須在組織的管理帳戶或委派管理員帳戶中部署管理員堆疊。

解決方案會在 Security Hub 問題清單上運作，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問題清單，該解決方案將無法在特定帳戶和區域中的問題清單上運作。

例如，組織擁有在區域 `us-east-1`和 中操作的帳戶`us-west-2`，其帳戶`111111111111`為區域 中的 Security Hub 委派管理員`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`。所有三個帳戶必須設定為將問題清單從 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 SSM Automation 的免費方案。

使用上述範例，如果您想要修復所有帳戶和區域的調查結果，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。

使用先前的範例，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

具有服務管理許可的 StackSets 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。很抱歉，此方法不支援巢狀堆疊，我們在 Admin 堆疊和成員堆疊中使用。以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，但無法使用具有服務受管許可的 StackSets 部署，因為它包含巢狀堆疊。因此，我們建議您使用具有自我管理許可的 StackSets 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，或在單一帳戶和區域中部署為具有自我管理許可的 StackSet。

合併的控制問題清單

您可以在開啟或關閉 Security Hub 的合併控制問題清單功能時，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，以與開啟此功能時產生的合併控制 IDs 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

automated-security-response-admin.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，以及您選擇啟用的每個安全標準一個巢狀堆疊。

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`automated-security-response-admin.template`。

automated-security-response-orchestrator-log.template - 為 Orchestrator Step Function 建立 CloudWatch 日誌群組。

AFSBPStack.template - AWS Foundational Security 最佳實務 1.0.0 版規則。

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

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

CIS300Stack.template - CIS Amazon Web Services Foundations 基準測試，3.0.0 版規則。

PCI321Stack.template - PCI-DSS 3.2.1 版規則。

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

SCStack.template - 安全控制 v2.0.0 規則。

成員角色

View template

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

成員帳戶

View template

automated-security-response-member.template - 在您設定核心解決方案，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 和許可後，請使用此範本。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`automated-security-response-member.template`安裝下列範本：

automated-security-response-remediation-runbooks.template - 一或多個安全標準所使用的常見修補程式碼。

AFSBPMemberStack.template - AWS Foundational Security 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、許可和修復執行手冊。

CIS140MemberStack.template - CIS Amazon Web Services Foundations 基準測試、1.4.0 版設定、許可和修復執行手冊。

CIS300MemberStack.template - CIS Amazon Web Services Foundations 基準測試、3.0.0 版設定、許可和修復執行手冊。

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 Runbook。

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

automated-security-response-member-cloudtrail.template - 用於動作日誌功能，以追蹤和稽核 和 服務活動。

票證系統整合

使用下列其中一個範本與您的票證系統整合。

View template

JiraBlueprintStack.template - 如果您使用 Jira 做為票證系統，請部署 。

View template

ServiceNowBlueprintStack.template - 如果您使用 ServiceNow 做為票證系統，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**
>
> 我們建議您使用 StackSets 部署 。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。遵循本節中的step-by-step說明，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。

先決條件

AWS Organizations 可協助您集中管理多帳戶 AWS 環境和資源。StackSets 最適合與 AWS Organizations 搭配使用。

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 Organization 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。
- 您應該在擁有 AWS 用量的每個區域中為組織啟用 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**
>
> 此解決方案的 StackSets 部署使用服務受管和自我管理 StackSets 的組合。自我管理的 StackSets 必須目前使用，因為它們使用巢狀 StackSets，服務管理的 StackSets 尚不支援。

從 AWS Organizations 中的委派管理員帳戶部署 StackSets。 https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-cloudformation.html 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，並將其做為管理堆疊的輸入提供（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

- 使用自我管理的 StackSet，在與 Security Hub 管理員位於相同區域的 AWS Security Hub 管理員帳戶中啟動 `automated-security-response-admin.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-ASR- Orchestrator`已存在，請選取 。

如需自我管理 StackSets 的詳細資訊，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 AWS Security Hub 成員帳戶中安裝修補角色

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

- 使用服務管理的 StackSet，在 `automated-security-response-member-roles.template` AWS Organizations 中每個帳戶中的單一區域中啟動 AWS CloudFormation 範本。 AWS Organizations
- 選擇在新帳戶加入組織時自動安裝此範本。
- 輸入您的 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

- 使用自我管理的 StackSets，在 AWS Organization `automated-security-response-member.template` 中擁有相同 Security Hub 管理員管理之每個帳戶中 AWS 資源的所有區域中啟動 AWS CloudFormation 範本。

> **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（由部分修復使用）。
- 輸入您的 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 ServiceNow 提供的整合堆疊，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。

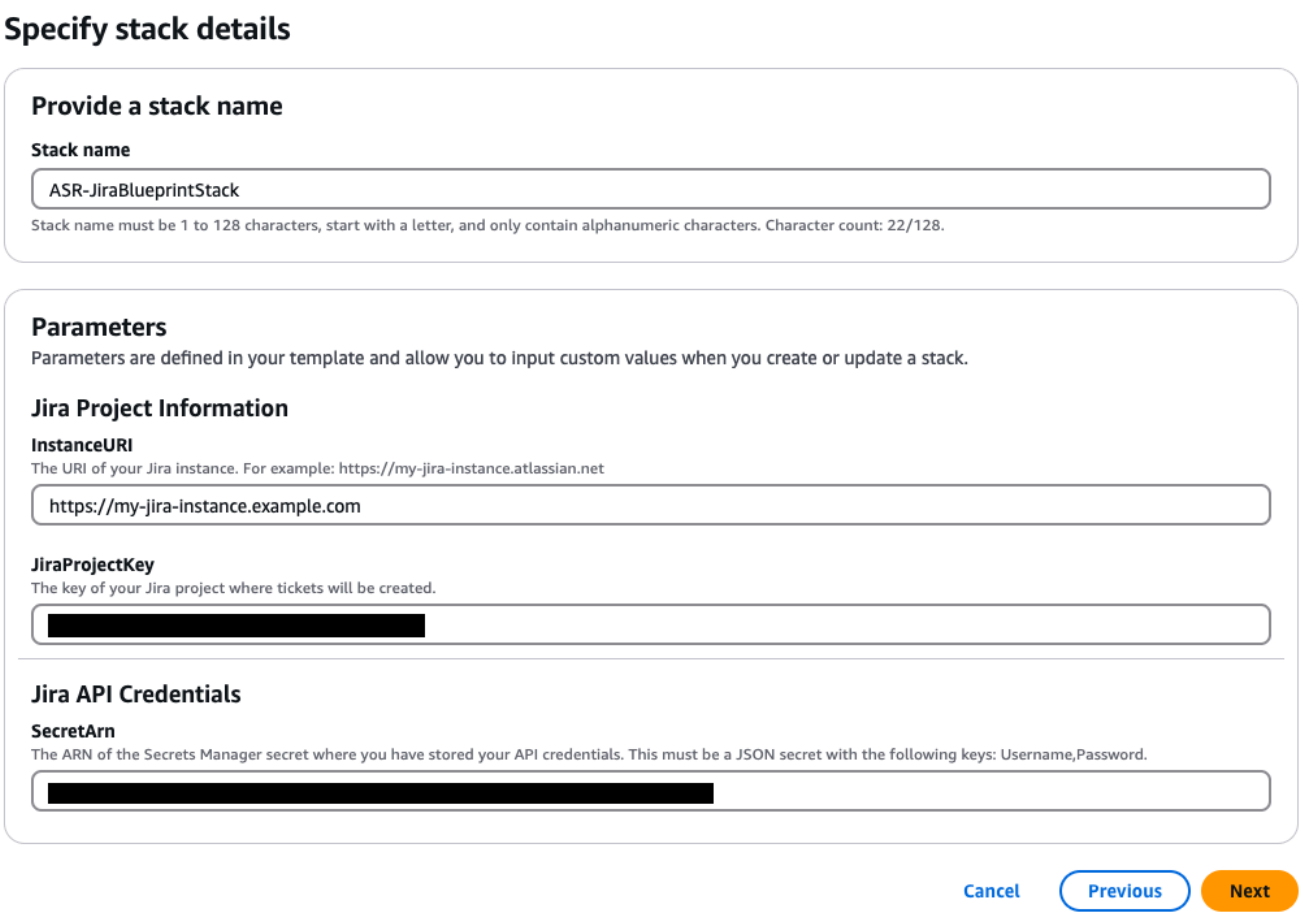
   c. 為您要傳送票證的 Jira 專案提供專案金鑰。

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

   > **Note**
   >
   > 您可以選擇使用 Jira API 金鑰來取代您的密碼，方法是將您的使用者名稱提供為 `Username`，並將您的 API 金鑰提供為 `Password`。

   e. 新增此秘密的 ARN 做為堆疊的輸入。

   提供堆疊名稱 Jira 專案資訊和 Jira API 登入資料。



若要部署 ServiceNow 堆疊：

f. 輸入堆疊的名稱。

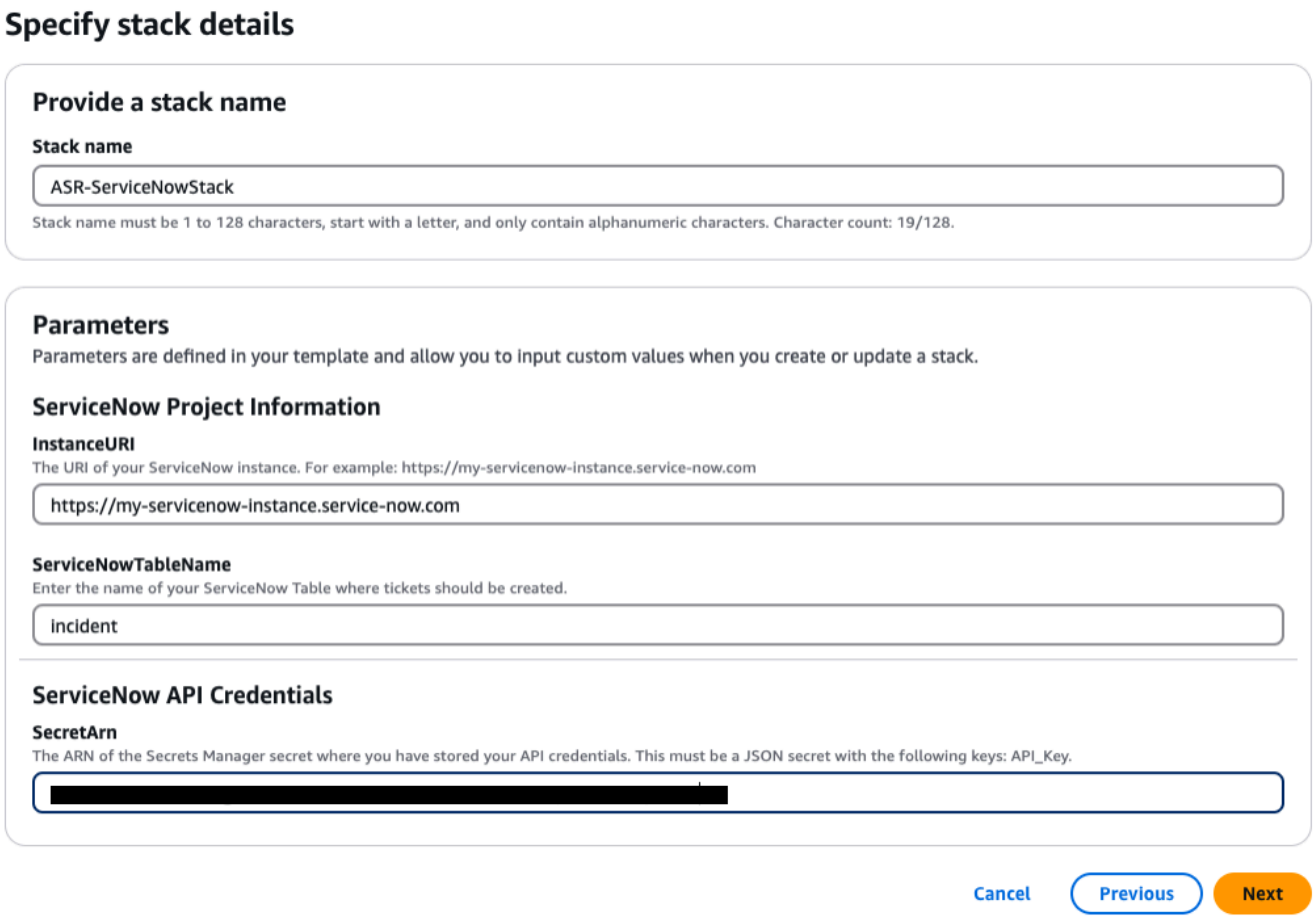
g. 提供 ServiceNow 執行個體的 URI。

h. 提供您的 ServiceNow 資料表名稱。

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

j. 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。

提供堆疊名稱 ServiceNow 專案資訊和 ServiceNow API 登入資料。

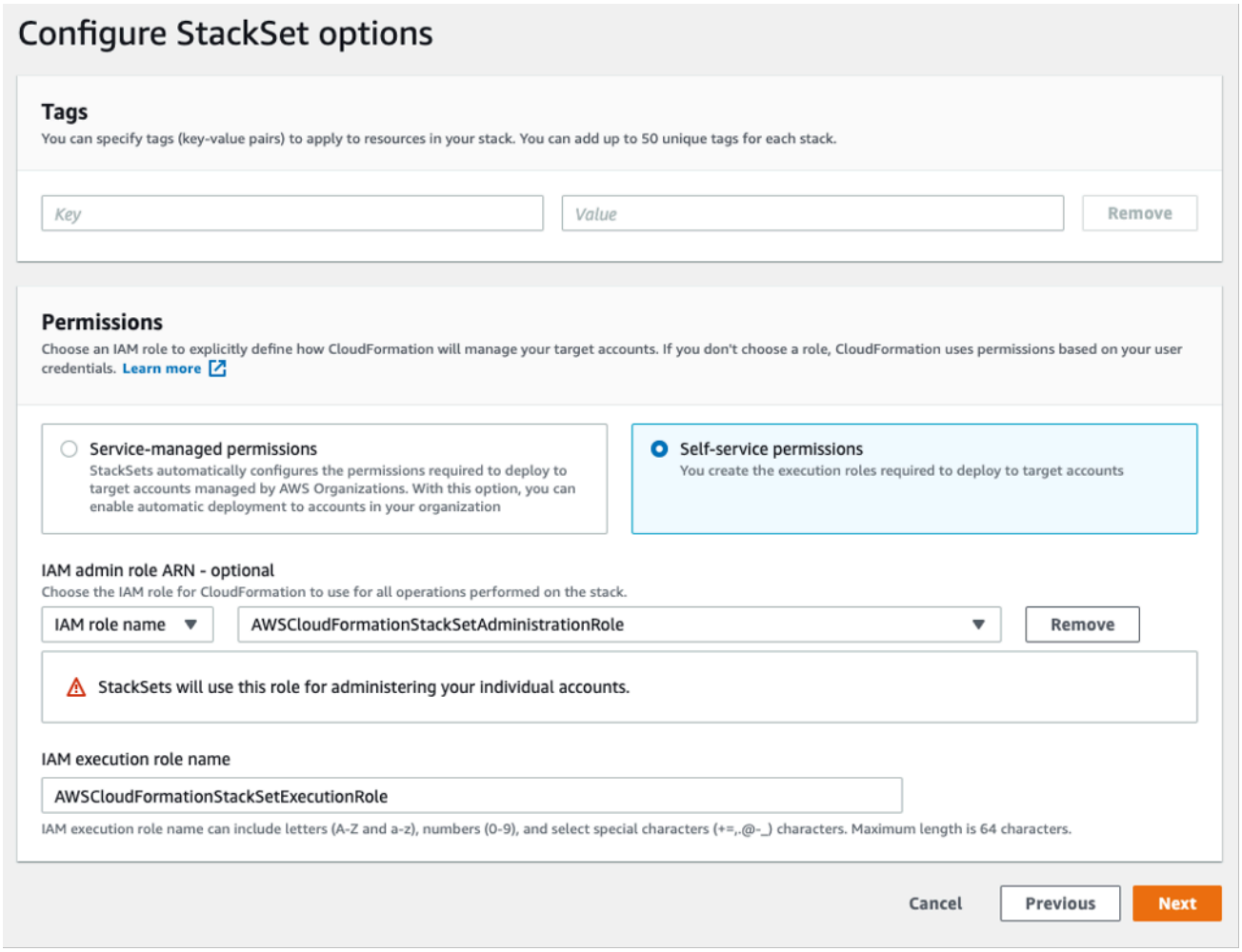


若要建立自訂整合堆疊：包含解決方案協調器 Step Functions 可以針對每個修復呼叫的 Lambda 函數。Lambda 函數應採用 Step Functions 提供的輸入，根據您的票證系統需求建構承載，並向您的系統提出建立票證的請求。

步驟 1：在委派的 Security Hub 管理員帳戶中啟動管理員堆疊

1. `automated-security-response-admin.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的 StackSet。

   設定 StackSet 選項



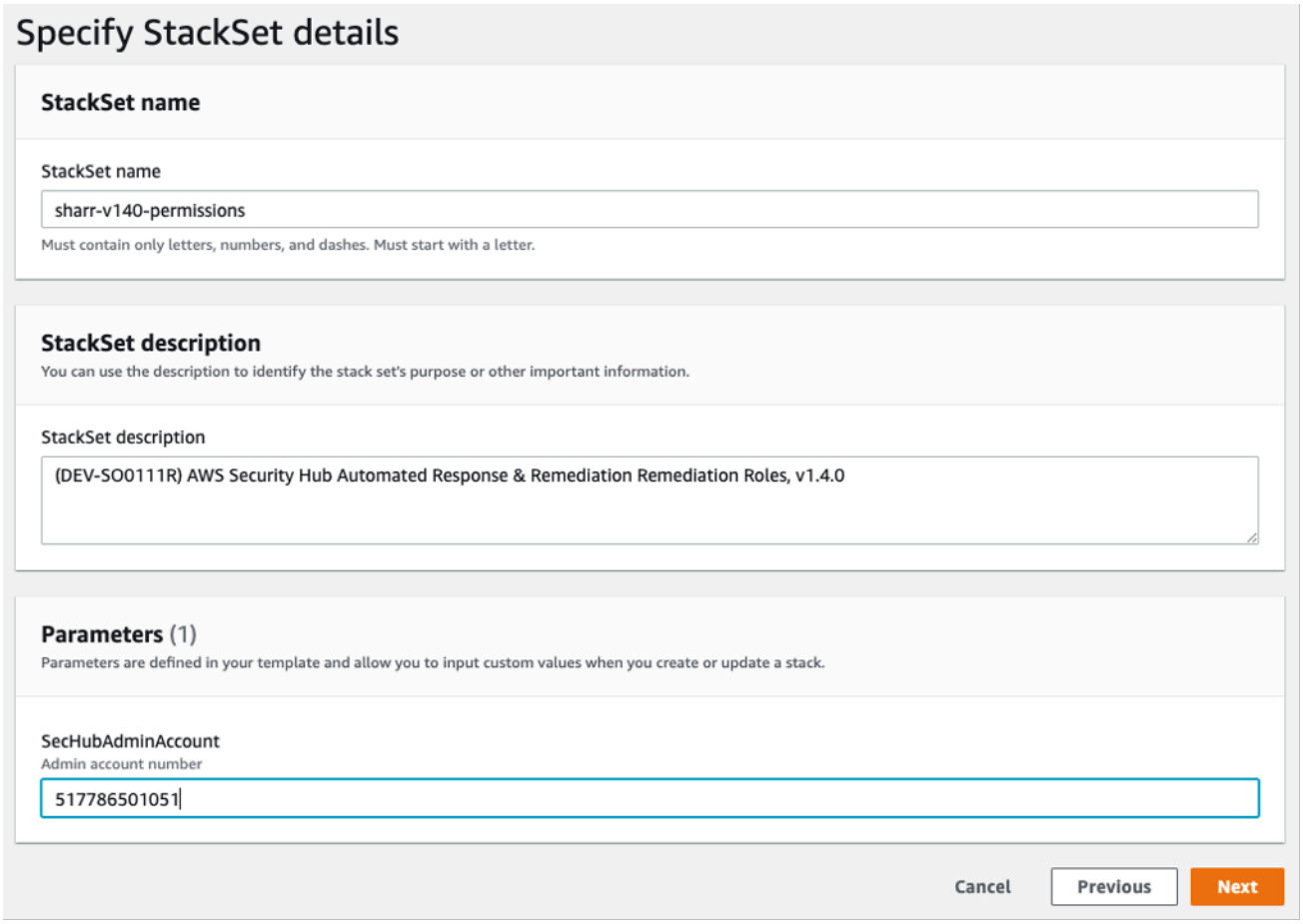
2. 針對帳戶號碼參數，輸入 AWS Security Hub 管理員帳戶的帳戶 ID。
3. 針對指定區域參數，僅選取開啟 Security Hub 管理員的區域。請等待此步驟完成，再繼續步驟 2。

步驟 2：在每個 AWS Security Hub 成員帳戶中安裝修復角色

使用服務受管 StackSets 來部署成員角色範本 `automated-security-response-member-roles.template`。此 StackSet 必須部署在每個成員帳戶的一個區域中。它定義了允許從 ASR Orchestrator 步驟函數進行跨帳戶 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。您可以在此 StackSet 部署時繼續執行步驟 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，您必須部署為自我管理的 StackSet。這不支援自動部署到 AWS Organization 中的新帳戶。

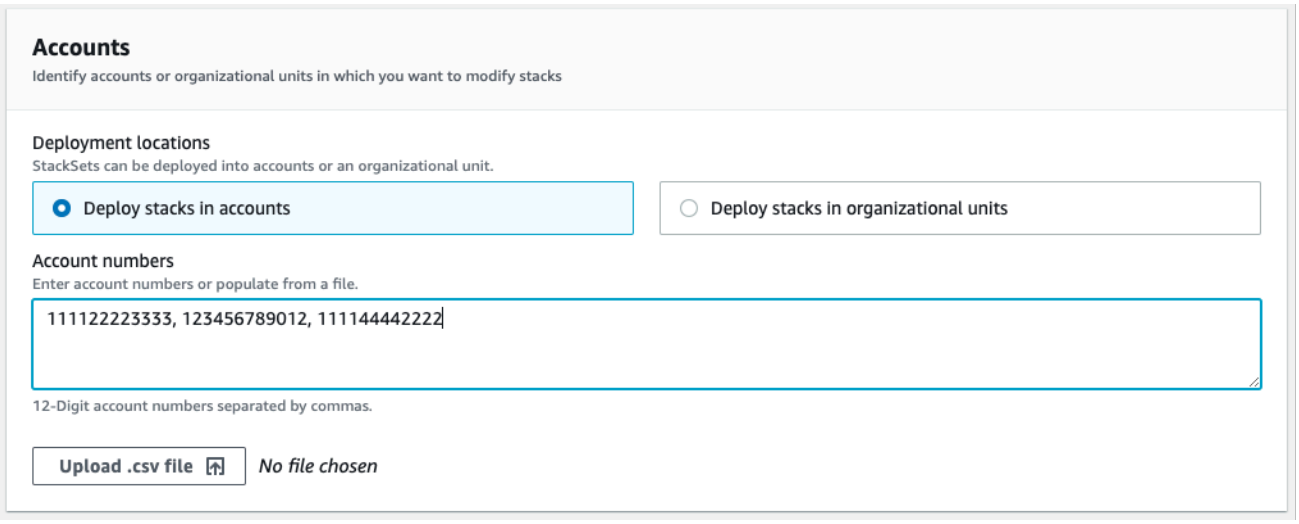
參數

LogGroup 組態：選擇接收 CloudTrail 日誌的日誌群組。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。帳戶管理員在為 CloudTrail 日誌建立 CloudWatch Logs 群組之後，必須更新 Systems Manager - Parameter Store /Solutions/SO0111/Metrics_LogGroupName 參數。這對於在 API 呼叫上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：輸入您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 StackSets 部署。

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。遵循本節中的step-by-step說明，設定解決方案並將其部署到您的帳戶。

部署時間：約 30 分鐘

先決條件

部署此解決方案之前，請確定 AWS Security Hub 與您的主要和次要帳戶位於相同的 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 AWS 上部署此解決方案。

（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，並提供它做為管理員堆疊的輸入（請參閱步驟 1)。

步驟 1：啟動管理員堆疊

- 在您的 `automated-security-response-admin.template` AWS Security Hub 管理員帳戶中啟動 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 (`Yes`如果`SO0111-ASR-Orchestrator`先前安裝已存在，請選取此選項）。

步驟 2：在每個 AWS Security Hub 成員帳戶中安裝修復角色

- 在每個成員帳戶的一個區域中啟動 `automated-security-response-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 CIS 3.1-3.14 修復搭配使用的 CloudWatch Logs 群組名稱。它必須是接收 CloudTrail 日誌的 CloudWatch Logs 日誌群組的名稱。 CloudTrail
- 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

- 根據每個成員帳戶移除任何修補。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 ServiceNow 提供的整合堆疊，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。

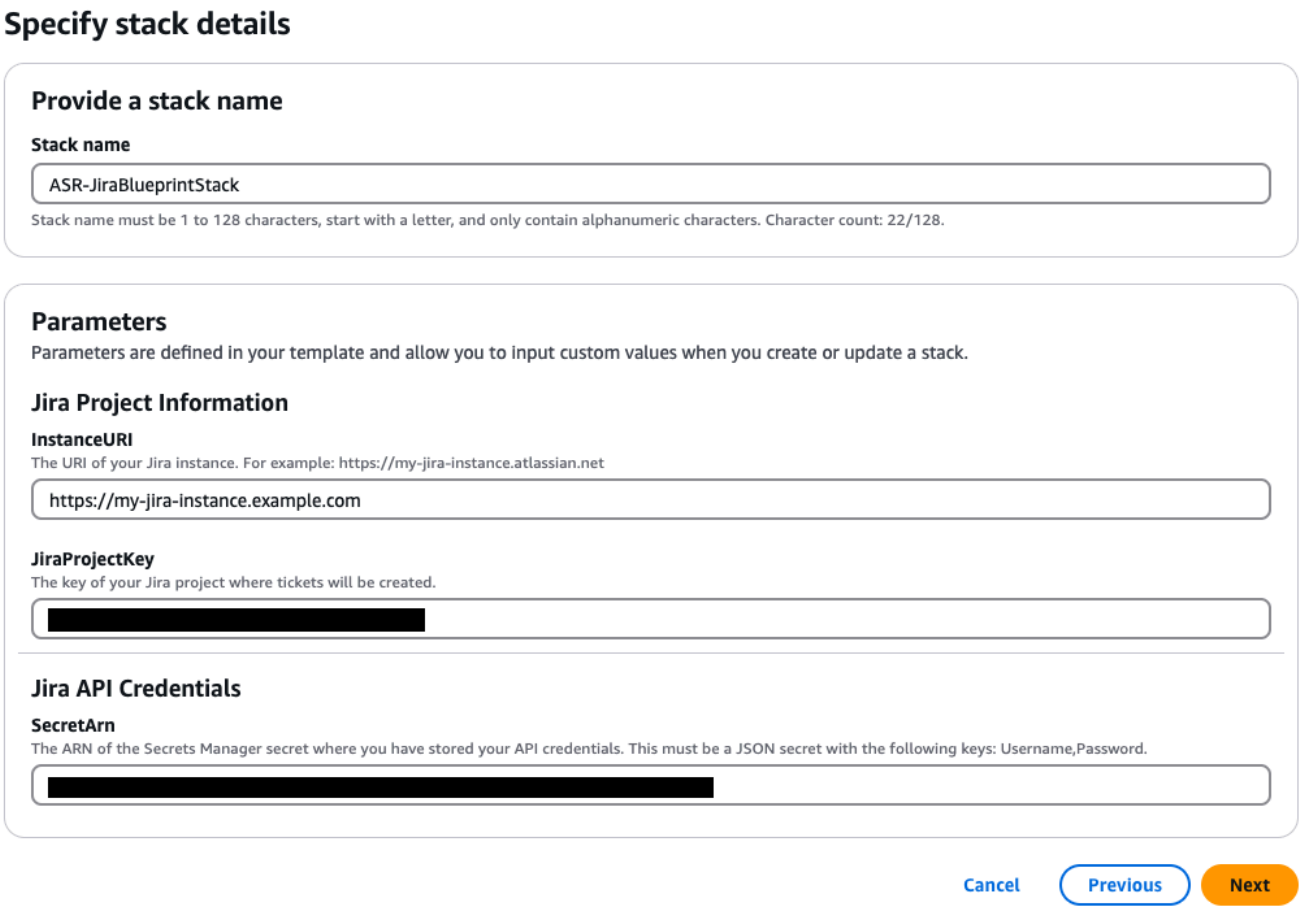
c. 為您要傳送票證的 Jira 專案提供專案金鑰。

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，方法是將您的使用者名稱提供為 `Username`，並將您的 API 金鑰提供為 `Password`。

e. 新增此秘密的 ARN 做為堆疊的輸入。

「提供堆疊名稱 Jira 專案資訊和 Jira API 登入資料。



若要部署 ServiceNow 堆疊：

f. 輸入堆疊的名稱。

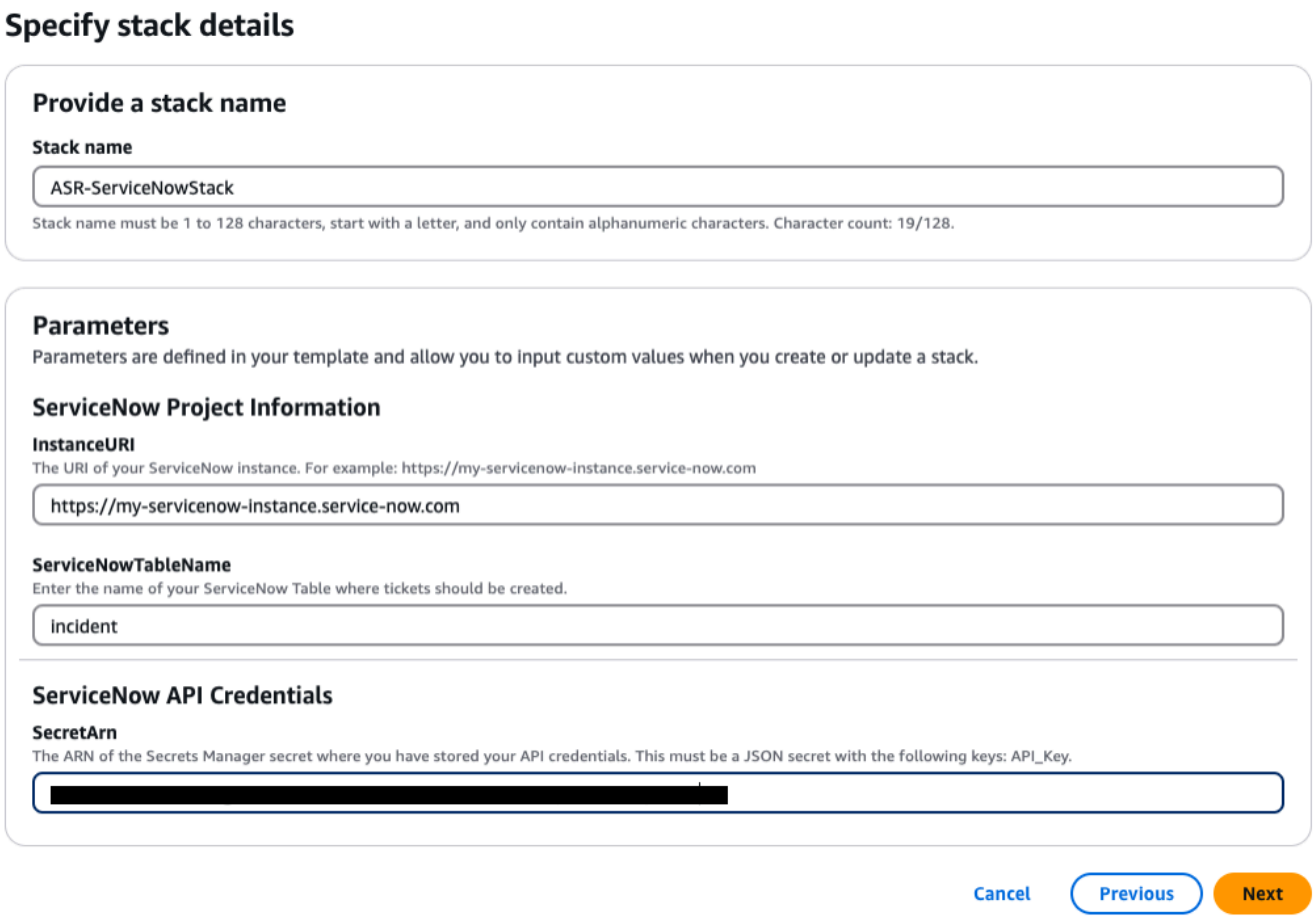
g. 提供 ServiceNow 執行個體的 URI。

h. 提供您的 ServiceNow 資料表名稱。

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

j. 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。

提供堆疊名稱 ServiceNow 專案資訊和 ServiceNow API 登入資料。



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 AWS 的選項。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。AWS 擁有透過此問卷收集的資料。資料收集受 AWS 隱私權聲明約束。
>
> 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 主控台上傳您的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 雲端中部署 AWS 解決方案上的自動化安全回應。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一節，並參閱此解決方案中使用的每個 AWS 服務的定價網頁。

1. 從目前設定 AWS Security Hub 的帳戶登入 AWS 管理主控台，並使用下面的按鈕啟動 `automated-security-response-admin.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。若要在不同的 AWS 區域中啟動此解決方案，請使用 AWS 管理主控台導覽列中的區域選擇器。

   > **Note**
   >
   > 此解決方案使用 AWS Systems Manager，目前僅適用於特定 AWS 區域。解決方案適用於所有支援此服務的 區域。如需各區域的最新可用性，請參閱 AWS 區域服務清單。

3. 在建立堆疊頁面上，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，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
載入 SC 管理員堆疊	yes	指定是否要安裝管理員元件以自動修復 SC 控制項。
載入 AFSBP 管理員堆疊	no	指定是否要安裝管理員元件以自動修復 FSBP 控制項。
載入 CIS120 管理員堆疊	no	指定是否要安裝管理員元件以自動修復 CIS120 控制項。
載入 CIS140 管理員堆疊	no	指定是否要安裝管理員元件以自動修復 CIS140 控制項。
載入 CIS300 管理員堆疊	no	指定是否要安裝管理員元件以自動修復 CIS300 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 Admin Stack	no	指定是否要安裝管理員元件以自動修復 NIST 控制項。
重複使用協調器日誌群組	no	選取是否要重複使用現有的 SO0111-ASR-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。如果此帳戶中先前部署Orchestrator Log Group仍存在 ，yes請重複使用現有的Orchestrator Log Group 選擇，否則為 no。如果您從比 v2.3.0

參數	預設	描述
		更舊的版本執行堆疊更新，請選擇 no
使用 CloudWatch 指標	yes	指定是否啟用 CloudWatch 指標來監控解決方案。這會建立 CloudWatch Dashboard 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，當控制 ID 在指定日期失敗超過 5% 的修復時，您會收到警示。 只有在建立警示時，此參數才會運作（請參閱使用 CloudWatch Metrics 警示參數）。
EnableEnhancedCloudWatchMetrics	no	如果 yes， 會建立其他 CloudWatch 指標，以個別追蹤 CloudWatch 儀表板上的所有控制項 IDs，並做為 CloudWatch 警示。 請參閱 成本 區段，以了解這會產生的額外成本。

參數	預設	描述
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，請從步驟 0 的堆疊輸出提供 Lambda 函數名稱，例如：SO0111-ASR-ServiceNow-TicketGenerator 。
TargetAccountIDs	ALL	用於控制自動化修復範圍的 AWS 帳戶 IDs 清單。 使用「ALL」以組織中的所有帳戶為目標。 或提供以逗號分隔的 12 位數 AWS 帳戶 IDs清單。範例："123456789012，098765432109"
TargetAccountIDsStrategy	INCLUDE	定義解決方案如何根據 TargetAccountIDs 清單套用自動化修復。 INCLUDE：僅對列出的帳戶執行自動修復。 EXCLUDE：為所有帳戶執行自動修復，但列出的帳戶除外。

> **Note**
>
> 部署或更新解決方案的 CloudFormation 堆疊後，您必須在 Admin 帳戶中手動啟用自動修復。

1. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。

2. 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。
3. 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 成員帳戶中安裝修復角色

StackSet `automated-security-response-member-roles.template` 只能部署在每個成員帳戶的一個區域中。它定義了允許從 ASR Orchestrator 步驟函數進行跨帳戶 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，也是成員）。選取按鈕以啟動 `automated-security-response-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。

2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同的 AWS 區域中啟動此解決方案，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，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，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	####	輸入最多 9 個小寫英數字元的字串。要新增為修補 IAM 角色名稱尾碼的唯一命名空間。成員角色和成員堆疊中應使用相同的命名空間。對於每個解決方案部署，此字串應該是唯一的，但不需要在堆疊更新期間變更。命名空間值不需要每個成員帳戶是唯一的。

參數	預設	描述
Sec Hub 帳戶管理員	####	輸入 AWS Security Hub 管理員帳戶的 12 位數帳戶 ID。此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 AWS 的選項。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。AWS 擁有透過此問卷收集的資料。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 主控台上傳您的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。

`automated-security-response-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透過此堆疊可用的修補。

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，也是成員）。選取按鈕以啟動 `automated-security-response-member.template` AWS CloudFormation 範本。

   Launch solution

您也可以下載範本做為自有實作的起點。根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同的 AWS 區域中啟動此解決方案，請使用 AWS 管理主控台導覽列中的區域選擇器。

+

> **Note**
>
> 此解決方案使用 AWS Systems Manager，目前可在大多數 AWS 區域使用。解決方案適用於所有支援這些服務的 區域。如需各區域的最新可用性，請參閱 AWS 區域服務清單。

1. 在建立堆疊頁面上，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，然後選擇下一步。
2. 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。
3. 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
提供用於建立指標篩選條件和警示的 LogGroup 名稱	####	指定 CloudTrail 記錄 API 呼叫的 CloudWatch 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 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 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 控制項。

參數	預設	描述
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。
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是否應為 FSBP RedShift.4 修復建立 S3 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	####	輸入 AWS Security Hub 管理員帳戶的 12 位數帳戶 ID。
命名空間	####	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。每個解決方案部署的字串應該是唯一的，但不需要在堆疊更新期間變更。
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 追蹤yes。您必須將解決方案部署到 AWS 組織，才能啟用此功能。請參閱 成本 一節，以了解這會產生的額外成本。

4. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。

5. 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。
6. 選擇 Create stack (建立堆疊) 以部署堆疊。

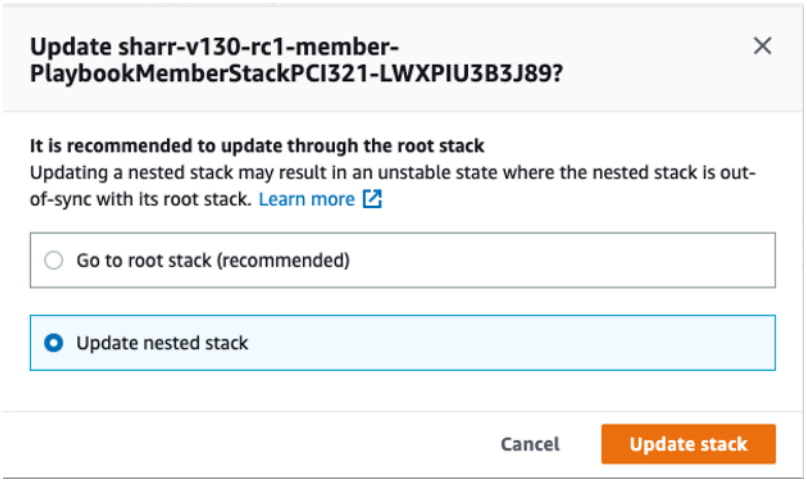
您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內收到 CREATE_COMPLETE 狀態。

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，您可以透過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. 調整可用的補救措施。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。

Control Tower (CT) 部署

適用於 AWS Control Tower (CfCT) 的自訂指南適用於管理員、DevOps 專業人員、獨立軟體供應商、IT 基礎設施架構師和系統整合商，他們想要為其公司和客戶自訂和擴展其 AWS Control Tower 環境。它提供使用 CfCT 自訂套件自訂和擴展 AWS Control Tower 環境的相關資訊。

部署時間：約 30 分鐘

先決條件

部署此解決方案之前，請確定其適用於 AWS Control Tower 管理員。

當您準備好使用 AWS Control Tower 主控台或 APIs 設定登陸區域時，請遵循下列步驟：

若要開始使用 AWS Control Tower，請參閱：AWS Control Tower 入門

若要了解如何自訂您的登陸區域，請參閱：自訂您的登陸區域

若要啟動和部署您的登陸區域，請參閱：登陸區域部署指南

部署概觀

使用下列步驟在 AWS 上部署此解決方案。

步驟 1：建置和部署 S3 儲存貯體

> **Note**
>
> S3 儲存貯體組態 – 僅適用於 ADMIN。這是一次性設定步驟，不應由最終使用者重複執行。S3 儲存貯體存放部署套件，包括執行 ASR 所需的 AWS CloudFormation 範本和 Lambda 程式碼。這些資源是使用 CfCt 或 StackSet 部署。

1. 設定 S3 儲存貯體

設定將用於存放和提供部署套件的 S3 儲存貯體。

2. 設定 環境

準備建置和部署程序所需的必要環境變數、登入資料和工具。

3. 設定 S3 儲存貯體政策

定義並套用適當的儲存貯體政策，以控制存取和許可。

4. 準備組建

編譯、封裝或以其他方式準備您的應用程式或資產以進行部署。

5. 將套件部署至 S3

將準備好的建置成品上傳到指定的 S3 儲存貯體。

步驟 2：堆疊部署至 AWS Control Tower

1. 建立 ASR 元件的建置資訊清單

定義組建資訊清單，列出所有 ASR 元件、其版本、相依性和組建指示。

2. 更新 CodePipeline

修改 AWS CodePipeline 組態，以包含部署 ASR 元件所需的新建置步驟、成品或階段。

步驟 1：建置並部署至 S3 儲存貯體

AWS 解決方案使用兩個儲存貯體：透過 HTTPS 存取之範本的全域存取儲存貯體，以及存取區域內資產的區域儲存貯體，例如 Lambda 程式碼。

1. 設定 S3 儲存貯體

選擇唯一的儲存貯體名稱，例如 asr-staging。在終端機上設定兩個環境變數，其中一個應為 - 參考為尾碼的基本儲存貯體名稱，另一個則為您預期部署區域的尾碼：

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

2. 環境設定

在您的 AWS 帳戶中，使用這些名稱建立兩個儲存貯體，例如 asr-staging-reference 和 asr-staging-us-east-1。（參考儲存貯體將保留 CloudFormation 範本，區域儲存貯體將保留所有其他資產，例如 lambda 程式碼套件。）您的儲存貯體應該加密並不允許公開存取

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

> **Note**
>
> 建立儲存貯體時，請確保它們不可公開存取。使用隨機儲存貯體名稱。停用公有存取。使用 KMS 加密。上傳之前，請確認儲存貯體擁有權。

3. S3 儲存貯體政策設定

更新 $TEMPLATE_BUCKET_NAME S3 儲存貯體政策，以包含執行帳戶 ID 的 PutObject 許可。將此許可指派給執行帳戶中有權寫入儲存貯體的 IAM 角色。此設定可讓您避免在 管理帳戶中建立儲存貯體。

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

```
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

修改資產 S3 儲存貯體政策以包含許可。將此許可指派給執行帳戶中有權寫入儲存貯體的 IAM 角色。為每個區域資產儲存貯體（例如asr-staging-us-east-1、asr-staging-eu-west-1 等）重複此設定，允許跨多個區域部署，而無需在 管理帳戶中建立儲存貯體。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
            "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
```

```
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

4. 組建準備

- 事前準備：
  - AWS CLI v2
  - Python 3.11+ 搭配 pip
  - AWS CDK 2.171.1+
  - Node.js 20+ 搭配 npm
  - Poetry v2 搭配要匯出的外掛程式
- Git 複製 https：//https://github.com/aws-solutions/automated-security-response-on-aws.git

首先，請確定您已在來源資料夾中執行 npm 安裝。

在複製儲存庫的部署資料夾中，執行 build-s3-dist.sh，傳遞儲存貯體的根名稱（例如 mybucket) 和您要建置的版本（例如 v1.0.0)。我們建議根據從 GitHub 下載的版本（例如 GitHub：v1.0.0，您的組建：v1.0.0.mybuild)

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

5. 將套件部署至 S3

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

步驟 2：堆疊部署至 AWS Control Tower

1. 建置 ASR 元件的資訊清單

將 ASR 成品部署至 S3 儲存貯體之後，請更新 Control Tower 管道資訊清單以參考新版本，然後觸發管道執行，請參閱：Controltower 部署

> **Important**
>
> 若要確保 ASR 解決方案的正確部署，請參閱官方 AWS 文件，以取得 CloudFormation 範本概觀和參數描述的詳細資訊。以下資訊連結：CloudFormation 範本參數概觀指南

ASR 元件的資訊清單如下所示：

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

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDsStrategy
        parameter_value: "INCLUDE"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
```

```
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDs
        parameter_value: "ALL"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

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

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

```
    - parameter_key: LoadAFSBPMemberStack
      parameter_value: "no"
    - parameter_key: LoadSCMemberStack
      parameter_value: "yes"
    - parameter_key: LoadPCI321MemberStack
      parameter_value: "no"
    - parameter_key: LoadCIS140MemberStack
      parameter_value: "no"
    - parameter_key: EnableCloudTrailForASRActionLog
      parameter_value: "no"
    - parameter_key: LogGroupName
      parameter_value: <LOG_GROUP_NAME>
    - parameter_key: LoadCIS300MemberStack
      parameter_value: "no"
  deploy_method: stack_set
  deployment_targets:
   accounts: # :type: list
      - <ACCOUNT_NAME> # and/or
      - <ACCOUNT_NUMBER>
  organizational_units:
    - <ORG UNIT>
  regions: # :type: list
    - <REGION_NAME>
```

2. 程式碼管道更新

將資訊清單檔案新增至 custom-control-tower-configuration.zip 並執行 CodePipeline，請參閱：程式碼管道概觀

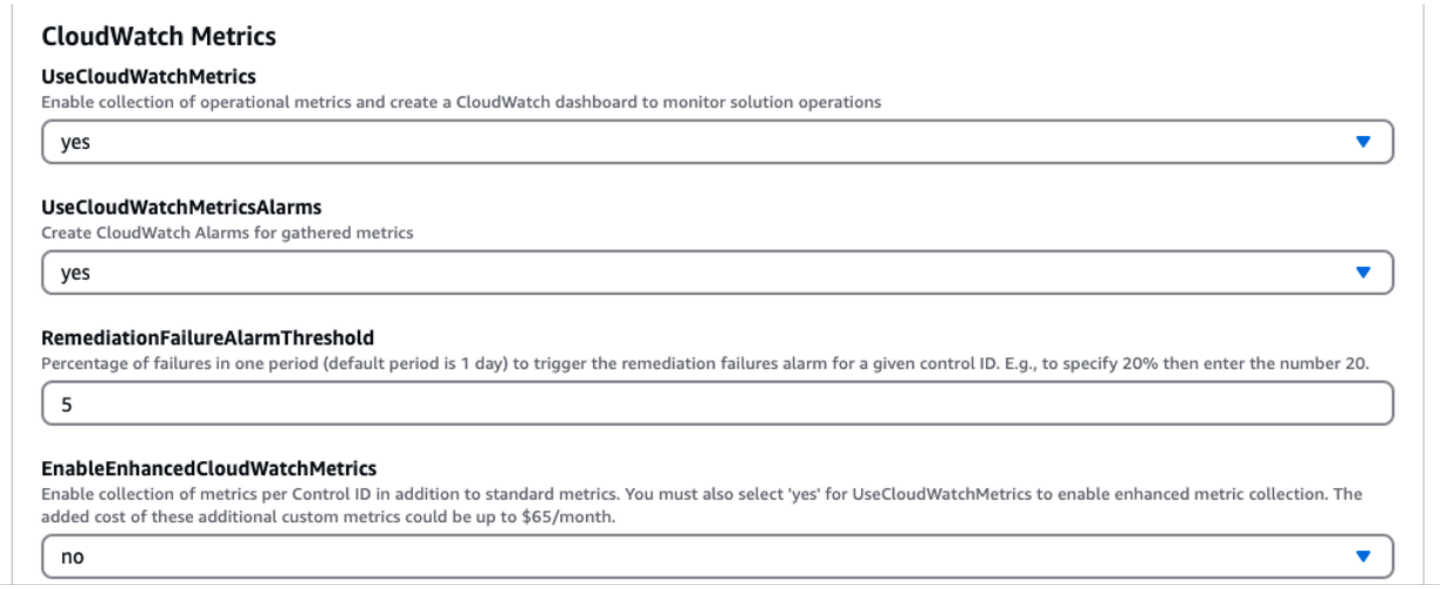
使用 Amazon CloudWatch 儀表板監控解決方案的操作

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

CloudWatch 功能有四個 CloudFormation 範本參數。



1. UseCloudWatchMetrics - 將此設定為yes啟用操作指標的集合，並建立 CloudWatch 儀表板以檢視這些指標。
2. UseCloudWatchAlarms - 將此設定為yes啟用解決方案的預設警示。
3. RemediationFailureAlarmThreshold - 一段時間內失敗的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，因此只會收集所有控制項 IDs指標。每個控制項 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。

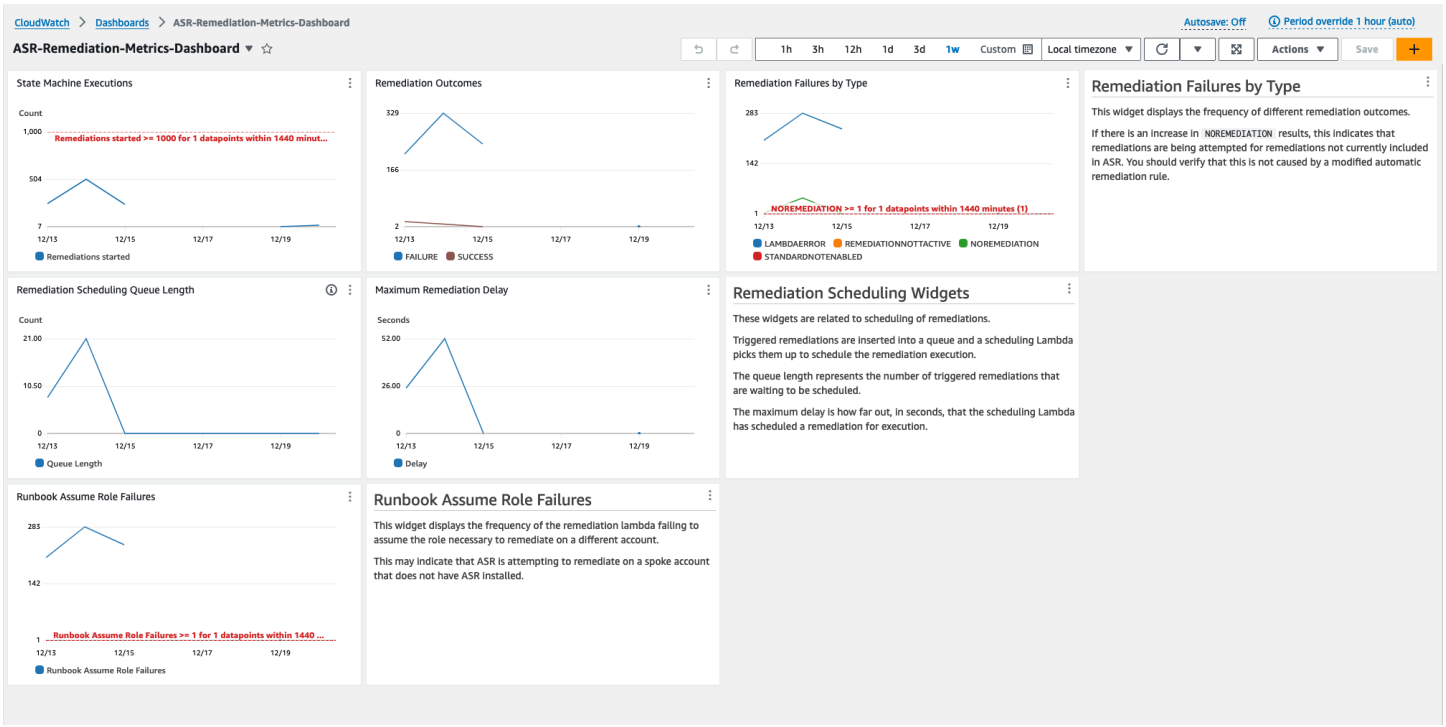
CloudWatch 儀表板包含下列區段：

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，以百分比為單位，以及失敗原因。大量失敗可能會暗示您可能需要更詳細的調查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失敗率時，本節會顯示失敗是分散到多個控制項 IDs，還是只有某些控制項 IDs 失敗。
4. Runbook 擔任角色失敗 - 顯示由於未安裝解決方案成員角色之帳戶中的修復嘗試而發生的失敗次數。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，或取消與 Security Hub 中帳戶的關聯，以緩解此問題。
5. 依 ASR 的雲端線索管理動作 - 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的解決方案管理動作。當您發現任何 AWS 帳戶中發生非預期的資源變更時，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。

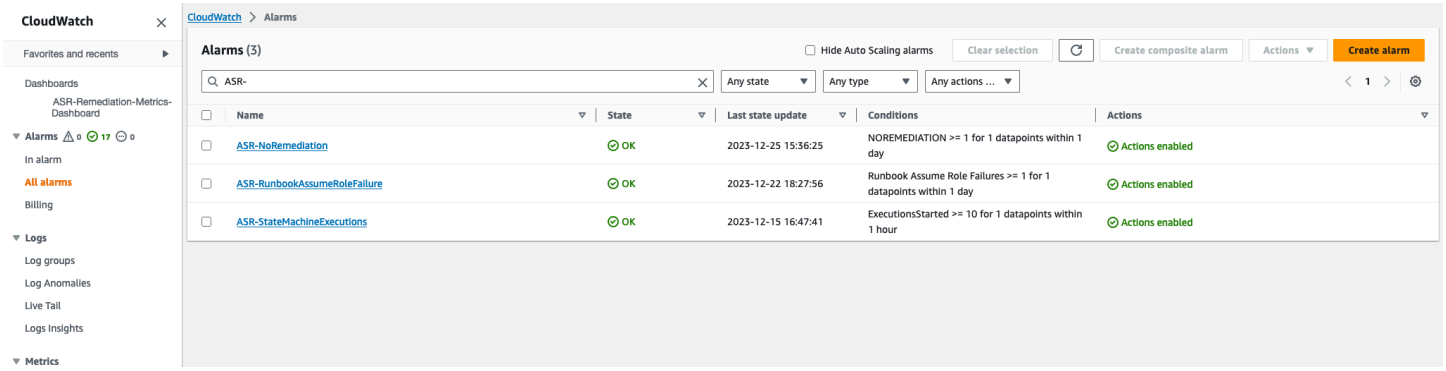
1. 狀態機器在 24 小時期間內執行 > 1000。
   a. 修復執行的大量峰值可能表示事件規則啟動的頻率高於預期。
   b. 您可以使用 CloudFormation 參數變更閾值。
2. 依類型 = NOREMEDIATION > 0 的修復失敗
   a. 正在嘗試修復不包含在 ASR 中的修復。這可能表示事件規則已修改為包含超過預期的修補。
3. Runbook 擔任角色失敗 > 0
   a. 在未正確部署解決方案的帳戶或區域上嘗試修復。這可能表示已修改事件規則，以包含比預期更多的帳戶。

您可以修改所有警示閾值，以符合個別部署需求。

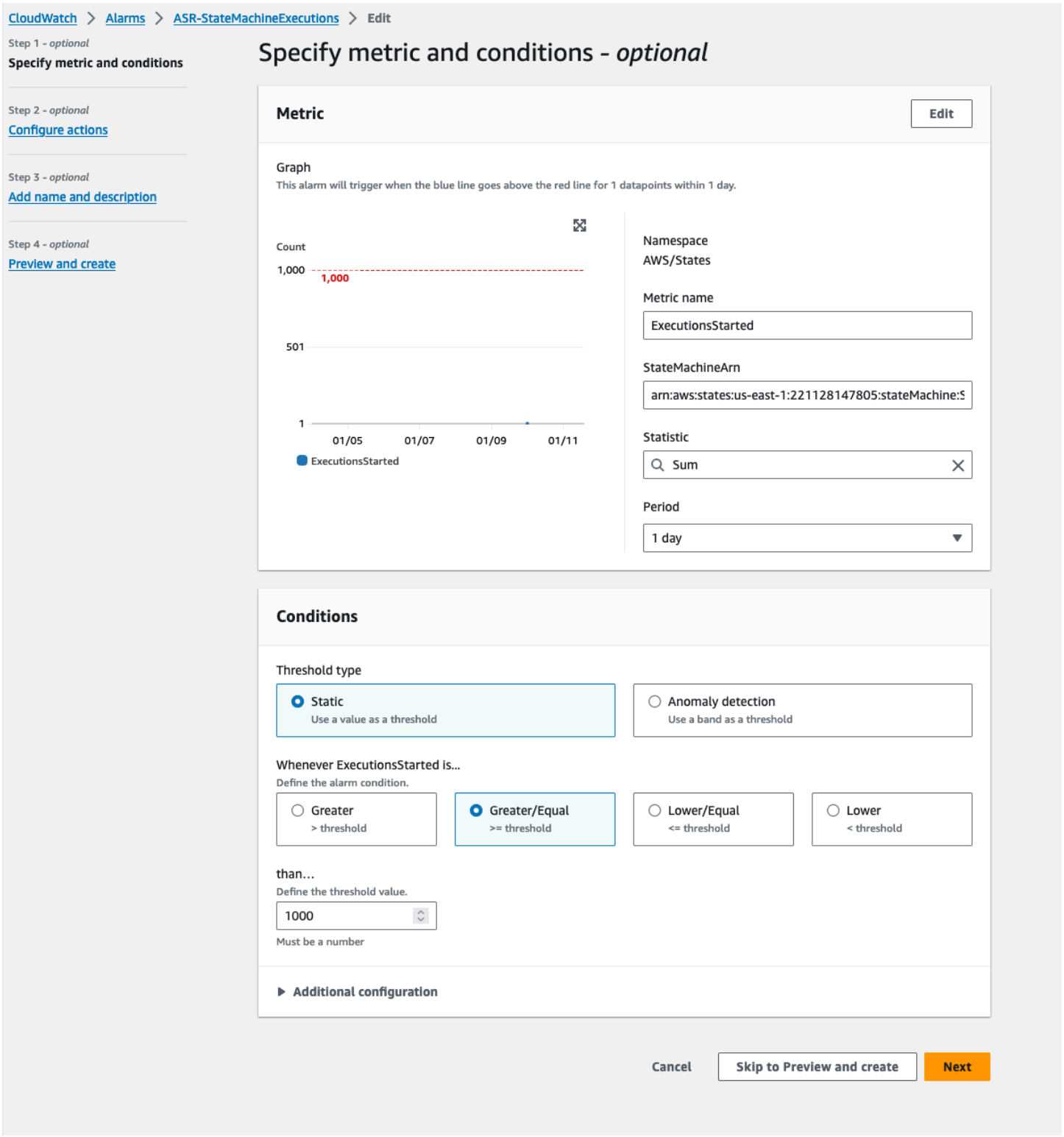


修改警示閾值

1. 導覽至 Amazon CloudWatch → 警示 → 所有警示。
2. 選擇您要修改的警示，然後選取動作 → 編輯。



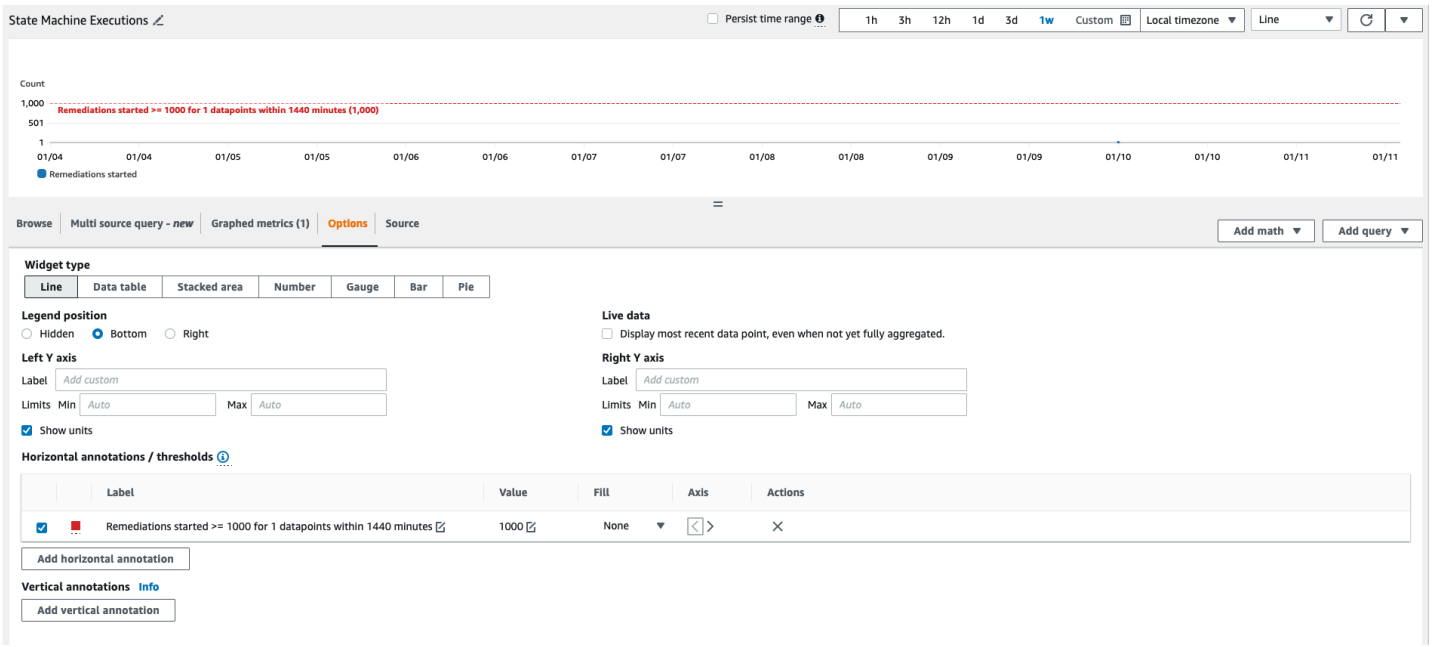
1. 將閾值變更為所需的值並儲存。



1. 導覽至 CloudWatch 儀表板來修改其中的圖表，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

如果您先前已在 v1.4.x 之前部署解決方案，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為此選項選取 。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

如果您是從 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

如果您是從 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 會在 CloudFormation 中失敗。

> **Note**
>
> - 更新解決方案時，可能需要在管理員帳戶中手動重新啟用自動修復規則。請參閱啟用全自動化修復。

- 如果您使用 `Reuse Orchestrator Log Group` 參數來保留日誌，請確保在堆疊更新期間正確設定，以避免日誌群組重新建立或遺失日誌保留設定。請參閱部署解決方案。如果您要從舊版執行 v2.3.0+ 的堆疊更新，請選擇「否」

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 Support 案例的說明。

解決方案日誌

本節包含此解決方案的故障診斷資訊，請參閱主題的左側導覽。

此解決方案會從在 AWS Systems Manager 下執行的修復 Runbook 收集輸出，並將結果記錄到 AWS Security Hub 管理員帳戶中S00111-ASR的 CloudWatch Logs 群組。每個控制項每天有一個串流。

Orchestrator Step Functions 會將所有步驟轉換記錄到 AWS Security Hub 管理員帳戶中的 S00111-ASR-Orchestrator CloudWatch Logs 群組。此日誌是稽核線索，可記錄 Step Functions 每個執行個體的狀態轉換。每個 Step Functions 執行都有一個日誌串流。

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

下列疑難排解資訊使用 S00111-ASR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 日誌來疑難排解問題。

如果修復失敗，類似以下內容的訊息將記錄到日誌串流S00111-ASR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 ASR Runbook，適用於安全標準和控制項。例如：ASR-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.
```

此資訊會指出失敗，在此案例中是在成員帳戶中執行的子自動化。若要疑難排解此問題，您必須登入成員帳戶中的 AWS 管理主控台 （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，並顯示 Amazon CloudWatch 中已有可用的資源。

  解決方案：檢查 CloudFormation 資源/事件區段中指出日誌群組已存在的錯誤訊息。ASR 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以錯誤進行部署

  解決方案：您可能已達到 EventBridge 規則的配額，並已部署手冊數量。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調查結果、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：在與 Security Hub 管理員相同的帳戶和區域中部署管理員堆疊。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，SO0111-ASR-Orchestrator 在取得自動化文件狀態失敗，出現 502 錯誤：「`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，了解未修復的原因。常見的原因是問題清單沒有自動修復。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 Logs。尋找 SO0111-ASR CloudWatch Logs 群組。排序清單，以先顯示最近更新的串流。選取您嘗試執行之問題清單的日誌串流。您應該會在那裡發現任何錯誤。故障的一些原因可能是：問題清單控制與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。問題清單的狀態應更新。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 的事件資料建立的，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，請參閱上述的「`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)。

  解決方案：成員範本尚未安裝在 ASR 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，因為記錄器或交付管道已存在。

  解決方案：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 AWS Config 設定。

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

  解決方案：這是此版本中的已知問題，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會導致堆疊追蹤的錯誤條件的機會，而不是錯誤訊息。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：

  a. 登入 AWS Security Hub 管理主控台。

  b. 在管理員帳戶中，前往設定。

  c. 選取自訂動作索引標籤

  d. 手動刪除使用 ASR 修復的項目。

  e. 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。您必須在所有成員帳戶中重新部署成員角色堆疊。

- 問題：CIS 3.x 修復在超過 24 小時`PASSED`後仍未顯示。

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

特定修復的問題

SetSSLBucketPolicy 因 AccessDenied 錯誤而失敗

相關聯的控制項：AWS FSBP 1.0.0 S3.5 版、PCI 3.2.1 PCI.S3.5 版、CIS 1.4.0 2.1.2 版、SC 2.0.0 S3.5 版

問題：SetSSLBucketPolicy 失敗，出現 AccessDenied 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。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，即可達到此狀態。

修復 ConfigureS3BucketPublicAccessBlock （相關控制項：AWS FSBP v1.0.0 S3.2、PCI v3.2.1 PCI.S3.2、CIS v1.4.0 2.1.5.2、SC v2.0.0 S3.2) 也可以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。

SetSSLBucketPolicy 會將陳述式新增至儲存貯體政策，以拒絕不使用 SSL 的請求。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，修補將無法嘗試放置仍包含這些陳述式的修改後儲存貯體政策。

解決方案：修改儲存貯體政策以移除允許公開存取與儲存貯體上封鎖公開存取設定衝突的陳述式。

PutS3BucketPolicyDeny 失敗

相關聯的控制項：AWS FSBP 1.0.0 S3.6 版、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委託人是「*」，解決方案就無法將拒絕政策新增至目標儲存貯體，因為它會封鎖所有委託人的所有儲存貯體動作。

解決方案：修改儲存貯體政策以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

如果發生事件，您可能會發現您需要停用解決方案，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 主控台中導覽至 EventBridge。
2. 在邊欄中選取規則。
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 主控台中導覽至 EventBridge。
2. 在邊欄中選取規則。
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 主控台中導覽至 EventBridge。
2. 在邊欄中選取規則。
3. 選取「預設」事件匯流排，並搜尋「Remediate_with_ASR_CustomAction」
4. 選取規則上的 ，然後選取「停用」按鈕。

聯絡 支援

如果您有 AWS 開發人員支援、AWS Business Support 或 AWS Enterprise Support，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，界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 Support 處理請求所需的資訊。

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，透過 AWS 管理主控台解除安裝解決方案。

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 手冊。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 Service Catalog 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. 從 Security Hub 管理員和成員帳戶移除輪輻`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 Logs 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. `automated-security-response-member.template` 從每個成員帳戶移除 。
2. `automated-security-response-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. 手動刪除使用 ASR 修復的項目。

5. 再次刪除堆疊。

V1.4.0 及更新版本

堆疊部署

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

StackSet 部署

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

請注意，即使移除範本，也會`automated-security-response-member-roles.template`保留來自 的 IAM 角色。如此一來，使用這些角色的修復就能繼續運作。在驗證 CloudTrail 到 CloudWatch CloudWatch 記錄或 RDS 增強型監控等作用中修復不再使用後，可以手動移除這些 SO0111-* 角色。

管理員指南

啟用和停用部分解決方案

身為解決方案管理員，您可以控制下列控制解決方案的哪些功能已啟用。

部署成員和成員角色堆疊的位置：

- 管理員堆疊只能在成員和成員角色堆疊已部署的帳戶中啟動修復（透過自訂動作或全自動 EventBridge 規則），其管理員帳戶號碼指定為參數值。
- 若要讓帳戶或區域完全不受解決方案控制，請勿將成員或成員角色堆疊部署到這些帳戶或區域。

Security Hub 中的帳戶和區域調查結果彙總組態：

- 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）。
- 若要讓帳戶或區域完全不受解決方案控制，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 的控制項啟動修補（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 EventBridge 規則啟動全自動修復，以控制具有管理員堆疊針對該標準部署的規則。這些會部署到管理員帳戶。
- 為求簡化，我們建議您在管理員和成員帳戶之間一致地部署標準。如果您關心 AWS FSBP 和 CIS 1.2.0 版，請將這兩個巢狀管理堆疊部署到管理員帳戶，然後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哪些控制 Runbook：

- 管理員堆疊只能針對由每個標準的成員堆疊在目標成員帳戶和區域中部署控制項 Runbook 的控制項啟動修補（透過自訂動作或全自動 EventBridge 規則）。
- 若要對特定標準啟用哪些控制項進行更精細的控制，標準的每個巢狀堆疊都有部署控制項 Runbook 的參數。將控制項的 參數設定為值 "NOT Available"，以取消部署該控制項 Runbook。

用於啟用和停用標準的 SSM 參數：

- 管理員堆疊只能針對透過標準管理員堆疊所部署的 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 ASR 的第一次部署。它將從部署解決方案的先決條件開始，最後會修復成員帳戶中的範例問題清單。

教學課程：AWS 自動化安全回應入門

這是將引導您完成第一次部署的教學課程。它將從部署解決方案的先決條件開始，最後會修復成員帳戶中的範例問題清單。

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將是管理員帳戶，而 222222222222 將是成員帳戶。我們將設定解決方案，以修復區域 us-east-1和 中資源的問題清單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帳戶所屬 AWS Organizations的 AWS Organization 管理員帳戶。

啟用 AWS Config

檢閱下列文件：

- AWS Config 文件
- AWS Config 定價
- 啟用 AWS Config

在帳戶和兩個區域中啟用 AWS Config。這會產生費用。

> **Important**
>
> 請務必選取「包含全域資源 （例如 AWS IAM 資源）」的選項。如果您在啟用 AWS Config 時未選取此選項，則不會看到與全域資源 （例如 AWS IAM 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 Config	啟用 AWS Config
222222222222	成員	啟用 AWS Config	啟用 AWS Config

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

啟用合併的控制問題清單

檢閱下列文件：

- 產生和更新控制問題清單

基於本教學的目的，我們將示範 解決方案的使用方式，並啟用 AWS Security Hub 的合併控制調查結果功能，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	啟用合併的控制問題清單	啟用合併的控制問題清單
222222222222	成員	啟用合併的控制問題清單	啟用合併的控制問題清單

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 的問題清單彙總。

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) 以 Security Hub 委派管理員身分接受管理員帳戶。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

我們將部署 CloudFormation 堆疊到多個帳戶，因此將使用 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的組態，以示範修補。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。請注意組織在偵測和報告此類資源時可能擁有的任何工具，並適時請求例外狀況。如果我們選取的控制項範例不適合您，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的情況下從 URL 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

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

AWS Config 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。

為相關控制項建立 CloudWatch 日誌群組

檢閱下列文件：

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

解決方案支援的各種 CloudTrail 控制項需要有 CloudWatch Log 群組，其為多區域 CloudTrail 的目的地。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 CloudTrail 與 CloudWatch Logs 的整合。

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

將解決方案部署至教學課程帳戶

收集管理員、成員和成員角色堆疊的三個 Amazon S3 URLs。

部署管理員堆疊

View template

automated-security-response-admin.template

在管理員帳戶中，導覽至 CloudFormation 主控台，並將管理員堆疊部署至 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

automated-security-response-member.template

在管理員帳戶中，導覽至 CloudFormation StackSets 主控台，並將成員堆疊部署至每個帳戶和區域。使用本教學課程中建立的 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的 參數值。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	確認已部署的成員堆疊
222222222222	成員	確認已部署的成員堆疊	確認已部署的成員堆疊

部署成員角色堆疊

automated-security-response-member-roles.template 範本按鈕 automated-security-response-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。使用本教學課程中建立的 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的 參數值。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	確認已部署的成員堆疊	無

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

訂閱 SNS 主題

修復更新

主題 -{https---us-east-1-console-aws-amazon-com-sns-v3-home-region-us-east-1—topic-arn-aws-sns-us-east-1-221128147805-SO0111-ASR-Topic}【SO0111-ASR_Topic】

在管理員帳戶中，訂閱管理員堆疊建立的 Amazon SNS 主題。這將在啟動修復以及成功或失敗時通知您。

警示

主題 -{https---us-east-1-console-aws-amazon-com-sns-v3-home-region-us-east-1—topic-arn-aws-sns-us-east-1-221128147805-SO0111-ASR-Alarm-Topic}【SO0111-ASR_Alarm_Topic】

在管理員帳戶中，訂閱管理員堆疊建立的 Amazon SNS 主題。這會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，並使用您在本教學課程中建立的不安全組態來尋找資源的問題清單。

這可以透過幾種方式完成：

1. 在支援合併控制項問題清單功能的分割區中，標示為「控制項」的頁面可讓您依合併控制項 ID 來尋找問題清單。
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 EventBridge 的通知。

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_ASR_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-ASR-Orchestrator" 的 AWS Step Functions。此步驟函數會呼叫目標帳戶和區域中的 SSM Automation 文件。您可以在此 AWS Step Functions 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 Automation 主控台。您將找到兩個名為「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，這可能不是問題清單的來源區域。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-ASR" 的日誌群組。此日誌群組是 Orchestrator Step Functions 中高階日誌的目的地。

啟用完全自動化的修補

解決方案的另一種操作模式是在問題清單送達 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。如果在安裝此控制項的任何帳戶和區域中偵測到此控制項，解決方案將修復此控制項。

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
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

在管理員帳戶中，找到名為 SC_2.0.0_Lambda.1_AutoTrigger 的 EventBridge 規則並加以啟用。

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
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	確認已刪除成員堆疊

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

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	確認已刪除成員角色堆疊	無

刪除保留的角色

在每個帳戶中，刪除保留的 IAM 角色。

重要：這些角色會保留給需要 角色才能繼續運作的修補 （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，將會產生費用。

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

使用解決方案建立的別名或從 CloudFormation 歷史記錄中識別解決方案部署的金鑰。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	識別並排程要刪除的管理員金鑰 識別和排程要刪除的成員金鑰	識別和排程要刪除的成員金鑰
222222222222	成員	識別和排程要刪除的成員金鑰	識別和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項目。

手冊

此解決方案包含網際網路安全中心 (CIS) AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices (FSBP) v.1.0.0、支付卡產業資料安全標準 (PCI-DSS) v3.2.1 和國家標準技術研究所 (NIST) 中所定義安全標準的手冊修補。

如果您已啟用合併控制項調查結果，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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
總計修補	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupELBHealthCheck	自動擴展。1		自動擴展。1		自動擴展。1		自動擴展。1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
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-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 Auto Scaling 群組啟動組態應該將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 (IMDSv2)					自動擴展。3		自動擴展。3

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-CreateCloudTrailMultiRegionTrail 應該啟用 CloudTrail，並使用至少一個多區域線索設定	CloudTrail.1	2.1	CloudTrail.2	3.1	CloudTrail.1	3.1	CloudTrail.1
ASR-EnableEncryption CloudTrail 應該啟用靜態加密	CloudTrail.2	2.7	CloudTrail.1	3.7	CloudTrail.2	3.5	CloudTrail.2
ASR-EnableLogFileValidation 確保 CloudTrail 日誌檔案驗證已啟用	CloudTrail.4	2.2	CloudTrail.3	3.2	CloudTrail.4		CloudTrail.4

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableCloudTrailToCloudWatchLogging 確保 CloudTrail 追蹤與 Amazon CloudWatch Logs 整合	CloudTrail.5	2.4	CloudTrail.4	3.4	CloudTrail.5		CloudTrail.5
ASR-ConfigureS3BucketLogging 確保 CloudTrail S3 儲存貯體已啟用 S3 儲存貯體存取日誌記錄		2.6		3.6		3.4	CloudTrail.7

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
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
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	EC2.1		EC2.1		EC2.1		EC2.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-RemoveVPCDefaultSecurityGroupRules VPC 預設安全群組應禁止傳入和傳出流量	EC2.2	4.3	EC2.2	5.3	EC2.2	5.4	EC2.2
ASR EnableVPCFlowLogs 應在所有 VPC 中啟用 VPCs 流程記錄	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-EnableEbsEncryptionByDefault 應啟用 EBS 預設加密	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-RevokeUnrotatedKeys 使用者存取金鑰應每 90 天或更短時間輪換一次	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
ASR-SetIAMPasswordPolicy 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，則應關閉使用者登入資料	IAM.8	1.3	IAM.7		IAM.8		IAM .8

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-RevokeUnusedIAMUserCredentials 如果未在 45 天內使用，則應關閉使用者登入資料				1.12		1.12	IAM.22
ASR-RemoveLambdaPublicAccess Lambda 函數應該禁止公開存取	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshotPrivate RDS 快照應禁止公開存取	RDS.1		RDS.1		RDS.1		RDS.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-DisablePublicAccessToRDSInstance RDS 資料庫執行個體應禁止公開存取	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2
ASR-EncryptRDSSnapshot RDS 叢集快照和資料庫快照應靜態加密	RDS.4				RDS.4		RDS.4
ASR-EnableMultiAZOnRDSInstance RDS 資料庫執行個體應該設定多個可用區域	RDS.5				RDS.5		RDS.5

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 應啟用 RDS 自動次要版本升級	RDS.13				RDS.13	2.3.2	RDS.13

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift 應該已啟用主要版本的自動升級	Redshift.6				Redshift.6		Redshift.6
ASR-ConfigureS3PublicAccessBlock 應啟用 S3 封鎖公開存取設定	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-SetSSLBucketPolicy S3 儲存貯體應要求請求使用 SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3BlockDenylist 應限制授予儲存貯體政策中其他 AWS 帳戶的 Amazon S3 許可	S3.6				S3.6		S3.6
S3 封鎖公開存取設定應在儲存貯體層級啟用	S3.8				S3.8		S3.8

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 CloudTrail S3 儲存貯體上啟用 S3 儲存貯體存取記錄		2.6					CloudTrail.7

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableKeyRotation 確保已啟用客戶建立CMKs輪換		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4
ASR-CreateLogMetricFilterAndAlarm 確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示		3.1		4.1			Cloudwatch.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保沒有 MFA 的 AWS 管理主控台登入存在日誌指標篩選條件和警示		3.2		4.2			Cloudwatch.2
ASR-CreateLogMetricFilterAndAlarm 確保存在用於「根」使用者的日誌指標篩選條件和警示		3.3	CW.1	4.3			Cloudwatch.3

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-CreateLogMetricFilterAndAlarm 確保 AWS 管理主控台身分驗證失敗存在日誌指標篩選條件和警示		3.6		4.6			Cloudwatch.6
ASR-CreateLogMetricFilterAndAlarm 確保停用或排定刪除客戶建立的 CMK 存在日誌指標篩選條件和警示		3.7		4.7			Cloudwatch.7

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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) 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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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	EC2.5		EC2.13		EC2.13

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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	CloudFormation.1				CloudFormation.1		CloudFormation.1
ASR-CreateIAMSupportRole		1.20		1.17		1.17	IAM.18

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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	CloudTrail.4	2.2	CloudTrail.3	3.2			CloudTrail.4
ASR-EnableEncryptionForSNSTopic	SNS.1				SNS.1		SNS.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableDeliveryStatusLoggingForSNSTopic 應針對傳送至主題的通知訊息啟用傳遞狀態的記錄	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionForSQSQueue	SQS.1				SQS.1		SQS.1
ASR-MakeRDSSnapshotPrivate RDS 快照應為私有	RDS.1		RDS.1				RDS.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-BlockSSMDocumentPublicAccess SSM 文件不應公開	SSM.4				SSM.4		SSM.4
ASR-EnableCloudFrontDefaultRootObject CloudFront 分佈應該設定預設根物件	CloudFront.1				CloudFront.1		CloudFront.1
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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-RemoveCodeBuildPrivilegedMode CodeBuild 專案環境應具有記錄 AWS 組態	CodeBuild.5				CodeBuild.5		CodeBuild.5
ASR-TerminateEC2Instance 停止的 EC2 執行個體應該在指定的期間之後移除	EC2.4				EC2.4		EC2.4

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnablIMDSV2OInstance 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-RevokeUnauthorizedInboudRules 安全群組應僅允許授權連接埠不受限制的傳入流量	EC2.18				EC2.18		EC2.18
在此插入標題 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

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-DisableTGWAutcAcceptSharedAttachments Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求	EC2.23				EC2.23		EC2.23
ASR-EnablePrivateRepositoryScanning ECR 私有儲存庫應設定映像掃描	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty 應啟用	GuardDuty.1		GuardDuty.1		GuardDuty.1		GuardDuty.1

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-ConfigureS3BucketLogging 應啟用 S3 儲存貯體伺服器存取記錄	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications S3 儲存貯體應該啟用事件通知	S3.11				S3.11		S3.11
ASR-SetS3LifecyclePolicy S3 儲存貯體應已設定生命週期政策	S3.13				S3.13		S3.13

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableAutoSecretRotation Secrets Manager 秘密應該啟用自動輪換	SecretsManager.1				SecretsManager.1		SecretsManager.1
ASR-RemoveUnusedSecret 移除未使用的 Secrets Manager 秘密	SecretsManager.3				SecretsManager.3		SecretsManager.3
ASR-UpdateSecretRotationPeriod Secrets Manager 秘密應該在指定的天數內輪換	SecretsManager.4				SecretsManager.4		SecretsManager.4

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableAPIGatewayCacheDataEncryption API Gateway REST API 快取資料應靜態加密					APIGateway.5		APIGateway.5
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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-AttachSSMPermissionsToEC2 Amazon EC2 執行個體應由 Systems Manager 管理	SSM.1		SSM.3				SSM.1
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 v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableAPIGatewayExecutionLogs	APIGateway.1						APIGateway.1
ASR-EnableMacie 應啟用 Amazon Macie	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging Athena 工作群組應該已啟用記錄	Athena.4						Athena.4

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnforceHTTPSFrALB Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS	ELB.1		ELB.1		ELB.1		ELB.1
ASR-LimitECSRootFilesystemAccess ECS 容器應僅限於對根檔案系統的唯讀存取	ECS.5				ECS.5		ECS.5

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableElastiCacheBackups ElastiCache (Redis OSS) 叢集應該啟用自動備份	ElastiCache.1				ElastiCache.1		ElastiCache.1
ASR-EnableElastiCacheVersionUpgrades ElastiCache 叢集應該啟用自動次要版本升級	ElastiCache.2				ElastiCache.2		ElastiCache.2

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache 複寫群組應該啟用自動容錯移轉	ElastiCache.3				ElastiCache.3		ElastiCache.3
ASR-ConfigureDynamoDBAutoScaling DynamoDB 資料表應隨著需求自動擴展容量	DynamoDB.1				DynamoDB.1		DynamoDB.1
ASR-TagDynamoDBTableResource DynamoDB 資料表應加上標籤							DynamoDB.5

描述	AWS FSBP	CIS v1.2.0	PCI 3.2.1 版	CIS 1.4.0 版	NIST	CIS 3.0.0 版	安全控制 ID
ASR-EnablDeletionProtection DynamoDB 資料表應該已啟用刪除保護					DynamoDB.6		DynamoDB.6

新增新的修補

您可以手動新增修補，方法是更新適當的手冊檔案，或以程式設計方式將解決方案延伸到 CDK 建構模組，視您偏好的工作流程而定。

> **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 ASR 和/或 SO0111，以便輕鬆找到和識別它們。

手動工作流程概觀

AWS Runbook 上的自動化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 ASR 支援的標準。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 ASR 支援的版本和調查結果資料中的版本。

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 (IAM)。
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（多個）中建立 Runbook

1. 登入 AWS Systems Manager 主控台並取得問題清單 JSON 的範例。
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. 管理員帳戶中的 AWS Step Functions 將執行您的 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 (IAM)

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，可從 AWS Security Hub 中的 ASR 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」）修復是 AWS Security Hub 收到調查結果後立即執行修復。使用此選項之前，請仔細考慮風險。

1. 檢視 CloudWatch Events 中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`值以符合問題清單 JSON `GeneratorId`中的 。
4. 儲存並啟用規則。

CDK 工作流程概觀

總而言之，ASR 儲存庫中的下列檔案將會修改或新增。在此範例中，ElastiCache.2 的新修補已新增至 SC 和 AFSBP 手冊。

> **Note**
>
> 所有新的修補都應新增至 SC 手冊，因為它會合併 ASR 中可用的所有修補。如果您只打算部署一組特定的手冊（例如 AFSBP)，則除了 SC 手冊之外，您還可以：(1) 僅將修補新增至預期的手冊 (s)，或 (2) 將修補新增至對應 Security Hub Standard 中存在的所有手冊。建議使用第二個選項來提高彈性。

在此範例中，ElastiCache.2 包含在下列 Security Hub 標準中：

- AFSBP
- NIST.800-53.r5 SI-2
- NIST.800-53.r5 SI-2(2)
- NIST.800-53.r5 SI-2(4)
- NIST.800-53.r5 SI-2(5)
- PCI DSS 4.0.1/6.3.3 版

由於 ASR 預設只會實作 AFSBP 和 NIST.800-53 的手冊，因此除了 SC 之外，我們會將此新修補新增至這些手冊。

Modify (修改)

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/【standard name】_remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/【standard name】_remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_remediations.ts
- source/test/regex_registry.ts

Add

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

> **Note**
>
> 為 Runbook 選擇的名稱可以是任何字串，只要它與所做的其餘變更一致。

- source/playbooks/NIST80053/ssmdocs/NIST80053_ElastiCache.2.ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ElastiCache.2.yaml

開發步驟

1. 建立修復 Runbook。
2. 建立 Control Runbook。
3. 將每個 Control Runbook 與 Playbook 整合。
4. 建立修復 IAM 角色和整合修復 Runbook
5. 更新單位測試

步驟 1：建立修復 Runbook

這是用於修復資源的 SSM 文件。它必須包含 `AutomationAssumeRole` 參數，這是具有執行修復許可的 IAM 角色。建立新的修復 Runbook 時，請檢視現有的 檔案`source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml`做為參考。

所有新的 Runbook 都應新增至 `source/remediation_runbooks/`目錄。

步驟 2：建立控制 Runbook

控制 Runbook 是手冊特定的 Runbook，可從指定的標準剖析調查結果資料，並執行適當的修復 Runbook。由於我們會將 ElastiCache.2 修復新增至 SC、AFSBP 和 NIST80053 手冊，因此我們必須為每個手冊建立新的控制執行手冊。系統會建立下列檔案：

- source/playbooks/SC/ssmdocs/SC_ElastiCache.2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ElastiCache.2.ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ElastiCache.2.yaml

Example

這些檔案的命名很重要，且必須遵循格式 <PLAYBOOK_NAME>_<CONTROL.ID>.ts/yaml

ASR 中的某些手冊支援 TypeScript 中的 IaC 控制 Runbook，而其他手冊必須以原始 YAML 撰寫。參考個別手冊中現有的修補做為範例。在此範例中，我們將介紹使用 IaC 的 SC 手冊。

在 SC 手冊中，您的新控制項 Runbook 應該匯出擴展 ControlRunbookDocument 並符合修復 Runbook 名稱的類別。請查看以下範例：

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

- `securityControlId` 是您新增之修復的控制項 ID，因為它在 Security Hub 的合併控制項檢視中定義。
- `remediationName` 是您為修復 Runbook 選擇的名稱。
- `scope` 是您要修復的資源範圍，指出它存在於全域還是特定區域中。
- `resourceIdRegex` 是用來擷取您要做為參數傳遞至修復 Runbook 之資源 ID 的 regex。僅應擷取一個群組，所有其他群組應為非擷取。如果您想要傳遞整個 ARN，請省略此欄位。
- `resourceIdName` 是您想要為使用 擷取的資源 ID 設定的名稱`resourceIdRegex`，這應與修復 Runbook 中的資源 ID 參數名稱相符。

- updateDescription 是一旦修補成功，您想要指派給 Security Hub 中調查結果的「備註」區段的字串。

您也必須匯出名為 的函數createControlRunbook，該函數會傳回您類別的新執行個體。對於 ElastiCache.2,如下所示：

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

其中 controlId 是與您正在操作的手冊相關聯的安全標準中定義的控制 ID。

如果 Security Hub 控制項具有您要傳遞至修復 Runbook 的參數，您可以透過將覆寫新增至下列方法來傳遞這些參數： - getExtraSteps： 為 Security Hub 中針對控制項實作的每個參數定義預設值

> **Note**
>
> 來自 Security Hub 的每個參數都必須指定預設值

- getInputParamsStepOutput：定義控制 Runbook 的 GetInputParams 步驟的輸出
- 每個輸出都有 name、 outputType和 selector。selector 應該是getExtraSteps方法覆寫中使用的相同選擇器。
- getRemediationParams：定義傳遞至修復 Runbook 的參數，從 GetInputParams 步驟輸出擷取。

若要檢視範例，請導覽至 source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts 檔案。

步驟 3：將每個控制 Runbook 與 Playbook 整合

對於在上一個步驟中建立的每個控制項 Runbook，您現在必須將其與相關聯程序手冊中的基礎設施定義整合。請遵循每個控制 Runbook 的下列步驟。

> **Important**
>
> 如果您使用原始 YAML 而非 typescript IaC 建立控制項 Runbook，請跳到下一節。

在*/<playbook_name>*/control_runbooks-construct.ts匯入新建立的控制 Runbook 檔案中，如下所示：

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

接著，前往 的 陣列

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

並將對應控制項 ID （手冊特定）的新項目新增至您建立createControlRunbook的方法：

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

將手冊特定的控制項 ID 新增至 中的修復清單， *<playbook_name>*_remediations.ts如下所示：

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

versionAdded 欄位應該是解決方案的最新版本。如果新增修復違反範本大小限制，請增加versionAdded。您可以調整 中每個手冊成員堆疊中包含的修補數量solution_env.sh。

步驟 4：建立修補 IAM 角色並整合修補 Runbook

每個修復都有自己的 IAM 角色，具有執行修復 Runbook 所需的自訂許可。此外，需要調用RunbookFactory.createRemediationRunbook方法，才能將您在步驟 1 中建立的修補 Runbook 新增至解決方案的 CloudFormation 範本。

在 中remediation-runook-stack.ts，每個修復在 RemediationRunbookStack類別中都有自己的程式碼區塊。下列程式碼區塊顯示為 ElastiCache.2 修復建立新的 IAM 角色和修復 Runbook 整合：

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

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

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

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

步驟 5：更新單位測試

建議您在新增修補之後更新並執行單元測試。

首先，您必須將任何新的規則表達式（尚未新增）新增至 `source/test/regex_registry.ts` 檔案。此檔案會對解決方案 Runbook 中包含的每個新規則表達式強制執行測試。以 `addElastiCacheClusterTestCases`函數為例，用於測試 ElastiCache 修復中使用的規則表達式。

最後，您將需要更新每個堆疊的快照。快照是版本控制的 CloudFormation 範本定義，用於追蹤對 ASR 基礎設施所做的變更。您可以從 `deployment`目錄執行下列命令來更新這些快照檔案：

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

現在您已準備好部署新的修補！導覽至下面的建置和部署區段，以取得使用新變更建置和部署解決方案的指示。

新增手冊

從 GitHub 儲存庫下載 AWS 解決方案手冊上的自動化安全回應和部署原始碼。

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 GitHub 中的 README.md 檔案。

AWS Systems Manager 參數存放區

AWS 上的自動化安全回應會使用 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	值	使用
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	用於加密 FSBP 修復資料的 AWS KMS 金鑰	在修復過程中加密客戶資料，例如 CloudTrail 日誌
`/Solutions/SO0111/CMK_ARN`	ASR 用來加密資料的 AWS KMS 金鑰	解決方案資料的加密
`/Solutions/SO0111/SNS_Topic_ARN`	解決方案的 Amazon SNS 主題 ARN	修補事件的通知
`/Solutions/SO0111/SNS_Topic_Config.1`	AWS Config 更新的 SNS 主題	Config.1 修復
`/Solutions/SO0111/sendAnonymousMetrics`	`Yes`	匿名指標集合
`/Solutions/SO0111/version`	解決方案版本	
`/Solutions/SO0111/<security`	`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

名稱	值	使用
standard long name/*<version>* /status		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

AWS 上的自動化安全回應會建立 Amazon SNS 主題 SO0111-ASR_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 [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

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

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

這是完成訊息。它表示修復已完成，沒有錯誤；不過，成功修復的最終測試是 AWS Config 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. 將您的政策新增至 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 警示

此解決方案會建立 Amazon SNS 主題 `SO0111-ASR_Alarm_Topic`。本主題用於發佈警示警示。

任何進入 ALARM 狀態的警示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 調查結果啟動 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 AWS Config 或 Security Hub 為此規則產生的調查結果中找到。
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/【.replaceable】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"

}
```

1. RunbookName 是必要欄位，將是修復此 Config 規則時執行的 Runbook。RunbookRole 是協調器在執行此角色時將擔任的角色。這不是必要欄位，如果遺失，協調器將預設為使用帳戶的成員角色。
2. 設定完成後，您可以使用 Security Hub 上的「Remediate with ASR」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 AWS 的選項。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，會收集下列資訊並傳送至 AWS：

- 解決方案 ID - AWS 解決方案識別符
- 唯一 ID (UUID) - 為每個 AWS Security Hub 回應和修復部署隨機產生的唯一識別符
- 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
- 解決方案組態 - 在初始啟動期間開啟的功能和設定的參數
- 狀態 - 部署狀態（已通過或失敗的解決方案）或（已通過或失敗的修補）
- 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 擁有透過此問卷收集的資料。資料收集受 AWS 隱私權聲明約束。若要選擇退出此功能，請先完成下列步驟，再啟動 AWS CloudFormation 範本。

1. 將 AWS CloudFormation 範本下載到您的本機硬碟。
2. 使用文字編輯器開啟 AWS CloudFormation 範本。
3. 從下列位置修改 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. 在建立堆疊頁面指定範本區段中，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，並遵循本指南自動化部署區段中啟動堆疊的步驟。

相關資源

- 使用 AWS Security Hub 自動化回應和修復
- 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 (PCI DSS)
- 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 Granat
- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky

- Josh Moss
- Ryan Garay
- Thiemo Belmega
- Mykhailo Markhain

修訂

發佈日期：2020 年 8 月 (上次更新日期：2025 年 1 月)

請造訪 GitHub 儲存庫中的 CHANGELOG.md，以追蹤版本特定的改進和修正。

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，這些產品和實務可能會有所變更，恕不另行通知，且 (c) 不會從 AWS 及其附屬公司、供應商或授權方建立任何承諾或保證。AWS 產品或服務「原樣」提供，不做任何明示或暗示的保證、表示或條件。AWS 對其客戶的責任和義務由 AWS 協議控制，本文件不屬於 AWS 與其客戶之間的任何協議，也不會對其進行修改。

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。