AWS 安全參考架構 (AWS SRA) – 核心架構

AWS 方案指引

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: AWS 安全參考架構 (AWS SRA) – 核心架構

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介 1
關於 AWS SRA 程式庫 3
AWS SRA 的值 5
  如何使用 AWS SRA 5
  AWS SRA 的關鍵實作準則 7
安全基礎 9
  安全功能 10
  安全設計原則 10
  如何搭配 AWS CAF 和 AWS Well-Architected Framework 使用 AWS SRA 11
SRA 建置區塊 – AWS Organizations、帳戶和護欄 12
  使用 AWS Organizations 確保安全 12
  管理帳戶、受信任存取和委派管理員 15
  專用帳戶結構 16
  AWS AWS SRA 的組織和帳戶結構 17
  在整個 AWS 組織中套用安全服務 20
    全組織或多個帳戶 22
    AWS 帳戶 23
    虛擬網路、運算和內容交付 23
    委託人和資源 24
AWS 安全參考架構 28
  組織管理帳戶 30
    服務控制政策 31
    資源控制政策 32
    宣告式政策 32
    集中式根存取 33
    IAM Identity Center 34
    IAM 存取顧問 35
    AWS Systems Manager 35
    AWS Control Tower 36
    AWS Artifact 36
    分散式和集中式安全服務護欄 37
  Security OU – 安全工具帳戶 38
    安全服務的委派管理員 39
    集中式根存取 39

AWS CloudTrail 40
AWS Security Hub CSPM 41
AWS Security Hub 43
Amazon GuardDuty 45
AWS Config 46
Amazon Security Lake 48
Amazon Macie 49
IAM Access Analyzer 50
AWS Firewall Manager 53
Amazon EventBridge 54
Amazon Detective 54
AWS Audit Manager 55
AWS Artifact 56
AWS KMS 57
AWS 私有 CA 58
Amazon Inspector 59
AWS 安全事件應變 61
在所有 中部署常見的安全服務 AWS 帳戶 62
安全 OU – Log Archive 帳戶 63
日誌類型 64
Amazon S3 作為中央日誌存放區 64
Amazon Security Lake 65
基礎設施 OU – 網路帳戶 66
網路架構 68
傳入 (輸入) VPC 68
傳出 (輸出) VPC 69
檢查 VPC 69
AWS Network Firewall 69
網路存取分析器 70
AWS RAM 71
AWS Verified Access 72
Amazon VPC Lattice 73
邊緣安全 73
Amazon CloudFront 74
AWS WAF 75
AWS Shield 76

AWS Certificate Manager (ACM) 77
Amazon Route 53 78
Infrastructure OU – 共用服務帳戶 79
AWS Systems Manager 79
AWS Managed Microsoft AD 80
IAM Identity Center 81
工作負載 OU – 應用程式帳戶 82
應用程式 VPC 84
VPC 端點 84
Amazon EC2 85
AWS Nitro Enclaves 85
Application Load Balancer 86
AWS 私有 CA 87
Amazon Inspector 87
AWS Systems Manager 88
Amazon Aurora 89
Amazon S3 89
AWS KMS 89
AWS CloudHSM 90
AWS Secrets Manager 90
Amazon Cognito 92
Amazon Verified Permissions 92
分層防禦 93
安全 AI/ML 95
適當的安全性 95
建置您的安全架構 – 分階段方法 98
階段 1：建置您的 OU 和帳戶結構 98
階段 2：實作強大的身分基礎 99
階段 3：維持可追蹤性 100
階段 4：在所有層套用安全性 101
階段 5：保護傳輸中和靜態的資料 102
階段 6：準備安全事件 102
AWS SRA 最佳實務檢查清單 105
AWS Organizations 105
AWS CloudTrail 106
AWS Security Hub CSPM 106

AWS Config 107
Amazon GuardDuty 107
IAM 108
IAM Access Analyzer 108
Amazon Detective 109
AWS Firewall Manager 109
Amazon Inspector 109
Amazon Macie 110
Amazon Security Lake 110
AWS WAF 111
AWS Shield Advanced 111
AWS 安全事件回應 112
AWS Audit Manager 112
IAM 資源 113
AWS SRA 範例的程式碼儲存庫 117
貢獻者 120
附錄： AWS 安全性、身分和合規服務 122
文件歷史紀錄 124
..... cxxix

AWS 安全參考架構 (AWS SRA) – 核心架構

Global Services 安全團隊、Amazon Web Services (參與者)

2025 年 12 月 (文件歷史記錄)

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

Amazon Web Services (AWS) 安全參考架構 (AWS SRA) 是在多帳戶環境中部署 AWS 安全服務完整補充的完整準則。使用它來協助設計、實作和管理 AWS 安全服務，使其符合 AWS 建議的實務。這些建議是以包含 AWS 安全服務的單頁架構為基礎建置，這些架構如何協助實現安全目標、在其中部署和管理它們的最佳方式 AWS 帳戶，以及它們如何與其他安全服務互動。此整體架構指引補充了詳細的服務特定建議，例如在AWS 安全文件網站上找到的建議。

架構和隨附的建議是以我們對 AWS 企業客戶的集體體驗為基礎。本文件是參考，這是一組使用 AWS 服務 保護特定環境的全方位指引，而 AWS SRA 程式碼儲存庫中的解決方案模式是專為本參考中說明的特定架構所設計。每個客戶都有不同的需求。因此，您 AWS 環境的設計可能與此處提供的範例不同。您將需要修改和量身打造這些建議，以符合您的個別環境和安全需求。 在適當情況下，在整個文件中，我們建議常用替代案例的選項。

AWS SRA 是一組活體指引，會根據新服務和功能版本、客戶意見回饋以及不斷變化的威脅態勢定期更新。每次更新都會包含修訂日期和相關聯的變更日誌。

雖然我們倚賴單頁圖表作為基礎，但架構比單一區塊圖表更深，而且必須建立在結構良好的基礎基礎上。您可以透過兩種方式使用此文件：做為敘述或參考。主題會組織為故事，因此您可以從開頭 （基礎安全指導） 到結尾 （您可以實作的程式碼範例討論） 閱讀主題。或者，您可以導覽文件以專注於與您的需求最相關的安全原則、服務、帳戶類型、指導和範例。

本文件分為以下章節和附錄：

- 關於 AWS SRA 程式庫提供 AWS SRA 出版物集合中包含的技術指引和程式碼概觀。
- AWS SRA 的值 討論建置 AWS SRA 的動機、說明如何使用它來協助改善安全性，以及列出關鍵要點。
- 安全基礎會檢閱 AWS 雲端採用架構 (AWS CAF)、 AWS Well-Architected 架構和 AWS 共同責任模型，並反白顯示與 AWS SRA 特別相關的元素。
- AWS Organizations、 帳戶和 IAM 護欄 介紹 AWS Organizations 服務、討論基本安全功能和護欄，並提供建議的多帳戶策略概觀。

- AWS 安全參考架構是單頁架構圖，顯示功能 AWS 帳戶，以及一般可用的安全服務和功能。
- 安全 AI/ML 說明不同的 如何在背景 AWS 服務 中使用人工智慧和機器學習 (AI/ML)，以協助您實現特定的安全目標。您可以在設計 AWS 服務 中包含這些項目，以利用進階安全功能。
- 建置您的安全架構 – 分階段方法根據 SRA 提供的 AWS 參考，提供如何以六個反覆階段建置自己的安全架構的指導。
- AWS SRA 最佳實務檢查清單會將本指南中討論的建議分割成檢查清單，供您在建置安全架構版本時遵循。
- IAM 資源提供對安全架構至關重要的 AWS Identity and Access Management (IAM) 指引的摘要和指標集。
- AWS SRA 程式碼儲存庫範例提供相關 GitHub 儲存庫的概觀，可協助開發人員和工程師部署本文件中呈現的一些指引和架構模式。您可以使用 AWS CloudFormation 或 HashiCorp 的 Terraform 部署範例。它們同時支援 AWS Control Tower 和非AWS Control Tower 環境。

附錄包含個別 AWS 安全性、身分和合規服務的清單，並提供每個服務的詳細資訊連結。文件歷史記錄區段提供用於追蹤本文件版本的變更日誌。您也可以訂閱 RSS 摘要以取得變更通知。

關於 AWS SRA 程式庫

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

本指南是程式庫的一部分，提供架構藍圖和技術指導，用於 設計和建置安全架構 AWS。程式庫包含實作程式碼 (AWS SRA 程式碼庫)、驗證工具 (SRA Verify)，以及涵蓋核心架構和深入探索架構的兩個互補類別指南。

AWS SRA – 核心架構 （ 本指南 ）

本指南代表建議 AWS 安全架構的基礎。這是適用於所有組織的起點，無論其產業、應用程式類型或任何其他考量。此基礎可協助您在 上建置強大且可擴展的架構， AWS 並協助建立強大的 AWS 多帳戶安全基準，以隨著業務成長安全地擴展。

AWS SRA – 深入探討架構

AWS SRA – 核心架構指南搭配其他出版物，提供符合特定安全功能、應用程式類型和合規或法規要求的架構模式。這些模式會擴展核心架構，並應與 AWS SRA – 核心架構指南搭配使用。

下列指南提供符合特定安全功能的架構模式：

- AWS SRA – 身分管理 提供如何實作可擴展、強大且集中式身分和存取管理解決方案的指引 AWS。
- AWS SRA – 周邊安全性討論架構模式 AWS 服務 ，以及在中央帳戶或個別帳戶中實作邊緣安全性。
- AWS SRA – 網路鑑識描述如何將 AWS 鑑識帳戶設定為開發組織鑑識功能的起點，並協助改善您的安全事件回應 (IR) 準備度。

下列指南提供特定應用程式類型的架構模式。在建置基準安全架構之後，您可能想要專注於這些項目：

- AWS SRA – AI 安全性提供安全架構建議，以設計和建置應用程式，透過使用生成式 AI 服務來整合生成式 AI AWS 功能。
- AWS SRA – IoT 提供設計和建置 IoT 應用程式的安全架構建議 AWS。

此外，以下指南說明符合特定合規或法規架構的架構模式：

- AWS 隱私權參考架構 (AWS PRA) 為處理個人資料的應用程式提供安全架構，且必須支援廣泛的隱私權合規要求，例如一般資料保護法規 (GDPR)、加州消費者隱私權法 (CCPA) 或巴西一般資料保護法 (LGPD)。 AWS PRA 提供一組專門針對其中隱私權控制設計和組態的指導方針 AWS 服務。

我們建議您從 AWS SRA – 核心架構指南開始，以了解基礎架構，然後參閱補充指南，以利用進階功能和實作。如需此內容集的詳細資訊，請參閱AWS 安全參考架構。

架構圖

若要根據您的業務需求自訂 AWS SRA 程式庫中的參考架構圖，您可以下載下列 .zip 檔案並解壓縮其內容。

下載圖表來源檔案 (Microsoft PowerPoint 格式)

AWS SRA 的值

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

AWS 有一組大型（和不斷成長）的安全和安全相關服務。客戶對我們的服務文件、部落格文章、教學課程、高峰會和會議提供的詳細資訊表示感謝。他們還告訴我們，他們想要更好地了解大局，並獲得 AWS 安全服務的策略觀點。當我們與客戶合作以更深入了解他們需要什麼時，會出現三個優先順序：

- 客戶需要更多資訊和建議模式，以了解如何全面部署、設定和操作 AWS 安全服務。服務應部署和管理於哪些帳戶和哪些安全目標？ 是否有一個安全帳戶，其中所有或大多數服務都應該操作？ 選擇位置（組織單位或 AWS 帳戶) 如何通知安全目標？ 客戶應該注意哪些權衡（設計考量）？
- 客戶有興趣查看邏輯組織許多 AWS 安全服務的不同觀點。除了每個服務的主要功能（例如身分服務或記錄服務）之外，這些替代觀點還協助客戶規劃、設計和實作其安全架構。本文件稍後共用的範例會根據符合您 AWS 環境建議結構的保護層，將服務分組。
- 客戶正在尋找指引和範例，以最有效的方式整合安全服務。例如，他們應該如何最好地與其他 服務協調和連線 AWS Config ，以便在自動化稽核和監控管道中繁重工作？ 客戶請求指導，了解每個 AWS 安全服務如何依賴或支援其他安全服務。

我們處理 AWS SRA 中的每個項目。清單中的第一個優先順序（實物移動的位置）是主架構圖和本文件中隨附討論的重點。我們提供建議的 AWS Organizations 架構和account-by-account描述，說明 服務的目的地。若要開始使用清單中的第二優先順序（如何考慮整組安全服務），請閱讀章節：將安全服務套用至整個 AWS 組織。本節說明根據 AWS 組織中元素結構將安全服務分組的方法。此外，這些相同的想法也反映在應用程式帳戶的討論中，重點介紹了如何操作安全服務以專注於帳戶的某些層：Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Virtual Private Cloud (Amazon VPC) 網路，以及更廣泛的帳戶。最後，第三優先順序（服務整合）會反映在整個指引中，尤其是在 AWS SRA 程式庫深入指南中的個別服務討論，以及 AWS SRA 程式碼儲存庫中的程式碼。

如何使用 AWS SRA

視您在雲端採用旅程中的位置而定，有多種不同的 SRA AWS 使用方式。以下是從 AWS SRA 資產取得最多洞見的方法清單（架構圖、書面指引和程式碼範例）。

- 為您自己的安全架構定義目標狀態。

無論您是剛開始 AWS 雲端 旅程，或是設定您的第一組帳戶，或是規劃強化已建立 AWS 的環境，AWS SRA 都是開始建置安全架構的地方。從帳戶結構和安全服務的完整基礎開始，然後根據您的特定技術堆疊、技能、安全目標和合規要求進行調整。如果您知道您要建置並啟動更多工作負載，您可以取得自訂版本的 AWS SRA，並將其用作組織安全參考架構的基礎。若要了解如何達到 AWS SRA 所述的目標狀態，請參閱建置安全架構 – 分階段方法一節。

- 檢閱 （和修訂） 您已實作的設計和功能。

  如果您已經有安全設計和實作，建議您花一些時間來比較與 AWS SRA 的關聯。 AWS SRA 的設計是全方位的，並提供診斷基準來檢閱您自己的安全性。如果您的安全設計與 AWS SRA 保持一致，您可以更有信心在使用 時遵循最佳實務 AWS 服務。如果您的安全設計與 SRA 中的指引不同或甚至不同，這不一定是您做錯事的 AWS 跡象。相反地，此觀察可讓您有機會檢閱您的決策程序。您可能會偏離 AWS SRA 最佳實務的合法商業和技術原因。您的特定合規、法規或組織安全需求可能需要特定的服務組態。或者，您可能會有來自 AWS Partner Network 或您所建置和管理之自訂應用程式的產品功能偏好設定 AWS 服務，而不是使用 。有時候，在此檢閱期間，您可能會發現您先前的決策是根據不再適用的舊技術、 AWS 功能或業務限制條件所做出。這是檢閱、排定任何更新的優先順序，並將其新增至您工程待處理項目適當位置的好機會。無論您在根據 AWS SRA 評估安全架構時發現什麼，都會發現記錄該分析很有價值。擁有決策及其理由的歷史記錄，有助於通知並排定未來決策的優先順序。

- 引導您實作自己的安全架構。

  AWS SRA 基礎設施即程式碼 (IaC) 模組提供快速、可靠的方法來開始建置和實作您的安全架構。這些模組在程式碼儲存庫區段和公有 GitHub 儲存庫中有更深入的說明。它們不僅讓工程師能夠根據 AWS SRA 指南中模式的高品質範例建置，還包含建議的安全控制，例如 IAM 密碼政策、Amazon Simple Storage Service (Amazon S3) 封鎖帳戶公開存取、Amazon EC2 預設 Amazon Elastic Block Store (Amazon EBS) 加密，以及與 的整合， AWS Control Tower 以便在新 AWS 帳戶 加入或取消委任時套用或移除控制項。

- 進一步了解 AWS 安全服務和功能。

  AWS SRA 中的指導和討論包括重要功能，以及個別 AWS 安全和安全相關服務的部署和管理考量。AWS SRA 的一項功能是提供安全 AWS 服務廣度的高階介紹，以及它們如何在多帳戶環境中一起運作。這補充了深入了解在其他來源中找到的每個服務的功能和組態。其中一個範例是討論 AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) 如何從各種 AWS 服務、 AWS Partner 產品，甚至是您自己的應用程式擷取安全調查結果。

- 推動組織治理和安全責任的討論。

設計和實作任何安全架構或策略的一個重要元素是了解組織中的哪些人員具有與安全相關的責任。例如，彙整和監控安全調查結果的問題，與負責該活動團隊的問題有關。整個組織的所有調查結果是否由需要存取專用安全工具帳戶的中央團隊監控？ 或者，個別應用程式團隊 （或業務單位） 是否負責特定監控活動，因此需要存取特定提醒和監控工具？ 另一個範例是，如果您的組織有一個集中管理所有加密金鑰的群組，這會影響誰具有建立 AWS Key Management Service (AWS KMS) 金鑰的許可，以及這些金鑰將管理的帳戶。了解組織的特性 – 各種團隊和責任 – 將協助您量身打造最適合需求的 AWS SRA。相反地，有時安全架構的討論會成為討論現有組織責任和考慮潛在變更的動力。AWS 建議一項分散式決策程序，其中工作負載團隊負責根據其工作負載函數和需求定義安全控制。集中式安全與控管團隊的目標是建置系統，讓工作負載擁有者能夠做出明智的決策，並讓各方都能了解組態、問題清單和事件。 AWS SRA 可以是識別和通知這些討論的工具。

AWS SRA 的關鍵實作準則

以下是 AWS SRA 的八個關鍵要點，供您在設計和實作安全性時謹記。

- AWS Organizations 和適當的多帳戶策略是您安全架構的必要元素。適當地分隔工作負載、團隊和函數，為職責分離和defense-in-depth策略提供了基礎。本指南在稍後的章節中進一步介紹了這一點。
- Defense-in-depth是為您的組織選擇安全控制的重要設計考量。它可協助您在 AWS Organizations 結構的不同層注入適當的安全控制，這有助於將問題的影響降至最低：如果一個層存在問題，則存在隔離其他寶貴 IT 資源的控制。 AWS SRA 會示範 AWS 技術堆疊不同層的不同 AWS 服務 函數如何運作，以及結合使用這些服務如何協助您達成defense-in-depth。稍後章節 AWS 會進一步討論 的defense-in-depth概念，其中包含應用程式帳戶下顯示的設計範例。
- 跨多個 AWS 服務 和 功能使用各種安全建置區塊，以建置強大且具彈性的雲端基礎設施。根據您的特定需求量身打造 AWS SRA 時，不僅要考慮 AWS 服務 和 功能的主要函數 （例如，身分驗證、加密、監控、許可政策），還要考慮它們如何符合您架構的結構。本指南稍後的章節說明一些 服務如何在整個 AWS 組織中運作。其他服務在單一 帳戶中運作最佳，有些服務旨在授予或拒絕個別委託人的許可。考慮這兩個觀點，可協助您建置更靈活、分層的安全方法。
- 在可能的情況下 （如後續章節所述），請利用 AWS 服務 來部署在每個帳戶中 （分散而非集中），並建置一組一致的共用護欄，以協助保護您的工作負載免於誤用，並協助降低安全事件的影響。AWS SRA 使用 AWS Security Hub CSPM （集中調查結果監控和合規檢查）、Amazon GuardDuty （威脅偵測和異常偵測）、 AWS Config （資源監控和變更偵測）、IAM Access Analyzer （資源存取監控）、 AWS CloudTrail （在整個環境中記錄服務 API 活動） 和 Amazon Macie （資料分類） 作為 AWS 服務 要部署在每個 的基礎集合 AWS 帳戶。
- 使用 AWS Organizations受支援之 的委派管理功能，如本指南稍後委派管理一節所述。這可讓您將 AWS 成員帳戶註冊為受支援服務的管理員。委派的管理為企業內不同團隊提供彈性，以根據其

責任使用不同的帳戶，來管理 AWS 服務 整個環境。此外，使用委派管理員可協助您限制對 AWS Organizations 管理帳戶的存取和管理許可額外負荷。

- 在您的 AWS 組織中實作集中式監控、管理和控管。透過使用 AWS 服務 支援多帳戶 （有時是多區域） 彙總，以及委派的管理功能，您可以讓您的中央安全、網路和雲端工程團隊能夠廣泛地了解和控制適當的安全組態和資料收集。此外，資料可以提供給工作負載團隊，讓他們能夠在軟體開發生命週期 (SDLC) 的早期做出有效的安全決策。
- 使用 透過實作預先建置的安全控制 AWS Control Tower 來設定和控管您的多帳戶 AWS 環境，以引導您的安全參考架構建置。 AWS Control Tower 提供藍圖，以提供身分管理、帳戶聯合存取、集中式記錄，以及用於佈建其他帳戶的已定義工作流程。然後，您可以使用 Customizations for AWS Control Tower (CfCT) 解決方案，透過 AWS Control Tower 額外的安全控制、服務組態和控管來基準化 管理的帳戶，如 AWS SRA 程式碼儲存庫所示。帳戶工廠功能會根據核准的帳戶組態，自動佈建具有可設定範本的新帳戶，以標準化 AWS 組織內的帳戶。您也可以將其 AWS 帳戶 註冊到已受管理的組織單位 (OU)，將控管擴展到現有的個別 AWS Control Tower。
- AWS SRA 程式碼範例示範如何使用基礎設施做為程式碼 (IaC)，自動化 AWS SRA 指南中的模式實作。透過編纂模式，您可以將 IaC 視為組織中的其他應用程式，並在部署程式碼之前自動化測試。IaC 也透過在多個 （例如 SDLC 或區域特定） 環境中部署護欄，協助確保一致性和可重複性。SRA 程式碼範例可以部署在 AWS Organizations 多帳戶環境中，無論是否有 AWS Control Tower。此儲存庫中需要 的解決方案 AWS Control Tower 已在AWS Control Tower環境中使用 AWS CloudFormation和 Customizations for AWS Control Tower (CfCT) 部署和測試。不需要 的解決方案 AWS Control Tower 已在AWS Organizations環境中使用 進行測試AWS CloudFormation。如果您不使用 AWS Control Tower，則可以使用 AWS Organizations型部署解決方案。

安全基礎

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

AWS SRA 符合三個 AWS 安全基礎： AWS 雲端採用架構 (AWS CAF)、 AWS Well-Architected 和 AWS 共同責任模型。

AWS Professional Services 建立了 AWS CAF，以協助公司設計和遵循加速路徑以成功採用雲端。架構提供的指引和最佳實務可協助您在整個企業和 IT 生命週期中建置雲端運算的全方位方法。 AWS CAF 會將指引整理成六個重點領域，稱為觀點。每個觀點都涵蓋了功能相關利益相關者所擁有或管理的不同責任。一般而言，業務、人員和控管觀點著重於業務功能；而平台、安全性和營運觀點則著重於技術功能。

AWS CAF 的安全觀點可協助您建構整個業務中控制項的選擇和實作。遵循安全支柱中的目前 AWS 建議，可協助您滿足業務和法規要求。

AWS Well-Architected 可協助雲端架構師為其應用程式和工作負載建置安全、高效能、彈性且高效率的基礎設施。此架構以六大支柱為基礎：卓越營運、安全性、可靠性、效能效率、成本最佳化和永續性，並為客戶提供 AWS 一致的方法來評估架構，並實作可隨時間擴展的設計。我們相信，擁有 Well-Architected 工作負載可大幅提高企業成功的可能性。

Well-Architected Framework 安全支柱說明如何利用雲端技術來協助保護資料、系統和資產，以改善您的安全狀態。這將協助您遵循目前的 AWS 建議，滿足您的業務和法規要求。還有其他 Well-Architected Framework 重點領域，可為控管、無伺服器、AI/ML 和遊戲等特定領域提供更多內容。這些稱為 AWS Well-Architected 鏡頭。

安全與合規是 AWS 和 客戶之間的共同責任。此共用模型有助於減輕您的操作負擔，因為 會 AWS 操作、管理和控制從主機作業系統和虛擬化層到服務操作所在設施實體安全性的元件。例如，您負責管理訪客作業系統（包括更新和安全修補程式）、應用程式軟體、伺服器端資料加密、網路流量路由表，以及 AWS所提供安全群組防火牆的組態。對於 Amazon S3 和 Amazon DynamoDB 等抽象服務， 會 AWS 操作基礎設施層、作業系統和平台，而且您可以存取端點來存放和擷取資料。您負責管理資料（包括加密選項）、分類資產，以及使用 IAM 工具來套用適當的許可。此共用模型通常描述為 AWS 負責雲端的安全性（也就是保護執行 中提供之所有服務的基礎設施 AWS 雲端），而您需負責雲端的安全性（取決於您選取的 AWS 雲端 服務）。

在這些基礎文件提供的指引中，兩組概念與 AWS SRA 的設計和理解特別相關：安全功能和安全設計原則。

安全功能

AWS CAF 的安全觀點概述了九種功能，可協助您實現資料和雲端工作負載的機密性、完整性和可用性。

- 安全控管，以在整個組織 AWS 環境中開發和傳達安全角色、責任、政策、程序和程序。
- 安全保證可監控、評估、管理和改善安全與隱私權計劃的有效性。
- 用於大規模管理身分和許可的身分和存取管理。
- 用於了解和識別潛在安全錯誤組態、威脅或非預期行為的威脅偵測。
- 漏洞管理，以持續識別、分類、修復和緩解安全漏洞。
- 基礎設施保護，以協助驗證工作負載中的系統和服務是否受到保護。
- 資料保護，以維護資料的可見性和控制，以及如何在您的組織中存取和使用資料。
- 應用程式安全性，以協助在軟體開發過程中偵測和解決安全漏洞。
- 透過有效回應安全事件來減少潛在傷害的事件回應。

安全設計原則

Well-Architected Framework 的安全支柱會擷取一組七種設計原則，將特定安全區域轉換為可協助您強化工作負載安全性的實際指引。在安全功能架構整體安全策略的位置，這些 Well-Architected Framework 原則會說明您可以開始執行的操作。它們在此 AWS SRA 中被刻意反映，並包含下列項目：

- 實作強大的身分基礎 – 實作最低權限原則，並針對每次與 AWS 資源的互動，以適當的授權強制執行職責分離。集中進行身分管理，旨在消除對長期靜態憑證的倚賴。
- 啟用可追蹤性 – 即時監控、產生警示，以及稽核您環境的動作和變更。將日誌和指標收集與系統進行整合，以自動調查並採取動作。
- 在所有層級套用安全性 – 使用多個安全控制套用defense-in-depth方法。將多種類型的控制（例如預防性和偵測性控制）套用至所有層，包括網路邊緣、虛擬私有雲端 (VPC)、負載平衡、執行個體和運算服務、作業系統、應用程式組態和程式碼。
- 自動化安全最佳實務 – 自動化、以軟體為基礎的安全機制可改善您更快速且符合成本效益地安全地擴展的能力。建立安全架構，並實作在版本控制範本中定義為程式碼和管理的控制項。
- 保護傳輸中和靜態資料 – 將您的資料分類為敏感層級，並在適當時使用加密、字符化和存取控制等機制。

- 讓人員遠離資料 – 使用機制和工具來減少或消除直接存取或手動處理資料的需求。在處理敏感資料時，這降低了處理不當或修改以及人為錯誤的風險。
- 為安全事件做好準備 – 透過制定符合您組織需求的事件管理和調查政策和流程，為事件做好準備。執行失敗回應模擬和使用工具與自動化，以提高偵測、調查和復原的速度。

如何搭配 AWS CAF 和 AWS Well-Architected Framework 使用 AWS SRA

AWS CAF、 AWS Well-Architected Framework 和 AWS SRA 是互補的架構，可共同支援雲端遷移和現代化工作。

- AWS CAF 利用 AWS 經驗和最佳實務，協助您將雲端採用的價值與所需的業務成果保持一致。使用 AWS CAF 來識別轉型機會並排定優先順序、評估和改善雲端準備度，以及反覆發展轉型藍圖。
- AWS Well-Architected Framework 為符合業務成果的各種應用程式和工作負載提供建置安全、高效能、彈性和高效基礎設施 AWS 的建議。
- AWS SRA 可協助您了解如何以符合 AWS CAF 和 AWS Well-Architected Framework 建議的方式部署和管理安全服務。

例如， AWS CAF 安全觀點建議您評估如何集中管理人力資源身分及其身分驗證 AWS。根據此資訊，您可以決定為此目的使用新的或現有的公司身分提供者 (IdP) 解決方案，例如 Okta、Active Directory 或 Ping Identity。您遵循 AWS Well-Architected Framework 中的指引，並決定將您的 IdP 與 整合 AWS IAM Identity Center ，為您的員工提供可同步其群組成員資格和許可的單一登入體驗。您可以檢閱 AWS SRA 建議，在 AWS 組織的管理帳戶中啟用 IAM Identity Center，並透過安全操作團隊使用的安全工具帳戶來管理它。此範例說明 AWS CAF 如何協助您對所需的安全狀態做出初始決策、 AWS Well-Architected Framework 提供如何評估可用於實現該目標 AWS 服務 的 的指引，以及 AWS SRA 接著提供有關如何部署和管理所選安全服務的建議。

SRA 建置區塊 – AWS Organizations、帳戶和護欄

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

AWS 安全服務、其控制項和互動最適合在 AWS多帳戶策略和身分和存取管理護欄的基礎上使用。這些護欄可設定您實作最低權限、職責分離和隱私權的能力，並提供決策支援，包括需要哪些類型的控制、管理每個安全服務的位置，以及他們如何在 AWS SRA 中共用資料和許可。

為您的 AWS 資源 AWS 帳戶 提供安全、存取和計費界限，並讓您能夠實現資源獨立性和隔離。使用多個 在如何滿足安全需求方面 AWS 帳戶 扮演重要角色，如使用多個 AWS 帳戶帳戶整理環境的效益白皮書中所述。 AWS 例如，您可以根據函數、合規要求或常見的控制項集，將工作負載組織在組織單位 (OU) 內的個別帳戶和群組帳戶中，而不是鏡像企業的報告結構。請記住安全性和基礎設施，讓您的企業在工作負載成長時設定常見的防護機制。此方法可在工作負載之間提供強大的界限和控制。帳戶層級區隔結合 AWS Organizations，用於隔離生產環境與開發和測試環境，或在處理支付卡產業資料安全標準 (PCI DSS) 或健康保險流通與責任法案 (HIPAA) 等不同分類資料的工作負載之間提供強大的邏輯界限。雖然您可以使用單一帳戶開始 AWS 旅程，但 AWS 建議您隨著工作負載的大小和複雜性增加而設定多個帳戶。

許可可讓您指定 AWS 資源的存取權。將許可授予稱為主體 （ 使用者、群組和角色 ） 的 IAM 實體。根據預設，主體會從沒有許可開始。IAM 主體在授予許可 AWS 之前，都不能在 中執行任何操作，而且您可以設定護欄，這些護欄廣泛套用到整個 AWS 組織，或細分為主體、動作、資源和條件的個別組合。

使用 AWS Organizations 確保安全

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

AWS Organizations 隨著資源的成長和擴展， 可協助您集中管理和控管您的環境 AWS 。透過使用 AWS Organizations，您可以透過程式設計方式建立新的 AWS 帳戶、配置資源、分組帳戶來組織工作負載，以及將政策套用至帳戶或帳戶群組以進行控管。 AWS 組織會合併您的 ， AWS 帳戶 以便您以單一單位管理它們。它有一個管理帳戶以及零個或多個成員帳戶。大多數工作負載都位於成員帳戶中，但某些中央受管程序必須位於管理帳戶或指定為特定 委派管理員的帳戶 AWS 服務。您可以從中央位置提供工具和存取權，讓您的安全團隊代表 AWS 組織管理安全需求。您可以透過在 AWS 組織內共用

關鍵資源來減少資源重複。您可以將帳戶分組為 AWS 組織單位 (OUs)，根據工作負載的需求和用途來代表不同的環境。 AWS Organizations 也提供數種政策，可讓您將額外的安全控制集中套用至組織中的所有成員帳戶。本節著重於服務控制政策 SCPs)、資源控制政策 (RCPs) 和宣告政策。

透過 AWS Organizations，您可以使用 SCPs 和 RCPs 在 AWS 組織、OU 或帳戶層級套用許可護欄。SCPs 是套用於組織帳戶中主體的護欄，但管理帳戶除外 （這是不在此帳戶中執行工作負載的一個原因）。當您將 SCP 連接到 OU 時，SCP 會由該 OUs 下的子 OU 和帳戶繼承。SCPs不會授予任何許可。相反地，它們會指定組織、OU AWS 或帳戶中主體可用的許可上限。您仍然需要將身分型或資源型政策連接到 AWS 帳戶 中的主體或資源，以實際授予許可。例如，如果 SCP 拒絕存取所有 Amazon S3，則受 SCP 影響的委託人將無法存取 Amazon S3，即使透過 IAM 政策明確 授予存取權。如需如何評估 IAM 政策、SCPs 角色以及如何最終授予或拒絕存取的詳細資訊，請參閱 IAM 文件中的政策評估邏輯。

RCPs 是套用於組織帳戶中資源的護欄，無論資源是否屬於同一個組織。如同 SCPs，RCPs不會影響管理帳戶中的資源，也不會授予任何許可。當您將 RCP 連接到 OU 時，RCP 由 OUs 下的子 OU 和帳戶繼承。RCPs可讓您集中控制組織中資源的最大可用許可，並目前支援 的子集 AWS 服務。當您為 OUs 設計 SCPs 時，建議您使用 IAM 政策模擬器來評估變更。您也應該在 IAM 中檢閱服務上次存取的資料，並使用 AWS CloudTrail 記錄 API 層級的服務用量，以了解 SCP 變更的潛在影響。

SCPs和 RCPs是獨立的控制項。您可以選擇僅啟用 SCPs 或 RCPs，或根據您要強制執行的存取控制，同時使用兩種政策類型。例如，如果您想要防止組織的主體存取組織外部的資源，您可以使用 SCPs強制執行此控制。如果您想要限制或防止外部身分存取您的 資源，您可以使用 RCPs強制執行此控制。如需 RCPs和 SCPs 的詳細資訊和使用案例，請參閱 AWS Organizations 文件中的使用 SCPs RCPs。

您可以使用 AWS Organizations 宣告式政策，集中宣告和強制執行整個組織中指定 AWS 服務 所需的組態。例如，您可以封鎖對整個組織的 Amazon VPC 資源的公有網際網路存取。與 SCPs 和 RCPs 等授權政策不同，宣告政策會在 AWS 服務的控制平面中強制執行。授權政策會規範對 APIs存取，而宣告政策會直接在服務層級套用，以強制執行持久性意圖。 這些政策有助於確保 AWS 服務 始終維護 的基準組態，即使服務引入新功能或 APIs。將新帳戶新增至組織或建立新主體和資源時，也會維護基準組態。宣告政策可以套用至整個組織或特定 OUs 或帳戶。

每個 AWS 帳戶 都有單一根使用者，預設具有所有 AWS 資源的完整許可。 作為安全最佳實務，建議您不要使用根使用者，除了明確需要根使用者的一些任務之外。如果您 AWS 帳戶 透過 管理多個 AWS Organizations，您可以集中停用根登入，然後代表所有成員帳戶執行根特權動作。在集中管理成員帳戶的根存取權之後，您可以刪除根使用者密碼、存取金鑰和簽署憑證，並停用成員帳戶的多重驗證 (MFA)。根據預設，在集中受管根存取下建立的新帳戶沒有根使用者憑證。成員帳戶無法使用其根使用者登入，或對其根使用者執行密碼復原。

AWS Control Tower 提供簡單的方法來設定和管理多個 帳戶。它可自動化組織中 AWS 帳戶的設定、自動化佈建、套用控制項（包括預防性和偵測性控制項），並提供儀表板讓您清楚可見。額外的 IAM 管理政策，即許可界限，會連接至特定 IAM 主體（使用者或角色），並設定身分型政策可授予 IAM 主體的最大許可。

AWS Organizations 可協助您設定AWS 服務套用至所有 帳戶的 。例如，您可以使用 CloudTrail 設定整個 AWS 組織執行之所有動作的中央記錄，並防止成員帳戶停用記錄。 CloudTrail 您也可以使用 集中彙總您已定義規則的資料AWS Config，以便稽核工作負載是否合規，並快速回應變更。您可以使用 AWS CloudFormation StackSets 集中管理 AWS 組織中跨帳戶和 OUs CloudFormation 堆疊，以便自動佈建新帳戶以符合您的安全需求。

的預設組態 AWS Organizations 支援使用 SCPs做為拒絕清單。透過使用拒絕清單策略，成員帳戶管理員可以委派所有服務和動作，直到您建立和連接拒絕特定服務或一組動作的 SCP 為止。拒絕陳述式需要的維護少於允許清單，因為您在 AWS 新增服務時不需要更新它們。拒絕陳述式的字元長度通常較短，因此更容易保持在 SCPs的大小上限內。在 `Effect` 元素的值為 `Deny` 的陳述式中，您也可以將存取限制在特定資源，或是定義決定 SCP 何時生效的條件。相反地，SCP 中的 `Allow`陳述式適用於所有資源 ("*")，且不受條件限制。如需詳細資訊和範例，請參閱 AWS Organizations 文件中的使用 SCPs 的策略。

設計考量

- 或者，若要使用 SCPs做為允許清單，您必須將 AWS 受管 `FullAWSAccess` SCP 取代為 SCP，以明確允許您想要允許的服務和動作。若要為指定帳戶啟用許可，每個 SCP（從根到帳戶直接路徑中的每個 OU，甚至連接到帳戶本身）必須允許該許可。此模型本質上更嚴格，可能適用於受到高度管制和敏感的工作負載。此方法要求您明確允許路徑中從 AWS 帳戶 到 OU 的每個 IAM 服務或動作。
- 理想情況下，您會使用拒絕清單和允許清單策略的組合。使用允許清單來定義允許在 AWS 組織中使用的 AWS 服務 核准清單，並將此 SCP 連接到組織的 AWS 根目錄。如果您的開發環境允許不同的服務集，您將在每個 OU 連接各自的 SCPs。然後，您可以使用拒絕清單明確拒絕特定 IAM 動作來定義企業護欄。
- RCPs適用於 子集的資源 AWS 服務。如需詳細資訊，請參閱 文件中的 AWS Organizations AWS 服務 支援 RCPs 清單。的預設組態 AWS Organizations 支援使用 RCPs做為拒絕清單。當您在組織中啟用 RCPs 時，稱為 的 AWS 受管政策`RCPFullAWSAccess`會自動連接到組織根目錄、每個 OU，以及您組織中的每個帳戶。您無法分離此政策。此預設 RCP 允許所有主體和動作存取通過 RCP 評估。這表示在您開始建立和連接 RCPs之前，所有現有的

IAM 許可都會繼續如預期般運作。此 AWS 受管政策不會授予存取權。然後，您可以撰寫新的 RCPs做為拒絕陳述式清單，以封鎖對組織中資源的存取。

管理帳戶、受信任存取和委派管理員

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

管理帳戶 （也稱為 AWS Organization Management 帳戶或 Org Management 帳戶） 是唯一的，並與其中的每個其他帳戶有所區別 AWS Organizations。這是建立 AWS 組織的帳戶。從此帳戶，您可以在 AWS 帳戶 AWS 組織中建立 、邀請其他現有帳戶加入組織 AWS （這兩種類型都視為成員帳戶)、從 AWS 組織中移除帳戶，以及將 IAM 政策套用至 AWS 組織中的根帳戶、OUs 帳戶或帳戶。

管理帳戶會透過會影響組織中所有成員帳戶的 AWS SCPs、RCPs 和服務部署 （例如 CloudTrail) 部署通用安全護欄。若要進一步限制管理帳戶中的許可，可以盡可能將這些許可委派給另一個適當的帳戶，例如安全帳戶。

管理帳戶擁有付款人帳戶的責任，並要負責支付成員帳戶累積的所有費用。您無法切換 AWS 組織的管理帳戶。一次 AWS 帳戶 只能是一個 AWS 組織的成員。

由於管理帳戶擁有的功能和影響範圍，我們建議您限制對此帳戶的存取，並僅將許可授予需要它們的角色。兩個可協助您執行此操作的功能是受信任的存取和委派的管理員。您可以使用信任的存取來啟用您指定的 AWS 服務 ，稱為信任的服務，以代表您在 AWS 組織及其帳戶中執行任務。這包括授予許可給信任的服務，但不會影響 IAM 使用者或角色的許可。您可以使用信任的存取來指定您希望信任的服務代表您在 AWS 組織的帳戶中維護的設定和組態詳細資訊。例如， AWS SRA 的組織管理帳戶區段說明如何授予 CloudTrail 服務信任的存取權，以在組織 AWS 中的所有帳戶中建立 CloudTrail 組織追蹤。

有些 AWS 服務 支援 中的委派管理員功能 AWS Organizations。透過此功能，相容服務可以將 AWS 組織中 AWS的成員帳戶註冊為該服務中 AWS 組織帳戶的管理員。此功能為企業內不同的團隊提供彈性，以根據其責任使用不同的帳戶來管理 AWS 服務 整個環境。 AWS SRA 中目前支援委派管理員 AWS 的安全服務包括 IAM Identity Center、 AWS Config、 AWS Firewall Manager、Amazon GuardDuty、IAM Access Analyzer、Amazon Macie、 AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM)、Amazon Detective AWS Audit Manager、Amazon Inspector 和 AWS Systems Manager。最佳實務是在 AWS SRA 中強調使用委派管理員功能，我們將安全相關服務的管理委派給安全工具帳戶。

專用帳戶結構

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

為您的 AWS 資源 AWS 帳戶 提供安全、存取和計費界限，並可讓您實現資源獨立性和隔離。根據預設，帳戶之間不允許存取。

設計 OU 和帳戶結構時，請從安全和基礎設施開始。我們建議為這些特定函數建立一組基礎 OUs，分為基礎設施和安全 OUs。這些 OU 和帳戶建議會擷取我們更廣泛、更全面的 AWS Organizations 和多帳戶結構設計的指導方針子集。如需完整的建議集，請參閱 文件中的 AWS 使用多個帳戶組織您的 AWS 環境，以及部落格文章 組織單位的最佳實務 AWS Organizations。

AWS SRA 利用下列帳戶來實現有效的安全操作 AWS。這些專用帳戶有助於確保職責分離、支援應用程式和資料不同敏感項目的不同控管和存取政策，以及協助減輕安全事件的影響。在接下來的討論中，我們專注於生產 (產品） 帳戶及其相關聯的工作負載。軟體開發生命週期 (SDLC) 帳戶 （通常稱為開發和測試帳戶） 適用於預備交付項目，並且可以在與生產帳戶不同的安全政策集下操作。

帳戶	OU	安全角色
管理	—	集中控管和管理所有 AWS 區域 和 帳戶。 AWS 帳戶 託管組織根的 AWS 。
安全工具	安全	專用 AWS 帳戶 於操作廣泛適用的安全服務 （例如 GuardDuty、Security Hub CSPM、Audit Manager、Detective、Amazon Inspector 和 AWS Config) AWS 帳戶、監控和自動化安全提醒和回應。（在 中 AWS Control Tower，Security OU 下帳戶的預設名稱為 Audit 帳戶。）
日誌存檔	安全	專用 AWS 帳戶 於擷取和封存所有 AWS 區域 和 的所有記錄

		和備份 AWS 帳戶。這應該設計為不可變儲存。
網路	基礎設施	應用程式與更廣泛的網際網路之間的閘道。網路帳戶會將更廣泛的聯網服務、組態和操作與個別應用程式工作負載、安全性和其他基礎設施隔離。
共用服務	基礎設施	此帳戶支援多個應用程式和團隊用來交付其結果的服務。範例包括 Identity Center 目錄服務 (Active Directory)、簡訊服務和中繼資料服務。
應用程式	工作負載	AWS 帳戶 託管 AWS 組織的應用程式並執行工作負載。（這些有時稱為工作負載帳戶。）應建立應用程式帳戶來隔離軟體服務，而不是映射至您的團隊。這可讓部署的應用程式對組織變更更具彈性。

AWS AWS SRA 的組織和帳戶結構

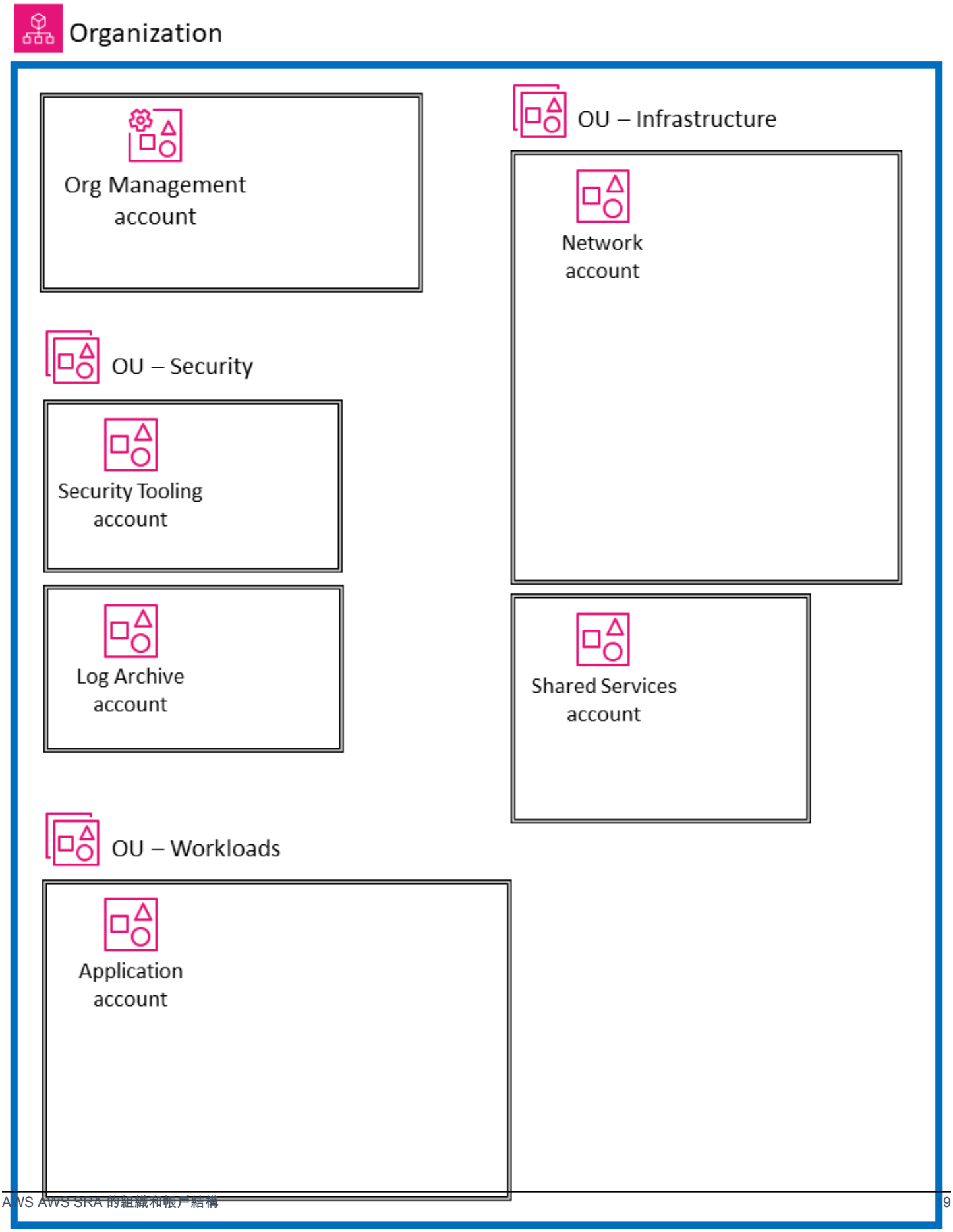
進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖擷取 AWS SRA 的高階結構，而不顯示特定服務。它反映上一節討論的專用帳戶結構，我們在此處包含圖表，以圍繞架構的主要元件引導討論：

- 圖表中顯示的所有帳戶都是單一 AWS 組織的一部分。
- 圖表左上角是組織管理帳戶，用於建立 AWS 組織。
- 組織管理帳戶下方有兩個特定帳戶的安全 OU：一個用於安全工具，另一個用於日誌存檔。
- 右側是具有網路帳戶和共用服務帳戶的基礎設施 OU。
- 下圖底部是工作負載 OU，它與存放企業應用程式的應用程式帳戶相關聯。

在本指引中，所有帳戶都視為在單一 中操作的生產 （ 生產 ） 帳戶 AWS 區域。Most AWS 服務 (全域服務除外 ） 有區域範圍，這表示服務的控制項和資料平面各自獨立存在 AWS 區域。因此，您必須將此架構複寫到 AWS 區域 您計劃使用的所有 ，以確保涵蓋整個 AWS 環境。如果您在特定 中沒有任何工作負載 AWS 區域，您應該使用 SCPs 或使用記錄和監控機制來停用區域。您可以使用 Security Hub CSPM 將調查結果和安全性分數從多個彙總 AWS 區域 到單一彙總區域，以實現集中可見性。

託管具有大量帳戶 AWS 的組織時，擁有協調層有助於帳戶部署和帳戶控管。 AWS Control Tower 提供設定和管理 AWS 多帳戶環境的簡單方法。GitHub 儲存庫中的 AWS SRA 程式碼範例示範如何使用 Customizations for AWS Control Tower (CfCT) 解決方案來部署 AWS SRA 建議的結構。

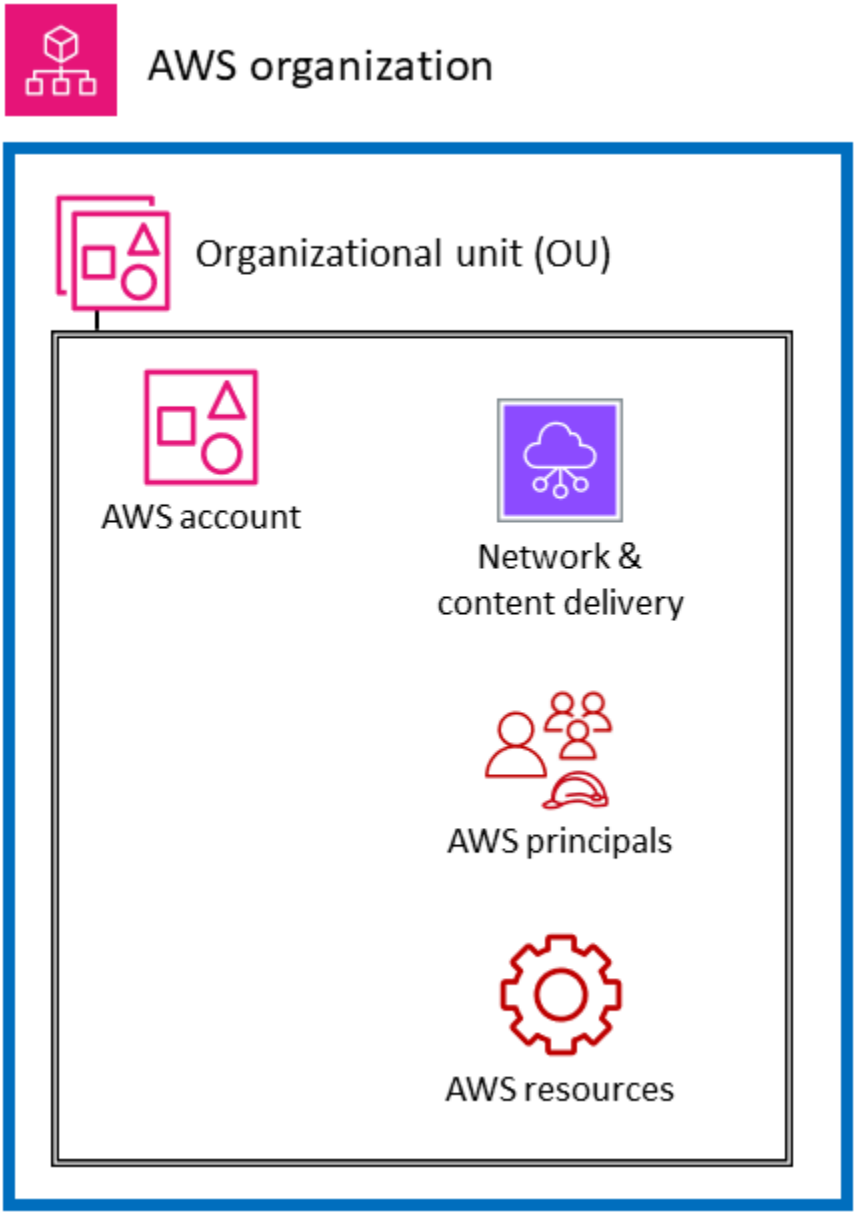

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

在整個 AWS 組織中套用安全服務

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

如上一節所述，客戶正在尋找一種額外的方法來思考並策略性地組織完整的安全服務。 AWS 目前最常見的組織方法是根據每個服務的功能，依主要函數將安全服務分組。 AWS CAF 的安全觀點列出九種功能，包括身分和存取管理、基礎設施保護、資料保護和威脅偵測。 AWS 服務 符合這些功能是在每個領域做出實作決策的實際方法。例如，查看身分和存取管理時，IAM 和 IAM Identity Center 是需要考慮的服務。架構您的威脅偵測方法時，GuardDuty 可能是您的首要考量。

作為此功能檢視的補充，您也可以使用交叉切割的結構檢視來檢視您的安全性。也就是說，除了詢問「 AWS 服務 我應該使用哪個來控制和保護我的身分、邏輯存取或威脅偵測機制？」之外，您也可以詢問「 AWS 服務 我應該在整個 AWS 組織中套用哪些項目？ 為保護應用程式核心的 Amazon EC2 執行個體，我應該設置哪些防禦層？」 在此檢視中，您會將 AWS 服務 和 功能映射到 AWS 環境中的圖層。有些服務和功能非常適合在整個 AWS 組織中實作控制項。例如，封鎖對 Amazon S3 儲存貯體的公開存取是此層的特定控制項。它最好是在根組織完成，而不是成為個別帳戶設定的一部分。其他服務和功能最適合用於協助保護 中的個別資源 AWS 帳戶。在需要私有 TLS 憑證的帳戶內實作次級憑證授權機構 (CA) 是此類別的範例。另一個同樣重要的分組包含對 AWS 基礎設施的虛擬網路層有影響的服務。下圖顯示典型 AWS 環境中的六層： AWS 組織、組織單位 (OU)、帳戶、網路基礎設施、主體和資源。



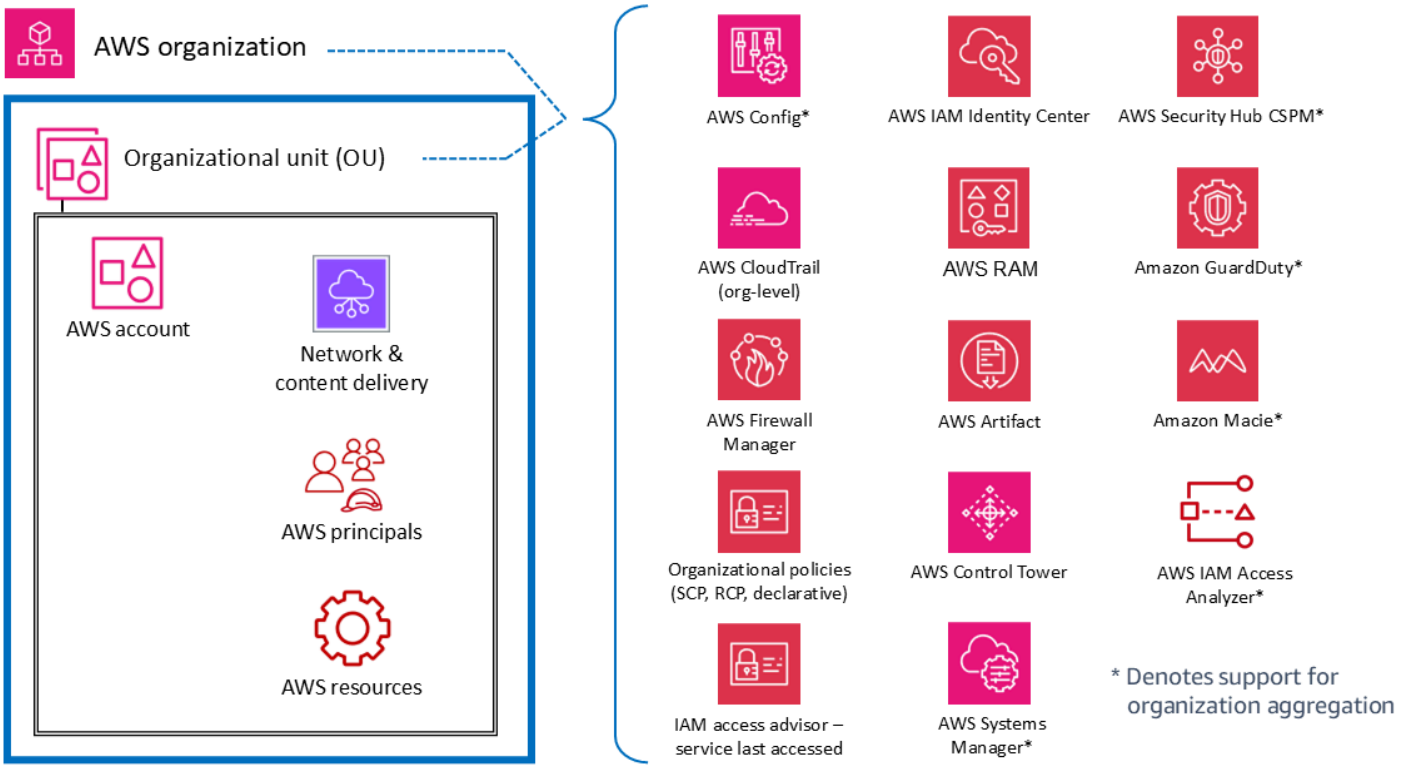
了解此結構內容中的服務，包括每一層的控制和保護，可協助您在整個 AWS 環境中規劃和實作 defense-in-depth策略。透過此觀點，您可以從上到下回答問題（例如，「我使用哪些服務在整個 AWS 組織中實作安全控制？」）和（例如，「哪些服務管理此 EC2 執行個體上的控制項？」）。在本節中，我們會逐步解說 AWS 環境的元素，並識別相關聯的安全服務和功能。當然，有些 AWS 服務 具有廣泛的功能集，並支援多個安全目標。這些服務可能支援您 AWS 環境的多個元素。

為了清楚起見，我們提供一些服務如何符合所述目標的簡短說明。下一節進一步討論每個 中的個別服務 AWS 帳戶。

全組織或多個帳戶

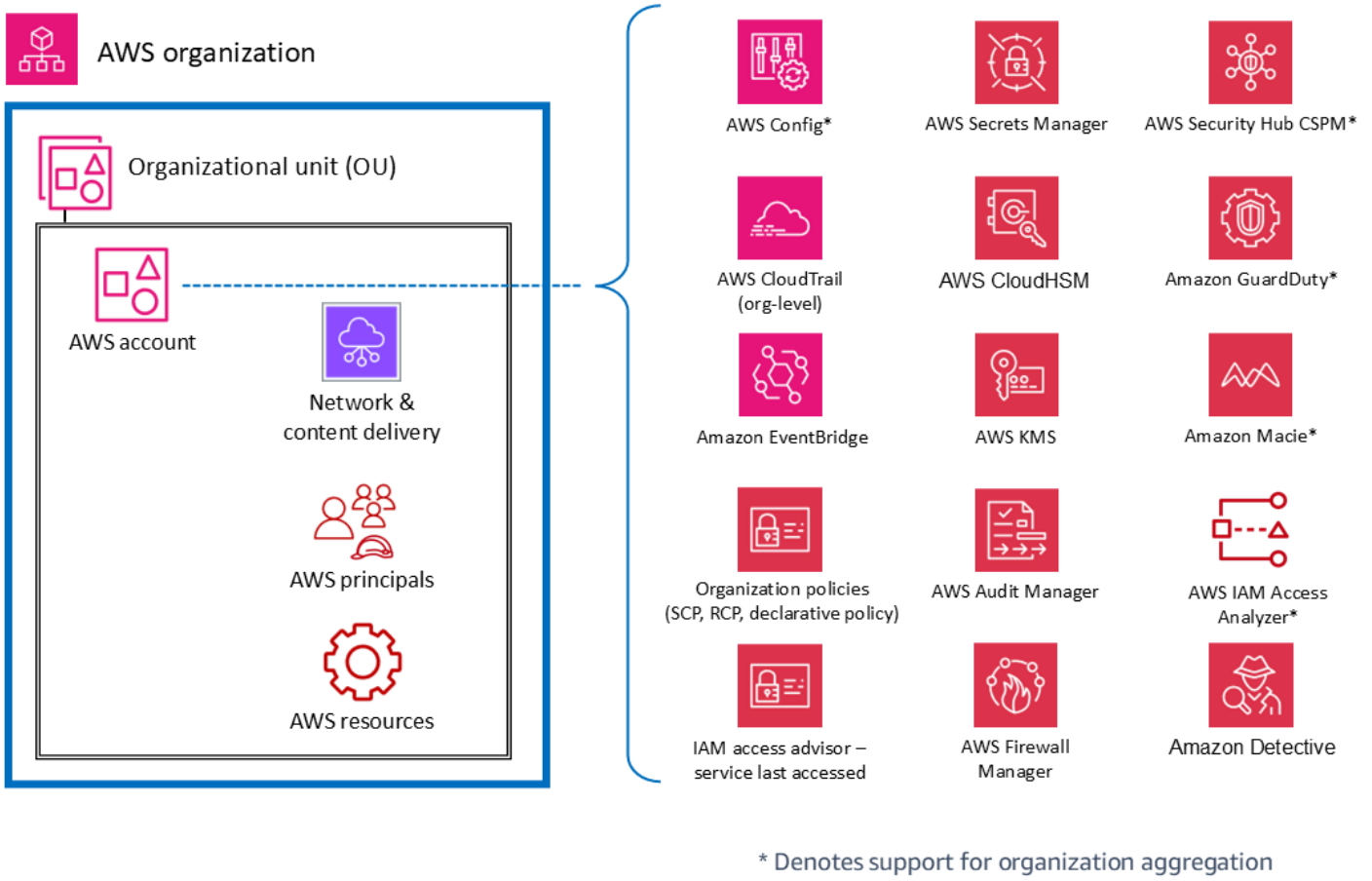
在最上層，有 AWS 服務 和 功能旨在 跨 AWS 組織中的多個帳戶 （ 包括整個組織或特定 OUs) 套用控管和控制功能或護欄。服務控制政策 SCPs) 和資源控制政策 (RCPs) 是 IAM 功能的良好範例，可提供預防性的全 AWS 組織護欄。 AWS Organizations 也提供宣告性政策，可集中定義和強制執行 AWS 服務 大規模 的基準組態。另一個範例是 CloudTrail，透過組織追蹤提供監控，該追蹤會記錄 AWS 帳戶 該組織中所有 的所有事件 AWS 。此全方位線索與每個帳戶中可能建立的個別線索不同。第三個範例是 AWS Firewall Manager，您可以用來設定、套用和管理 AWS 組織中所有帳戶的多個資源： AWS WAF 規則、 AWS WAF 傳統規則、 AWS Shield Advanced 保護、Amazon Virtual Private Cloud (Amazon VPC) 安全群組、 AWS Network Firewall 政策和 Amazon Route 53 Resolver DNS 防火牆政策。

下圖中以星號 (*) 標記的服務使用雙範圍運作：全組織和以帳戶為中心。這些服務基本上會監控或協助控制個別帳戶中的安全性。不過，他們還支援將多個帳戶的結果彙總到整個組織的帳戶中，以實現集中可見性和管理。為了清楚起見，請考慮適用於整個 OU AWS 帳戶或 AWS 組織的 SCPs。相反地，您可以在帳戶層級 （ 產生個別調查結果的位置 ） 和 AWS 組織層級 （ 使用委派管理員功能 ） 設定和管理 GuardDuty，其中調查結果可以彙總檢視和管理。



AWS 帳戶

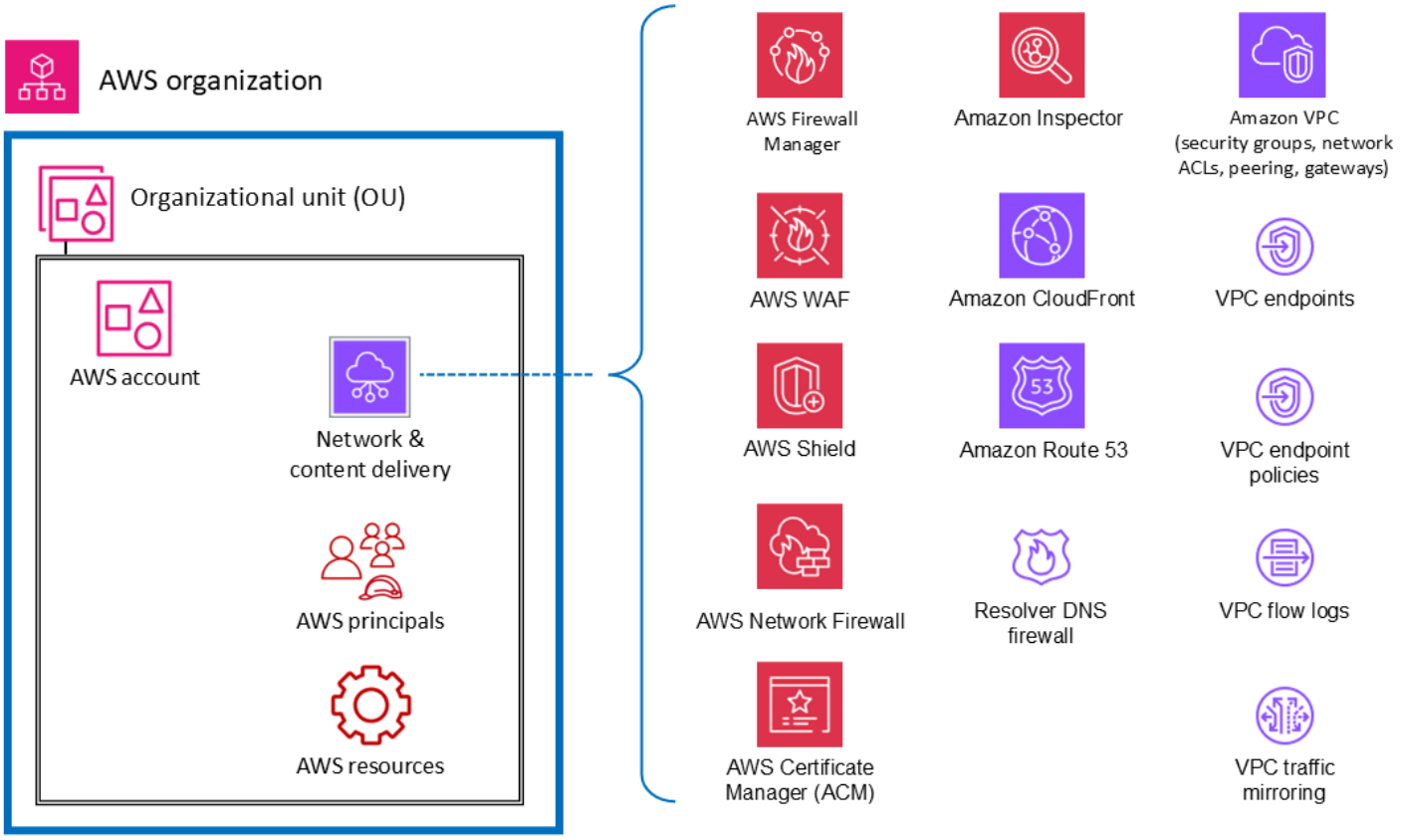
在 OUs中，有服務可協助保護 中的多種元素類型 AWS 帳戶。例如， AWS Secrets Manager 通常由特定帳戶管理，並保護 AWS 服務 該帳戶中的資源 （ 例如資料庫登入資料或身分驗證資訊 ）、應用程式和 。IAM Access Analyzer 可設定為在指定的資源可供 外部主體存取時產生問題清單 AWS 帳戶。如上一節所述，許多 這些服務也可以在 中設定和管理 AWS Organizations，以便跨多個帳戶進行管理。這些服務在圖表中以星號 (*) 標記。它們也可讓您更輕鬆地彙總多個帳戶的結果，並將這些結果交付至單一帳戶。這可為個別應用程式團隊提供彈性和可見性，以管理工作負載特有的安全需求，同時允許集中式安全團隊的控管和可見性。GuardDuty 是這類服務的範例。GuardDuty 會監控與單一帳戶相關聯的資源和活動，而且可以從委派管理員帳戶收集、檢視和管理來自多個成員帳戶的 GuardDuty 調查結果 （ 例如 AWS 組織中的所有帳戶 ）。



虛擬網路、運算和內容交付

由於網路存取在安全性方面至關重要，而運算基礎設施是許多 AWS 工作負載的基本元件，因此有許多 AWS 安全服務和功能專用於這些資源。例如，Amazon Inspector 是一種漏洞管理服務，可持續掃描 AWS 工作負載是否有漏洞。這些掃描包含網路連線能力檢查，指出您環境中允許 Amazon EC2 執行個

體的網路路徑。Amazon VPC 可讓您定義可啟動 AWS 資源的虛擬網路。這個虛擬網路與傳統網路非常相似，並包含各種功能和優點。VPC 端點可讓您將 VPC 私下連線至支援的 AWS 服務 和 提供的端點服務， AWS PrivateLink 而不需要網際網路的路徑。下圖說明專注於網路、運算和內容交付基礎設施的安全服務。



委託人和資源

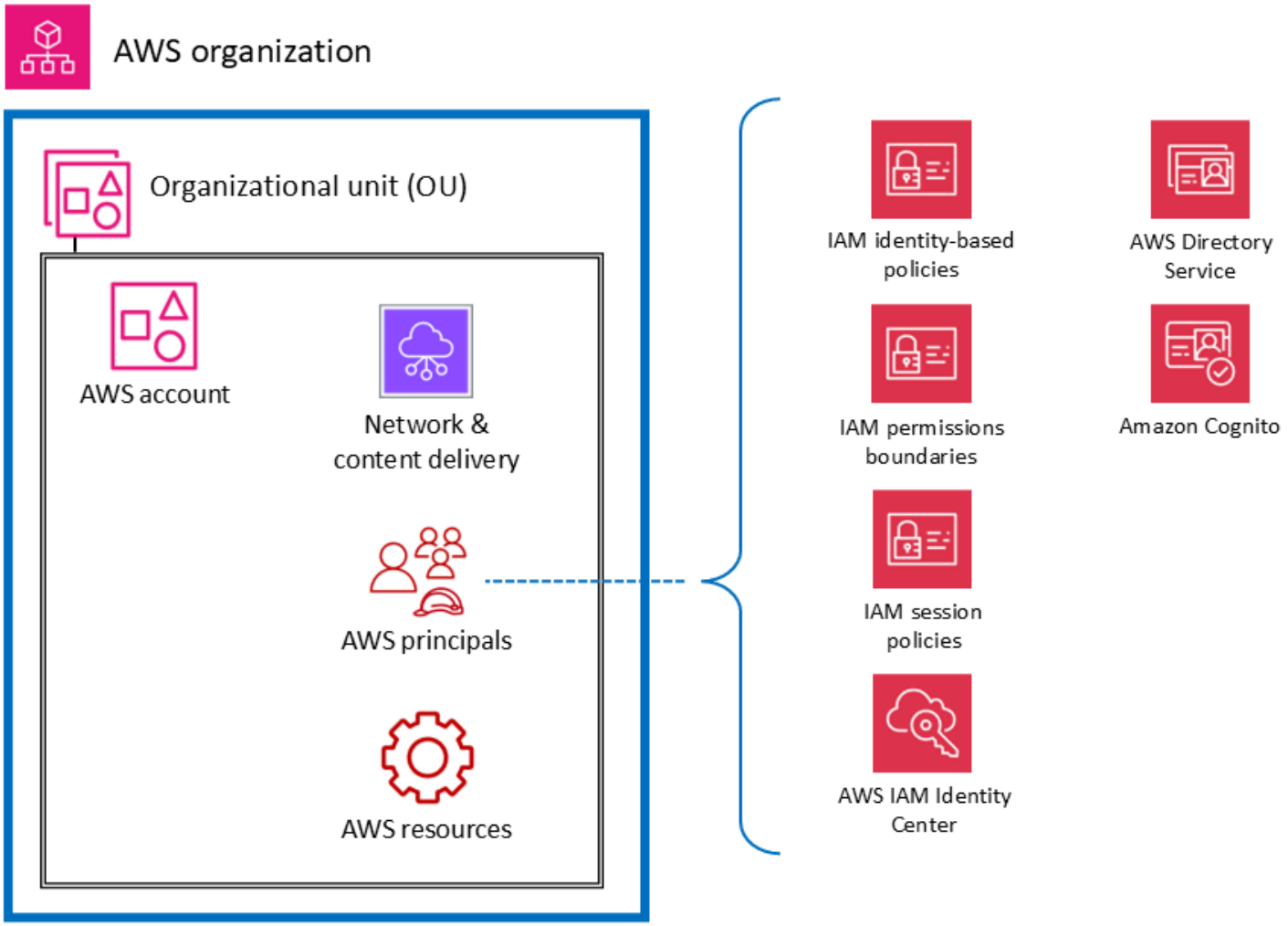
AWS 主體 AWS 和資源 （以及 IAM 政策） 是身分和存取管理的基礎元素 AWS。中的已驗證主體 AWS 可以執行動作和存取 AWS 資源。委託人可以驗證為 AWS 帳戶 根使用者和 IAM 使用者，或擔任角色。

> **Note**
>
> 請勿建立與 AWS 根使用者帳戶相關聯的持久性 API 金鑰。對根使用者帳戶的存取應僅限於需要根使用者的任務，然後僅透過嚴格的例外狀況和核准程序。如需保護您帳戶的根使用者的最佳實務，請參閱 IAM 文件。

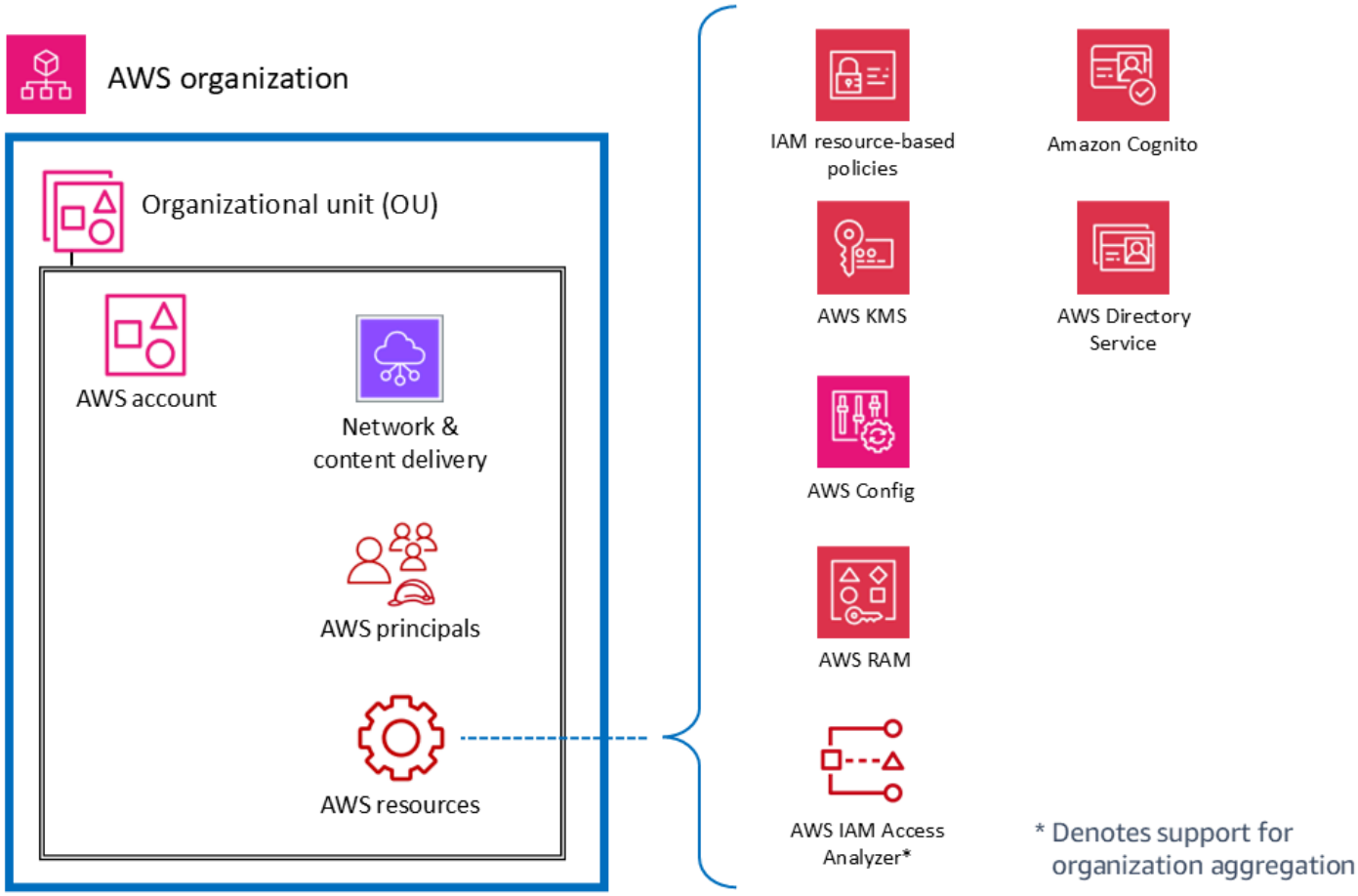
AWS 資源是存在於 中的物件 AWS 服務 ，可供您使用。範例包括 EC2 執行個體、 CloudFormation 堆疊、Amazon Simple Notification Service (Amazon SNS) 主題和 S3 儲存貯體。IAM 政策是在與 IAM 主體 （使用者、群組或角色） 或 AWS 資源建立關聯時定義許可的物件。身分型政策 是您連接到委託人 （角色、使用者和使用者群組） 的政策文件，以控制委託人可以執行的動作、資源和條件。以資源為基礎的政策 是您連接到資源的政策文件，例如 S3 儲存貯體。這些政策會授予指定的委託人許可，以對該資源執行特定動作，並定義該許可的條件。以資源為基礎的政策是內嵌政策。IAM 資源區段深入探討 IAM 政策的類型及其使用方式。

為了在此討論中保持簡單，我們會列出主要目的為操作或套用到帳戶主體的 IAM 主體 AWS 的安全服務和功能。我們保持這種簡單性，同時認可 IAM 許可政策的靈活性和廣度。政策中的單一陳述式可能會影響多種類型的 AWS 實體。例如，雖然 IAM 身分型政策與 IAM 主體相關聯，並定義該主體的許可（允許、拒絕），但政策也會隱含定義所指定動作、資源和條件的許可。透過這種方式，身分型政策可以是定義資源許可的關鍵元素。

下圖說明 主體 AWS 的安全服務和功能 AWS 。以身分為基礎的政策會連接至 IAM 使用者、群組或角色。這些政策可讓您指定該身分可以執行哪些動作 (其許可)。IAM 工作階段政策是使用者擔任角色時在工作階段中傳遞的 內嵌許可政策 。您可以自行傳遞政策，也可以將身分代理程式設定為在 身分聯合時 AWS插入政策。這可讓您的管理員減少他們必須建立的角色數量，因為多個使用者可以擔任相同的角色，但具有唯一的工作階段許可。IAM Identity Center 服務已與 AWS Organizations 和 AWS API 操作整合，可協助您管理 AWS 帳戶 中的 SSO 存取和使用者許可 AWS Organizations。



下圖說明 帳戶資源的服務和功能。以資源為基礎的政策會連接至資源。例如，您可以將資源型政策連接至 S3 儲存貯體、Amazon Simple Queue Service (Amazon SQS) 佇列、VPC 端點和 AWS KMS 加密金鑰。您可以使用資源型政策來指定誰可以存取資源，以及他們可以對其執行哪些動作。S3 儲存貯體政策 AWS KMS 、金鑰政策和 VPC 端點政策是資源型政策的類型。IAM Access Analyzer 可協助您識別組織和帳戶中與外部實體共用的資源，例如 S3 儲存貯體或 IAM 角色。這可讓您識別意外存取資源和資料，這是安全風險。 AWS Config 可讓您評估、稽核和評估 中支援 AWS 資源的組態 AWS 帳戶。 AWS Config 會持續監控和記錄 AWS 資源組態，並根據所需的組態自動評估記錄的組態。


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

AWS 安全參考架構

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明 AWS SRA。此架構圖將所有 AWS 安全相關的服務整合在一起。它以簡單的三層 Web 架構為基礎建置，可在單一頁面上使用。在這類工作負載中，有一個 Web 層，使用者可透過該 Web 層與應用程式層連線和互動，處理應用程式的實際商業邏輯：從使用者取得輸入、進行一些運算，以及產生輸出。應用程式層會從資料層存放和擷取資訊。此架構是刻意模組化的，可為許多現代 Web 應用程式提供高階抽象。

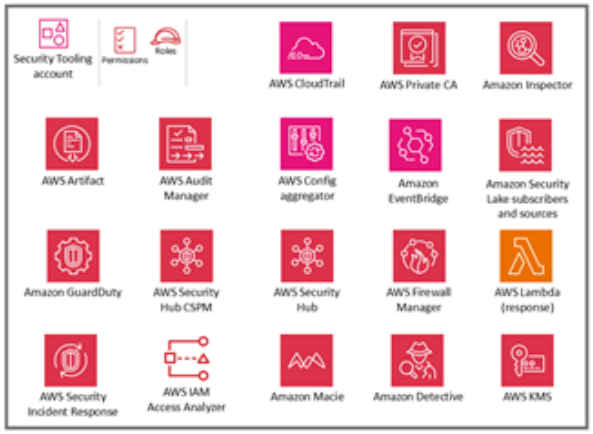
架構圖

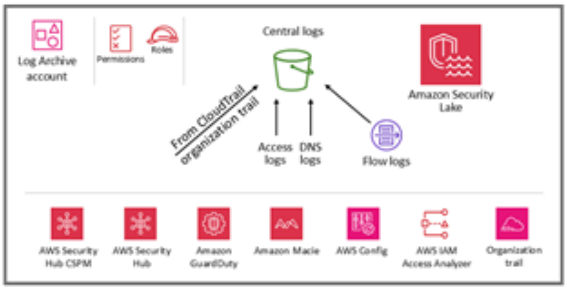
若要根據您的業務需求自訂本指南中的參考架構圖，您可以下載下列 .zip 檔案並解壓縮其內容。

下載圖表來源檔案 (Microsoft PowerPoint 格式)

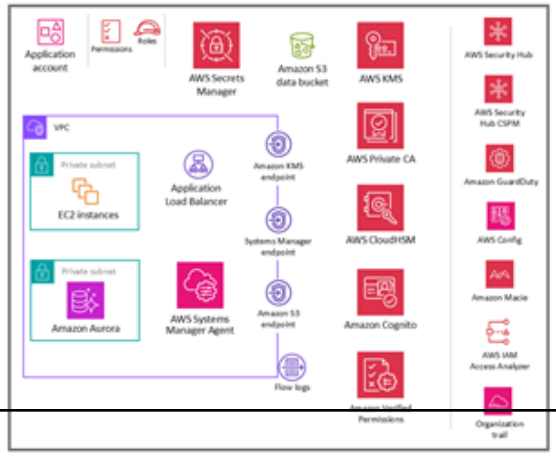
Organization

OU – Security

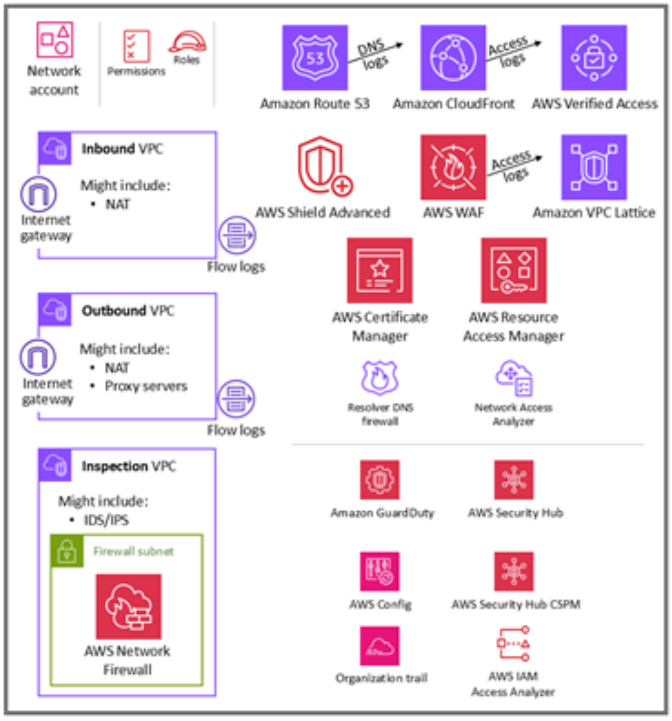


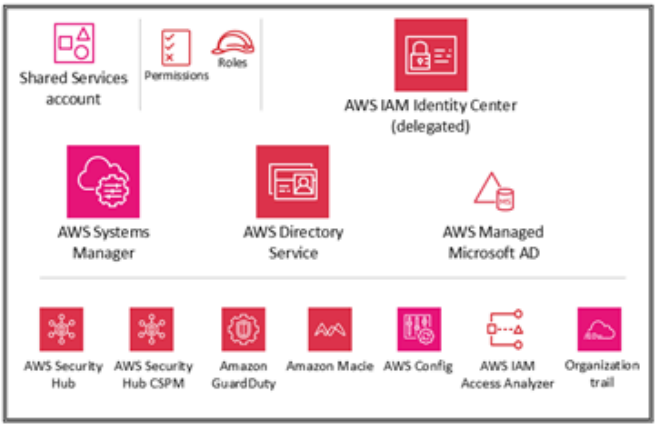


OU – Workloads



OU – Infrastructure





對於此參考架構，實際的 Web 應用程式和資料層會透過 Amazon EC2 執行個體和 Amazon Aurora 資料庫，以盡可能簡單的方式刻意表示。大多數架構圖著重於 Web、應用程式和資料層，並深入探討。為了方便閱讀，它們通常會省略安全控制。此圖表會翻轉，強調盡可能顯示安全性，並盡可能讓應用程式和資料層保持簡單，以有意義的方式顯示安全性功能。

AWS SRA 包含發佈時可用的所有 AWS 安全相關服務。（請參閱文件歷史記錄。）不過，不是每個工作負載或環境，根據其獨特的威脅暴露，都必須部署每個安全服務。我們的目標是提供一系列選項的參考，包括這些服務在架構上如何結合在一起的描述，以便您的企業可以根據風險做出最適合您基礎設施、工作負載和安全需求的決策。

以下各節會逐步解說每個 OU 和帳戶，以了解其目標和與其相關聯的個別 AWS 安全服務。對於每個元素（通常是 AWS 服務），本文件提供下列資訊：

- AWS SRA 中 元素及其安全用途的簡短概觀。如需個別服務的詳細說明和技術資訊，請參閱附錄。
- 建議放置，以最有效地啟用和管理服務。這會在每個帳戶和 OU 的個別架構圖表中擷取。
- 其他安全服務的組態、管理和資料共用連結。此服務如何依賴或支援其他安全服務？
- 設計考量事項。首先，文件重點介紹具有重要安全性影響的選用功能或組態。其次，當團隊的經驗包含建議的常見變化時，通常是由於替代要求或限制，文件會說明這些選項。

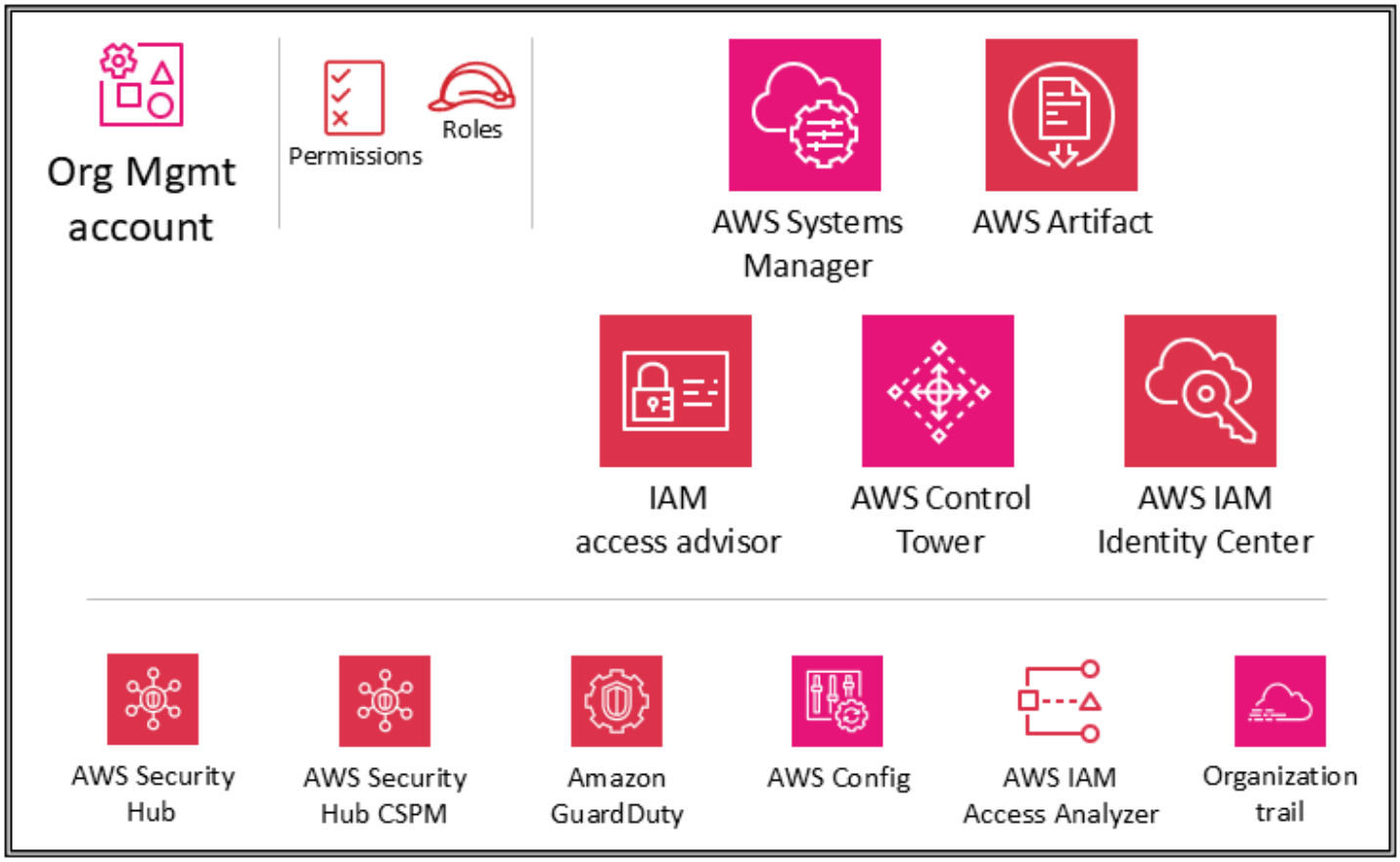
OUs和帳戶

- 組織管理帳戶
- Security OU – 安全工具帳戶
- 安全 OU – Log Archive 帳戶
- 基礎設施 OU – 網路帳戶
- Infrastructure OU – 共用服務帳戶
- 工作負載 OU – 應用程式帳戶

組織管理帳戶

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明組織管理帳戶中設定 AWS 的安全服務。



本指南稍早的「使用 AWS Organizations 安全」和「管理帳戶」、「信任存取」和「委派管理員」章節討論了組織管理帳戶的目的和安全性目標。遵循組織管理帳戶的安全最佳實務。這包括使用由您企業管理的電子郵件地址、維護正確的管理和安全聯絡資訊（例如，在需要 AWS 聯絡帳戶擁有者的情況下將電話號碼連接至帳戶）、為所有使用者啟用多重要素驗證 (MFA)，以及定期檢閱誰有權存取組織管理帳戶。組織管理帳戶中部署的服務應使用適當的角色、信任政策和其他許可進行設定，以便這些服務的管理員（必須在組織管理帳戶中存取這些服務）也無法不當存取其他 服務。

服務控制政策

使用 AWS Organizations，您可以集中管理多個政策 AWS 帳戶。例如，您可以在屬於組織成員的多個之間套用 服務控制政策 AWS 帳戶 (SCPs)。SCPs 可讓您定義組織成員中的 IAM 主體（例如 IAM 使用者和角色）可以和不可以執行哪些 AWS 服務 APIs AWS 帳戶。SCPs 是從組織管理帳戶建立和套用，這是您在建立組織時使用 AWS 帳戶 的 。閱讀本參考前面的使用 AWS Organizations 安全章節中有關 SCPs的詳細資訊。

如果您使用 AWS Control Tower 來管理您的 AWS 組織，它會部署一組 SCPs 做為預防性護欄（分類為強制性、強烈建議或選擇性）。這些護欄透過強制執行整個組織的安全控制，協助您管理資源。這些

SCPs 會自動使用值為 managed-by-control-tower 的 aws-control-tower 標籤。 managed-by-control-tower

> **設計考量事項**
>
> SCPs只會影響組織中的成員帳戶 AWS 。雖然它們是從組織管理帳戶套用，但不會影響該帳戶中的使用者或角色。若要了解 SCP 評估邏輯的運作方式，以及查看建議結構的範例，請參閱 AWS 部落格文章如何使用 中的服務控制政策 AWS Organizations。

資源控制政策

資源控制政策 RCPs) 可讓您集中控制組織中資源的可用許可上限。RCP 會定義許可護欄，或設定身分可對組織中資源採取的動作限制。您可以使用 RCPs來限制誰可以存取您的資源，並強制要求如何在組織的成員 中存取您的資源 AWS 帳戶。您可以直接將 RCPs 連接到個別帳戶、OUs 或組織根目錄。如需 RCPs運作方式的詳細說明，請參閱 AWS Organizations 文件中的 RCP 評估。閱讀本參考前面的使用 AWS Organizations 安全一節中有關 RCPs的詳細資訊。

如果您使用 AWS Control Tower 來管理您的 AWS 組織，它會部署一組 RCPs作為預防性護欄 （分類為強制性、強烈建議或選擇性）。這些護欄透過強制執行整個組織的安全控制，協助您管理資源。這些SCPs會自動使用值為 的`aws-control-tower`標籤`managed-by-control-tower`。

> **設計考量**
>
> - RCPs只會影響組織中 成員 帳戶中的資源。它們不會影響管理帳戶中的資源。這也表示RCPs適用於指定為委派管理員的成員帳戶。
> - RCPs適用於 子集的資源 AWS 服務。如需詳細資訊，請參閱 文件中的 AWS Organizations AWS 服務 支援 RCPs 清單。您可以使用 AWS Config 規則 和 AWS Lambda 函數 來監控和自動化對 RCPs 目前不支援的資源實施安全控制。

宣告式政策

宣告政策是一種 AWS Organizations 管理政策，可協助您集中宣告和強制執行整個組織中 AWS 服務大規模指定 所需的組態。宣告政策目前支援 Amazon EC2、 Amazon VPC 和 Amazon EBS 服務。可用的服務屬性包括強制執行執行個體中繼資料服務第 2 版 (IMDSv2)、允許透過 EC2 序列主控台進行故障診斷、允許 Amazon Machine Image (AMI) 設定，以及封鎖 Amazon EBS 快照、Amazon EC2

AMIs 和 Amazon VPC 資源的公開存取。如需最新支援的服務和屬性，請參閱 AWS Organizations 文件中的宣告政策。

您可以在 AWS Organizations 和 AWS Control Tower 主控台上進行一些選擇 AWS 服務 ，或使用幾個 AWS Command Line Interface (AWS CLI) 和 AWS SDK 命令，以強制執行 的基準組態。宣告政策會在服務的控制平面中強制執行，這表示 的基準組態一律 AWS 服務 會維持，即使服務引入新功能或 APIs、將新帳戶新增至組織，或建立新主體和資源時也是如此。宣告政策可以套用至整個組織或特定 OUs 或帳戶。 有效政策 是從組織根目錄和 OUs 繼承的一組規則，以及直接連接到帳戶的政策。 如果已 分離宣告政策，則屬性狀態會在連接宣告政策之前回復至其狀態。

您可以使用宣告式政策來建立自訂錯誤訊息。例如，如果 API 操作因為宣告性政策而失敗，您可以設定錯誤訊息或提供自訂 URL，例如內部 wiki 的連結或描述失敗的訊息連結。這有助於為使用者提供更多資訊，以便他們可以自行對問題進行故障診斷。您也可以使用 稽核建立宣告政策、更新宣告政策，以及刪除宣告政策的程序 AWS CloudTrail。

宣告政策提供帳戶狀態報告， 可讓您檢閱範圍內帳戶宣告政策支援的所有屬性的目前狀態。您可以選擇要包含在報告範圍中的帳戶和 OUs，或選取根來選擇整個組織。此報告透過提供明細 AWS 區域 ，並指定屬性的目前狀態 跨帳戶 （透過 值） 是否一致 或跨帳戶 不一致 （透過 `numberOfUnmatchedAccounts`值） ， `numberOfMatchedAccounts`來協助您評估整備程度。

> **設計考量事項**
>
> 當您使用宣告性政策設定服務屬性時，政策可能會影響多個 APIs。任何不合規動作都會失敗。帳戶管理員將無法修改個別帳戶層級的服務屬性值。

集中式根存取

中的所有成員帳戶 AWS Organizations 都有自己的根使用者，這是可存取該成員帳戶中所有 AWS 服務 和資源的身分。IAM 提供集中式根存取管理，以管理所有成員帳戶的根存取。這有助於防止成員根使用者使用，並有助於大規模復原。集中式根存取功能有兩個基本功能：根憑證管理和 根工作階段。

- 根憑證管理功能允許集中管理，並協助保護所有管理帳戶的根使用者。此功能包括移除長期根憑證、防止成員帳戶復原根憑證，以及佈建預設沒有根憑證的新成員帳戶。它也提供示範合規的簡單方法。當根使用者管理集中時，您可以移除根使用者密碼、存取金鑰和簽署憑證，並從所有成員帳戶停用多重驗證 (MFA)。
- 根工作階段功能可讓您在來自組織管理帳戶或委派管理員帳戶的成員帳戶上使用短期憑證，以執行特權根使用者動作。此功能可協助您啟用範圍限定於特定動作的短期根存取權，並遵循最低權限原則。

對於集中式根憑證管理，您需要從組織管理帳戶或在委派管理員帳戶中，在組織層級啟用根憑證管理和根工作階段功能。遵循 AWS SRA 最佳實務，我們會將此功能委派給安全工具帳戶。如需有關設定和使用集中式根使用者存取的資訊，請參閱 AWS 安全部落格文章，集中管理使用 的客戶根存取 AWS Organizations。

IAM Identity Center

AWS IAM Identity Center 是一種聯合身分服務，可協助您集中管理對所有 AWS 帳戶、主體和雲端工作負載的 SSO 存取。IAM Identity Center 也可協助您管理常用第三方軟體即服務 (SaaS) 應用程式的存取和許可。身分提供者使用 SAML 2.0 與 IAM Identity Center 整合。您可以使用跨網域身分管理 (SCIM) 系統來完成大量和just-in-time佈建。IAM Identity Center 也可以透過使用 與內部部署 AWS 或受管 Microsoft Active Directory (AD) 網域整合為身分提供者 AWS Directory Service。IAM Identity Center 包含使用者入口網站，您的最終使用者可以在同一個位置尋找和存取其指派的 AWS 帳戶 IAM Identity Center、角色、雲端應用程式和自訂應用程式。

IAM Identity Center 預設會原生與 整合， AWS Organizations 並在組織管理帳戶中執行。不過，若要行使最低權限並嚴格控制對管理帳戶的存取，可以將 IAM Identity Center 管理委派給特定的成員帳戶。在 AWS SRA 中，共享服務帳戶是 IAM Identity Center 的委派管理員帳戶。在啟用 IAM Identity Center 的委派管理之前，請檢閱這些考量事項。您可以在共用服務帳戶區段中找到有關委派的詳細資訊。即使您啟用委派，IAM Identity Center 仍需要在 Org Management 帳戶中執行，才能執行特定 IAM Identity Center 相關任務，包括管理在 Org Management 帳戶中佈建的許可集。

在 IAM Identity Center 主控台中，帳戶會以其封裝的 OU 顯示。這可讓您快速探索您的 AWS 帳戶、套用常見的許可集，以及從中央位置管理存取權。

IAM Identity Center 包含身分存放區，其中必須存放特定使用者資訊。不過，IAM Identity Center 不一定是人力資源資訊的授權來源。如果您的企業已有授權來源，IAM Identity Center 會支援以下類型的身分提供者 (IdPs)。

- IAM Identity Center 身分存放區 – 如果下列兩個選項無法使用，請選擇此選項。建立使用者、進行群組指派，並在身分存放區中指派許可。即使您的授權來源位於 IAM Identity Center 外部，委託人屬性的副本也會存放在身分存放區中。
- Microsoft Active Directory (AD) – 如果您想要繼續管理 中的目錄 AWS Directory Service for Microsoft Active Directory 或 Active Directory 中的自我管理目錄中的使用者，請選擇此選項。
- 外部身分提供者 – 如果您想要管理外部第三方 SAML 型 IdP 中的使用者，請選擇此選項。

您可以依賴企業內現有的 IdP。這可讓您更輕鬆地跨多個應用程式和服務管理存取權，因為您是從單一位置建立、管理和撤銷存取權。例如，如果有人離開您的團隊，您可以從一個位置撤銷他們對所有應用

程式和服務（包括 AWS 帳戶) 的存取權。這可減少對多個登入資料的需要，並讓您有機會與您的人力資源 (HR) 程序整合。

> **設計考量事項**
>
> 如果您的企業可以使用該選項，請使用外部 IdP。如果您的 IdP 支援跨網域身分管理 (SCIM) 系統，請利用 IAM Identity Center 中的 SCIM 功能來自動化使用者、群組和許可佈建（同步）。這可讓新員工、即將調到另一個團隊的員工，以及即將離開公司的員工 AWS ，存取與您的公司工作流程保持同步。在任何指定時間，您只能有一個目錄或一個 SAML 2.0 身分提供者連接到 IAM Identity Center。不過，您可以切換到另一個身分提供者。

IAM 存取顧問

IAM 存取建議程式以您 AWS 帳戶 和 OUs 的服務上次存取資訊形式提供可追蹤性資料。使用此偵測性控制項有助於實現最低權限策略。對於 IAM 主體，您可以檢視兩種類型的上次存取資訊：允許 AWS 服務 的資訊和允許的動作資訊。這些資訊包括嘗試的日期和時間。

組織管理帳戶中的 IAM 存取可讓您檢視組織中 AWS 組織管理帳戶、OU、成員帳戶或 IAM 政策的服務上次存取資料。此資訊可在 管理帳戶中的 IAM 主控台中取得，也可以使用 中的 IAM 存取建議程式 APIs AWS CLI 或程式設計用戶端以程式設計方式取得。這些資訊會指出組織或帳戶中哪些主參與者上次嘗試存取服務，以及何時存取服務。上次存取的資訊可提供實際服務用量的洞見（請參閱範例案例)，因此您只能將 IAM 許可減少為實際使用的服務。

AWS Systems Manager

Quick Setup 和 Explorer 是 的功能AWS Systems Manager，可支援 AWS Organizations 並從 Org Management 帳戶操作。

快速設定是 Systems Manager 的自動化功能。它可讓組織管理帳戶輕鬆定義組態，讓 Systems Manager 代表您在 AWS 組織中跨帳戶互動。您可以在整個組織中啟用快速設定， AWS 或選擇特定的 OUs。快速設定可以排程 AWS Systems Manager 代理程式 (SSM 代理程式） 在 EC2 執行個體上執行每兩週更新一次，並可以設定這些執行個體的每日掃描，以識別遺失的修補程式。

Explorer 是可自訂的操作儀表板，可報告 AWS 資源的相關資訊。Explorer 會顯示您 AWS 帳戶和跨帳戶的操作資料的彙總檢視 AWS 區域。這包括 EC2 執行個體和修補程式合規詳細資訊的資料。在 中完成整合式設定（也包含 Systems Manager OpsCenter) 之後 AWS Organizations，您可以依 OU 或整個 AWS 組織彙總 Explorer 中的資料。Systems Manager 在 Explorer 中顯示資料之前，會將資料彙總到 AWS 組織管理帳戶。

本指南稍後的工作負載 OU 區段討論在應用程式帳戶中的 EC2 執行個體上使用 SSM 代理程式。

AWS Control Tower

AWS Control Tower 提供設定和管理安全多帳戶 AWS 環境的直接方式，稱為登陸區域。 會使用 AWS Control Tower 建立您的登陸區域 AWS Organizations，並提供持續的帳戶管理和控管，以及實作最佳實務。您可以使用 以幾個步驟 AWS Control Tower 佈建新帳戶，同時確保帳戶符合您的組織政策。您甚至可以將現有的帳戶新增至新的 AWS Control Tower 環境。

AWS Control Tower 有一組廣泛且靈活的功能。關鍵功能是能夠協調其他數個 的功能 AWS Organizations AWS Service Catalog，AWS 服務包括 和 IAM Identity Center，以建置登陸區域。例如，根據預設， AWS Control Tower 會使用 AWS CloudFormation 來建立基準、 AWS Organizations 服務控制政策 (SCPs) 來防止組態變更，以及 AWS Config 規則 規則來持續偵測不一致性。 AWS Control Tower employs 藍圖，協助您快速將多帳戶 AWS 環境與 AWS Well Architected 安全基礎設計原則保持一致。在控管功能中， AWS Control Tower 提供防護機制，可防止部署不符合所選政策的資源。

您可以開始使用 實作 AWS SRA 指引 AWS Control Tower。例如， 會使用建議的多帳戶架構 AWS Control Tower 建立 AWS 組織。它提供藍圖來提供身分管理、提供帳戶的聯合存取、集中記錄、建立跨帳戶安全稽核、定義佈建新帳戶的工作流程，以及使用網路組態實作帳戶基準。

在 AWS SRA 中， AWS Control Tower 位於組織管理帳戶中，因為 AWS Control Tower 使用此帳戶自動設定 AWS 組織，並將該帳戶指定為管理帳戶。此帳戶用於整個 AWS 組織的計費。它也用於帳戶的帳戶工廠佈建、管理 OUs，以及管理護欄。如果您在 AWS Control Tower 現有的 AWS 組織中啟動 ，您可以使用現有的管理帳戶。 AWS Control Tower 會使用該帳戶做為指定的管理帳戶。

> **設計考量事項**
>
> 如果您想要跨帳戶執行額外的控制項和組態基準，您可以使用 AWS Control Tower (CfCT) 的自訂。透過 CfCT，您可以使用 CloudFormation 範本和 SCPs自訂 AWS Control Tower 登陸區域。您可以將自訂範本和政策部署到組織中的個別帳戶和 OUs。CfCT 與 AWS Control Tower 生命週期事件整合，以確保資源部署與您的登陸區域保持同步。

AWS Artifact

AWS Artifact 提供隨需存取 AWS 安全性和合規報告，並選取線上協議。中可用的報告 AWS Artifact 包括系統和組織控制 (SOC) 報告、支付卡產業 (PCI) 報告，以及跨地理位置和合規垂直機構的認證，

可驗證 AWS 安全控制的實作和操作有效性。 AWS Artifact 可協助您對安全控制環境進行增強透明度 AWS 的盡職調查。它還可讓您持續監控 的安全性和合規性 AWS ，並立即存取新的報告。

AWS Artifact 協議可讓您檢閱、接受和追蹤協議的狀態 AWS ，例如個別帳戶的商業夥伴增補合約 (BAA)，以及屬於您組織一部分的帳戶 AWS Organizations。

您可以提供 AWS 稽核成品給您的稽核人員或監管機構，做為 AWS 安全控制的證據。您也可以使用一些 AWS 稽核成品提供的責任指引來設計雲端架構。本指南有助於判斷您可以實施的額外安全控制，以支援系統的特定使用案例。

AWS Artifact 託管於組織管理帳戶中，以提供中央位置供您檢閱、接受和管理協議 AWS。這是因為管理帳戶接受的協議會向下流到成員帳戶。

> **設計考量事項**
>
> 組織管理帳戶中的使用者應僅限於使用 的協議功能 AWS Artifact ，而不使用其他功能。為了實作職責分離， AWS Artifact 也託管在安全工具帳戶中，您可以在其中將許可委派給您的合規利益相關者和外部稽核人員，以存取稽核成品。您可以透過定義精細的 IAM 許可政策來實作此分隔。如需範例，請參閱 AWS 文件中的範例 IAM 政策。

分散式和集中式安全服務護欄

在 AWS SRA AWS Security Hub AWS Security Hub CSPM、Amazon GuardDuty AWS Config、IAM Access Analyzer、 AWS CloudTrail 組織線索和 Amazon Macie 中，通常使用適當的委派護欄組跨帳戶部署，並在整個 AWS 組織中提供集中式監控、管理和管控。您可以在 AWS SRA 中呈現的每個帳戶類型中找到此服務群組。這些應該是 的一部分 AWS 服務 ，必須在帳戶加入和基礎程序中佈建。GitHub 程式碼儲存庫會在您的帳戶間提供以安全為重心的服務範例實作 AWS ，包括 AWS 組織管理帳戶。

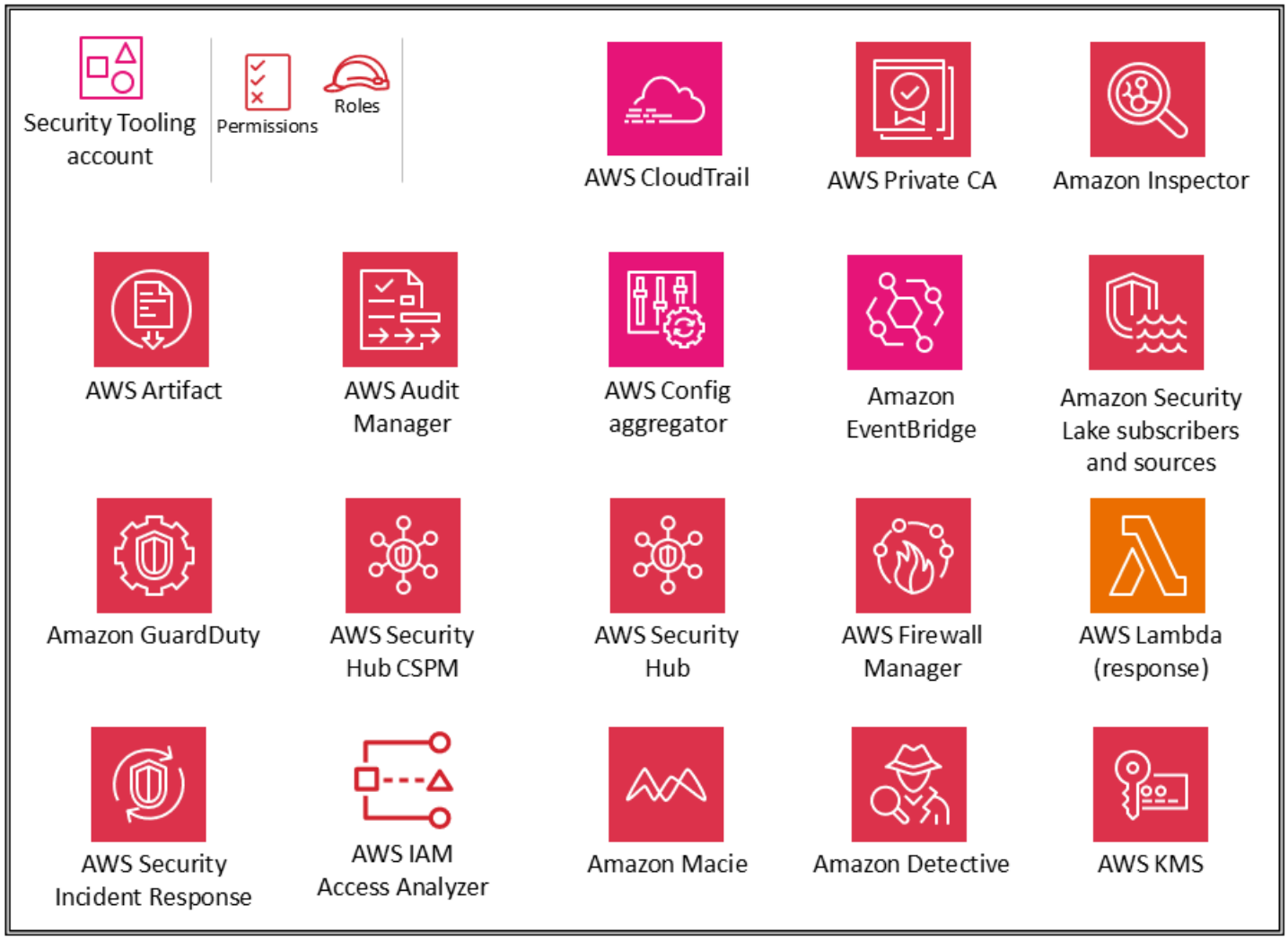
除了這些服務之外， AWS SRA 還包含兩個以安全為重心的服務：Amazon Detective 和 AWS Audit Manager，支援 中的整合和委派管理員功能 AWS Organizations。不過，這些不包含在帳戶基準的建議服務中。我們看到這些服務最適合在下列案例中使用：

- 您擁有執行這些數位鑑識和 IT 稽核函數的專用團隊或資源群組。Detective 最適合安全分析師團隊使用，而 Audit Manager 有助於您的內部稽核或合規團隊。
- 您想要在專案 AWS Security Hub AWS Security Hub CSPM 開始時專注於一組核心工具 AWS Config，例如 Amazon GuardDuty，然後使用提供額外的功能的服務來建置這些工具。

Security OU – 安全工具帳戶

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明 AWS Security Tooling 帳戶中設定的安全服務。



Security Tooling 帳戶專用於操作安全服務、監控 AWS 帳戶，以及自動化安全提醒和回應。安全性目標包括下列項目：

- 提供具有受控存取權的專用帳戶，以管理對安全護欄、監控和回應的存取。
- 維護適當的集中式安全基礎設施，以監控安全操作資料並維持可追蹤性。偵測、調查和回應是安全生命週期的重要部分，可用於支援品質程序、法律或合規義務，以及威脅識別和回應工作。

- 透過對適當的安全組態和操作保持另一層控制，例如加密金鑰和安全群組設定，進一步支援defense-in-depth組織策略。這是安全操作員運作所在的帳戶。用於檢視整個 AWS 組織的唯讀/稽核角色是典型的，而寫入/修改角色的數量有限、受到嚴格控制、監控和記錄。

> **設計考量**
>
> - AWS Control Tower 根據預設， 會在稽核帳戶的安全 OU 下為帳戶命名。您可以在 AWS Control Tower 設定期間重新命名帳戶。
> - 可能有多個安全工具帳戶是適當的。例如，監控和回應安全事件通常會指派給專用團隊。網路安全可能需要自己與雲端基礎設施或網路團隊合作的帳戶和角色。此類分割保留分離集中式安全環境的目標，並進一步強調職責分離、最低權限和團隊指派的潛在簡單性。如果您使用的是 AWS Control Tower，它會限制在安全 OU AWS 帳戶 下建立其他 。

安全服務的委派管理員

Security Tooling 帳戶是 中以管理員/成員結構管理之安全服務的管理員帳戶 AWS 帳戶。如前所述，這會透過 AWS Organizations 委派的管理員功能來處理。 AWS SRA 中目前支援委派管理員的服務包括根存取 AWS Config AWS Firewall Manager、、Amazon GuardDuty、IAM Access Analyzer、Amazon Macie、 AWS Security Hub、 AWS Security Hub CSPM、Amazon Detective AWS Audit Manager、Amazon Inspector AWS CloudTrail和 的 IAM 集中管理 AWS Systems Manager。您的安全團隊會管理這些服務的安全功能，並監控任何安全特定的事件或問題清單。

AWS IAM Identity Center 支援將管理委派給成員帳戶。 AWS SRA 使用共用服務帳戶做為 IAM Identity Center 的委派管理員帳戶，如共用服務帳戶的 IAM Identity Center 一節稍後所述。

集中式根存取

Security Tooling 帳戶 是 IAM 集中管理根存取功能的委派管理員帳戶。 此功能必須在組織層級啟用，方法是在成員帳戶中啟用登入資料管理和特權根動作。委派的管理員必須明確獲得`sts:AssumeRoot`許可，才能代表成員帳戶採取特權根動作。只有在組織管理或委派管理員帳戶中啟用成員帳戶中的特權根動作之後，才能使用此許可。透過此許可，使用者可以在成員帳戶上執行特權根使用者任務，而這些任務集中來自安全工具帳戶。啟動特權工作階段後，您可以刪除設定錯誤的 S3 儲存貯體政策、刪除設定錯誤的 SQS 佇列政策、刪除成員帳戶的根使用者憑證，以及為成員帳戶重新啟用根使用者憑證。您可以使用 AWS Command Line Interface (AWS CLI) 或透過 APIs 從主控台執行這些動作。

AWS CloudTrail

AWS CloudTrail 是一項服務，可支援您 中活動的控管、合規和稽核 AWS 帳戶。使用 CloudTrail，您可以記錄、持續監控和保留 AWS 與基礎設施中動作相關的帳戶活動。CloudTrail 已與 整合 AWS Organizations，該整合可用來建立單一線索，記錄組織中所有帳戶 AWS 的所有事件。這類線索稱為組織線索。您只能從組織的管理帳戶中或從委派管理員帳戶建立和管理組織線索。當您建立組織線索時，會在屬於您 AWS 組織的每個 中建立具有您指定名稱 AWS 帳戶 的線索。線索會記錄 AWS 組織中所有帳戶的活動，包括管理帳戶，並將日誌存放在單一 S3 儲存貯體中。由於此 S3 儲存貯體的敏感度，您應該遵循本指南稍後的 Amazon S3 作為中央日誌存放區一節中概述的最佳實務來保護它。 AWS 組織中的所有帳戶都可以在其線索清單中查看組織線索。不過，成員 AWS 帳戶 只能檢視此線索。根據預設，當您在 CloudTrail 主控台中建立組織追蹤時，該追蹤是多區域追蹤。如需其他安全最佳實務，請參閱 CloudTrail 文件。

在 AWS SRA 中，安全工具帳戶是管理 CloudTrail 的委派管理員帳戶。用於存放組織追蹤日誌的對應 S3 儲存貯體會在 Log Archive 帳戶中建立。這是為了區隔 CloudTrail 日誌權限的管理和使用。如需有關如何建立或更新 S3 儲存貯體以存放組織追蹤日誌檔案的資訊，請參閱 CloudTrail 文件。作為安全最佳實務， `aws:SourceArn` 請將組織追蹤的條件索引鍵新增至 S3 儲存貯體 （以及 KMS 索引鍵或 SNS 主題等任何其他資源） 的資源政策。這可確保 S3 儲存貯體僅接受與特定追蹤相關聯的資料。線索是使用日誌檔案驗證來設定日誌檔案完整性驗證。日誌和摘要檔案會使用 SSE-KMS 加密。組織追蹤也會與 CloudWatch Logs 中的日誌群組整合，以傳送事件以進行長期保留。

> **Note**
>
> 您可以從管理和委派的管理員帳戶建立和管理組織追蹤。不過，最佳實務是，您應該限制對管理帳戶的存取，並使用可用的委派管理員功能。

> **設計考量**
>
> - CloudTrail 預設不會記錄資料事件，因為這些通常是大量活動。不過，您應該擷取特定關鍵 AWS 資源的資料事件，例如 S3 儲存貯體、Lambda 函數、從外部 AWS 傳送至 CloudTrail 湖的日誌事件，以及 SNS 主題。若要這樣做，請指定每個個別資源ARNs，以設定您的組織追蹤來包含來自特定資源的資料事件。
> - 如果成員帳戶需要存取自己帳戶的 CloudTrail 日誌檔案，您可以選擇從中央 S3 儲存貯體共用組織的 CloudTrail 日誌檔案。不過，如果成員帳戶需要本機 Amazon CloudWatch 日誌群組做為其帳戶的 CloudTrail 日誌，或想要設定與組織追蹤不同的日誌管理和資料事件 （唯

讀、唯讀、管理事件、資料事件），則可以使用適當的控制項建立本機追蹤。本機帳戶特定的追蹤會產生額外費用。

AWS Security Hub CSPM

AWS Security Hub 雲端安全狀態管理 (AWS Security Hub CSPM) 先前稱為 AWS Security Hub，可讓您全面檢視 中的安全狀態 AWS ，並協助您根據安全產業標準和最佳實務檢查環境。Security Hub CSPM 會跨 AWS 整合服務、支援的第三方產品，以及您可能使用的其他自訂安全產品，從 收集安全資料。它可協助您持續監控和分析安全趨勢，並識別最高優先級的安全問題。除了擷取來源之外，Security Hub CSPM 還會產生自己的調查結果，這些調查結果是由對應至一或多個安全標準的安全控制項所表示。這些標準包括 AWS 基礎安全最佳實務 (FSBP)、網際網路安全中心 (CIS) AWS 基準測試 1.20 版和 1.4.0 版、國家標準技術研究所 (NIST) SP 800-53 修訂版 5、支付卡產業資料安全標準 (PCI DSS) 和服務受管標準。如需目前安全標準和特定安全控制詳細資訊的清單，請參閱 Security Hub CSPM 文件中的 Security Hub CSPM 標準參考。

Security Hub CSPM 與 整合 AWS Organizations ，可簡化 AWS 組織中所有現有和未來帳戶的安全狀態管理。您可以使用委派管理員帳戶的 Security Hub CSPM 中央組態功能 （在此案例中為安全工具），指定如何在您的組織帳戶和跨區域的組織單位 (OUs) 中設定 Security Hub CSPM 服務、安全標準和安全控制。 您可以從一個主要區域透過幾個步驟來設定這些設定，稱為 主要區域。如果您不使用中央組態，則必須在每個帳戶和區域中分別設定 Security Hub CSPM。委派管理員可以將帳戶和 OUs 指定為自我管理，成員可以在每個區域中分別設定設定，也可以指定 為集中管理，委派管理員可以在區域中設定成員帳戶或 OU。您可以將組織中的所有帳戶和 OUs 指定為集中管理、所有自我管理或兩者的組合。這可簡化一致性組態的強制執行，同時提供為每個 OU 和帳戶修改組態的彈性。

Security Hub CSPM 委派管理員帳戶也可以檢視所有成員帳戶的調查結果、檢視洞見和控制詳細資訊。您也可以在委派的管理員帳戶中指定彙總區域，以集中您帳戶和連結區域的調查結果。您的問題清單會在彙總工具區域與所有其他區域之間持續雙向同步。

Security Hub CSPM 支援與數個 整合 AWS 服務。Amazon GuardDuty AWS Config、Amazon Macie、IAM Access Analyzer AWS Firewall Manager、Amazon Inspector、 Amazon Route 53 Resolver DNS Firewall 和 AWS Systems Manager 修補程式管理員可以將問題清單饋送至 Security Hub CSPM。Security Hub CSPM 會使用稱為安全調查結果格式 AWS (ASFF) 的標準格式來處理調查結果。Security Hub CSPM 會關聯整合產品的調查結果，以排定最重要的問題清單優先順序。您可以充實 Security Hub CSPM 調查結果的中繼資料，以協助更完善內容化、排定優先順序，並對安全調查結果採取動作。此擴充功能會將資源標籤、新的 AWS 應用程式標籤和帳戶名稱資訊新增至擷取至 Security Hub CSPM 的每個調查結果。這可協助您微調自動化規則的問題清單、搜尋或篩選問題清單和洞見，以及依應用程式評估安全狀態。此外，您可以使用自動化規則自動更新問題清單。當 Security

Hub CSPM 擷取問題清單時，可以套用各種規則動作，例如隱藏問題清單、變更問題清單的嚴重性，以及新增問題清單的備註。這些規則動作會在問題清單符合您指定的條件時生效，例如與問題清單相關聯的資源或帳戶 IDs，或其標題。您可以使用自動化規則來更新 ASFF 中的選取問題清單欄位。規則同時適用於新的和更新的調查結果。

在調查安全事件期間，您可以從 Security Hub CSPM 導覽至 Amazon Detective，以調查 GuardDuty 調查結果。Security Hub CSPM 建議針對 Detective（當它們存在時）等服務調整委派管理員帳戶，以便更順暢地整合。例如，如果您未在 Detective 和 Security Hub CSPM 之間對齊管理員帳戶，則從調查結果導覽至 Detective 將無法運作。如需完整清單，請參閱 Security Hub CSPM 文件中的 Security Hub CSPM AWS 服務 整合概觀。

您可以使用 Security Hub CSPM 搭配 Amazon VPC 的網路存取分析器功能，以協助持續監控 AWS 網路組態的合規性。這可協助您封鎖不需要的網路存取，並協助防止關鍵資源外部存取。如需進一步的架構和實作詳細資訊，請參閱 AWS 部落格文章使用 Amazon VPC Network Access Analyzer 和 持續驗證網路合規 AWS Security Hub CSPM。

除了監控功能之外，Security Hub CSPM 還支援與 Amazon EventBridge 整合，以自動修復特定問題清單。您可以定義在收到問題清單時要採取的自訂動作。例如，您可以設定自訂動作，將問題清單傳送到售票系統或自動化修補系統。如需其他討論和範例，請參閱 AWS 部落格文章使用 自動化回應和修復 AWS Security Hub CSPM，以及如何部署 Security Hub CSPM 自動化回應和修復 AWS 的解決方案。

Security Hub CSPM 使用服務連結 AWS Config 規則 來執行其控制項的大部分安全檢查。若要支援這些控制項， AWS Config 必須在啟用 Security Hub CSPM 的每個帳戶中啟用所有帳戶，包括管理員（或委派管理員）帳戶和成員帳戶。 AWS 區域

設計考量

- 如果 PCI-DSS 等合規標準已存在於 Security Hub CSPM 中，則全受管 Security Hub CSPM 服務是最簡單的操作方式。不過，如果您想要組合自己的合規或安全標準，其中可能包括安全性、操作或成本最佳化檢查， AWS Config 一致性套件可提供簡化的自訂程序。（如需 AWS Config 和 一致性套件的詳細資訊，請參閱 AWS Config一節。）
- Security Hub CSPM 的常見使用案例包括下列項目：
  - 作為儀表板，可讓應用程式擁有者查看其 AWS 資源的安全性和合規狀態
  - 作為安全操作、事件回應者和威脅獵人使用的安全調查結果的集中檢視，對 和 區域 AWS 的安全和合規調查結果進行分類 AWS 帳戶 和採取行動
  - 若要從 AWS 帳戶 和 區域彙總安全性和合規調查結果，並將其路由至集中式安全性資訊和事件管理 (SIEM) 或其他安全性協同運作系統

如需這些使用案例的其他指導，包括如何設定這些使用案例，請參閱部落格文章三個週期性 Security Hub CSPM 使用模式，以及如何部署這些使用案例。

實作範例

AWS SRA 程式碼庫提供 Security Hub CSPM 的範例實作。它包括自動啟用服務、將管理委派給成員帳戶（安全工具），以及為 AWS 組織中所有現有和未來帳戶啟用 Security Hub CSPM 的組態。

AWS Security Hub

AWS Security Hub 是一種統一的雲端安全解決方案，可優先考慮您的關鍵安全威脅，並協助您大規模回應。Security Hub 透過自動關聯和豐富來自多個來源的安全訊號，例如狀態管理 (AWS Security Hub CSPM)、漏洞管理 (Amazon Inspector)、敏感資料 (Amazon Macie) 和威脅偵測 (Amazon GuardDuty)，以近乎即時的方式偵測安全問題。這可讓安全團隊透過自動化分析和情境洞察，優先考慮其雲端環境中的主動風險。Security Hub 提供潛在攻擊路徑的視覺化呈現，攻擊者可以利用這些路徑來存取與公開調查結果相關聯的資源。這會將複雜的安全訊號轉換為可行的洞察，讓您可以快速做出有關安全性的明智決策。

Security Hub 經過策略性重新設計，可簡化相關安全服務建置區塊的啟用，以達成安全成果。透過近乎即時地將威脅矩陣中的安全調查結果與不同安全訊號相互關聯，您可以優先考慮最關鍵的風險。調查結果與偵測與 AWS 資源相關聯的暴露相關。暴露在安全控制、設定錯誤或其他可能被作用中威脅利用的領域中代表更廣泛的弱點。例如，暴露可能是可從網際網路連線的 EC2 執行個體，且具有高入侵可能性的軟體漏洞。

Security Hub 和 Security Hub CSPM 是補充服務。Security Hub CSPM 可全面檢視您的安全狀態，並協助您根據安全產業標準和最佳實務評估雲端環境。 Security Hub 提供統一的體驗，協助您排定優先順序並回應重大安全問題。Security Hub CSPM 調查結果會自動路由到 Security Hub，它們與其他安全服務的問題清單相關聯，例如 Amazon Inspector，以產生公開。這可協助您識別環境中最關鍵的風險。

Security Hub 也會依類型和相關聯的調查結果，提供 AWS 環境中資源的摘要。資源的優先順序是公開和攻擊序列。選擇資源類型時，您可以檢閱與該資源類型相關聯的所有資源。

為了獲得最佳體驗，我們建議您啟用 Security Hub 和 Security Hub CSPM，以及啟用這些其他安全服務：Amazon GuardDuty、Amazon Inspector 和 Amazon Macie。您可以使用 Security Hub 涵蓋範圍調查結果，了解所有組織的成員帳戶是否統一啟用這些服務和功能。

在 AWS SRA 中，安全工具帳戶做為 Security Hub、Security Hub CSPM 和其他 AWS 安全服務的委派管理員。在安全工具帳戶中，您可以檢視與成員帳戶相關聯的所有資源。您也可以 AWS 區域 從連結檢視您家中的所有資源 AWS 區域。

實作備註

啟用 Security Hub 需要三個步驟，包括考慮先前是否啟用 Security Hub CSPM 的程序。Security Hub 原生與 整合 AWS Organizations，可簡化組態和實作程序，並將所有調查結果集中並彙總到單一位置。根據 AWS SRA 最佳實務，使用 Security Tooling 帳戶做為委派管理員帳戶來管理和設定 Security Hub。使用 Security Hub 組態設定自動啟用所有區域、OUs 和帳戶，包括未來的區域和帳戶。您也應該設定跨區域彙總，將多個 的問題清單、資源和趨勢彙總 AWS 區域 到單一主區域。在組態期間，您也可以啟用任何原生整合，例如 Jira Cloud 或 ServiceNow。

設計考量

- Security Hub 調查結果在開放網路安全結構描述架構 (OCSF) 中格式化。Security Hub 在 OCSF 中產生調查結果，並從 Security Hub CSPM 和其他 收到 OCSF 中的調查結果 AWS 服務。這些 OCSF 調查結果可以透過 Amazon EventBridge 傳送以進行自動化，或存放在中央日誌彙總帳戶中，以執行安全日誌分析和保留。
- AWS 組織管理帳戶無法將自己指定為 Security Hub 中的委派管理員。這符合將安全工具帳戶指定為委派管理員的 AWS SRA 最佳實務。另請注意：
  - Security Hub CSPM 的指定管理員帳戶會自動成為 Security Hub 的指定管理員。
  - 透過 Security Hub 移除委派管理也會移除 Security Hub CSPM 的委派管理。同樣地，透過 Security Hub CSPM 移除委派的管理也會為 Security Hub 移除它。
- Security Hub 包含根據您的規格自動修改問題清單並對其採取動作的功能，Security Hub 支援下列類型的自動化：
  - 自動化規則會根據定義的條件，以近乎即時的方式自動更新問題清單、隱藏問題清單，以及將問題清單傳送至票證工具。
  - 自動化回應和修復，這會建立自訂 EventBridge 規則，定義針對特定調查結果和洞見採取的自動動作。

- Security Hub 可以透過政策在所有成員帳戶和區域中設定 Amazon Inspector，也可以透過部署設定 GuardDuty 和 Security Hub CSPM。政策會為帳戶和區域 產生 AWS Organizations 政策。部署 是一次性動作，可在所選帳戶和區域中啟用安全功能。部署不適用於新啟用的帳戶。或者，您可以在 GuardDuty 和 Security Hub CSPM 中為新成員帳戶自動啟用功能。

Amazon GuardDuty

Amazon GuardDuty 是一種威脅偵測服務，可持續監控惡意活動和未經授權的行為，以保護 AWS 帳戶 和 工作負載。您必須一律為監控和稽核目的擷取和存放適當的日誌，但 GuardDuty 會直接從 AWS CloudTrail Amazon VPC 流程日誌和 AWS DNS 日誌提取獨立的資料串流。您不需要管理 Amazon S3 儲存貯體政策或修改收集和存放日誌的方式。GuardDuty 許可是以服務連結角色管理，您可以透過停用 GuardDuty 隨時撤銷。這可讓您輕鬆地在沒有複雜組態的情況下啟用服務，並消除 IAM 許可修改或 S3 儲存貯體政策變更會影響服務操作的風險。

除了提供基礎資料來源之外，GuardDuty 還提供選用功能來識別安全問題清單。其中包括 EKS 保護、RDS 保護、S3 保護、惡意軟體保護和 Lambda 保護。對於新的偵測器，這些選用功能預設為啟用，但 EKS 保護除外，必須手動啟用。

- 透過 GuardDuty S3 保護，除了預設 CloudTrail 管理事件之外，GuardDuty 還會監控 CloudTrail 中的 Amazon S3 資料事件。監控資料事件可讓 GuardDuty 監控物件層級 API 操作，以找出 S3 儲存貯體內資料的潛在安全風險。
- GuardDuty 惡意軟體防護透過在連接的 Amazon Elastic Block Store (Amazon EBS) 磁碟區上啟動無代理程式掃描，來偵測 Amazon EC2 執行個體或容器工作負載上是否存在惡意軟體。GuardDuty 也會掃描新上傳的物件或現有物件的新版本，以偵測 S3 儲存貯體中的潛在惡意軟體。
- GuardDuty RDS Protection 旨在分析和監控 Amazon Aurora 資料庫的存取活動，而不會影響資料庫效能。
- GuardDuty EKS 保護包括 EKS 稽核日誌監控和 EKS 執行期監控。透過 EKS 稽核日誌監控，GuardDuty 會從 Amazon EKS 叢集監控 Kubernetes 稽核日誌，並分析這些日誌是否有潛在的惡意和可疑活動。EKS 執行期監控使用 GuardDuty 安全代理程式 (Amazon EKS 附加元件） 來提供個別 Amazon EKS 工作負載的執行期可見性。GuardDuty 安全代理程式可協助識別 Amazon EKS 叢集中可能遭到入侵的特定容器。它也可以偵測將權限從個別容器提升到基礎 Amazon EC2 主機或更廣泛 AWS 環境的嘗試。

GuardDuty 也提供稱為延伸威脅偵測的功能，可自動偵測跨資料來源、多種 AWS 資源類型和 內時間的多階段攻擊 AWS 帳戶。GuardDuty 會將這些稱為訊號的事件相互關聯，以識別對 AWS 環境造成潛

在威脅的案例，然後產生攻擊序列調查結果。這涵蓋與 AWS 憑證濫用相關的威脅案例，以及 中的資料入侵嘗試 AWS 帳戶。 GuardDuty 會將所有攻擊序列調查結果類型視為 關鍵。此功能預設為啟用，而且沒有與其相關聯的額外費用。

在 AWS SRA 中，GuardDuty 會透過 在所有帳戶中啟用 AWS Organizations，且 GuardDuty 委派管理員帳戶中的適當安全團隊（在此案例中為安全工具帳戶）可檢視和操作所有調查結果。GuardDuty 作用中調查結果會匯出至 Log Archive 帳戶中的中央 S3 儲存貯體，因此您可以將調查結果保留超過 90 天。問題清單會從委派的管理員帳戶匯出，並包含相同區域中相關聯成員帳戶的所有問題清單。S3 儲存貯體中的調查結果會使用 AWS KMS 客戶受管金鑰加密。S3 儲存貯體政策和 KMS 金鑰政策設定為僅允許 GuardDuty 使用資源。

啟用 AWS Security Hub CSPM 時，GuardDuty 調查結果會自動流向 Security Hub CSPM 和 Security Hub。啟用 Amazon Detective 時，GuardDuty 調查結果會包含在 Detective 日誌擷取程序中。GuardDuty 和 Detective 支援跨服務使用者工作流程，其中 GuardDuty 提供從主控台的連結，將您從選取的調查結果重新導向至 Detective 頁面，其中包含一組精選的視覺化效果，用於調查該調查結果。例如，您也可以將 GuardDuty 與 Amazon EventBridge 整合，以自動化 GuardDuty 的最佳實務，例如自動回應新的 GuardDuty 調查結果。

> **實作範例**
>
> AWS SRA 程式碼庫提供 GuardDuty 的範例實作。它包含組織中所有現有和未來帳戶的加密 S3 儲存貯體組態、委派管理和 GuardDuty 啟用 AWS 。

AWS Config

AWS Config 是一項服務，可讓您評估、稽核和評估 中支援 AWS 資源的組態 AWS 帳戶。 AWS Config 會持續監控和記錄 AWS 資源組態，並根據所需的組態自動評估記錄的組態。您也可以 AWS Config 與其他 服務整合，在自動化稽核和監控管道中執行繁重工作。例如， AWS Config 可以監控 中個別秘密的變更 AWS Secrets Manager。

您可以使用 來評估 AWS 資源的組態設定AWS Config 規則。 AWS Config 提供可自訂的預先定義規則程式庫，稱為 受管規則，或者您可以撰寫自己的自訂規則。您可以 AWS Config 規則 主動模式（在部署資源之前）或偵測模式（在部署資源之後）執行 。當發生組態變更、定期排程或兩者同時發生時，即可評估資源。

一致性套件是 AWS Config 規則和修補動作的集合，可部署為帳戶和區域中或組織中的單一實體 AWS Organizations。一致性套件是透過撰寫包含 AWS Config 受管或自訂規則和修復動作清單的 YAML 範本來建立。若要開始評估您的 AWS 環境，請使用其中一個範例一致性套件範本。

AWS Config 與 整合 AWS Security Hub CSPM ，將 AWS Config 受管和自訂規則評估的結果作為調查結果傳送至 Security Hub CSPM。

AWS Config 規則 可與 搭配使用 AWS Systems Manager ，以有效修復不合規的資源。您可以使用 Systems Manager Explorer 來收集 AWS 帳戶 跨 中規則的 AWS Config 合規狀態， AWS 區域 然後使用 Systems Manager Automation 文件（執行手冊） 來解決不合規 AWS Config 的規則。如需實作詳細資訊，請參閱部落格文章AWS Config 使用 AWS Systems Manager Automation Runbook 修復不合規規則。

AWS Config 彙整工具會跨多個帳戶、區域和組織收集組態和合規資料 AWS Organizations。彙總工具儀表板會顯示彙總資源的組態資料。庫存和合規儀表板提供組織跨 AWS 帳戶、跨 AWS 區域或內部 AWS AWS 資源組態和合規狀態的基本和最新資訊。它們可讓您視覺化和評估 AWS 資源庫存，而無需撰寫 AWS Config 進階查詢。 您可以取得基本洞見，例如資源的合規摘要、擁有不合規資源的前 10 個帳戶、按類型比較執行和停止的 EC2 執行個體，以及按磁碟區類型和大小的 EBS 磁碟區。

如果您使用 AWS Control Tower 來管理您的 AWS 組織，則會將一組 AWS Config 規則部署為偵測性護欄（分類為強制性、強烈建議或選擇性）。這些護欄可協助您管理 資源，並監控 AWS 組織中帳戶之間的合規性。這些 AWS Config 規則會自動使用值為 的`aws-control-tower`標籤`managed-by-control-tower`。

AWS Config 必須針對 AWS 組織中的每個成員帳戶啟用 AWS 區域 ，其中包含您要保護的資源。您可以集中管理 （例如，建立、更新和刪除） AWS 組織內所有帳戶的 AWS Config 規則。從 AWS Config 委派管理員帳戶，您可以跨所有帳戶部署一組常見的 AWS Config 規則，並指定不應建立 AWS Config 規則的帳戶。 AWS Config 委派管理員帳戶也可以彙總來自所有成員帳戶的資源組態和合規資料，以提供單一檢視。使用委派管理員帳戶的 APIs 來強制執行控管，方法是確保 AWS 組織中的成員帳戶無法修改基礎 AWS Config 規則。如果 Security Hub CSPM 已啟用且至少有一個 AWS Config 受管或自訂規則存在 AWS Security Hub CSPM， AWS Config 則 會原生整合以傳送問題清單至 。

在 AWS SRA 中， AWS Config 委派的管理員帳戶是安全工具帳戶。 AWS Config 交付管道設定為在 Log Archive 帳戶中的集中式 S3 儲存貯體中交付資源組態快照。由於 Log Archive 帳戶是中央日誌儲存庫，因此會用來存放資源組態。

設計考量

- AWS Config 會將組態和合規變更通知串流至 Amazon EventBridge。這表示您可以使用 EventBridge 中的原生篩選功能來篩選AWS Config 事件，以便將特定類型的通知路由到特定目標。例如，您可以將特定規則或資源類型的合規通知傳送至特定電子郵件地址，或將組態變更通知路由至外部 IT 服務管理 (ITSM) 或組態管理資料庫 (CMDB) 工具。如需詳細資訊，請參閱部落格文章AWS Config 最佳實務。

- 除了使用 AWS Config 主動規則評估之外，您還可以使用 AWS CloudFormation Guard，這是一種policy-as-code評估工具，可主動檢查資源組態合規性。 AWS CloudFormation Guard 命令列界面 (CLI) 為您提供宣告性、網域特定語言 (DSL)，可用來將政策表達為程式碼。此外，您可以使用 AWS CLI 命令來驗證 JSON 格式或 YAML 格式的結構化資料，例如 CloudFormation 變更集、JSON 型 Terraform 組態檔案或 Kubernetes 組態。您可以使用 AWS CloudFormation Guard CLI 做為撰寫程序的一部分，在本機執行評估，或在部署管道中執行評估。如果您有AWS Cloud Development Kit (AWS CDK)應用程式，您可以使用 cdk-nag 主動檢查最佳實務。

實作範例

AWS SRA 程式碼庫提供範例實作，可將一致性套件部署至 AWS 組織內的所有 AWS Config AWS 帳戶 和 區域。AWS Config 彙總器模組可協助您設定彙總器，方法是將管理委派給組織管理帳戶中的成員帳戶 AWS Config （安全工具），然後為組織中所有現有和未來的帳戶 AWS 在委派管理員帳戶中設定 AWS Config 彙總器。您可以使用 AWS Config Control Tower 管理帳戶模組在組織管理帳戶 AWS Config 內啟用 – 它未由 啟用 AWS Control Tower。

Amazon Security Lake

Amazon Security Lake 是全受管的安全資料湖服務。您可以使用 Security Lake 自動集中來自 AWS 環境、軟體即服務 (SaaS) 供應商、內部部署和第三方來源的安全資料。Security Lake 可協助您建置標準化的資料來源，以簡化對安全資料的分析工具使用，因此您可以更完整地了解整個組織的安全狀態。資料湖由 Amazon Simple Storage Service (Amazon S3) 儲存貯體提供支援，您可以保留資料的所有權。Security Lake 會自動收集 日誌 AWS 服務，包括 Amazon VPC AWS CloudTrail、Amazon Route 53、Amazon S3 AWS Lambda、Amazon EKS 稽核日誌、 AWS Security Hub CSPM 調查結果和 AWS WAF 日誌。

AWS SRA 建議您使用 Log Archive 帳戶做為 Security Lake 的委派管理員帳戶。如需設定委派管理員帳戶的詳細資訊，請參閱 Security OU – Log Archive 帳戶區段中的 Amazon Security Lake。想要存取 Security Lake 資料或需要能夠使用自訂擷取、轉換和載入 (ETL) 函數將 非原生 日誌寫入 Security Lake 儲存貯體的安全團隊應在安全工具帳戶中操作。

Security Lake 可以從不同的雲端供應商、第三方解決方案的日誌或其他自訂日誌收集日誌。我們建議您使用安全工具帳戶來執行 ETL 函數，將日誌轉換為開放網路安全結構描述架構 (OCSF) 格式，並以 Apache Parquet 格式輸出檔案。Security Lake 會建立具有安全工具帳戶適當許可的跨帳戶角色，以及 Lambda 函數或 AWS Glue 爬蟲程式支援的自訂來源，以將資料寫入 Security Lake 的 S3 儲存貯體。

Security Lake 管理員應設定使用 Security Tooling 帳戶的安全團隊，並要求存取 Security Lake 收集為訂閱者的日誌。 Security Lake 支援兩種類型的訂閱者存取：

- 資料存取 – 訂閱者可以直接存取 Security Lake 的 Amazon S3 物件。Security Lake 會管理基礎設施和許可。當您將 Security Tooling 帳戶設定為 Security Lake 資料存取訂閱者時，系統會透過 Amazon Simple Queue Service (Amazon SQS) 通知該帳戶 Security Lake 儲存貯體中的新物件，而 Security Lake 會建立存取這些新物件的許可。
- 查詢存取 – 訂閱者可以使用 Amazon Athena 等服務，從 S3 儲存貯體中的 AWS Lake Formation 資料表查詢來源資料。使用 Lake Formation 自動設定查詢存取的跨帳戶存取。當您將 Security Tooling 帳戶設定為 Security Lake 查詢存取訂閱者時，帳戶會獲得 Security Lake 帳戶中日誌的唯讀存取權。當您使用此訂閱者類型時，Athena 和 AWS Glue 資料表會透過 AWS Resource Access Manager () 從 Security Lake Log Archive 帳戶與 Security Tooling 帳戶共用AWS RAM。若要啟用此功能，您必須將 跨帳戶資料共用設定更新 為第 3 版。

如需建立訂閱者的詳細資訊，請參閱 Security Lake 文件中的訂閱者管理。

如需擷取自訂來源的最佳實務，請參閱 Security Lake 文件中的從自訂來源收集資料。

您可以使用 Amazon Quick Sight、Amazon OpenSearch Service 和 Amazon SageMaker，針對存放在 Security Lake 中的安全資料設定分析。

> **設計考量事項**
>
> 如果應用程式團隊需要查詢 Security Lake 資料的存取權以滿足業務需求，Security Lake 管理員應將該應用程式帳戶設定為 訂閱者。

Amazon Macie

Amazon Macie 是全受管的資料安全和資料隱私權服務，使用機器學習和模式比對來探索和協助保護您的敏感資料 AWS。您需要識別工作負載正在處理的資料類型和分類，以確保強制執行適當的控制。您可以使用 Macie 以兩種方式自動化敏感資料的探索和報告：透過執行自動化敏感資料探索，以及透過建立和執行敏感資料探索任務。透過自動敏感資料探索，Macie 會每天評估您的 S3 儲存貯體庫存，並使用抽樣技術來識別和選取儲存貯體中的代表性 S3 物件。然後，Macie 會擷取和分析選取的物件，檢查它們是否有敏感資料。敏感資料探索任務可提供更深入且更具針對性的分析。使用此選項，您可以定義分析的廣度和深度，包括要分析的 S3 儲存貯體、取樣深度，以及衍生自 S3 物件屬性的自訂條件。如果 Macie 偵測到儲存貯體安全性或隱私權的潛在問題，它會為您建立政策調查結果。根據預設，所有新的 Macie 客戶都會啟用自動資料探索，而現有的 Macie 客戶只要按一下即可啟用。

Macie 已透過 在所有帳戶中啟用 AWS Organizations。在委派管理員帳戶中具有適當許可的委託人（在此案例中為安全工具帳戶）可以在任何帳戶中啟用或停用 Macie、為成員帳戶擁有的儲存貯體建立敏感資料探索任務，以及檢視所有成員帳戶的所有政策調查結果。敏感資料調查結果只能由建立敏感調查結果任務的帳戶檢視。如需詳細資訊，請參閱 Macie 文件中的以組織身分管理多個 Macie 帳戶。

Macie 調查結果會流向 AWS Security Hub CSPM 以供檢閱和分析。Macie 也與 Amazon EventBridge 整合，以促進對警示、安全資訊和事件管理 (SIEM) 系統摘要和自動化修復等問題清單的自動回應。

設計考量

- 如果 S3 物件使用您管理的 AWS Key Management Service (AWS KMS) 金鑰加密，您可以將 Macie 服務連結角色新增為該 KMS 金鑰的金鑰使用者，讓 Macie 掃描資料。
- Macie 已針對掃描 Amazon S3 中的物件進行最佳化。因此，任何可放置在 Amazon S3（永久或暫時）的 Macie 支援物件類型都可以掃描敏感資料。這表示來自其他來源的資料，例如，Amazon Relational Database Service (Amazon RDS) 或 Amazon Aurora 資料庫的定期快照匯出、 匯出的 Amazon DynamoDB 資料表，或從原生或第三方應用程式擷取的文字檔案，可以移至 Amazon S3 並由 Macie 評估。

實作範例

AWS SRA 程式碼庫提供 Amazon Macie 的範例實作。它包括將管理委派給成員帳戶，以及在委派管理員帳戶中為 AWS 組織中所有現有和未來的帳戶設定 Macie。Macie 也設定為將調查結果傳送至使用 中客戶受管金鑰加密的中央 S3 儲存貯體 AWS KMS。

IAM Access Analyzer

隨著您加速 AWS 雲端 採用旅程並繼續創新，維持對精細存取（許可）的嚴格控制、包含存取擴散，並確保有效使用許可至關重要。過多和未使用的存取會帶來安全挑戰，並使企業更難以強制執行最低權限原則。此原則是重要的安全架構支柱，涉及持續調整適當大小的 IAM 許可，以平衡安全需求與操作和應用程式開發需求。這項工作涉及多個利益相關者角色，包括中央安全與雲端卓越中心 (CCoE) 團隊以及分散式開發團隊。

AWS Identity and Access Management Access Analyzer 提供工具，透過移除未使用的存取權來有效設定精細許可、驗證預期許可和精簡許可，以協助您符合企業安全標準。它可讓您透過儀表板 和 ，查看對 AWS 資源的外部和內部存取，以及未使用的存取問題 清單AWS Security Hub CSPM。此外，它支援 Amazon EventBridge 以事件為基礎的自訂通知和修復工作流程。

IAM Access Analyzer 外部存取分析器調查結果功能可協助您識別 AWS 組織和帳戶中與外部實體共用的資源，例如 Amazon S3 儲存貯體或 IAM 角色。您選擇的 AWS 組織或帳戶稱為信任區域。分析器使用 自動推理 來分析信任區域內所有 支援的資源 ，並為可以從信任區域外存取資源的主體產生調查結果。這些調查結果有助於識別與外部實體共用的資源，並在部署資源許可之前，協助您預覽政策如何影響對資源的公有和跨帳戶存取。這可免費使用。

同樣地，IAM Access Analyzer 內部存取分析器調查結果功能可協助您識別 AWS 組織和帳戶中與組織或帳戶內部主體共用的資源。此分析透過確保您指定的資源只能由組織內的預期主體存取，來支援最低權限原則。這是付費功能，需要明確設定資源才能檢查。謹慎使用此功能來監控特定的敏感資源，根據設計，這些資源需要鎖定，甚至在內部鎖定。

IAM Access Analyzer 調查結果也可協助您識別組織 AWS 和帳戶中授予的未使用存取權，包括：

- 未使用的 IAM 角色 – 在指定的使用時段內沒有存取活動的角色。
- 未使用的 IAM 使用者、登入資料和存取金鑰 – 屬於 IAM 使用者的登入資料，用於存取 AWS 服務 和資源。
- 未使用的 IAM 政策和許可 – 未在指定用量時段內由角色使用的服務層級和動作層級許可。IAM Access Analyzer 使用連接到角色的身分型政策，來判斷這些角色可以存取的服務和動作。分析器會針對所有服務層級許可，提供未使用的許可的檢閱。

您可以使用從 IAM Access Analyzer 產生的調查結果，根據組織的政策和安全標準，了解並修復任何非預期或未使用的存取。修復之後，下次分析器執行時，這些調查結果會標記為 已解析 。如果問題清單是刻意的，您可以將其標記為 封存 在 IAM Access Analyzer 中，並優先考慮具有更大安全風險的其他問題清單。此外，您可以設定 封存規則來自動封存特定問題清單。例如，您可以建立封存規則，以針對您定期授予存取權的特定 Amazon S3 儲存貯體，自動封存任何調查結果。

身為建置器，您可以使用 IAM Access Analyzer 在開發和部署 (CI/CD) 程序中稍早執行自動化 IAM 政策檢查 ，以遵循您的公司安全標準。您可以將 IAM Access Analyzer 自訂政策檢查和政策審查與 整合 AWS CloudFormation ，將政策審查自動化，做為開發團隊 CI/CD 管道的一部分。其中包含：

- IAM 政策驗證 – IAM Access Analyzer 會根據 IAM 政策文法和 AWS 最佳實務來驗證您的政策。您可以檢視政策驗證檢查的問題清單，包括安全警告、錯誤、一般警告和政策的建議。目前有超過 100 個 政策驗證檢查 可供使用，並且可以使用 AWS Command Line Interface (AWS CLI) 和 APIs。
- IAM 自訂政策檢查 – IAM Access Analyzer 自訂政策檢查會根據您指定的安全標準驗證您的政策。自訂政策檢查使用自動推理來提供更高層級的保證，以滿足您的公司安全標準。自訂政策檢查的類型包括：

- 檢查參考政策：編輯政策時，您可以將其與參考政策進行比較，例如政策的現有版本，以檢查更新是否授予新的存取權。 CheckNoNewAccess API 會比較兩個政策（更新的政策和參考政策），以判斷更新的政策是否會引入對參考政策的新存取權，並傳回通過或失敗回應。
- 檢查 IAM 動作清單：您可以使用 CheckAccessNotGranted API，確保政策不會授予對安全標準中定義之關鍵動作清單的存取權。此 API 會取得政策和最多 100 個 IAM 動作的清單，以檢查政策是否允許至少一個動作，並傳回通過或失敗回應。

安全團隊和其他 IAM 政策作者可以使用 IAM Access Analyzer 來撰寫符合 IAM 政策文法和安全標準的政策。手動編寫適當大小的政策可能容易出錯且耗時。 IAM Access Analyzer 政策產生 功能可協助根據委託人的存取活動撰寫 IAM 政策。IAM Access Analyzer 會檢閱受支援服務的 AWS CloudTrail 日誌，並產生政策範本，其中包含委託人在指定日期範圍內使用的許可。然後，您可以使用此範本來建立具有精細許可的政策，該許可僅授予必要的許可。

- 您必須啟用 CloudTrail 追蹤，您的帳戶才能根據存取活動產生政策。
- IAM Access Analyzer 不會在產生的政策中識別資料事件的動作層級活動，例如 Amazon S3 資料事件。
- CloudTrail 不會追蹤`iam:PassRole`動作，也不會包含在產生的政策中。

IAM Access Analyzer 透過 中的委派管理員功能部署在 Security Tooling 帳戶中 AWS Organizations。委派管理員具有建立和管理分析器的許可，以 AWS 組織為信任區域。

設計考量事項

若要取得帳戶範圍的問題清單（其中帳戶做為信任的界限），您可以在每個成員帳戶中建立帳戶範圍分析器。這可以作為帳戶管道的一部分來完成。帳戶範圍的問題清單會在成員帳戶層級流入 Security Hub CSPM。從那裡，它們會流向 Security Hub CSPM 委派管理員帳戶（安全工具）。

實作範例

- AWS SRA 程式碼庫提供 IAM Access Analyzer 的範例實作。它示範如何在委派管理員帳戶中設定組織層級分析器，以及在每個帳戶中設定帳戶層級分析器。
- 如需有關如何將自訂政策檢查 整合到建置器工作流程的資訊，請參閱 AWS 部落格文章簡介 IAM Access Analyzer 自訂政策檢查。

AWS Firewall Manager

AWS Firewall Manager 透過簡化跨多個帳戶和資源的 AWS WAF、、Amazon VPC 安全群組和 Amazon Route 53 Resolver DNS AWS Shield Advanced防火牆的管理和維護任務 AWS Network Firewall，協助保護您的網路。使用 Firewall Manager，您只需設定 AWS WAF 防火牆規則、Shield Advanced 保護、Amazon VPC 安全群組、網路防火牆防火牆和 DNS 防火牆規則群組關聯一次。此服務自動在帳號和資源中套用規則和防護，甚至在您新增資源時也可套用。

當您想要保護整個 AWS 組織，而不是少量的特定帳戶和資源，或者您經常新增想要保護的新資源時，防火牆管理員特別有用。Firewall Manager 使用安全政策來定義一組組態，包括必須部署的相關規則、保護和動作，以及要包含或排除的帳戶和資源（以標籤表示）。您可以建立精細且靈活的組態，同時仍然能夠將控制擴展到大量帳戶和 VPCs。即使建立新帳戶和資源，這些政策也會自動且一致地強制執行您設定的規則。Firewall Manager 會透過 在所有帳戶中啟用 AWS Organizations，並由 Firewall Manager 委派管理員帳戶中的適當安全團隊（在此案例中為安全工具帳戶）執行組態和管理。

您必須 AWS Config 為每個包含您要保護之資源 AWS 區域 的 啟用 。如果您不想 AWS Config 為所有資源啟用 ，則必須為與您使用的 Firewall Manager 政策類型相關聯的資源啟用它。當您同時使用 AWS Security Hub CSPM 和 Firewall Manager 時，防火牆管理員會自動將您的問題清單傳送至 Security Hub CSPM。Firewall Manager 會針對不合規的資源及其偵測到的攻擊建立問題清單，並將問題清單傳送至 Security Hub CSPM。當您為 設定 Firewall Manager 政策時 AWS WAF，您可以為所有範圍內帳戶集中啟用 Web 存取控制清單 (Web ACLs) 上的記錄，並將日誌集中在單一帳戶下。

使用 Firewall Manager，您可以有一或多個管理員可以管理組織的防火牆資源。當您指派多個管理員時，您可以套用限制性管理範圍條件來定義每個管理員可以管理的資源（帳戶、OUs、區域、政策類型）。這可讓您彈性地在組織內擁有不同的管理員角色，並協助您維持最低權限存取的主體。 AWS SRA 使用一個管理員，將完整的管理範圍委派給安全工具帳戶。

設計考量事項

AWS 組織中個別成員帳戶的帳戶管理員可以根據其特定需求，在 Firewall Manager 受管服務中設定其他控制項（例如 AWS WAF 規則和 Amazon VPC 安全群組）。

實作範例

AWS SRA 程式碼庫提供 Firewall Manager 的範例實作。它示範委派的管理（安全工具）、部署允許的最大安全群組、設定安全群組政策，以及設定多個 AWS WAF 政策。

Amazon EventBridge

Amazon EventBridge 為無伺服器事件匯流排服務，可讓您直觀地應用程式與來自各種來源的資料互相連線。它經常用於安全自動化。您可以設定路由規則來判斷要將資料傳送到何處，以建置可即時回應所有資料來源的應用程式架構。除了在每個帳戶中使用預設事件匯流排之外，您還可以建立自訂事件匯流排來接收來自自訂應用程式的事件。您可以在安全工具帳戶中建立事件匯流排，該匯流排可以從 AWS 組織中的其他帳戶接收安全特定事件。例如，透過將 AWS Config 規則 Amazon GuardDuty 和 AWS Security Hub CSPM 與 EventBridge 連結，您可以建立彈性的自動化管道來路由安全資料、引發警示和管理動作以解決問題。

設計考量

- EventBridge 能夠將事件路由到許多不同的目標。自動化安全動作的一個重要模式是將特定事件連接到個別 AWS Lambda 回應者，以採取適當的動作。例如，在某些情況下，您可能想要使用 EventBridge 將公有 S3 儲存貯體調查結果路由到 Lambda 回應程式，以更正儲存貯體政策並移除公有許可。這些回應者可以整合到您的調查手冊和執行手冊中，以協調回應活動。
- 成功安全營運團隊的最佳實務是將安全事件和調查結果的流程整合到通知和工作流程系統中，例如票證系統、錯誤/問題系統，或其他安全資訊和事件管理 (SIEM) 系統。這會將工作流程從電子郵件和靜態報告中移除，並協助您路由、升級和管理事件或調查結果。EventBridge 中的彈性路由功能是此整合的強大啟用器。

Amazon Detective

Amazon Detective 透過直接分析、調查和快速識別安全分析師的安全調查結果或可疑活動的根本原因，來支援回應式安全控制策略。Detective 會自動從 AWS CloudTrail 日誌和 Amazon VPC 流程日誌擷取以時間為基礎的事件，例如登入嘗試、API 呼叫和網路流量。Detective 會使用 CloudTrail 日誌和 Amazon VPC 流程日誌的獨立串流來取用這些事件。您可以使用 Detective 存取長達一年的歷史事件資料。Detective 使用機器學習和視覺化來建立統一的互動式檢視，了解資源的行為以及它們之間的互動，這稱為行為圖表。您可以探索行為圖表來檢查不同的動作，例如失敗的登入嘗試或可疑的 API 呼叫。

Detective 與 Amazon Security Lake 整合，讓安全分析師能夠查詢和擷取存放在 Security Lake 中的日誌。您可以使用此整合，從存放在 Security Lake 的 CloudTrail 日誌和 Amazon VPC 流程日誌取得其他資訊，同時在 Detective 中進行安全調查。

Detective 也會擷取 Amazon GuardDuty 偵測到的問題清單，包括 GuardDuty 執行期監控偵測到的威脅。當帳戶啟用 Detective 時，它會成為行為圖表的管理員帳戶。在您嘗試啟用 Detective 之前，請確定您的帳戶已在 GuardDuty 中註冊至少 48 小時。如果您不符合此要求，則無法啟用 DetectiveDetective。

Detective 的其他選用資料來源包括 Amazon EKS 稽核日誌和 AWS Security Hub CSPM。Amazon EKS 稽核日誌資料來源可增強下列實體類型的相關資訊：Amazon EKS 叢集、Kubernetes Pod、容器映像和 Kubernetes 主體。Security Hub 資料來源是AWS 安全調查結果的一部分，它會將跨產品的調查結果關聯至 Security Hub，並將其擷取至 Detective。

Detective 會自動將多個與單一安全性入侵事件相關的調查結果分組為調查結果群組。威脅執行者通常會執行一系列動作，導致多個安全性問題清單分散在時間和資源中。因此，調查結果群組應該是涉及多個實體和調查結果的調查起點。Detective 也會使用生成式 AI 來提供調查結果群組摘要，該 AI 會自動分析調查結果群組，並以自然語言提供洞見，以協助您 加速安全調查。

Detective 與 整合 AWS Organizations。Org Management 帳戶會將成員帳戶委派為 Detective 管理員帳戶。在 AWS SRA 中，這是安全工具帳戶。Detective 管理員帳戶能夠自動將組織中所有目前的成員帳戶啟用為 Detective 成員帳戶，並在新增至 AWS 組織時新增新成員帳戶。Detective 管理員帳戶也可以邀請目前不在 AWS 組織中但位於相同區域內的成員帳戶，將其資料提供給主要帳戶的行為圖表。當成員帳戶接受邀請並啟用時，Detective 會開始擷取成員帳戶的資料並將其擷取到該行為圖表中。

> **設計考量事項**
>
> 您可以從 GuardDuty 和 AWS Security Hub CSPM 主控台導覽至 Detective 問題清單設定檔。這些連結有助於簡化調查程序。您的帳戶必須是 Detective 和您要從中樞紐之服務的管理帳戶 (GuardDuty 或 Security Hub CSPM)。如果服務的主要帳戶相同，則整合連結可順暢運作。

AWS Audit Manager

AWS Audit Manager 可協助您持續稽核 AWS 用量，以簡化如何管理稽核，以及是否符合法規和業界標準。它可讓您從手動收集、檢閱和管理證據，轉移到自動化證據收集的解決方案、提供追蹤稽核證據來源的簡單方法、啟用團隊合作，以及協助管理證據安全和完整性。進行稽核時，Audit Manager 可協助您管理控制項的利益相關者檢閱。

透過 Audit Manager，您可以針對預先建置的架構進行稽核，例如網際網路安全中心 (CIS) 基準、CIS AWS Foundations Benchmark、系統和組織控制 2 (SOC 2)，以及支付卡產業資料安全標準 (PCI DSS)。它還可讓您根據內部稽核的特定需求，使用標準或自訂控制項建立自己的架構。

Audit Manager 會收集四種類型的證據。三種類型的證據是自動化的：來自 AWS Config 和 的合規檢查證據 AWS Security Hub CSPM、來自 的管理事件證據 AWS CloudTrail，以及來自 AWS service-to-service組態證據。對於無法自動化的證據，Audit Manager 可讓您上傳手動證據。

根據預設，Audit Manager 中的資料會使用 AWS 受管金鑰加密。 AWS SRA 使用客戶受管金鑰進行加密，以更好地控制邏輯存取。您也應該在 AWS 區域 Audit Manager 發佈評估報告的 中設定 S3 儲存貯體。此儲存貯體應使用客戶受管金鑰加密，並具有設定為僅允許 Audit Manager 發佈報告的儲存貯體政策。

> **Note**
>
> Audit Manager 可協助收集與驗證是否符合特定合規標準和法規相關的證據。不過，它不會評估您的合規。因此，透過 Audit Manager 收集的證據可能不會包含稽核所需的操作程序詳細資訊。Audit Manager 無法取代法律顧問或合規專家。我們建議您使用第三方評估者的服務，該評估者已通過評估的合規架構認證 （這些評估者）。

Audit Manager 評估可以在 AWS 組織中的多個帳戶上執行。Audit Manager 會收集證據並將其合併到其中的委派管理員帳戶 AWS Organizations。此稽核功能主要由合規和內部稽核團隊使用，且只需要您的 的讀取存取權 AWS 帳戶。

> **設計考量**
>
> - Audit Manager 補充其他 AWS 安全服務 AWS Security Hub CSPM，例如 AWS Security Hub和 AWS Config ，以協助實作風險管理架構。Audit Manager 提供獨立的風險保證功能，而 Security Hub CSPM AWS Config 可協助您監督風險和一致性套件，協助您管理風險。熟悉 由內部稽核研究所 (IIA) 開發的三行模型 的稽核專業人員應注意，此 組合 AWS 服務 可協助您涵蓋這三道防線。如需詳細資訊，請參閱 AWS 雲端 Operations & Migrations 部落格上的兩部分部落格系列。
> - 為了讓 Audit Manager 收集 Security Hub CSPM 證據，這兩個服務的委派管理員帳戶必須相同 AWS 帳戶。因此，在 AWS SRA 中，Security Tooling 帳戶是 Audit Manager 的委派管理員。

AWS Artifact

AWS Artifact 託管在安全工具帳戶中，以將合規成品管理功能與 AWS 組織管理帳戶分開。此職責分離很重要，因為除非絕對必要，否則建議您避免使用 AWS 組織管理帳戶進行部署。而是將部署傳遞給成

員帳戶。由於稽核成品管理可以從成員帳戶完成，而且 函數與安全與合規團隊密切保持一致，因此安全工具帳戶會指定為管理員帳戶 AWS Artifact。您可以使用 AWS Artifact 報告來下載 AWS 安全與合規文件，例如 AWS ISO 認證、支付卡產業 (PCI) 和系統和組織控制 (SOC) 報告。

AWS Artifact 不支援委派的管理功能。反之，您可以將此功能限制為僅與稽核和合規團隊相關的 安全工具帳戶中的 IAM 角色，以便他們可以視需要下載、檢閱這些報告，並將這些報告提供給外部稽核人員。此外，您可以限制特定 IAM 角色只能透過 IAM 政策存取特定 AWS Artifact 報告。如需範例 IAM 政策，請參閱 AWS Artifact 文件。

> **設計考量事項**
>
> 如果您選擇專用 AWS 帳戶 於稽核和合規團隊，則可以 AWS Artifact 託管在安全稽核帳戶中，該帳戶與安全工具帳戶分開。 AWS Artifact 報告提供證據，證明組織正在遵循文件化程序或滿足特定要求。系統會在整個系統開發生命週期中收集和封存稽核成品，並可在內部或外部稽核和評估中做為證據。

AWS KMS

AWS Key Management Service (AWS KMS) 可協助您建立和管理密碼編譯金鑰，並控制其在各種 AWS 服務 和應用程式中的使用。 AWS KMS 是一種安全且彈性的服務，使用硬體安全模組來保護密碼編譯金鑰。它遵循金鑰材料的產業標準生命週期程序，例如儲存、輪換和金鑰的存取控制。 AWS KMS 可以透過加密和簽署金鑰協助保護您的資料，並且可以透過AWS 加密 SDK 用於伺服器端加密和用戶端加密。為了保護和彈性， AWS KMS 支援三種類型的金鑰：客戶受管金鑰、受 AWS 管金鑰和 AWS 擁有的金鑰。客戶受管金鑰是您 AWS 帳戶 建立、擁有和管理 AWS KMS 的 金鑰。 AWS 受管金鑰是您帳戶中的 AWS KMS 金鑰，由與 整合 AWS 服務 的 代表您建立、管理和使用 AWS KMS。AWS 擁有的金鑰是 AWS 服務 擁有和管理的 AWS KMS 金鑰集合，可用於多個 AWS 帳戶。如需使用 AWS KMS 金鑰的詳細資訊，請參閱 AWS KMS 文件和AWS KMS 密碼編譯詳細資訊。

其中一個部署選項是將 AWS KMS 金鑰管理的責任集中到單一帳戶，同時透過使用金鑰和 IAM 政策的組合，委派應用程式資源在應用程式帳戶中使用金鑰的能力。這種方法安全且易於管理，但由於限流限制、帳戶服務限制和安全團隊被操作金鑰管理任務淹沒，您可能會遇到障礙 AWS KMS 。另一個部署選項是具有分散式模型，您可以在其中允許 AWS KMS 駐留在多個帳戶中，並允許負責特定帳戶中基礎設施和工作負載的人員管理自己的金鑰。相較於使用加密金鑰，此模型可讓您的工作負載團隊擁有更多控制、彈性和敏捷性。它還有助於避免 API 限制，將影響範圍限制為 AWS 帳戶 僅一個，並簡化報告、稽核和其他合規相關任務。在分散式模型中，部署和強制執行護欄非常重要，以便以相同的方式管理分散式金鑰，並根據已建立的 AWS KMS 最佳實務和政策稽核金鑰的使用。如需詳細資訊，請參閱白皮書AWS Key Management Service 最佳實務。 AWS SRA 建議分散式金鑰管理模型，其中

AWS KMS 金鑰位於本機使用金鑰的帳戶中。建議您避免在一個帳戶中針對所有密碼編譯函數 使用單一金鑰。您可以根據函數和資料保護需求建立金鑰，並強制執行最低權限原則。在某些情況下，加密許可會與解密許可分開，管理員會管理生命週期函數，但無法使用其管理的金鑰來加密或解密資料。

在安全工具帳戶中， AWS KMS 用於管理集中式安全服務的加密，例如由 AWS CloudTrail AWS 組織管理的組織線索。

AWS 私有 CA

AWS 私有憑證授權單位 (AWS 私有 CA) 是一種受管私有 CA 服務，可協助您安全地管理 EC2 執行個體、容器、IoT 裝置和內部部署資源的私有終端實體 TLS 憑證生命週期。它允許加密的 TLS 通訊執行應用程式。使用 AWS 私有 CA，您可以建立自己的 CA 階層 （根 CA，透過次級 CAs，到終端實體憑證），並發行憑證來驗證內部使用者、電腦、應用程式、服務、伺服器和其他裝置，以及簽署電腦程式碼。私有 CA 發行的憑證僅在您的 AWS 組織中受信任，而不是在網際網路上受信任。

公有金鑰基礎設施 (PKI) 或安全團隊可以負責管理所有 PKI 基礎設施。這包括私有 CA 的管理和建立。不過，必須有允許工作負載團隊自行提供憑證需求的佈建。 AWS SRA 描述集中式 CA 階層，其中根 CA 託管在安全工具帳戶中。這可讓安全團隊強制執行嚴格的安全控制，因為根 CA 是整個 PKI 的基礎。不過，透過使用 AWS Resource Access Manager (AWS RAM) 將 CA 共用到應用程式帳戶，從私有 CA 建立私有憑證會委派給應用程式開發團隊。 會 AWS RAM 管理跨帳戶共用所需的許可。這消除了每個帳戶中私有 CA 的需求，並提供更具成本效益的部署方式。如需工作流程和實作的詳細資訊，請參閱部落格文章如何使用 AWS RAM 來共用您的 AWS 私有 CA 跨帳戶。

> **Note**
>
> AWS Certificate Manager (ACM) 也可協助您佈建、管理和部署可搭配 使用的公有 TLS 憑證 AWS 服務。若要支援此功能，ACM 必須位於將使用公 AWS 帳戶 有憑證的 中。本指南稍後會在應用程式帳戶一節中討論。

> **設計考量**
>
> - 使用 AWS 私有 CA，您可以建立最多五個層級的憑證授權單位階層。您也可以建立多個階層，每個階層都具有自己的根。 AWS 私有 CA 階層應遵循組織的 PKI 設計。不過，請記住，增加 CA 階層會增加憑證路徑中的憑證數量，進而增加終端實體憑證的驗證時間。明確定義的 CA 階層提供好處，包括適合每個 CA 的精細安全控制、將次級 CA 委派給不同的應用程式，這會導致管理任務的劃分、使用具有有限可撤銷信任的 CA、定義不同有效期間的能力，以及強制執行路徑限制的能力。理想情況下，您的根和次級 CAs位於不同的 中 AWS

帳戶。如需使用 規劃 CA 階層的詳細資訊 AWS 私有 CA，請參閱 AWS 私有 CA 文件和部落格文章如何保護汽車和製造業的企業規模 AWS 私有 CA 階層。

- AWS 私有 CA 可以與您現有的 CA 階層整合，這可讓您使用 ACM 的自動化和原生 AWS 整合功能，以及您目前使用的現有信任根。您可以在 中建立由內部部署上父 CA AWS 私有 CA 支援的次級 CA。如需實作的詳細資訊，請參閱 AWS 私有 CA 文件中的安裝由外部父 CA 簽署的次級 CA 憑證。

Amazon Inspector

Amazon Inspector 是一種自動化漏洞管理服務，可自動探索和掃描來源程式碼管理員中的 Amazon Elastic Container Registry (Amazon ECR)、函數和程式碼儲存庫中的 Amazon EC2 執行個體、容器映像，以找出已知的軟體漏洞和意外的網路暴露。 AWS Lambda

Amazon Inspector 會在您變更資源時自動掃描資源，在整個資源生命週期內持續評估您的環境。啟動重新掃描資源的事件包括在 EC2 執行個體上安裝新套件、安裝修補程式，以及發佈會影響資源的新常見漏洞和暴露 (CVE) 報告。Amazon Inspector 支援 EC2 執行個體中作業系統的網際網路安全中心 (CIS) 基準評估。

Amazon Inspector 與 Jenkins 和 TeamCity 等開發人員工具整合，以進行容器映像評估。您可以在持續整合和持續交付 (CI/CD) 工具中評估容器映像是否有軟體漏洞，並將安全性推送到軟體開發生命週期的早期階段。評估調查結果可在 CI/CD 工具的儀表板中取得，因此您可以執行自動化動作以回應重大安全問題，例如封鎖的建置或將映像推送至容器登錄檔。如果您有作用中的 AWS 帳戶，您可以從 CI/CD 工具市集安裝 Amazon Inspector 外掛程式，並在建置管道中新增 Amazon Inspector 掃描，而不需要啟用 Amazon Inspector 服務。此功能適用於託管於任何地方 AWS的 CI/CD 工具，無論是在現場部署或混合雲端中，因此您可以一致地在所有開發管道中使用單一解決方案。啟用 Amazon Inspector 時，會自動探索所有 EC2 執行個體、Amazon ECR 和 CI/CD 工具中的容器映像，以及大規模的 Lambda 函數，並持續監控它們是否有已知的漏洞。

Amazon Inspector 的網路連線能力調查結果會評估 EC2 執行個體透過虛擬閘道往返 VPC 邊緣的存取能力，例如網際網路閘道、VPC 互連連線或虛擬私有網路 (VPNs)。這些規則有助於自動監控您的 AWS 網路，並識別 EC2 執行個體的網路存取可能透過錯誤管理的安全群組、存取控制清單 (ACLs)、網際網路閘道等設定錯誤。如需詳細資訊，請參閱 Amazon Inspector 文件。

當 Amazon Inspector 識別漏洞或開放網路路徑時，會產生您可以調查的問題清單。調查結果包含漏洞的完整詳細資訊，包括風險分數、受影響的資源和修補建議。風險分數專為您的環境量身打造，其計算方式是將up-to-date CVE 資訊與時間與環境因素相互關聯，例如網路可存取性和可利用性資訊，以提供情境調查結果。

Amazon Inspector Code Security 會掃描第一方應用程式原始碼、第三方應用程式相依性和基礎設施做為程式碼 (IaC) 是否有漏洞。啟用 Code Security 之後，您可以建立掃描組態並將其套用至您的程式碼儲存庫，以判斷要掃描的頻率、掃描類型和儲存庫。 Code Security 支援 靜態應用程式安全測試 (SAST)、軟體合成分析 (SCA) 和 IaC 掃描。若要設定頻率，您可以隨需、程式碼變更或定期定義掃描。程式碼掃描會擷取程式碼片段，以反白顯示偵測到的漏洞。程式碼片段是以 KMS 金鑰加密儲存。組織的委派管理員無法檢視屬於成員帳戶的程式碼片段。將原始程式碼管理員 (SCMs) 與 Code Security 整合之後，所有程式碼儲存庫都會在 Amazon Inspector 主控台中列為專案。Code Security 只會監控每個儲存庫的預設分支。Amazon Inspector 透過直接在開發人員工作的地方提供特定的程式碼修正建議，簡化安全修補。與 SCM 的雙向整合會自動將修正建議為關鍵和高調查結果的提取請求 (PRs) 和合併請求 (MRs) 中的註解，並提醒開發人員解決最重要的漏洞，而不會中斷其工作流程。

若要掃描漏洞，必須使用 AWS Systems Manager 代理程式 (SSMAgent) 在 中 AWS Systems Manager 管理 EC2 執行個體。 Amazon ECR 或 Lambda 函數中 EC2 執行個體的網路連線能力或容器映像的漏洞掃描不需要任何代理程式。

Amazon Inspector 已與 整合 AWS Organizations ，並支援委派的管理。在 AWS SRA 中，安全工具帳戶會成為 Amazon Inspector 的委派管理員帳戶。Amazon Inspector 委派管理員帳戶可以管理 AWS 組織成員的問題清單資料和特定設定。這包括檢視所有成員帳戶彙總調查結果的詳細資訊、啟用或停用成員帳戶的掃描，以及檢閱 AWS 組織內掃描的資源。

設計考量

- 啟用兩個服務時，Amazon Inspector 會自動與 AWS Security Hub CSPM 和 Security Hub 整合。您可以使用此整合，將所有調查結果從 Amazon Inspector 傳送至 Security Hub CSPM，然後將這些調查結果包含在安全性狀態的分析中。
- Amazon Inspector 會自動將調查結果的事件、資源涵蓋範圍變更，以及個別資源的初始掃描匯出至 Amazon EventBridge，以及選擇性地匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。若要將作用中問題清單匯出至 S3 儲存貯體，您需要 Amazon Inspector 可用來加密問題清單的 AWS KMS 金鑰，以及具有允許 Amazon Inspector 上傳物件許可的 S3 儲存貯體。EventBridge 整合可讓您在現有的安全與合規工作流程中，近乎即時地監控和處理問題清單。除了 Amazon Inspector 委派的管理員帳戶之外，EventBridge 事件也會發佈到他們源自的成員帳戶。
- Amazon Inspector Code Security 與 GitHub SaaS、GitHub Enterprise Cloud 和 GitHub Enterprise Server 整合需要公有網際網路存取。

實作範例

AWS SRA 程式碼庫提供 Amazon Inspector 的範例實作。它示範委派的管理（安全工具），並為組織中的所有現有和未來帳戶 AWS 設定 Amazon Inspector。

AWS 安全事件應變

AWS 安全事件應變 是一項服務，可協助您準備和回應環境中 AWS 的安全事件。它會分類問題清單、呈報安全事件，並管理需要您立即注意的案例。 此外，它可讓您存取 AWS 客戶事件回應團隊 (CIRT)，調查受影響的資源。 AWS 安全事件應變 也透過 AWS Systems Manager 文件 (SSM 文件) 提供自動化回應和修復功能，協助安全團隊更有效率地回應和復原安全事件。 AWS 安全事件應變 與 Amazon GuardDuty 整合，並 AWS Security Hub CSPM接收安全問題清單和協調自動化回應。

在 AWS SRA 中， AWS 安全事件應變 是以委派管理員帳戶的形式部署在安全工具帳戶中。已選取安全工具帳戶，因為它符合帳戶操作安全服務的目的，以及自動化安全提醒和回應。Security Tooling 帳戶也做為 Security Hub CSPM 和 GuardDuty 的委派管理員帳戶，這有助於 AWS 安全事件應變簡化工作流程管理。 AWS 安全事件應變 已設定為使用 AWS Organizations，因此您可以從 Security Tooling 帳戶管理組織帳戶中的事件回應。

AWS 安全事件應變 可協助您實作事件回應生命週期的下列階段：

- 準備：建立和維護遏制動作的回應計畫和 SSM 文件。
- 偵測和分析：自動分析安全調查結果並判斷事件嚴重性。
- 偵測和分析：開啟服務支援的案例，並與 AWS CIRT 互動以取得其他協助。CIRT 是在作用中安全事件期間提供支援的一組人員。
- 遏制和消除：透過 SSM 文件執行自動遏制動作。
- 事件後活動：記錄事件詳細資訊並進行事件後分析。

您也可以使用 AWS 安全事件應變 來建立自我管理的案例。當您需要知道或採取行動時， AWS 安全事件應變 可以建立傳出通知或案例，這可能會影響您的帳戶或資源。此功能只有在您啟用主動回應並提醒在訂閱中分類工作流程時才能使用。

設計考量

- 當您實作 時 AWS 安全事件應變，請仔細檢閱和測試自動化回應動作，再於生產環境中啟用它們。自動化可以加速事件回應，但設定不當的自動化動作可能會影響合法的工作負載。

- 請考慮在 中使用 SSM 文件 AWS 安全事件應變 來實作組織特定的遏制程序，同時維護服務針對常見事件類型的內建最佳實務。
- 如果您計劃 AWS 安全事件應變 在 VPC 中使用 ，請確定您已為 Systems Manager 和其他整合服務設定適當的 VPC 端點，以在私有子網路中啟用遏制動作。

在所有 中部署常見的安全服務 AWS 帳戶

在此參考前面的跨組織 AWS 套用安全服務一節中，強調了保護 的安全服務 AWS 帳戶，並指出其中許多 服務也可以進行設定和管理 AWS Organizations。其中一些服務應該部署在所有帳戶中，您會在 AWS SRA 中看到它們。這可啟用一組一致的護欄，並在整個 AWS 組織中提供集中式監控、管理和管控。

Security Hub CSPM、GuardDuty AWS Config、IAM Access Analyzer 和 CloudTrail 組織線索會出現在所有帳戶中。前三個支援先前在管理帳戶、信任存取和委派管理員一節中討論的委派管理員功能。CloudTrail 目前使用不同的彙總機制。

AWS SRA GitHub 程式碼儲存庫提供範例實作，讓您在所有帳戶中啟用 Security Hub CSPM AWS Config AWS Firewall Manager、GuardDuty 和 CloudTrail 組織追蹤，包括 AWS 組織管理帳戶。

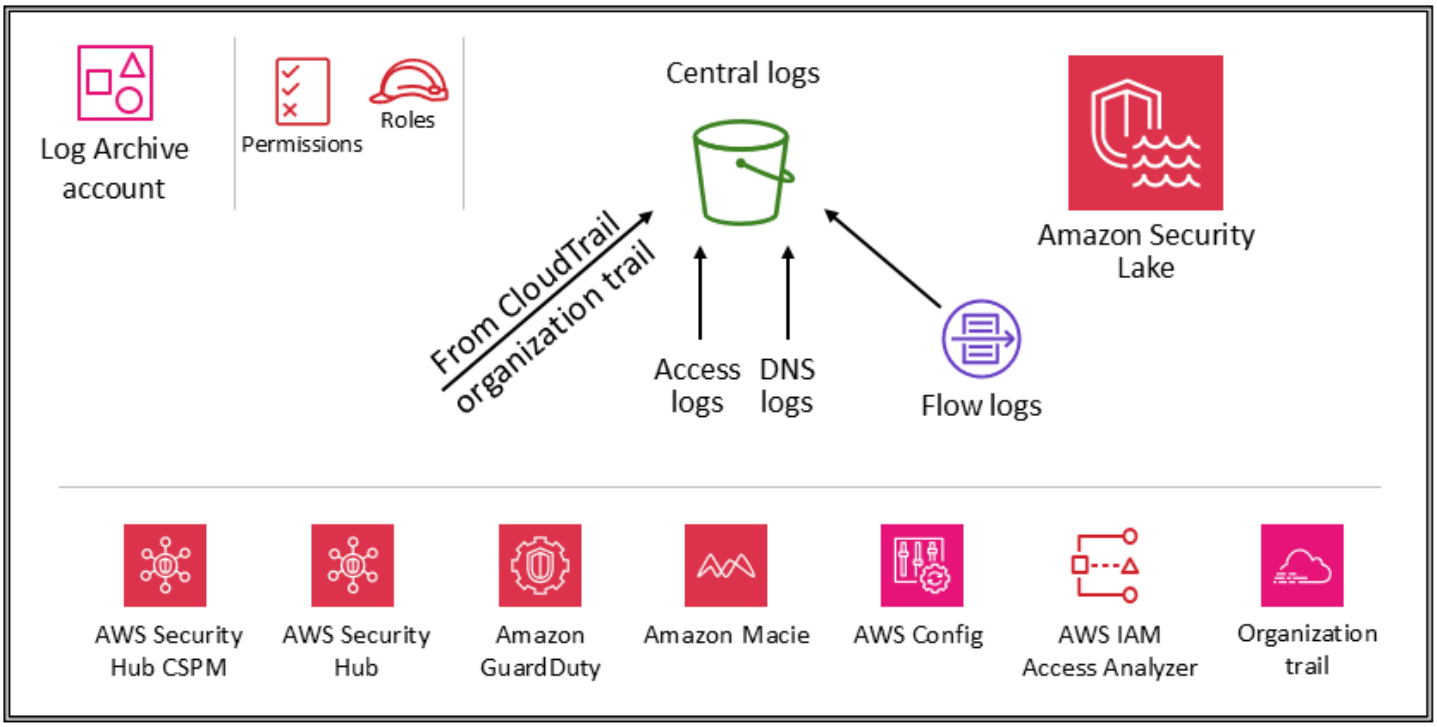
設計考量

- 特定帳戶組態可能需要額外的安全服務。例如，管理 S3 儲存貯體的帳戶 （ 應用程式和日誌封存帳戶 ） 也應該包含 Amazon Macie，並考慮在這些常見的安全服務中開啟 CloudTrail S3 資料事件記錄。(Macie 支援使用集中式組態和監控的委派管理。) 另一個範例是 Amazon Inspector，僅適用於託管 EC2 執行個體或 Amazon ECR 映像的帳戶。
- 除了本節先前所述的服務之外， AWS SRA 還包含兩個以安全為重心的服務：Amazon Detective 和 AWS Audit Manager，支援 AWS Organizations 整合和委派的管理員功能。不過，這些不包含在帳戶基準的建議服務中，因為我們已經看到這些服務最適合在下列案例中使用：
  - 您有一個執行這些函數的專用團隊或資源群組。安全分析師團隊最好使用 Detective，而 Audit Manager 有助於您的內部稽核或合規團隊。
  - 您想要在專案開始時專注於一組核心工具，例如 GuardDuty 和 Security Hub CSPM，然後使用提供額外的功能的服務來建置這些工具。

安全 OU – Log Archive 帳戶

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明在 Log Archive 帳戶中設定 AWS 的安全服務。



Log Archive 帳戶專用於擷取和封存所有與安全相關的日誌和備份。透過集中式日誌，您可以監控、稽核和提醒 Amazon S3 物件存取、身分未經授權的活動、IAM 政策變更，以及對敏感資源執行的其他關鍵活動。安全目標是直接的：這應該是不可變的儲存體，只能由受控制、自動化和監控的機制存取，並且專為耐用性而建置（例如，使用適當的複寫和封存程序）。可以深入實作控制項，以保護日誌和日誌管理程序的完整性和可用性。除了預防性控制之外，例如指派用於存取的最低權限角色，以及使用受控 AWS KMS 金鑰加密日誌，使用偵測性控制 AWS Config ，例如監控（和提醒和修復）此許可集合是否有非預期的變更。

設計考量事項

基礎設施、操作和工作負載團隊所使用的操作日誌資料，通常會與安全、稽核和合規團隊所使用的日誌資料重疊。建議您將操作日誌資料合併至 Log Archive 帳戶。根據您的特定安全和控管需求，您可能需要篩選儲存至此帳戶的操作日誌資料。您可能還需要指定誰可以存取 Log Archive 帳戶中的操作日誌資料。

日誌類型

AWS SRA 中顯示的主要日誌包括 AWS CloudTrail （組織線索）、Amazon VPC 流程日誌、從 Amazon CloudFront 存取日誌 AWS WAF，以及從 Amazon Route 53 存取 DNS 日誌。這些日誌提供使用者、角色或網路實體 （例如透過 IP 地址識別） 所採取（AWS 服務或嘗試） 動作的稽核。也可以擷取和封存其他日誌類型 （例如應用程式日誌或資料庫日誌）。如需日誌來源和記錄最佳實務的詳細資訊，請參閱每個服務的安全文件。

Amazon S3 作為中央日誌存放區

Amazon S3 中的許多 AWS 服務 日誌資訊，無論是預設或專屬。 AWS CloudTrail、Amazon VPC 流程日誌、Elastic Load Balancing AWS Config、Amazon GuardDuty 和 AWS WAF 是記錄 Amazon S3 中資訊的一些服務範例。這表示日誌完整性是透過 S3 物件完整性實現的；日誌機密性是透過 S3 物件存取控制實現的；日誌可用性是透過 S3 物件鎖定、S3 物件版本和 S3 生命週期規則實現的。透過在位於專用帳戶中的專用和集中式 S3 儲存貯體中記錄資訊，您可以在幾個儲存貯體中管理這些日誌，並強制執行嚴格的安全控制、存取和職責分離。

在 AWS SRA 中，Amazon S3 中存放的主要日誌來自 CloudTrail，因此本節說明如何保護這些物件。本指南也適用於由您自己的應用程式或其他應用程式建立的任何其他 S3 物件 AWS 服務。每當您在 Amazon S3 中擁有需要高完整性、強大的存取控制和自動保留或銷毀的資料時，就會套用這些模式。

上傳至 S3 儲存貯體的所有新物件 （包括 CloudTrail 日誌） 預設會使用 Amazon 伺服器端加密搭配 Amazon S3-managed加密金鑰 (SSE-S3) 進行加密。這有助於保護靜態資料，但存取控制僅由 IAM 政策控制。若要提供額外的受管安全層，您可以在所有安全 S3 儲存貯體上使用伺服器端加密與您管理的 AWS KMS 金鑰 (SSE-KMS)。這會新增第二層級的存取控制。若要讀取日誌檔案，使用者必須同時擁有 SAmazon S33 讀取許可和套用的 IAM 政策或角色，以允許他們透過相關聯的金鑰政策解密許可。

兩個選項可協助您保護或驗證存放在 Amazon S3 中的 CloudTrail 日誌物件的完整性。CloudTrail 提供日誌檔案完整性驗證，以判斷日誌檔案是否在 CloudTrail 交付後遭到修改或刪除。另一個選項是 S3 物件鎖定。

除了保護 S3 儲存貯體本身之外，您還可以遵守記錄服務 （例如 CloudTrail) 和 Log Archive 帳戶的最低權限原則。例如，具有 AWS 受管 IAM 政策授予許可的使用者可以`AWSCloudTrail_FullAccess`停用或重新設定其中最敏感和重要的稽核函數 AWS 帳戶。將此 IAM 政策的套用限制為盡可能少的個人。

使用偵測性控制項，例如 AWS Config 和 IAM Access Analyzer 交付的控制項，來監控 （並提醒和修復） 這個更廣泛的預防性控制項集合，以找出非預期的變更。

如需 S3 儲存貯體安全最佳實務的深入討論，請參閱 Amazon S3 文件、線上技術講座，以及部落格文章 Amazon S3 中保護資料的十大安全最佳實務。

> **實作範例**
>
> AWS SRA 程式碼庫提供 Amazon S3 封鎖帳戶公開存取的範例實作。本單元會封鎖 AWS 組織中所有現有和未來帳戶的 Amazon S3 公有存取權。

Amazon Security Lake

AWS SRA 建議您使用 Log Archive 帳戶做為 Amazon Security Lake 的委派管理員帳戶。當您這樣做時，Security Lake 會在與其他 SRA 建議的安全性日誌相同的帳戶中的專用 S3 儲存貯體中收集支援的日誌。

為了保護日誌和日誌管理程序的可用性，Security Lake 的 S3 儲存貯體只能由 Security Lake 服務或由 Security Lake 為來源或訂閱者管理的 IAM 角色存取。除了使用預防性控制之外，例如為存取指派最低權限角色，以及使用受控 AWS KMS 金鑰加密日誌，使用偵測性控制，例如 AWS Config 監控 （和提醒和修復） 此許可集合是否有非預期的變更。

Security Lake 管理員可以在整個 AWS 組織中啟用日誌收集。這些日誌存放在 Log Archive 帳戶中的區域 S3 儲存貯體中。此外，為了集中日誌並簡化儲存和分析，Security Lake 管理員可以選擇一或多個彙總區域，其中整合和儲存所有區域 S3 儲存貯體的日誌。支援的日誌 AWS 服務 會自動轉換為稱為開放網路安全結構描述架構 (OCSF) 的標準化開放原始碼結構描述，並以 Apache Parquet 格式儲存在 Security Lake S3 儲存貯體中。透過 OCSF 支援，Security Lake 可有效率地標準化和合併來自 AWS 和其他企業安全來源的安全資料，以建立統一且可靠的安全相關資訊儲存庫。

Security Lake 可以收集與 Amazon S3 和 的 AWS CloudTrail 管理事件和 CloudTrail 資料事件相關聯的日誌 AWS Lambda。 若要在 Security Lake 中收集 CloudTrail 管理事件，您必須擁有至少一個 CloudTrail 多區域組織線索，以收集讀取和寫入 CloudTrail 管理事件。必須針對追蹤啟用記錄。多區域線索會將日誌檔案從多個區域交付到單一 的單一 S3 儲存貯體 AWS 帳戶。 如果區域位於不同國家/地區，請考慮資料匯出需求，以判斷是否可以啟用多區域線索。

AWS Security Hub CSPM 是 Security Lake 中支援的原生資料來源，您應該將 Security Hub CSPM 調查結果新增至 Security Lake。Security Hub CSPM 會從許多不同的 AWS 服務 第三方整合產生問題清單。這些調查結果可協助您取得合規狀態的概觀，以及您是否遵循 AWS 和 AWS Partner 解決方案的安全建議。

若要從日誌和事件中取得可見性和可行的洞見，您可以使用 Amazon Athena、Amazon OpenSearch Service、Amazon Quick 和第三方解決方案等工具來查詢資料。需要存取 Security Lake 日誌資料的

使用者不應直接存取 Log Archive 帳戶。他們應該只從安全工具帳戶存取資料。或者，他們可以使用其他 AWS 帳戶 或內部部署位置來提供分析工具，例如 OpenSearch Service、Quick 或第三方工具，例如安全資訊和事件管理 (SIEM) 工具。若要提供資料的存取權，管理員應在 Log Archive 帳戶中設定 Security Lake 訂閱者，並將需要存取資料的帳戶設定為查詢存取訂閱者。如需詳細資訊，請參閱本指南安全 OU – 安全工具帳戶區段中的 Amazon Security Lake。

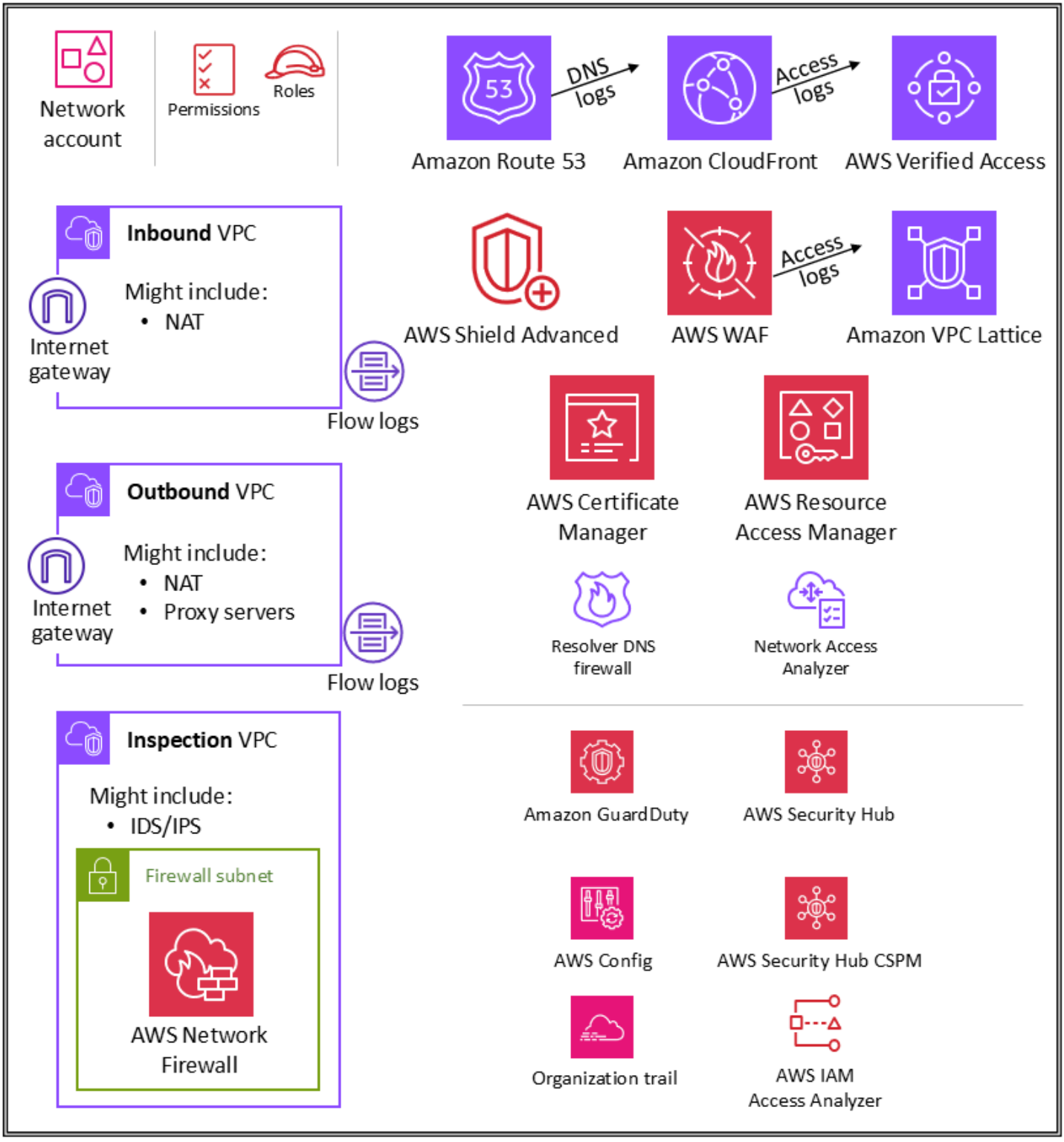
Security Lake 提供 AWS 受管政策，協助您管理 服務的管理員存取權。如需詳細資訊，請參閱 Security Lake 使用者指南。最佳實務是建議您透過開發管道限制 Security Lake 的組態，並防止透過 AWS 主控台或 AWS Command Line Interface () 變更組態AWS CLI。此外，您應該設定嚴格的 IAM 政策和服務控制政策 (SCPs)，只提供管理 Security Lake 所需的許可。您可以設定通知來偵測對這些 S3 儲存貯體的任何直接存取。

> **設計考量事項**
>
> 當您在 Security Lake 中啟用 CloudTrail 管理事件時，它們會產生 Security Lake 費用。在 Security Lake 中收集 CloudTrail 管理事件需要收集讀取和寫入 CloudTrail 管理事件的 CloudTrail 多區域組織追蹤。此第一個線索免費提供給您。CloudTrail 管理事件通常佔 CloudTrail 事件總數的一小部分 （ 約 5%)。這適用於在 Log Archive 帳戶中使用或 AWS Control Tower 具有集中式 CloudTrail 日誌的客戶。

基礎設施 OU – 網路帳戶

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明網路帳戶中設定 AWS 的安全服務。



網路帳戶管理您的應用程式與更廣泛的網際網路之間的閘道。請務必保護雙向介面。網路帳戶會將聯網服務、組態和操作與個別應用程式工作負載、安全和其他基礎設施隔離。此安排不僅限制連線、許可和資料流程，還支援需要在這些帳戶中操作之團隊的職責分離和最低權限。透過將網路流程分為單獨的傳

入和傳出虛擬私有雲端 (VPC)，您可以保護敏感基礎設施和流量免遭不必要的存取。傳入網路通常視為風險較高，需要適當的路由、監控和潛在問題緩解措施。這些基礎設施帳戶將從組織管理帳戶和基礎設施 OU 繼承許可防護機制。聯網 (和安全) 團隊會管理此帳戶中的大部分基礎設施。

網路架構

雖然網路設計和細節超出本文件的範圍，但我們建議在各種帳戶之間進行這三個網路連線的選項：VPC 對等互連 AWS PrivateLink，以及 AWS Transit Gateway。在其中進行選擇時的重要考量是操作規範、預算和特定頻寬需求。

- VPC 對等互連 – 連接兩個 VPC 的最簡單方法是使用 VPC 對等互連。連線可實現 VPC 之間的完全雙向連線。位於不同帳戶中的 VPCs， AWS 區域 也可以對等互連。在規模上，當您具有數十至數百個 VPC 時，將其與對等互連會導致形成數百至數千個對等互連的網格，這對於管理和擴展來說可能具有挑戰性。當一個 VPC 中的資源必須與另一個 VPC 中的資源通訊、兩個 VPC 的環境都受到控制和保護，以及要連接的 VPC 數量少於 10 個 (以允許個別管理每個連線) 時，最好使用 VPC 對等互連。
- AWS PrivateLink – PrivateLink 提供 VPCs、服務和應用程式之間的私有連線。您可以在您的 VPC 中建立自己的應用程式，並將其設定為採用 PrivateLink 技術的服務 (稱為端點服務)。其他 AWS 主體可以使用介面 VPC 端點或 Gateway Load Balancer 端點，從其 VPC 建立與端點服務的連線，視服務類型而定。 Load Balancer 當您使用 PrivateLink 時，服務流量不會通過公開可路由網路。當您具有一個用戶端-伺服器設定，想要為一個或多個消費者 VPC 提供對服務供應商 VPC 中的特定服務或一組執行個體的單向存取時，使用 PrivateLink。當兩個 VPC 中的用戶端和伺服器具有重疊的 IP 地址時，這也是一個很好的選擇，因為 PrivateLink 在用戶端 VPC 內使用彈性網路介面，因此不會與服務供應商發生 IP 衝突。
- AWS Transit Gateway – Transit Gateway hub-and-spoke設計，可將 VPCs 和內部部署網路連線為全受管服務，而無需您佈建虛擬設備。 AWS 管理高可用性和可擴展性。傳輸閘道是區域資源，可以連接相同區域內的數千個 VPCs AWS 區域。您可以將混合連線 (VPN 和 AWS Direct Connect 連線） 連接到單一傳輸閘道，藉此在一個位置整合和控制 AWS 組織的整個路由組態。傳輸閘道解決了大規模建立和管理多個 VPC 對等互連所涉及的複雜性。它是大多數網路架構的預設值，但圍繞成本、頻寬和延遲的特定需求可能會使 VPC 對等互連更適合您的需求。

傳入 (輸入) VPC

傳入 VPC 旨在接受、檢查和路由從應用程式外部啟動的網路連線。根據應用程式的具體情況，您可能會在此 VPC 中看到部分網路位址轉譯 (NAT)。來自此 VPC 的流程日誌將擷取並儲存在日誌存檔帳戶中。

傳出 (輸出) VPC

傳出 VPC 旨在處理從應用程式內啟動的網路連線。根據應用程式的詳細資訊，您可以預期在此 VPC 中看到流量 NAT、 AWS 服務特定 VPC 端點和外部 API 端點託管。來自此 VPC 的流程日誌將擷取並儲存在日誌存檔帳戶中。

檢查 VPC

專用檢查 VPC 提供簡化且集中的方法，用於管理 VPCs（相同或不同 AWS 區域)、網際網路和內部部署網路之間的檢查。對於 AWS SRA，請確保 VPCs之間的所有流量通過檢查 VPC，並避免將檢查 VPC 用於任何其他工作負載。

AWS Network Firewall

AWS Network Firewall 是適用於 VPC 的高可用性受管網路防火牆服務。它可讓您輕鬆地部署和管理狀態檢查、入侵預防和偵測，以及 Web 篩選，以協助保護您的虛擬網路 AWS。您可以使用 Network Firewall 解密 TLS 工作階段，並檢查傳入和傳出流量。如需設定 Network Firewall 的詳細資訊，請參閱 AWS Network Firewall VPC 中的 – 新的受管防火牆服務部落格文章。

您可以在 VPC 中依可用區域使用防火牆。對於每個可用區域，您選擇一個子網路來託管篩選流量的防火牆端點。可用區域中的防火牆端點可以保護此區域內除其所在子網路之外的所有子網路。根據使用案例和部署模型，防火牆子網路可以是公有或私有子網路。防火牆對流量流程完全透明，且不會執行網路位址轉譯 (NAT)。它會保留來源和目的地地址。在此參考架構中，防火牆端點託管在檢查 VPC 中。從傳入 VPC 至傳出 VPC 的所有流量都將透過此防火牆子網路路由以進行檢查。

Network Firewall 透過 Amazon CloudWatch 指標即時顯示防火牆活動，並透過將日誌傳送至 Amazon Simple Storage Service (Amazon S3)、CloudWatch 和 Amazon Data Firehose 來提高網路流量的可見性。Network Firewall 可與您現有的安全方法互通，包括來自 AWS 合作夥伴的技術。您也可以匯入現有的 Suricata 規則集，這些規則集可能是內部編寫的，也可能是從第三方供應商或開放原始碼平台外部取得的。

在 AWS SRA 中，網路防火牆是在網路帳戶中使用，因為服務的網路控制導向功能符合帳戶的意圖。

設計考量

- AWS Firewall Manager 支援 Network Firewall，因此您可以集中設定和部署整個組織的 Network Firewall 規則。（如需詳細資訊，請參閱 AWS 文件中的在 Firewall Manager 中使用 AWS Network Firewall 政策。）在您設定 Firewall Manager 時，它會自動建立一個防

火牆，其中包含您指定的帳戶和 VPC 中的規則集。它還在包含公有子網路的每個可用區域的專用子網路中部署端點。同時，對集中設定的規則集的任何變更都會在部署的 Network Firewall 防火牆上自動更新至下游。

- Network Firewall 有多種可用的部署模型。正確的模型取決於您的使用案例和需求。範例如下：
  - 分散式部署模型，其中 Network Firewall 部署到個別 VPC。
  - 集中式部署模型，其中 Network Firewall 部署到集中式 VPC，用於東西向 (VPC 至 VPC) 或南北向 (網際網路輸出和輸入、內部部署) 流量。
  - 合併的部署模型，其中 Network Firewall 部署到集中式 VPC，用於東西向流量和南北向流量的子集。
- 作為最佳實務，請勿使用 Network Firewall 子網路部署任何其他服務。這是因為 Network Firewall 無法檢查來自防火牆子網路內的來源或目的地的流量。

網路存取分析器

網路存取分析器是 Amazon VPC 的一項功能，可識別對您的資源的意外網路存取。您可以使用網路存取分析器來驗證網路分隔、識別可從網際網路存取的資源或只能從可信 IP 地址範圍存取的資源，並驗證您是否對所有網路路徑具有適當的網路控制。

Network Access Analyzer 使用自動推理演算法來分析封包可在網路中資源之間採取 AWS 的網路路徑，並針對符合您定義的網路存取範圍的路徑產生問題清單。網路存取分析器會對網路組態執行靜態分析，這表示在此分析過程中不會在網路中傳輸任何封包。

Amazon Inspector 網路連線能力規則提供了相關功能。這些規則產生的調查結果將在應用程式帳戶中使用。Network Access Analyzer 和 Network Reachability 都使用AWS 來自可用安全計畫的最新技術，並採用具有不同重點領域的這項技術。網路連線能力套件特別著重於 EC2 執行個體及其網際網路可存取性。

網路帳戶定義關鍵網路基礎設施，控制進出您 AWS 環境的流量。需要嚴格監控此流量。在 AWS SRA 中，Network Access Analyzer 用於網路帳戶，以協助識別意外的網路存取、透過網際網路閘道識別可存取網際網路的資源，並確認資源和網際網路閘道之間的所有網路路徑上都存在適當的網路控制，例如網路防火牆和 NAT 閘道。

設計考量事項

Network Access Analyzer 是 Amazon VPC 的一項功能，可用於具有 VPC 的任何 AWS 帳戶 。網路管理員可以取得範圍緊密的跨帳戶 IAM 角色，以驗證每個角色內是否強制執行核准的網路路徑 AWS 帳戶。

AWS RAM

AWS Resource Access Manager (AWS RAM) 可協助您安全地 AWS 帳戶 與其他 共用您在其中建立 AWS 的資源 AWS 帳戶。 AWS RAM 提供集中位置來管理資源的共用，並跨帳戶標準化此體驗。這使得在利用管理和帳單隔離的同時管理資源更加簡單，並減少多帳戶策略提供的影響限制優勢的範圍。如果您的帳戶由 管理 AWS Organizations，則 AWS RAM 可讓您與組織中的所有帳戶共用資源，或僅與一或多個指定組織單位 (OUs內的帳戶共用資源。您也可以 AWS 帳戶 透過帳戶 ID 與特定 共用，無論帳戶是否為組織的一部分。您也可以與指定的 IAM 角色和使用者共用部分支援的資源類型。

AWS RAM 可讓您共用不支援 IAM 資源型政策的資源，例如 VPC 子網路和 Route 53 規則。此外，透過 AWS RAM，資源的擁有者可以看到哪些主體可以存取他們共用的個別資源。IAM 主體可以直接擷取與他們共用的資源清單，這些資源無法用於 IAM 資源政策共用的資源。 如果 AWS RAM 用於在 AWS 組織外部共用資源，則會啟動邀請程序。收件人必須先接受邀請，才能存取資源。 這提供額外的檢查和餘額。

AWS RAM 在部署共用資源的帳戶中，由資源擁有者叫用和管理。 AWS SRA 中 AWS RAM 說明的常見使用案例是讓網路管理員與整個 AWS 組織共用 VPC 子網路和傳輸閘道。這可讓您解耦 AWS 帳戶和 網路管理函數，並協助實現職責分離。如需 VPC 共用的詳細資訊，請參閱 AWS 部落格文章 VPC 共用：多個帳戶的新方法、VPC 管理和AWS 網路基礎設施白皮書。

設計考量事項

雖然 AWS RAM 服務僅部署在 AWS SRA 的網路帳戶中，但通常會部署在多個帳戶中。例如，您可以將資料湖管理集中到單一資料湖帳戶，然後與 AWS 組織中的其他帳戶共用 AWS Lake Formation 資料目錄資源 （資料庫和資料表）。如需詳細資訊，請參閱 AWS Lake Formation 文件和 AWS 部落格文章AWS 帳戶 使用 安全地跨 共用您的資料 AWS Lake Formation。 此外，安全管理員可以在建置 AWS 私有憑證授權單位 階層時，使用 AWS RAM 遵循最佳實務。 CAs可以與外部第三方共用，這些第三方無需存取 CA 階層即可發行憑證。這允許發起組織限制和撤銷第三方存取權。

AWS Verified Access

AWS Verified Access 提供不使用 VPN 的安全存取公司應用程式和資源。它改善了安全狀態，並透過根據預先定義的要求即時評估每個存取請求，協助套用零信任存取。您可以根據身分資料和裝置狀態，為每個應用程式定義具有條件的唯一存取政策。Verified Access 透過 TCP、SSH 和 RDP 通訊協定，為 Git 儲存庫、資料庫和 EC2 執行個體群組等應用程式提供對 HTTP(S) 應用程式的安全存取，例如以瀏覽器為基礎的應用程式和非 HTTP(S) 應用程式。您可以使用命令列終端機或從桌面應用程式存取這些項目。Verified Access 還可以透過協助管理員有效地設定和監控存取策略，來簡化安全操作。這樣可騰出時間來更新政策、回應安全性和連線事件，以及稽核合規標準。Verified Access 也支援與 整合 AWS WAF ，以協助您篩選掉常見威脅，例如 SQL Injection 和跨網站指令碼 (XSS)。Verified Access 與 無縫整合 AWS IAM Identity Center，可讓使用者透過 SAML 型第三方身分提供者 (IdPs) 進行身分驗證。如果您已具有與 OpenID Connect (OIDC) 相容的自訂 IdP 解決方案，Verified Access 還可以透過直接與您的 IdP 連接來對使用者進行身分驗證。Verified Access 會記錄每次存取嘗試，以便您可以快速回應安全事件和稽核請求。Verified Access 支援將這些日誌交付至 Amazon Simple Storage Service (Amazon S3)、Amazon CloudWatch Logs 和 Amazon Data Firehose。

Verified Access 支援兩種常見的企業應用程式模式：內部和面向網際網路。Verified Access 透過使用 Application Load Balancer 或彈性網路介面與應用程式整合。如果您使用的是 Application Load Balancer，Verified Access 需要內部負載平衡器。由於 Verified Access AWS WAF 在執行個體層級支援 ，因此與 AWS WAF Application Load Balancer 整合的現有應用程式可以將政策從負載平衡器移至 Verified Access 執行個體。企業應用程式表示為 Verified Access 端點。每個端點都與一個 Verified Access 群組關聯，並繼承此群組的存取政策。Verified Access 群組是 Verified Access 端點和群組層級 Verified Access 政策的集合。群組簡化了政策管理，且可讓 IT 管理員設定基準條件。應用程式擁有者可以根據應用程式的敏感度進一步定義精細政策。

在 AWS SRA 中，已驗證存取託管在網路帳戶中。中心 IT 團隊會設定集中管理的組態。例如，他們可以連接身分提供者 (例如 Okta) 和裝置信任提供者 (例如 Jamf) 等信任提供者、建立群組並確定群組層級政策。然後，您可以使用 與數十個、數百個或數千個工作負載帳戶共用這些組態 AWS RAM。這可讓應用程式團隊管理管理其應用程式的基礎端點，而不需要其他團隊的額外負荷。 為託管在不同工作負載帳戶中的公司應用程式 AWS RAM 提供可擴展的方式來利用 Verified Access。

> **設計考量事項**
>
> 您可以將具有類似安全要求的應用程式的端點分組，以簡化政策管理，然後與應用程式帳戶共用此群組。群組中的所有應用程式都會共用群組政策。如果群組中的某個應用程式因邊緣案例而需要特定政策，您可以為該應用程式套用應用程式層級政策。

Amazon VPC Lattice

Amazon VPC Lattice 是一種應用程式聯網服務，可連接、監控和保護service-to-service通訊。 服務通常稱為微服務，是一種可獨立部署的軟體單位，可提供特定任務。VPC Lattice 會自動管理跨 VPCs 的服務之間的網路連線和應用程式層路由， AWS 帳戶 而不需要您管理基礎網路連線、前端負載平衡器或附屬代理。它提供了全受管應用程式層代理，此代理根據請求特性 (例如路徑和標頭) 提供應用程式層路由。VPC Lattice 內建於 VPC 基礎設施中，因此可在 Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service (Amazon EKS) 和 等各種運算類型中提供一致的方法 AWS Lambda。VPC Lattice 還支援藍/綠和金絲雀式部署的加權路由。您可以使用 VPC Lattice 建立具有邏輯界限 的服務網路 ，以自動實作服務探索和連線。VPC Lattice 與 IAM 整合，以使用 身分驗證政策service-to-service身分驗證和授權。

VPC Lattice 與 整合 AWS RAM ，以啟用 服務與服務網路的共用。 AWS SRA 描述了開發人員或服務擁有者在其應用程式帳戶中建立 VPC Lattice 服務的分散式架構。服務擁有者會定義接聽程式、路由規則、目標群組以及授權政策。然後，他們與其他帳戶共用服務，並將服務與 VPC Lattice 服務網路關聯。這些網路由網路管理員在網路帳戶中建立並與應用程式帳戶共用。網路管理員會設定服務網路層級授權政策和監控。管理員將 VPC 和 VPC Lattice 服務與一或多個服務網路關聯。如需此分散式架構的詳細演練，請參閱 AWS 部落格文章 使用 Amazon VPC Lattice 為您的應用程式建置安全的多帳戶多 VPC 連線

設計考量

- 視您組織的服務或服務網路可見性運作模式而定，網路管理員可以共用其服務網路，並可讓服務擁有者控制將其服務和 VPCs 與這些服務網路建立關聯。或者，服務擁有者可以共用其服務，網路管理員可以將服務與服務網路關聯。
- 只有當用戶端位於與相同服務網路關聯的 VPC 中時，用戶端才可以將請求傳送至與該服務網路關聯的服務。周遊 VPC 對等互連或傳輸閘道的用戶端流量將遭拒。

邊緣安全

邊緣安全通常需要三種類型的保護：安全內容交付、網路和應用程式層保護以及分散式阻斷服務 (DDoS) 緩解措施。資料、影片、應用程式和 API 等內容必須快速且安全地交付，使用建議版本的 TLS 來加密端點之間的通訊。內容也應透過簽章的 URL、簽章的 Cookie 和字符身分驗證進行存取限制。應用程式層級安全應旨在控制機器人流量、阻止 SQL 隱碼攻擊或跨網站指令碼 (XSS) 等常見攻擊模式，並提供 Web 流量可見性。在邊緣，DDoS 緩解措施提供了重要的防禦層，可確保關鍵任務業務營運和

服務的持續可用性。應保護應用程式和 API 免受 SYN 洪水攻擊、UDP 洪水攻擊或其他反射攻擊，並具有內嵌緩解措施以阻止基本網路層攻擊。

AWS 提供多種 服務，協助提供從核心雲端到 AWS 網路邊緣的安全環境。Amazon CloudFront、AWS Certificate Manager (ACM) AWS Shield AWS WAF和 Amazon Route 53 一起合作，協助建立彈性的分層安全周邊。透過 CloudFront，內容、APIs或應用程式可以透過 HTTPS 使用 TLSv1.3 來加密和保護檢視器用戶端與 CloudFront 之間的通訊。您可以使用 ACM 建立 自訂 SSL 憑證 ，並將其免費部署到 CloudFront 分佈。ACM 會自動處理憑證續約。Shield 是一項受管 DDoS 保護服務，可協助保護在其上執行的應用程式 AWS。它提供動態偵測和自動內嵌緩解措施，可將應用程式停機時間和延遲降至最低。 AWS WAF 您可以建立規則，根據特定條件 (IP 地址、HTTP 標頭和內文，或自訂 URIs)、常見 Web 攻擊和普遍的機器人來篩選 Web 流量。Route 53 是一種可用性高、可擴展性強的 DNS Web 服務。Route 53 會將使用者請求連線至在內部部署 AWS 或內部部署上執行的網際網路應用程式。 AWS SRA 使用網路帳戶中託管的 AWS Transit Gateway，採用集中式網路輸入架構，因此邊緣安全基礎設施也會集中在此帳戶中。

Amazon CloudFront

Amazon CloudFront 是一種安全的內容交付網路 (CDN)，可針對常見網路層和傳輸 DDoS 嘗試提供固有保護。您可以使用 TLS 憑證交付內容、API 或應用程式，且進階 TLS 功能會自動啟用。您可以使用 AWS Certificate Manager (ACM) 建立自訂 TLS 憑證，並在檢視器和 CloudFront 之間強制執行 HTTPS 通訊，如 ACM 章節稍後所述。您還可以要求 CloudFront 與您的自訂原始伺服器之間的通訊在傳輸中實作端對端加密。對於此案例，您必須在原始伺服器上安裝 TLS 憑證。如果您的原始伺服器是彈性負載平衡器，您可以使用 ACM 產生的憑證或由第三方憑證授權機構 (CA) 驗證並匯入至 ACM 的憑證。如果 S3 儲存貯體網站端點做為 CloudFront 的原始伺服器，則您無法將 CloudFront 設定為搭配原始伺服器使用 HTTPS，因為 Amazon S3 不支援網站端點的 HTTPS。(但是，您仍然可能需要在檢視器與 CloudFront 之間使用 HTTPS。) 對於支援安裝 HTTPS 憑證的所有其他原始伺服器，您必須使用可信第三方 CA 簽署的憑證。

CloudFront 提供了多個選項來保護和限制對您的內容的存取。例如，它可以透過使用簽章的 URL 和簽章的 Cookie 來限制對您的 Amazon S3 原始伺服器的存取。如需詳細資訊，請參閱 CloudFront 文件中的設定安全存取和限制對內容的存取。

AWS SRA 說明網路帳戶中的集中式 CloudFront 分佈，因為它們符合使用 實作的集中式網路模式 AWS Transit Gateway。透過在網路帳戶中部署和管理 CloudFront 分佈，您可以取得集中控制的優勢。您可以在單一位置管理所有 CloudFront 分佈，讓您更輕鬆地控制存取、進行設定和監控所有帳戶的使用情況。此外，您還可以從一個集中式帳戶管理 ACM 憑證、DNS 記錄和 CloudFront 日誌記錄。

CloudFront 安全儀表板可直接在 CloudFront 分佈中提供 AWS WAF 可見性和控制。您可以了解應用程式的主要安全趨勢、允許和封鎖的流量，以及機器人活動。您可以使用視覺化日誌分析器和內建封鎖控制等調查工具來隔離流量模式和封鎖流量，而無需查詢日誌或撰寫安全規則。

設計考量

- 或者，您可以在應用程式帳戶中部署 CloudFront 作為應用程式的一部分。在此案例中，應用程式團隊做出諸如如何部署 CloudFront 分佈等決策，確定適當的快取政策，並負責 CloudFront 分佈的控管、稽核和監控。透過將 CloudFront 分佈分散在多個帳戶中，您可以從額外的服務配額中受益。另一個好處是，您可以使用 CloudFront 的固有和自動原始存取身分 (OAI) 和原始存取控制 (OAC) 組態來限制對 Amazon S3 原始伺服器的存取。
- 透過 CloudFront 等 CDN 交付 Web 內容時，您必須防止檢視者繞過 CDN 直接存取您的原始內容。若要實現此原始存取限制，您可以使用 CloudFront 和 AWS WAF 新增自訂標頭，並在將請求轉送到自訂原始伺服器之前驗證標頭。如需此解決方案的詳細說明，請參閱 AWS 安全部落格文章如何使用 AWS WAF 和 增強 Amazon CloudFront 原始伺服器安全性 AWS Secrets Manager。另一種方法是限制安全群組中與 Application Load Balancer 相關聯的 CloudFront 字首清單。這將有助於確保只有 CloudFront 分佈才能存取負載平衡器。

AWS WAF

AWS WAF 是一種 Web 應用程式防火牆，可協助保護您的 Web 應用程式免受 Web 入侵，例如可能影響應用程式可用性、危及安全性或消耗過多資源的常見漏洞和機器人。 它可以與 Amazon CloudFront 分佈、Amazon API Gateway REST API、Application Load Balancer、 AWS AppSync GraphQL API、Amazon Cognito 使用者集區和服務整合 AWS App Runner 。

AWS WAF 使用 Web 存取控制清單 ACLs) 來保護一組 AWS 資源。Web ACL 是一組規則，可定義檢查條件，以及在 Web 請求符合條件時要採取的相關動作 （封鎖、允許、計數或執行機器人控制）。AWS WAF 提供一組 受管規則 ，可針對常見的應用程式漏洞提供保護。這些規則由 AWS 和 AWS Partners 策劃和管理。 AWS WAF 也提供強大的規則語言來撰寫自訂規則。您可以使用自訂規則來撰寫符合您特定需求的檢查條件。範例包括 IP 限制、地理限制以及更適合您的特定應用程式行為的受管規則的自訂版本。

AWS WAF 為常見和目標機器人和帳戶接管保護 (ATP) 提供一組智慧型層受管規則。使用機器人控制功能和 ATP 規則群組時，您需要支付訂閱費用和流量檢查費用。因此，我們建議您先監控流量，然後再決定要使用什麼。您可以使用主控台上 AWS WAF 免費提供的機器人管理和帳戶接管儀表板來監控這些活動，然後決定是否需要智慧型層 AWS WAF 規則群組。

在 AWS SRA 中， AWS WAF 與網路帳戶中的 CloudFront 整合。在此組態中， AWS WAF 規則處理發生在節點，而不是 VPC 內。這樣可篩選更接近請求內容的最終使用者的惡意流量，並有助於限制惡意流量進入您的核心網路。

您可以透過設定 S3 儲存貯體的跨帳戶存取，將完整 AWS WAF 日誌傳送至 Log Archive 帳戶中的 S3 儲存貯體。如需詳細資訊，請參閱本主題的 AWS re：Post 文章。

設計考量

- 作為在網路帳戶中 AWS WAF 集中部署的替代方案，透過 AWS WAF 在應用程式帳戶中部署，可以更好地滿足某些使用案例。例如，當您在應用程式帳戶中部署 CloudFront 分佈或擁有公開的 Application Load Balancer，或如果您在 Web 應用程式前面使用 API Gateway 時，可以選擇此選項。如果您決定 AWS WAF 在每個應用程式帳戶中部署 ，請使用 從集中式安全工具帳戶 AWS Firewall Manager 管理 AWS WAF 這些帳戶中的規則。
- 您也可以在 CloudFront 層新增一般 AWS WAF 規則，並在區域資源新增其他應用程式特定的 AWS WAF 規則，例如 Application Load Balancer 或 API 閘道。

AWS Shield

AWS Shield 是一種受管 DDoS 保護服務，可保護在 上執行的應用程式 AWS。Shield 有兩種方案：Shield Standard 和 Shield Advanced。Shield Standard 為所有 AWS 客戶提供針對最常見基礎設施 （ 第 3 層和第 4 層 ） 事件的保護，無需額外付費。Shield Advanced 為以受保護 Amazon EC2、Elastic Load Balancing (Elastic Load Balancing) AWS Global Accelerator、CloudFront 和 Route 53 託管區域上的應用程式為目標的未經授權事件提供更複雜的自動緩解措施。 如果您擁有高可見性網站或容易頻繁 DDoS 攻擊，您可以考慮 Shield Advanced 提供的其他功能。

您可以使用 Shield Advanced 自動應用程式層 DDoS 緩解功能來設定 Shield Advanced 自動回應，以緩解針對受保護 CloudFront 分佈、Elastic Load Balancing (Elastic Load Balancing) 負載平衡器 (Application、Network 和 Classic)、Amazon Route 53 託管區域、Amazon EC2 Elastic IP 地址和 AWS Global Accelerator 標準加速器的應用程式層 （ 第 7 層 ） 攻擊。當您啟用此功能時，Shield Advanced 會自動產生自訂 AWS WAF 規則以緩解 DDoS 攻擊。Shield Advanced 也可讓您存取AWS Shield 回應團隊 (SRT)。您可以隨時聯絡 SRT，為您的應用程式或在主動 DDoS 攻擊期間建立和管理自訂緩解措施。如果您希望 SRT 主動監控受保護的資源，並在 DDoS 嘗試期間與您聯絡，請考慮啟用主動參與功能。

設計考量

- 如果您有應用程式帳戶中面向網際網路的資源所面對的任何工作負載，例如 CloudFront、Application Load Balancer 或 Network Load Balancer，請在應用程式帳戶中設定 Shield Advanced，並將這些資源新增至 Shield 保護。您可以使用 大規模 AWS Firewall Manager 設定這些選項。
- 如果您在資料流程中有多個資源，例如 Application Load Balancer 前方的 CloudFront 分佈，請僅使用進入點資源做為受保護的資源。這將確保您不會為兩個資源支付兩次 Shield 資料傳出 (DTO) 費用。
- Shield Advanced 記錄您可以在 Amazon CloudWatch 中監控的指標。（如需詳細資訊，請參閱 AWS 文件中的 使用 Amazon CloudWatch 進行監控 。）設定 CloudWatch 警示，以在偵測 DDoS 事件時接收安全中心的 SNS 通知。在可疑的 DDoS 事件中，請提交支援票證並將其指派為最高優先順序，以聯絡AWS 企業支援團隊。處理此事件時，Enterprise Support 團隊將包括 Shield 回應團隊 (SRT)。此外，您可以預先設定 AWS Shield 參與 Lambda 函數來建立支援票證，並傳送電子郵件給 SRT 團隊。

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) 可讓您佈建、管理和部署公有和私有 TLS 憑證，以搭配 AWS 服務和您的內部連線資源使用。使用 ACM，您可以快速請求憑證、將其部署在 ACM 整合 AWS 的資源上，例如 Elastic Load Balancing 負載平衡器、CloudFront 分佈和 Amazon API Gateway 上的 APIs，並讓 ACM 處理憑證續約。當您請求 ACM 公有憑證 時，不需要產生金鑰對或憑證簽署請求 (CSR)、向憑證授權機構 (CA) 提交 CSR，或在接收憑證時上傳並安裝憑證。ACM 還提供匯入第三方 CA 發行的 TLS 憑證並使用 ACM 整合服務進行部署的選項。當您使用 ACM 管理憑證時，會使用強式加密和金鑰管理最佳事務來安全地保護和儲存憑證私有金鑰。使用 ACM，佈建公有憑證無需額外付費，且 ACM 可管理續約程序。

ACM 在網路帳戶中用於產生公有 TLS 憑證，CloudFront 分佈再使用此憑證在檢視器和 CloudFront 之間建立 HTTPS 連線。如需詳細資訊，請參閱 CloudFront 文件。

設計考量事項

對於面向外部的憑證，ACM 必須與為其佈建憑證的資源駐留在相同帳戶中。憑證不能跨帳戶共用。

Amazon Route 53

Amazon Route 53 是一種可用性高、可擴展性強的 DNS Web 服務。您可以使用 Route 53 執行以下三個主要功能：網域註冊、DNS 路由和運作狀態檢查。

您可以使用 Route 53 做為 DNS 服務，將網域名稱映射到您的 EC2 執行個體、S3 儲存貯體、CloudFront 分佈和其他 AWS 資源。 AWS DNS 伺服器的分散式性質有助於確保您的最終使用者一致地路由到您的應用程式。Route 53 流量和路由控制等 功能可協助您改善可靠性。如果您的主要應用程式端點不可用，您可以設定容錯移轉以將使用者重新路由至替代位置。Route 53 Resolver 透過 AWS Direct Connect 或 AWS 受管 VPN 為您的 VPC 和內部部署網路提供遞迴 DNS。

透過搭配 Route 53 使用 IAM 服務，您可以精細控制誰可以更新您的 DNS 資料。您可以啟用 DNS 安全延伸 (DNSSEC) 簽署，讓 DNS 解析程式驗證 DNS 回應是否來自 Route 53，並且尚未遭到竄改。

Route 53 Resolver DNS 防火牆為來自 VPC 的傳出 DNS 請求提供保護。這些請求會通過 Route 53 Resolver 進行網域名稱解析。DNS 防火牆保護的主要用途是協助防止 DNS 洩漏您的資料。透過 DNS 防火牆，您可以監控和控制應用程式可查詢的網域。您可以拒絕存取您已知行為不良的網域，並允許所有其他查詢通過。或者，您可以拒絕對除明確信任網域之外的所有網域的存取。您也可以使用 DNS 防火牆來封鎖對私人託管區域 (共用或本機) 中資源 (包括 VPC 端點名稱) 的解析請求。它也可以封鎖對公有或私有 EC2 執行個體名稱的請求。

依預設，Route 53 解析器會作為每個 VPC 的一部分建立。在 AWS SRA 中，Route 53 主要用於 DNS 防火牆功能的網路帳戶。

設計考量事項

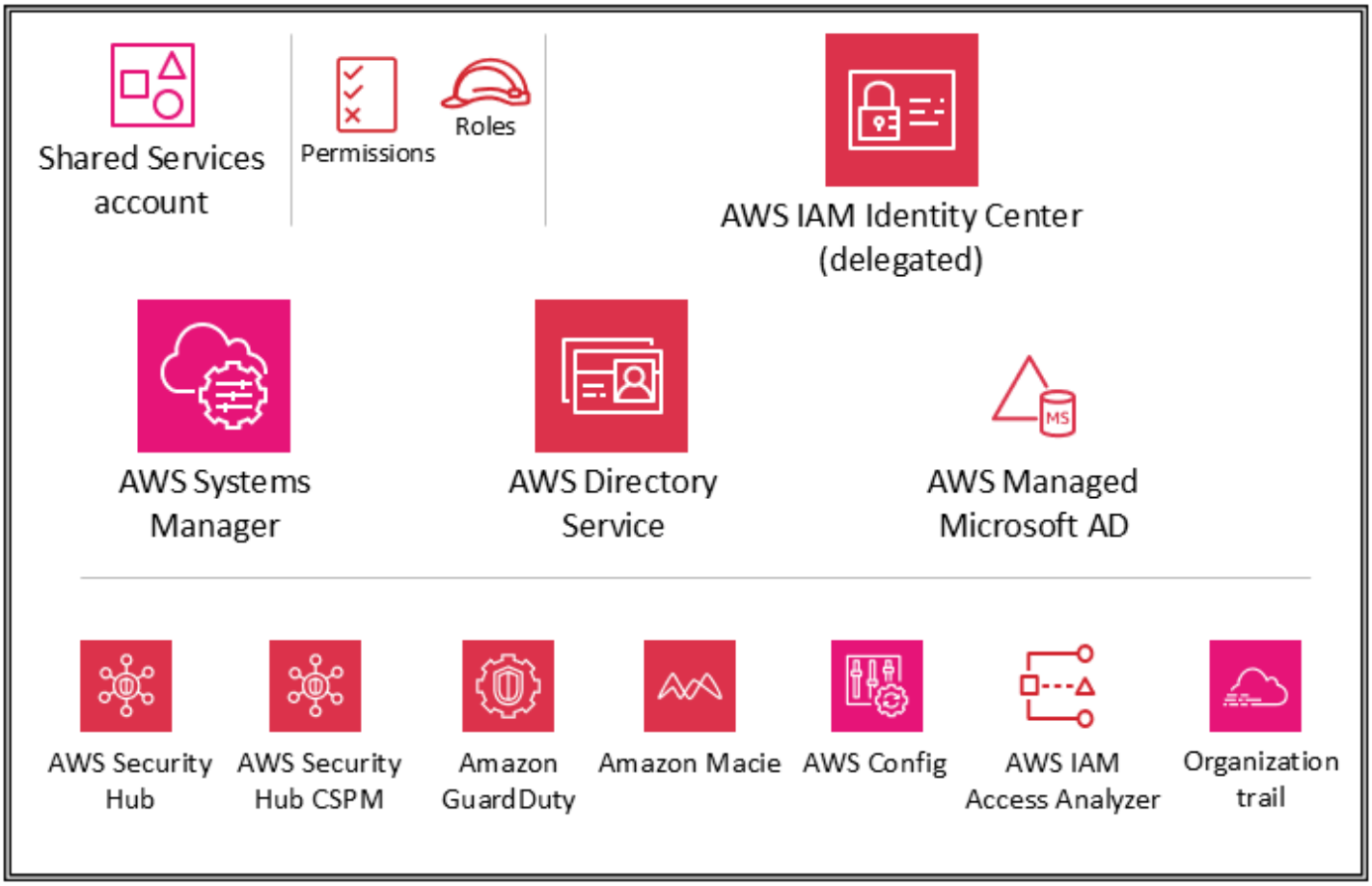
DNS 防火牆和 AWS Network Firewall 都提供網域名稱篩選，但適用於不同類型的流量。您可以同時使用 DNS 防火牆和 Network Firewall，為透過兩種不同網路路徑的應用程式層流量設定網域型篩選：

- DNS 防火牆針對從 VPC 內的應用程式透過 Route 53 Resolver 傳遞的傳出 DNS 查詢提供篩選功能。您也可以設定 DNS 防火牆，將查詢的自訂回應傳送至封鎖的網域名稱。
- Network Firewall 同時提供網路層和應用程式層流量的篩選功能，但是沒有 Route 53 Resolver 所實現的查詢可見性。

Infrastructure OU – 共用服務帳戶

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明共用服務帳戶中設定 AWS 的安全服務。



共享服務帳戶是基礎設施 OU 的一部分，其目的是支援多個應用程式和團隊用來實現其結果的服務。例如，目錄服務 (Active Directory)、簡訊服務和中繼資料服務都屬於此類別。 AWS SRA 會反白顯示支援安全控制的共用服務。雖然網路帳戶也是基礎設施 OU 的一部分，但它們會從共用服務帳戶中移除，以支援職責分離。將管理這些服務的團隊不需要網路帳戶的許可或存取權。

AWS Systems Manager

AWS Systems Manager （也包含在組織管理帳戶和應用程式帳戶中） 提供一組功能，可讓您了解和控制 AWS 資源。其中一個功能 Systems Manager Explorer 是可自訂的操作儀表板，可報告 AWS 資源的相關資訊。您可以使用 AWS Organizations 和 Systems Manager Explorer 來同步 AWS 組織

中所有帳戶的操作資料。Systems Manager 透過 中的委派管理員功能部署在共用服務帳戶中 AWS Organizations。

Systems Manager 會掃描您的受管執行個體，並在偵測到任何政策違規時回報 （或採取修正動作），以協助您維護安全性和合規性。透過將 Systems Manager 與個別成員 AWS 帳戶 （例如應用程式帳戶） 中的適當部署配對，您可以協調執行個體庫存資料收集，並集中自動化，例如修補和安全性更新。

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory也稱為 AWS Managed Microsoft AD，可讓您的目錄感知工作負載 AWS 和資源在 上使用受管 Active Directory AWS。您可以使用 AWS Managed Microsoft AD 將 Amazon EC2 for Windows Server、Amazon EC2 for Linux 和 Amazon RDS for SQL Server 執行個體加入您的網域，並使用 AWS 最終使用者運算 (EUC) 服務，例如 Amazon WorkSpaces，搭配 Active Directory 使用者和群組。

AWS Managed Microsoft AD 可協助您將現有的 Active Directory 擴展到 AWS ，並使用現有的現場部署使用者登入資料來存取雲端資源。您也可以管理您的現場部署使用者、群組、應用程式和系統，而無須執行和維護現場部署、高可用性 Active Directory 的複雜性。您可以將現有的電腦、筆記型電腦和印表機加入 AWS Managed Microsoft AD 網域。

AWS Managed Microsoft AD 是以 Microsoft Active Directory 為基礎，不需要您將現有 Active Directory 中的資料同步或複寫至雲端。您可以使用熟悉的 Active Directory 管理工具和功能，例如群組政策物件 (GPOs)、網域信任、精細密碼政策、群組受管服務帳戶 (gMSAs)、結構描述延伸和 Kerberos 型單一登入。您也可以委派管理任務，並使用 Active Directory 安全群組授權存取。

多區域複寫可讓您跨多個部署和使用單一 AWS Managed Microsoft AD 目錄 AWS 區域。這可讓您更輕鬆且更具成本效益地在全球部署和管理 Microsoft Windows 和 Linux 工作負載。當您使用自動多區域複寫功能時，您會在應用程式使用本機目錄以獲得最佳效能時獲得更高的彈性。

AWS Managed Microsoft AD 在用戶端和伺服器角色中都支援透過 SSL/TLS 的輕量型目錄存取通訊協定 (LDAP)，也稱為 LDAPS。做為伺服器時， AWS Managed Microsoft AD 透過連接埠 636 (SSL) 和 389 (TLS) 支援 LDAPS。您可以從 AWS型 Active Directory Certificate Services (AD CS) 憑證授權機構 (CA) 在 AWS Managed Microsoft AD 網域控制站上安裝憑證，以啟用伺服器端 LDAPS 通訊。當做為用戶端 時， 透過連接埠 636 (SSL) AWS Managed Microsoft AD 支援 LDAPS。您可以從伺服器憑證發行者註冊 CA 憑證，然後在目錄上啟用 LDAPS AWS，以啟用用戶端 LDAPS 通訊。

在 AWS SRA 中， Directory Service 會在共用服務帳戶中使用，為多個 AWS 成員帳戶的 Microsoft 感知工作負載提供網域服務。

設計考量事項

您可以使用 IAM Identity Center 並選取 AWS Managed Microsoft AD 作為身分來源，授予現場部署 Active Directory 使用者使用現有 Active Directory 憑證登入 和 AWS 管理主控台 AWS Command Line Interface (AWS CLI) 的存取權。這可讓您的使用者在登入時擔任其中一個指派的角色，並根據角色定義的許可來存取資源並對其採取動作。另一種方法是使用 AWS Managed Microsoft AD ，讓您的使用者擔任 IAM 角色。

IAM Identity Center

AWS SRA 使用 支援的委派管理員功能 AWS IAM Identity Center ，將大部分的 IAM Identity Center 管理委派給共用服務帳戶。這有助於限制需要存取組織管理帳戶的使用者數量。仍需要在組織管理帳戶中啟用 IAM Identity Center，才能執行特定任務，包括管理在組織管理帳戶中佈建的許可集。

使用共用服務帳戶做為 IAM Identity Center 委派管理員的主要原因是 Active Directory 位置。如果您打算使用 Active Directory 做為 IAM Identity Center 身分來源，則需要在您指定為 IAM Identity Center 委派管理員帳戶的成員帳戶中尋找目錄。在 AWS SRA 中，共享服務帳戶託管 AWS Managed Microsoft AD，讓帳戶成為 IAM Identity Center 的委派管理員。

IAM Identity Center 支援一次將單一成員帳戶註冊為委派管理員。只有在使用管理帳戶的登入資料登入時，才能註冊成員帳戶。若要啟用委派，您必須考慮 IAM Identity Center 文件中列出的先決條件。委派管理員帳戶可以執行大多數 IAM Identity Center 管理任務，但有一些限制會列在 IAM Identity Center 文件中。應嚴格控制對 IAM Identity Center 委派管理員帳戶的存取。

設計考量

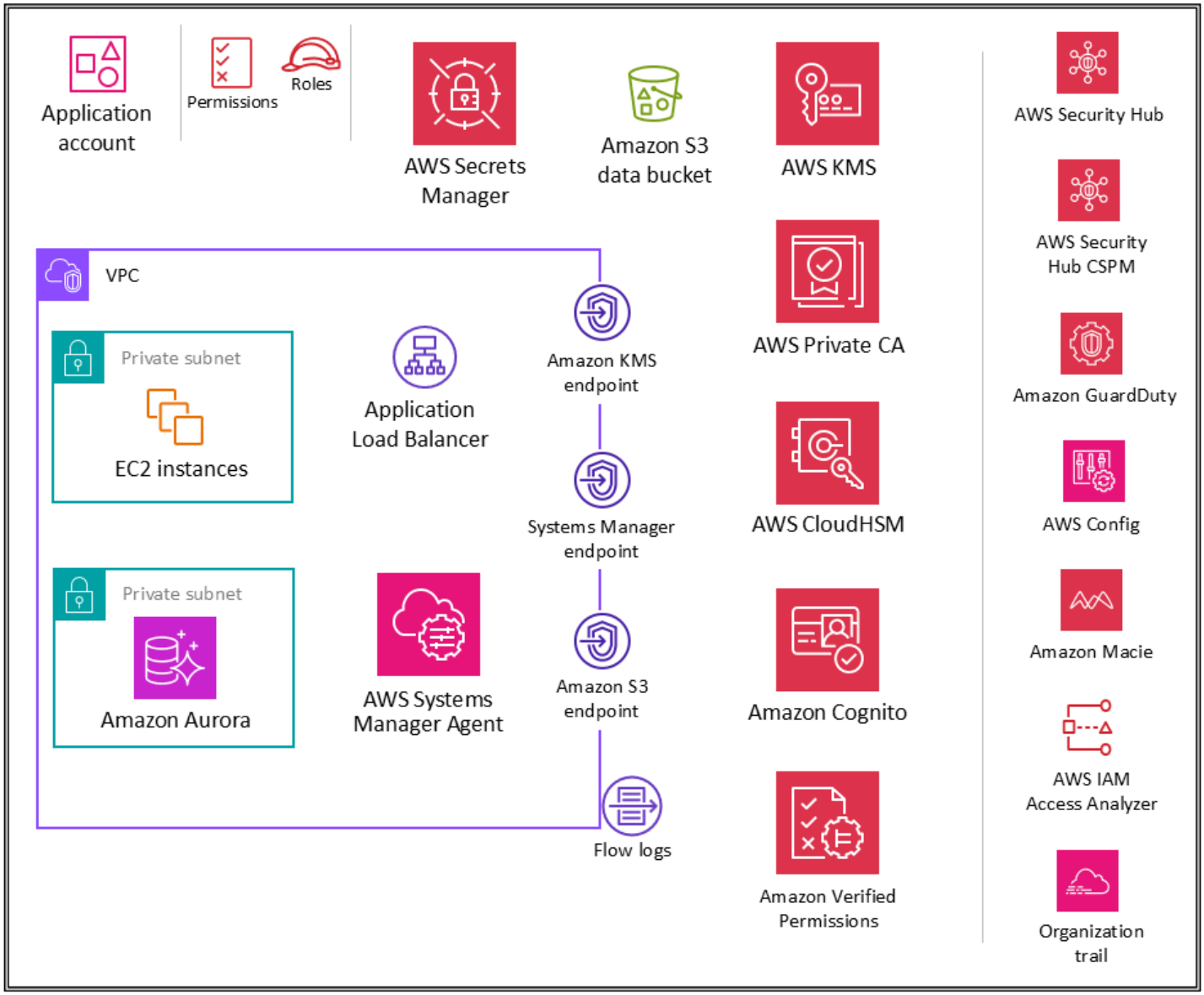
- 如果您決定將 IAM Identity Center 身分來源從任何其他來源變更為 Active Directory，或從 Active Directory 變更為任何其他來源，則目錄必須位於（由 擁有） IAM Identity Center 委派管理員成員帳戶，如果有的話；否則，必須位於管理帳戶中。
- 您可以在不同帳戶中的專用 VPC AWS Managed Microsoft AD 中託管您的 ，然後使用 AWS Resource Access Manager (AWS RAM) 將這個其他帳戶的子網路共用到委派的管理員帳戶。如此一來， AWS Managed Microsoft AD 執行個體在委派的管理員帳戶中受到控制，但從網路的角度來看，它就像在另一個帳戶的 VPC 中部署一樣。當您有多個 AWS Managed Microsoft AD 執行個體，而且您想要將它們部署到工作負載執行所在的本機，但透過一個帳戶集中管理它們時，這會很有幫助。

- 如果您有執行定期身分和存取管理活動的專用身分團隊，或具有嚴格的安全要求，可將身分管理函數與其他共用服務函數分開，則您可以託管專用 AWS 帳戶 身分管理。在此案例中，您將此帳戶指定為 IAM Identity Center 的委派管理員，同時也託管您的 AWS Managed Microsoft AD 目錄。您可以在單一共用服務帳戶中使用精細的 IAM 許可，在身分管理工作負載和其他共用服務工作負載之間達成相同層級的邏輯隔離。
- IAM Identity Center 目前不提供多區域支援。（若要在不同區域中啟用 IAM Identity Center，您必須先刪除目前的 IAM Identity Center 組態。）此外，它不支援將不同的身分來源用於不同的帳戶集，或讓您將許可管理委派給組織的不同部分（即多個委派管理員）或不同的管理員群組。如果您需要任何這些功能，您可以使用 IAM 聯合來管理 外部身分提供者 (IdP) 內的使用者身分， AWS 並提供這些外部使用者身分許可，以使用您帳戶中 AWS 的資源。IAM 支援與 OpenID Connect (OIDC) 或 SAML 2.0 相容的 IdPs。最佳實務是將 SAML 2.0 聯合與第三方身分提供者搭配使用，例如 Active Directory Federation Service (AD FS)、Okta、Azure Active Directory (Azure AD) 或 Ping Identity，以提供單一登入功能，讓使用者登入 AWS 管理主控台 或呼叫 AWS API 操作。如需 IAM 聯合和身分提供者的詳細資訊，請參閱 IAM 文件中的關於 SAML 2.0 型聯合。

工作負載 OU – 應用程式帳戶

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

下圖說明應用程式帳戶中設定 AWS 的安全服務（以及應用程式本身）。



應用程式帳戶託管主要基礎設施和服務，以執行和維護企業應用程式。應用程式帳戶和工作負載 OU 提供幾個主要安全目標。首先，您可以為每個應用程式建立單獨的帳戶，以提供工作負載之間的界限和控制，以避免即將發佈的角色、許可、資料和加密金鑰的問題。您想要提供單獨的帳戶容器，讓應用程式團隊有權管理自己的基礎設施，而不會影響其他人。接著，您可以為安全營運團隊提供監控和收集安全資料的機制，以新增保護層。使用由安全團隊設定和監控的組織追蹤和帳戶安全服務的本機部署 (Amazon GuardDuty AWS Config、 AWS Security Hub CSPM、Amazon EventBridge、IAM Access Analyzer)。最後，您可以讓企業集中設定控制項。您可以讓應用程式帳戶成為工作負載 OU 的成員，藉此繼承適當的服務許可、限制條件和護欄，使其符合更廣泛的安全結構。

設計考量事項

在您的組織中，您可能會有一個以上的商業應用程式。Workloads OU 旨在容納大部分的業務特定工作負載，包括生產和非生產環境。這些工作負載可以是商業off-the-shelf(COTS) 應用程式和您自己的內部開發自訂應用程式和資料服務的組合。組織不同業務應用程式及其開發環境的模式很少。一種模式是根據您的開發環境擁有多個子 OUs，例如生產、預備、測試和開發，並在這些 OUs AWS 帳戶 下使用與不同應用程式相關的個別子系。另一個常見的模式是每個應用程式有個別的子 OUs，然後 AWS 帳戶 針對個別開發環境使用個別的子 OU。確切的 OU 和帳戶結構取決於您的應用程式設計和管理這些應用程式的團隊。考慮您要強制執行的安全控制，無論它們是環境特定還是應用程式特定，因為在 OUs 上將這些控制作為 SCPs 實作更容易。如需組織工作負載導向 OUs的進一步考量，請參閱 AWS 白皮書的應用程式 OUs 一節使用多個帳戶組織您的 AWS 環境。

應用程式 VPC

應用程式帳戶中的虛擬私有雲端 (VPC) 需要傳入存取（適用於您正在建模的簡單 Web 服務）和傳出存取（適用於應用程式需求）AWS 服務。根據預設，VPC 內的資源可以彼此路由。有兩個私有子網路：一個用於託管 EC2 執行個體（應用程式層），另一個用於 Amazon Aurora（資料庫層）。不同層之間的網路分割，例如應用程式層和資料庫層，是透過限制執行個體層級流量的 VPC 安全群組來完成。對於彈性，工作負載跨越兩個或多個可用區域，並在每個區域使用兩個子網路。

設計考量事項

您可以使用流量鏡像從 EC2 執行個體的彈性網路界面複製網路流量。然後，您可以將流量傳送到out-of-band安全和監控設備，以進行內容檢查、威脅監控或故障診斷。例如，您可能想要監控離開 VPC 的流量，或來源位於 VPC 外部的流量。在此情況下，您將鏡像 VPC 內傳遞的流量以外的所有流量，並將其傳送至單一監控設備。Amazon VPC 流程日誌不會擷取鏡像流量；它們通常只會從封包標頭擷取資訊。流量鏡射可讓您分析實際流量內容，包括承載，藉此更深入了解網路流量。僅針對可能作為敏感工作負載一部分操作的 EC2 執行個體彈性網路界面，或預期在發生問題時需要詳細診斷的執行個體啟用流量鏡射。

VPC 端點

VPC 端點提供另一層安全控制，以及可擴展性和可靠性。使用這些項目將您的應用程式 VPC 連接到其他 VPC AWS 服務。（在應用程式帳戶中， AWS SRA 會為 AWS KMS AWS Systems Manager

和 Amazon S3 使用 VPC 端點。) 端點是虛擬裝置。這些端點是水平擴展、冗餘且高度可用的 VPC 元件。其可讓您 VPC 中的執行個體與服務進行通訊，而不會強加網路流量的可用性風險或頻寬限制。您可以使用 VPC 端點將 VPC 私下連線至支援 AWS 服務 且採用 技術的 VPC 端點服務， AWS PrivateLink 而不需要網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可與其他 通訊 AWS 服務。您的 VPC 與另一個 VPC 之間的流量 AWS 服務 不會離開 Amazon 網路。

使用 VPC 端點的另一個好處是啟用端點政策的組態。當您建立或修改端點時，VPC 端點政策是您連接至端點的 IAM 資源政策。如果您在建立端點時未連接 IAM 政策， 會為您 AWS 連接允許完整存取服務的預設 IAM 政策。端點原則不會覆寫或取代 IAM 使用者原則或服務特定原則 (例如 S3 儲存貯體原則)。這是單獨的 IAM 政策，用於控制從端點到指定服務的存取。如此一來，它會新增另一層控制，讓 AWS 主體可以與資源或服務進行通訊。

Amazon EC2

構成我們應用程式的 Amazon EC2 執行個體會使用執行個體中繼資料服務 (IMDSv2) 第 2 版。IMDSv2 為四種類型的漏洞新增了保護，可用於嘗試存取 IMDS：網站應用程式防火牆、開放反向代理、伺服器端請求偽造 (SSRF) 漏洞、開放第 3 層防火牆和 NATs。如需詳細資訊，請參閱部落格文章 新增對開放防火牆的深度防禦、反向代理和對 EC2 執行個體中繼資料服務的增強功能的 SSRF 漏洞。

使用個別 VPCs（做為帳戶邊界的子集） 依工作負載區段隔離基礎設施。使用子網來隔離單一 VPC 內的應用程式層 (例如，Web、應用程式及資料庫)。如果不應該從網際網路直接存取，則針對您的執行個體使用私有子網。若要從私有子網路呼叫 Amazon EC2 API，而不使用網際網路閘道，請使用 AWS PrivateLink。使用 安全群組限制對執行個體的存取。 使用 VPC 流程日誌 來監控到達執行個體的流量。使用 的 Session Manager 來遠端存取您的執行個體 AWS Systems Manager，而不是開啟傳入 SSH 連接埠和管理 SSH 金鑰。為作業系統和您的資料使用單獨的 Amazon Elastic Block Store (Amazon EBS) 磁碟區。 您可以設定 AWS 帳戶來強制加密您建立的新 EBS 磁碟區和快照副本。

> **實作範例**
>
> AWS SRA 程式碼庫提供在 Amazon EC2 中預設 Amazon EBS 加密的範例實作。它示範如何在 AWS 區域 AWS 組織中的每個 AWS 帳戶 和 內啟用帳戶層級的預設 Amazon EBS 加密。

AWS Nitro Enclaves

AWS Nitro Enclaves 是一種 Amazon EC2 功能，可讓您從 EC2 執行個體建立稱為 enclaves 的隔離執行環境。隔離區是獨立、強化且高度受限的虛擬機器。單一父系 EC2 執行個體的 CPU 和記憶體會分

割為隔離的 enclaves。每個 enclave 都會執行獨立的核心。Enclaves 僅提供與其父執行個體的安全本機通訊端連線。不具有持久性儲存、互動式存取或外部聯網功能。使用者無法 SSH 進入 enclave，而且父執行個體的程序、應用程式或使用者（根或管理員）無法存取 enclave 內的資料和應用程式。您可以在 EC2 執行個體中保護最敏感的資料，例如個人身分識別資訊 (PII)、醫療保健、財務和智慧財產權資料。Nitro Enclaves 可讓您專注於應用程式，而不必擔心與外部服務的整合。Nitro Enclaves 包含軟體的密碼編譯認證，因此您可以確定只有授權的程式碼正在執行，並與 整合， AWS KMS 以便只有您的 Enclaves 可以存取敏感材料。這有助於減少最敏感資料處理應用程式的攻擊面區域。使用 Nitro Enclaves 無需額外費用。

密碼編譯認證是一種用來證明 enclave 身分的程序。認證程序是透過 Nitro Hypervisor 完成，它會為 enclave 產生簽署的認證文件，以向其他第三方或服務證明其身分。證明文件包含 enclave 的金鑰詳細資訊，例如 enclave 的公有金鑰、enclave 映像和應用程式的雜湊等。

透過適用於 Nitro Enclaves 的 AWS Certificate Manager (ACM)，您可以將公有和私有 SSL/TLS 憑證與在具有 Nitro Enclaves 的 EC2 執行個體上執行的 Web 應用程式和 Web 伺服器搭配使用。SSL/TLS 憑證用於保護網路通訊，並透過網際網路和私有網路上的資源建立網站身分。ACM for Nitro Enclaves 會移除購買、上傳和續約 SSL/TLS 憑證時耗時且容易出錯的手動程序。ACM for Nitro Enclaves 會建立安全的私有金鑰、將憑證及其私有金鑰分發至您的 enclave，以及管理憑證續約。使用適用於 Nitro Enclaves 的 ACM，憑證的私有金鑰在 enclave 中保持隔離，以防止執行個體及其使用者存取它。如需詳細資訊，請參閱 AWS Certificate Manager Nitro Enclaves 文件中的 for Nitro Enclaves。

Application Load Balancer

Application Load Balancer 會將傳入應用程式流量分散到多個可用區域中的多個目標，例如 EC2 執行個體。在 AWS SRA 中，負載平衡器的目標群組是應用程式 EC2 執行個體。 AWS SRA 使用 HTTPS 接聽程式來確保通訊管道已加密。Application Load Balancer 使用伺服器憑證來終止前端連線，然後解密用戶端的請求，再將請求傳送至目標。

AWS Certificate Manager (ACM) 原生與 Application Load Balancer 整合，SRA AWS 使用 ACM 來產生和管理必要的 X.509 (TLS 伺服器）公有憑證。您可以透過 Application Load Balancer 安全政策強制執行前端連線的 TLS 1.2 和強式密碼。如需詳細資訊，請參閱 Elastic Load Balancing 說明文件。

設計考量

- 對於在 Application Load Balancer 上需要私有 TLS 憑證的嚴格內部應用程式等常見案例，您可以使用此帳戶中的 ACM 從中產生私有憑證 AWS 私有 CA。在 AWS SRA 中，ACM 根私有 CA 託管在安全工具帳戶中，並且可以與整個 AWS 組織或特定於 AWS 帳戶 發行終端實體憑證共用，如安全工具帳戶一節中所述。

- 對於公有憑證，您可以使用 ACM 產生這些憑證並進行管理，包括自動輪換。或者，您可以使用 SSL/TLS 工具建立憑證簽署請求 (CSR)、取得憑證授權單位 (CA) 簽署的 CSR 來產生憑證，然後將憑證匯入 ACM 或上傳憑證至 IAM，以搭配 Application Load Balancer 使用。如果您將憑證匯入 ACM，則必須監控憑證的過期日期，並在憑證過期之前續約。
- 對於額外的防禦層，您可以部署 AWS WAF 政策來保護 Application Load Balancer。擁有邊緣政策、應用程式政策，甚至是私有或內部政策強制執行層，可提高通訊請求的可見性，並提供統一的政策強制執行。如需詳細資訊，請參閱部落格文章使用 for 深入部署防禦 AWS 受管規則AWS WAF。

AWS 私有 CA

AWS 私有憑證授權單位 (AWS 私有 CA) 用於應用程式帳戶中，以產生要與 Application Load Balancer 搭配使用的私有憑證。Application Load Balancer 透過 TLS 提供安全內容的常見案例。這需要在 Application Load Balancer 上安裝 TLS 憑證。對於嚴格內部的應用程式，私有 TLS 憑證可以提供安全頻道。

在 AWS SRA 中， AWS 私有 CA 託管在安全工具帳戶中，並使用 與應用程式帳戶共用 AWS RAM。這可讓應用程式帳戶中的開發人員向共用私有 CA 請求憑證。跨組織或跨組織共用 CAs， AWS 帳戶有助於降低在所有 中建立和管理重複 CAs的成本和複雜性 AWS 帳戶。當您使用 ACM 從共用 CA 發行私有憑證時，憑證會在請求帳戶中本機產生，ACM 會提供完整的生命週期管理和續約。

Amazon Inspector

AWS SRA 使用 Amazon Inspector 自動探索和掃描 Amazon Elastic Container Registry (Amazon ECR) 中存在 的軟體漏洞和意外網路暴露的 EC2 執行個體和容器映像。

Amazon Inspector 會放置在應用程式帳戶中，因為它會為此帳戶中的 EC2 執行個體提供漏洞管理服務。此外，Amazon Inspector 會報告往返 EC2 執行個體的不需要網路路徑。

成員帳戶中的 Amazon Inspector 由委派管理員帳戶集中管理。在 AWS SRA 中，安全工具帳戶是委派的管理員帳戶。委派的管理員帳戶可以管理組織成員的問題清單資料和特定設定。這包括檢視所有成員帳戶的彙總調查結果詳細資訊、啟用或停用成員帳戶的掃描，以及檢閱 AWS 組織內掃描的資源。

設計考量事項

您可以使用 的修補程式管理員 AWS Systems Manager來觸發隨需修補，以修復 Amazon Inspector 零時差或其他重大安全漏洞。修補程式管理員可協助您修補這些漏洞，而不必等待

正常的修補排程。修復是透過使用 Systems Manager Automation Runbook 來執行。如需詳細資訊，請參閱兩部分部落格系列AWS 使用 Amazon Inspector 和 在 中自動化漏洞管理和修復 AWS Systems Manager。

AWS Systems Manager

AWS Systems Manager 是 AWS 服務 ，可用來檢視來自多個 的操作資料， AWS 服務 並自動化整個 AWS 資源的操作任務。透過自動化 核准工作流程和 Runbook，您可以努力減少人為錯誤，並簡化 AWS 資源的維護和部署任務。

除了這些一般自動化功能之外，Systems Manager 還支援許多預防性、偵測性和回應式安全功能。AWS Systems Manager Agent (SSM Agent) 是可在 EC2 執行個體、內部部署伺服器或虛擬機器 (VM) 上安裝和設定的 Amazon 軟體。SSM Agent 讓 Systems Manager 能夠更新、管理和設定這些資源。Systems Manager 會掃描這些受管執行個體，並在修補程式、組態和自訂政策中偵測到的任何違規時回報 （或採取修正動作），以協助您維護安全性和合規性。

AWS SRA 使用 Systems Manager 的功能 Session Manager，以提供互動式、以瀏覽器為基礎的 shell 和 CLI 體驗。這可提供安全且可稽核的執行個體管理，而不需要開啟傳入連接埠、維護堡壘主機或管理 SSH 金鑰。 AWS SRA 使用 Systems Manager 的修補程式管理員功能，將修補程式套用至作業系統和應用程式的 EC2 執行個體。

AWS SRA 也使用 Systems Manager 的自動化功能，來簡化 Amazon EC2 執行個體和其他 AWS 資源的常見維護和部署任務。Automation 可以簡化一般 IT 任務，例如變更一個或多個節點的狀態 (使用核准自動化) 和根據排程管理節點狀態。Systems Manager 包含的功能可協助您使用標籤以大型執行個體群組為目標，而速度控制可協助您根據您定義的限制推出變更。自動化提供一鍵式自動化，可簡化複雜的任務，例如建立黃金 Amazon Machine Image (AMIs) 和復原無法連線的 EC2 執行個體。此外，您可以讓 IAM 角色存取特定 Runbook 以執行特定函數，而無需直接授予這些角色許可，從而增強營運安全性。例如，如果您希望 IAM 角色在修補程式更新後具有重新啟動特定 EC2 執行個體的許可，但您不想直接將許可授予該角色，您可以改為建立 Automation Runbook，並授予角色僅執行 Runbook 的許可。

設計考量

- Systems Manager 依賴 EC2 執行個體中繼資料才能正確運作。Systems Manager 可以使用執行個體中繼資料服務 (IMDSv1 和 IMDSv2 2) 的第 1 版或第 2 版存取執行個體中繼資料。
- SSM 代理程式必須與不同的 AWS 服務 和 資源通訊，例如 Amazon EC2 訊息、Systems Manager 和 Amazon S3。若要進行此通訊，子網路需要傳出網際網路連線或佈建適當的

VPC 端點。 AWS SRA 使用 SSM Agent 的 VPC 端點來建立各種 的私有網路路徑 AWS 服務。

- 使用 Automation 可讓您與整個組織分享最佳實務。您可以在 Runbook 中建立資源管理的最佳實務，並在 AWS 區域 和 群組之間共用 Runbook。您也可以限制 Runbook 參數的允許值。對於這些使用案例，您可能需要在 Security Tooling 或 Shared Services 等中央帳戶中建立 Automation Runbook，並與 AWS 組織的其餘部分共用。常見的使用案例包括集中實作修補和安全性更新、修復 VPC 組態或 S3 儲存貯體政策上的偏離，以及大規模管理 EC2 執行個體的功能。如需實作詳細資訊，請參閱 Systems Manager 文件。

Amazon Aurora

在 AWS SRA 中，Amazon Aurora 和 Amazon S3 會組成邏輯資料層。Aurora 為全受管關聯式資料庫引擎，可與 MySQL 和 PostgreSQL 相容。在 EC2 執行個體上執行的應用程式會視需要與 Aurora 和 Amazon S3 通訊。Aurora 是使用資料庫子網路群組內的資料庫叢集進行設定。

設計考量事項

如同許多資料庫服務一樣，Aurora 的安全管理分為三個層級。若要控制誰可以在 Aurora 資料庫叢集和資料庫執行個體上執行 Amazon Relational Database Service (Amazon RDS) 管理動作，請使用 IAM。若要控制哪些裝置和 EC2 執行個體可以開啟與 VPC 中 Aurora 資料庫叢集之叢集端點和資料庫執行個體連接埠的連線，您可以使用 VPC 安全群組。若要驗證 Aurora 資料庫叢集的登入和許可，您可以採取與 MySQL 或 PostgreSQL 獨立資料庫執行個體相同的方法，也可以針對 Aurora MySQL 相容版本使用 IAM 資料庫身分驗證。透過此後一種方法，您可以使用 IAM 角色和身分驗證字符，向 Aurora MySQL 相容資料庫叢集進行身分驗證。

Amazon S3

Amazon S3 是一種物件儲存服務，可提供業界領先的可擴展性、資料可用性、安全性和效能。它是許多應用程式建置的資料骨幹 AWS，適當的許可和安全控制對於保護敏感資料至關重要。如需 Amazon S3 的建議安全最佳實務，請參閱 部落格文章中的文件、線上技術講座和深入探討。最重要的最佳實務是封鎖對 S3 儲存貯體的過度允許存取 （特別是公開存取）。

AWS KMS

AWS SRA 說明建議的金鑰管理分佈模型，其中 AWS KMS key 與要加密 AWS 帳戶 的資源位於相同的 內。因此，除了包含在 安全工具帳戶中之外， AWS KMS 也會在應用程式帳戶中使用。在應用程式

帳戶中，AWS KMS 用於管理應用程式資源特有的金鑰。您可以使用金鑰政策將金鑰使用許可授予本機應用程式角色，以及限制金鑰託管人的管理和監控許可，以實作職責分離。

設計考量事項

在分散式模型中，AWS KMS 金鑰管理責任屬於應用程式團隊。不過，您的中央安全團隊可以負責控管和監控重要的密碼編譯事件，例如：

- KMS 金鑰中匯入的金鑰材料接近其過期日期。
- KMS 金鑰中的金鑰材料會自動輪換。
- 已刪除 AKMS 金鑰。
- 解密失敗率很高。

AWS CloudHSM

AWS CloudHSM 在 中提供受管硬體安全模組 HSMs) AWS 雲端。它可讓您 AWS 使用您控制存取的 FIPS 140-2 第 3 級驗證 HSMs，在 上產生和使用自己的加密金鑰。您可以使用 AWS CloudHSM 卸載 Web 伺服器的 SSL/TLS 處理。這可減輕 Web 伺服器的負擔，並透過將 Web 伺服器的私有金鑰存放在其中來提供額外的安全性 AWS CloudHSM。您可以類似的方式 AWS CloudHSM ，從 網路帳戶中的傳入 VPC 中部署 HSM，以存放私有金鑰，並在需要做為發行憑證授權單位時簽署憑證請求。

設計考量事項

如果您有 FIPS 140-2 第 3 級的硬性需求，您也可以選擇 AWS KMS 將 設定為使用 AWS CloudHSM 叢集做為自訂金鑰存放區，而不是使用原生 KMS 金鑰存放區。透過這樣做，您可以從加密資料的 AWS KMS 和 AWS 服務 之間的整合中受益，同時負責保護 KMS 金鑰 HSMs。這結合了您控制的單一租用戶 HSMs，以及 的易用性和整合 AWS KMS。若要管理您的 AWS CloudHSM 基礎設施，您必須採用公有金鑰基礎設施 (PKI)，並擁有具備管理 HSMs 經驗的團隊。

AWS Secrets Manager

AWS Secrets Manager 可協助您保護存取應用程式、服務和 IT 資源所需的登入資料 (秘密)。此服務可讓您在整個生命週期中有效率地輪換、管理和擷取資料庫登入資料、API 金鑰和其他秘密。您可以使用對 Secrets Manager 的 API 呼叫取代程式碼中的硬式編碼登入資料，以程式設計方式擷取秘密。這有

助於確保檢查程式碼的人員不會洩露秘密，因為該秘密不再存在於程式碼中。此外，Secrets Manager 可協助您在環境之間移動應用程式（開發、生產前、生產）。您可以確保環境中有適當命名和參考的秘密，而不是變更程式碼。這可提升不同環境中應用程式程式碼的一致性和重複使用性，同時在測試程式碼之後，需要的變更和人為互動較少。

透過 Secrets Manager，您可以使用精細的 IAM 政策和以資源為基礎的政策來管理對秘密的存取。您可以使用您管理的加密金鑰來加密秘密，以協助保護秘密 AWS KMS。Secrets Manager 也與 AWS 記錄和監控服務整合，以進行集中式稽核。

Secrets Manager 使用信封加密搭配 AWS KMS keys 和 資料金鑰來保護每個秘密值。建立秘密時，您可以選擇 AWS 帳戶 和 區域中的任何對稱客戶受管金鑰，也可以使用 Secrets Manager 的 AWS 受管金鑰。

最佳實務是，您可以監控秘密，以記錄對秘密的任何變更。這可協助您確保可以調查任何非預期的使用或變更。不需要的變更可以復原。Secrets Manager 目前支援兩個 AWS 服務 ，可讓您監控您的組織和活動： AWS CloudTrail 以及 AWS Config。CloudTrail 將 Secrets Manager 的所有 API 呼叫擷取為事件，包括來自 Secrets Manager 主控台的呼叫以及來自對 Secrets Manager API 發出的程式碼呼叫。此外，CloudTrail 會擷取可能對您的安全或合規造成影響的其他相關（非 API) 事件， AWS 帳戶 或可協助您疑難排解操作問題。其中包括特定秘密輪換事件和刪除秘密版本。 AWS Config 可以透過追蹤和監控 Secrets Manager 中秘密的變更，提供偵測性控制。這些變更包括秘密的描述、輪換組態、標籤，以及與其他 AWS 來源的關係，例如 KMS 加密金鑰或用於秘密輪換的 AWS Lambda 函數。您也可以設定 Amazon EventBridge 接收來自 的組態和合規變更通知 AWS Config，以路由特定秘密事件以進行通知或修復動作。

在 AWS SRA 中，Secrets Manager 位於應用程式帳戶中，以支援本機應用程式使用案例和管理接近其用量的秘密。在這裡，執行個體描述檔會連接到應用程式帳戶中的 EC2 執行個體。然後，可以在 Secrets Manager 中設定個別的秘密，以允許該執行個體描述檔擷取秘密，例如，加入適當的 Active Directory 或 LDAP 網域，以及存取 Aurora 資料庫。Secrets Manager 與 Amazon RDS 整合，可在您建立、修改或還原 Amazon RDS 資料庫執行個體或多可用區域資料庫叢集時管理使用者憑證。這可協助您管理金鑰的建立和輪換，並將程式碼中的硬式編碼登入資料取代為對 Secrets Manager 的程式設計 API 呼叫。

設計考量事項

一般而言，請在最接近將使用秘密的帳戶中設定和管理 Secrets Manager。此方法利用使用案例的當地知識，並為應用程式開發團隊提供速度和靈活性。對於可能適合額外控制層的嚴格控制資訊，可以在安全工具帳戶中由 Secrets Manager 集中管理秘密。

Amazon Cognito

Amazon Cognito 可讓您快速且有效率地將使用者註冊、登入和存取控制新增至您的 Web 和行動應用程式。Amazon Cognito 擴展到數百萬使用者，並支援透過 SAML 2.0 和 OpenID Connect 等社交身分提供者登入，例如 Apple、Facebook、Google 和 Amazon，以及企業身分提供者。Amazon Cognito 的兩個主要元件是使用者集區和身分集區。使用者集區是為應用程式使用者提供註冊和登入選項的使用者目錄。身分集區可讓您授予使用者對其他 的存取權 AWS 服務。您可以單獨或一併使用身分集區和使用者集區。如需常見使用案例，請參閱 Amazon Cognito 文件。

Amazon Cognito 為使用者註冊和登入提供內建且可自訂的 UI。您可以使用適用於 Amazon Cognito 的 Android、iOS 和 JavaScript SDKs，將使用者註冊和登入頁面新增至您的應用程式。Amazon Cognito Sync 是 AWS 服務 和 用戶端程式庫，可跨裝置同步應用程式相關的使用者資料。

Amazon Cognito 支援靜態資料和傳輸中資料的多重驗證和加密。 Amazon Cognito 使用者集區提供進階安全功能，可協助保護對應用程式中使用者帳戶的存取。這些進階安全功能提供以風險為基礎的適應性身分驗證，並防止使用遭入侵的登入資料。

設計考量

- 您可以建立 AWS Lambda 函數，然後在使用者集區操作期間觸發該函數，例如使用 Lambda 觸發器的使用者註冊、確認和登入 （驗證）。您可以新增驗證挑戰、遷移使用者，以及自訂驗證訊息。如需常見操作和使用者流程，請參閱 Amazon Cognito 文件。Amazon Cognito 會同步呼叫 Lambda 函數。
- 您可以使用 Amazon Cognito 使用者集區來保護小型、多租用戶應用程式。多租戶設計的常見使用案例是執行工作負載，以支援測試多個版本的應用程式。多重租用戶設計對於使用不同資料集測試單一應用程式也很實用，可讓您充分利用叢集資源。不過，請確定租戶和預期數量符合相關的 Amazon Cognito 服務配額。應用程式中的所有租用戶會共用這些配額。

Amazon Verified Permissions

Amazon Verified Permissions 是您建置之應用程式的可擴展許可管理和精細授權服務。開發人員和管理員可以使用 Cedar，這是一種專門建置且安全優先的開放原始碼政策語言，搭配角色和屬性來定義更精細、內容感知的政策型存取控制。開發人員可以透過外部化授權並集中管理政策，更快速地建置更安全的應用程式。Verified Permissions 包含結構描述定義、政策陳述式文法，以及跨數百萬個許可擴展的 自動化推理 ，因此您可以強制執行預設拒絕和最低權限的原則。此服務也包含評估模擬器工具，可協助您測試授權決策和作者政策。這些功能有助於部署深入的精細授權模型，以支援您的 零信任 目

標。Verified Permissions 會集中政策存放區中的許可，並協助開發人員使用這些許可來授權其應用程式中的使用者動作。

您可以透過 API 將應用程式連線至 服務，以授權使用者存取請求。對於每個授權請求，服務會擷取相關政策並評估這些政策，以根據使用者、角色、群組成員資格和屬性等內容輸入，判斷是否允許使用者對資源採取動作。您可以設定並連接 Verified Permissions 以傳送您的政策管理和授權日誌 AWS CloudTrail。如果您使用 Amazon Cognito 做為身分存放區，則可以與 Verified Permissions 整合，並使用 Amazon Cognito 在應用程式中的授權決策中傳回的 ID 和存取權杖。您可以將 Amazon Cognito 權杖提供給 Verified Permissions，這會使用權杖包含的屬性來代表委託人並識別委託人的權利。如需此整合的詳細資訊，請參閱 AWS 部落格文章 使用 Amazon Verified Permissions 和 Amazon Cognito 簡化精細授權。

Verified Permissions 可協助您定義以政策為基礎的存取控制 (PBAC)。PBAC 是一種存取控制模型，使用以政策表示的許可來判斷誰可以存取應用程式中的哪些資源。PBAC 將角色型存取控制 (RBAC) 和屬性型存取控制 (ABAC) 結合在一起，產生更強大且靈活的存取控制模型。若要進一步了解 PBAC 以及如何使用 Verified Permissions 設計授權模型，請參閱 AWS 部落格文章使用 Amazon Verified Permissions 在應用程式開發中以政策為基礎的存取控制。

在 AWS SRA 中，Verified Permissions 位於應用程式帳戶中，透過與 Amazon Cognito 的整合支援應用程式的許可管理。

分層防禦

應用程式帳戶提供機會說明 AWS 啟用的分層防禦主體。考慮組成 AWS SRA 中呈現之簡單範例應用程式核心的 EC2 執行個體的安全性，您可以看到在分層防禦中一起 AWS 服務 運作的方式。此方法符合 AWS 安全服務的結構檢視，如本指南稍早在組織中套用安全服務 AWS一節所述。

- 最內層是 EC2 執行個體。如前所述，EC2 執行個體預設包含許多原生安全功能或 選項。範例包括 IMDSv2、 Nitro 系統和 Amazon EBS 儲存加密。
- 第二層保護著重於在 EC2 執行個體上執行的作業系統和軟體。Amazon Inspector 等服務AWS Systems Manager可讓您監控、報告這些組態並採取修正動作。Amazon Inspector 會監控您的軟體是否有漏洞，Systems Manager 會掃描受管執行個體的修補程式和組態狀態，然後報告並採取您指定的任何修正動作，以協助您維護安全性和合規性。
- 執行個體和在這些執行個體上執行的軟體會與您的 AWS 聯網基礎設施一起運作。除了使用 Amazon VPC 的安全功能之外， AWS SRA 還利用 VPC 端點，在 VPC 和支援之間提供私有連線 AWS 服務，並提供機制以在網路邊界放置存取政策。

- EC2 執行個體、軟體、網路和 IAM 角色和資源的活動和組態，會受到 AWS 帳戶聚焦服務的監控 AWS Security Hub CSPM AWS Security Hub，例如 Amazon GuardDuty、 AWS CloudTrail AWS Config、IAM Access Analyzer 和 Amazon Macie。
- 最後，除了應用程式帳戶之外， AWS RAM 可協助控制與其他帳戶共用的資源，而 IAM 服務控制政策可協助您在整個 AWS 組織中強制執行一致的許可。

安全 AI/ML

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

人工智慧和機器學習 (AI/ML) 正在改變企業。AI/ML 已成為 Amazon 的焦點超過 20 年，客戶與 搭配使用的許多功能 AWS，包括安全服務，都由 AI/ML 驅動。這可建立內建差異化值，因為您可以安全地建置 ， AWS 而不需要您的安全或應用程式開發團隊具備 AI/ML 的專業知識。

AI 是一種進階技術，可讓機器和系統取得智慧和預測功能。AI 系統透過其耗用或訓練的資料，從過去的經驗中學習。ML 是 AI 最重要的層面之一。ML 是電腦無需明確程式設計即可從資料中學習的能力。在傳統程式設計中，程式設計人員會撰寫規則，定義程式在電腦或機器上應如何運作。在 ML 中，模型會從資料中學習規則。ML 模型可以探索資料中的隱藏模式，或對訓練期間未使用的新資料進行準確的預測。多個 AWS 服務 使用 AI/ML 從巨型資料集學習，並進行安全推論。

- Amazon Macie 是一種資料安全服務，使用 ML 和模式比對來探索和協助保護您的敏感資料。Macie 會自動偵測大量且不斷增長的敏感資料類型清單，包括個人身分識別資訊 (PII)，例如姓名、地址和信用卡號碼等財務資訊。它還可讓您持續查看存放在 Amazon Simple Storage Service (Amazon S3) 中的資料。Macie 使用自然語言處理 (NLP) 和 ML 模型，這些模型在不同類型的資料集上進行訓練，以了解您現有的資料，並指派商業值以排定業務關鍵資料的優先順序。Macie 接著會產生敏感的資料調查結果。
- Amazon GuardDuty 是一種威脅偵測服務，使用 ML、異常偵測和整合式威脅情報來持續監控惡意活動和未經授權的行為，以協助保護您的 AWS 帳戶、執行個體、無伺服器和容器工作負載、使用者、資料庫和儲存體。GuardDuty 整合了 ML 技術，這些技術可有效分辨潛在惡意使用者活動與其中異常但良性的操作行為 AWS 帳戶。此功能會持續在帳戶中建立 API 調用模型，並納入機率預測，以更準確地隔離和提醒高度可疑的使用者行為。此方法有助於識別與已知威脅策略相關的惡意活動，包括探索、初始存取、持久性、權限提升、防禦逃避、登入資料存取、影響和資料外洩。若要進一步了解 GuardDuty 如何使用機器學習，請參閱 AWS re：Inforce 2023 分組工作階段在 Amazon GuardDuty (TDR310) 中使用機器學習開發新問題清單。

適當的安全性

AWS 開發自動化推理工具，使用數學邏輯來回答有關基礎設施的關鍵問題，並偵測可能公開您資料的錯誤組態。此功能稱為可證明的安全性，因為它可在雲端和雲端中提供更高的安全性保證。可能的安全性使用自動推理，這是 AI 的特定領域，可將邏輯扣除套用至電腦系統。例如，自動化推理工具可以分析政策和網路架構組態，並證明沒有可能公開易受攻擊資料的意外組態。此方法可為雲端的關鍵安全

特性提供最高層級的保證。如需詳細資訊，請參閱 AWS 網站上的 Provable Security Resources。下列 AWS 服務 和 功能目前使用自動化推理來協助您為應用程式實現可靠的安全性：

- Amazon Verified Permissions 是您建置之應用程式的可擴展許可管理和精細授權服務。Verified Permissions 使用 Cedar，這是一種用於存取控制的開放原始碼語言，是使用自動推理和差異測試所建置。Cedar 是一種將許可定義為政策的語言，描述誰應有權存取哪些資源。它也是評估這些政策的規格。使用 Cedar 政策來控制允許應用程式的每個使用者執行的動作，以及他們可以存取的資源。Cedar 政策是permitorforbid 陳述式，可判斷使用者是否可以對資源採取行動。政策與資源相關聯，您可以將多個政策連接到資源。禁止政策覆寫許可政策。當您的應用程式使用者嘗試對資源執行動作時，您的應用程式會向 Cedar 政策引擎提出授權請求。Cedar 會評估適用的政策，並傳回 `ALLOW`或 `DENY`決策。Cedar 支援任何類型的委託人和資源的授權規則，允許角色型和屬性型存取控制，並支援透過自動化推理工具進行分析，以協助最佳化您的政策並驗證您的安全模型。
- AWS Identity and Access Management Access Analyzer 可協助您簡化許可管理。您可以使用此功能來設定精細的許可、驗證預期的許可，以及透過移除未使用的存取來精簡許可。IAM Access Analyzer 會根據日誌中擷取的存取活動產生精細的政策。它還提供超過 100 個政策檢查，以協助您撰寫和驗證您的政策。IAM Access Analyzer 使用可用的安全性來分析存取路徑，並提供對資源的公有和跨帳戶存取的完整調查結果。此工具建置在 Zelkova 上，可將 IAM 政策轉換為同等的邏輯陳述式，並針對問題執行一套一般用途和專門的邏輯求解器（滿意模數理論）。IAM Access Analyzer 會將 Zelkova 重複套用至具有越來越特定查詢的政策，以根據政策的內容來描述政策允許的行為類別特徵。分析器不會檢查存取日誌，以判斷外部實體是否存取信任區域內的資源。當資源型政策允許存取資源時，即使外部實體未存取資源，也會產生問題清單。若要進一步了解滿意度模數理論，請參閱滿意度手冊中的滿意度模數理論。*
- Amazon S3 Block Public Access 是 Amazon S3 的一項功能，可讓您封鎖可能導致儲存貯體和物件公開存取的可能錯誤設定。您可以為存取點、儲存貯體、帳戶和 AWS 組織啟用Amazon S3 封鎖公開存取（這會影響帳戶中的現有儲存貯體和新儲存貯體）。透過存取控制清單 (ACL)、儲存貯體政策或兩者來授予對儲存貯體和物件的公開存取許可。使用 Zelkova 自動化推理系統來判斷指定政策或 ACL 是否視為公有。Amazon S3 使用 Zelkova 檢查每個儲存貯體政策，並在未經授權的使用者能夠讀取或寫入您的儲存貯體時警告您。如果儲存貯體標記為公有，則允許某些公有請求存取儲存貯體。如果儲存貯體標記為非公有，則會拒絕所有公有請求。Zelkova 能夠做出此類判斷，因為它具有精確的 IAM 政策數學表示法。它會為每個政策建立公式，並證明該公式的理論。
- Amazon VPC Network Access Analyzer 是 Amazon VPC 的一項功能，可協助您了解 資源的潛在網路路徑，並識別潛在的意外網路存取。Network Access Analyzer 可協助您驗證網路分段、識別網際網路可存取性，以及驗證信任的網路路徑和網路存取。此功能使用自動推理演算法來分析封包可在網路中的資源之間採取 AWS 的網路路徑。然後，它會針對符合您網路存取範圍的路徑產生調查結果，以定義傳出和傳入流量模式。網路存取分析器會對網路組態執行靜態分析，這表示在此分析過程中不會在網路中傳輸任何封包。

- Amazon VPC Reachability Analyzer 是 Amazon VPC 的一項功能，可讓您偵錯、了解和視覺化 AWS 網路中的連線。Reachability Analyzer 是一種組態分析工具，可讓您在虛擬私有雲端 (VPC) 中的來源資源和目的地資源之間執行連線測試。當目的地可連線時， Reachability Analyzer 會產生來源與目的地之間虛擬網路路徑的hop-by-hop詳細資訊。當目的地無法連線時， Reachability Analyzer 會識別封鎖元件。Reachability Analyzer 使用自動化推理，透過在來源和目的地之間建立網路組態模型來識別可行的路徑。然後，它會根據組態檢查連線能力。它不會傳送封包或分析資料平面。

* Biere、A. M. Heule、H. van Maaren 和 T. Walsh。2009 年。滿意度手冊。IOS Press、NLD。

建置您的安全架構 – 分階段方法

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

AWS SRA 建議的多帳戶安全架構是一種基準架構，可協助您在設計過程中提早注入安全性。每個組織的雲端旅程都是獨一無二的。若要成功 發展您的雲端安全架構，您需要設想所需的目標狀態、了解目前的雲端準備程度，並採用敏捷方法來消除任何差距。 AWS SRA 為您的安全架構提供參考目標狀態。逐步轉換可讓您快速示範值，同時將進行遙遠預測的需求降到最低。

AWS 雲端採用架構 (AWS CAF) 建議四個疊代和增量雲端轉換階段： 設想、調整、啟動和擴展。當您進入啟動階段並專注於在生產環境中交付試行計劃時，您應該專注於建置強大的安全架構作為擴展階段的基礎，以便您能夠放心地遷移和操作最關鍵業務的工作負載。如果您是新創公司、想要擴展業務的小型或中型公司，或是正在取得新業務單位或正在進行合併和收購的企業，則適用此分階段方法。AWS SRA 可協助您實現該安全基準架構，以便您可以在 中擴展的組織之間統一套用安全控制 AWS Organizations。基準架構包含多個 AWS 帳戶 和 服務。規劃和實作應該是一個多階段程序，讓您可以反覆執行較小的里程碑，以達到設定基準安全架構的更大目標。本節說明以結構化方法為基礎的雲端旅程典型階段。這些階段符合 AWS Well-Architected Framework 安全設計原則。

階段 1：建置您的 OU 和帳戶結構

強大安全基礎的先決條件是設計良好的 AWS 組織和帳戶結構。如本指南先前 SRA 建置區塊一節所述，擁有多個 AWS 帳戶 可協助您透過設計隔離不同的業務和安全功能。這看起來像是一開始不必要的工作，但這是一項投資，可協助您快速安全地擴展。本節也說明如何使用 AWS Organizations 來管理多個 AWS 帳戶，以及如何使用信任存取和委派管理員功能來 AWS 服務 集中管理這些多個帳戶。

您可以使用本指南前面AWS Control Tower所述的 來協調您的登陸區域。如果您目前正在使用單一 AWS 帳戶，請參閱 轉換為多個 AWS 帳戶 指南，以盡早遷移到多個帳戶。例如，如果您的新創公司目前在單一 中構想和原型設計產品 AWS 帳戶，您應該考慮在市場上啟動產品之前採用多帳戶策略。同樣地，小型、中型和企業組織應在規劃初始生產工作負載後立即開始建置其多帳戶策略。從基礎 OUs 和 開始 AWS 帳戶，然後新增與工作負載相關的 OUs和帳戶。

如需 SRA 所提供的 AWS AWS 帳戶 和 OU 結構建議，請參閱 中小型企業的多帳戶策略 部落格文章。當您完成 OU 和帳戶結構時，請考慮要使用服務控制政策 (SCPs)、資源控制政策 (RCPs) 和宣告政策強制執行的高階全組織安全控制。

設計考量事項

請勿在設計 OU 和帳戶結構時複寫公司的報告結構。您的 OUs 應以工作負載函數和一組適用於工作負載的常見安全控制為基礎。請勿嘗試從頭開始設計完整的帳戶結構。專注於基礎 OUs，然後視需要新增工作負載 OUs。您可以在 OUs 之間移動帳戶，以便在設計的早期階段嘗試替代方法。不過，這可能會導致管理邏輯許可的一些額外負荷，取決於以 OU 和帳戶路徑為基礎的 SCPs、RCPs、宣告政策和 IAM 條件。

實作範例

AWS SRA 程式碼庫提供帳戶替代聯絡人的範例實作。此解決方案會 設定組織內所有帳戶的帳單、操作和安全替代聯絡人。

階段 2：實作強大的身分基礎

建立多個 後 AWS 帳戶，您應該讓團隊存取這些帳戶中 AWS 的資源。身分管理有兩種一般類別：人力資源身分和存取管理，以及客戶身分和存取管理 (CIAM)。Workforce IAM 適用於員工和自動化工作負載需要登入 AWS 才能執行其任務的組織。當組織需要一種方法來驗證使用者，以提供組織應用程式的存取權時，會使用 CIAM。首先您需要人力 IAM 策略，讓您的團隊可以建置和遷移應用程式。您應該一律使用 IAM 角色，而不是 IAM 使用者來提供人類或機器使用者的存取權。遵循 AWS SRA 指引，了解如何 AWS IAM Identity Center 在組織管理和共享服務帳戶中使用 ，以集中管理對 的單一登入 (SSO) 存取 AWS 帳戶。當您無法使用 IAM Identity Center 時，本指南也提供使用 IAM 聯合的設計考量。

當您使用 IAM 角色來提供使用者對 AWS 資源的存取權時，您應該使用 IAM Access Analyzer 和 IAM 存取顧問，如本指南的安全工具與組織管理章節所述。這些服務可協助您實現最低權限，這是重要的預防性控制，可協助您建立良好的安全狀態。

設計考量事項

為了實現最低權限，設計程序來定期檢閱和了解您的身分與其正常運作所需的許可之間的關係。當您學習時，請微調這些許可，並逐步將其縮減為盡可能最少的許可。為了可擴展性，這應該是您中央安全與應用程式團隊之間的共同責任。使用 資源型政策、 許可界限、 屬性型存取控制 和 工作階段政策 等功能，協助應用程式擁有者定義精細存取控制。

實作範例

AWS SRA 程式碼庫提供兩個適用於此階段的範例實作：

- IAM 密碼政策會設定帳戶密碼政策，讓使用者符合常見的合規標準。
- Access Analyzer 會設定委派管理員帳戶內的組織層級分析器，以及每個帳戶內的帳戶層級分析器。

階段 3：維持可追蹤性

當您的使用者可以存取 AWS 並開始建置時，您會想要知道誰正在執行什麼操作、何時執行和從何處執行。您也需要了解潛在的安全錯誤組態、威脅或意外行為。更了解安全威脅可讓您優先考慮適當的安全控制。若要監控 AWS 活動，請遵循 AWS SRA 建議，使用 AWS CloudTrail 並在 Log Archive 帳戶中集中您的日誌來設定組織線索。針對安全事件監控，請使用 AWS Config、Amazon GuardDuty AWS Security Hub CSPM和 Amazon Security Lake，如安全工具帳戶一節中所述。

設計考量事項

當您開始使用新的 時 AWS 服務，請務必為服務啟用 服務特定的日誌 ，並將其儲存為中央日誌儲存庫的一部分。

實作範例

AWS SRA 程式碼庫提供適用於此階段的下列範例實作：

- Organization CloudTrail 會建立組織追蹤，並設定預設值來設定資料事件 （ 例如，在 Amazon S3 和 中 AWS Lambda)，以減少由 設定的 CloudTrail 重複 AWS Control Tower。此解決方案提供設定管理事件的選項。
- AWS Config Control Tower 管理帳戶 可讓 管理帳戶中 AWS Config 的 監控資源合規。
- 一致性套件組織規則會將一致性套件部署到組織內的帳戶和指定區域。
- AWS Config 彙總工具 透過將管理委派給稽核帳戶以外的成員帳戶來部署彙總工具。
- Security Hub CSPM Organization 會在委派管理員帳戶中為帳戶和組織內的受管區域設定 Security Hub CSPM。
- GuardDuty Organization 在組織的委派管理員帳戶中設定 GuardDuty。

階段 4：在所有層套用安全性

此時，您應該有：

- 適用於您 的適當安全控制 AWS 帳戶。
- 定義明確的帳戶和 OU 結構，具有透過 SCPs、RCPs、宣告政策和最低權限 IAM 角色和政策定義的預防性控制。
- 使用 記錄 AWS 活動的能力 AWS CloudTrail；使用 AWS Security Hub CSPM、Amazon GuardDuty 和 偵測安全事件 AWS Config；以及使用 Amazon Security Lake 在專用資料湖上執行進階分析以確保安全。

在此階段中，計劃在 AWS 組織的其他層套用安全，如 在 AWS 組織中套用安全服務一節所述。您可以使用網路 帳戶區段中概述的服務，例如 AWS WAF AWS Shield、 AWS Firewall Manager、AWS Network Firewall AWS Certificate Manager (ACM)、Amazon CloudFront、Amazon Route 53 和 Amazon VPC，來建置聯網層的安全控制。當您向下移動技術堆疊時，請套用工作負載或應用程式堆疊專屬的安全控制。使用應用程式帳戶 區段中概述的 VPC 端點 AWS Systems Manager AWS Secrets Manager、Amazon Inspector 和 Amazon Cognito。

設計考量事項

當您設計深度防禦 (DiD) 安全控制時，請考慮擴展因素。您的中央安全團隊將無法擁有頻寬或完全了解每個應用程式在環境中的行為。讓您的應用程式團隊能夠負責為應用程式識別和設計正確的安全控制。中央安全團隊應專注於提供適當的工具和諮詢，以啟用應用程式團隊。若要了解 用來 AWS 採用更左移安全方法的擴展機制，請參閱部落格文章 如何 AWS 建置 Security Guardians 程式，這是一種分配安全擁有權的機制。

實作範例

AWS SRA 程式碼庫提供適用於此階段的下列範例實作：

- EC2 預設 EBS 加密 會將 Amazon EC2 中的預設 Amazon EBS 加密設定為在提供的 AWS KMS key 中使用預設值 AWS 區域。
- S3 封鎖帳戶公開存取 會為組織內的帳戶設定 Amazon S3 中的帳戶層級封鎖公開存取 (BPA) 設定。
- Firewall Manager 示範如何為組織內的帳戶設定安全群組政策和 AWS WAF 政策。

- Inspector Organization 會在委派的管理員帳戶中設定 Amazon Inspector，用於組織內的帳戶和受管區域。

階段 5：保護傳輸中和靜態的資料

您的業務和客戶資料是您需要保護的寶貴資產。 AWS 提供各種安全服務和功能，以保護動態和靜態資料。如 網路帳戶 一節所述 AWS Certificate Manager，使用 Amazon CloudFront 搭配 來保護透過網際網路收集的動態資料。對於內部網路內動態的資料，請使用 Application Load Balancer AWS 私有憑證授權單位，如 應用程式帳戶一節所述。 AWS KMS 和 AWS CloudHSM 可協助您提供密碼編譯金鑰管理來保護靜態資料。

階段 6：準備安全事件

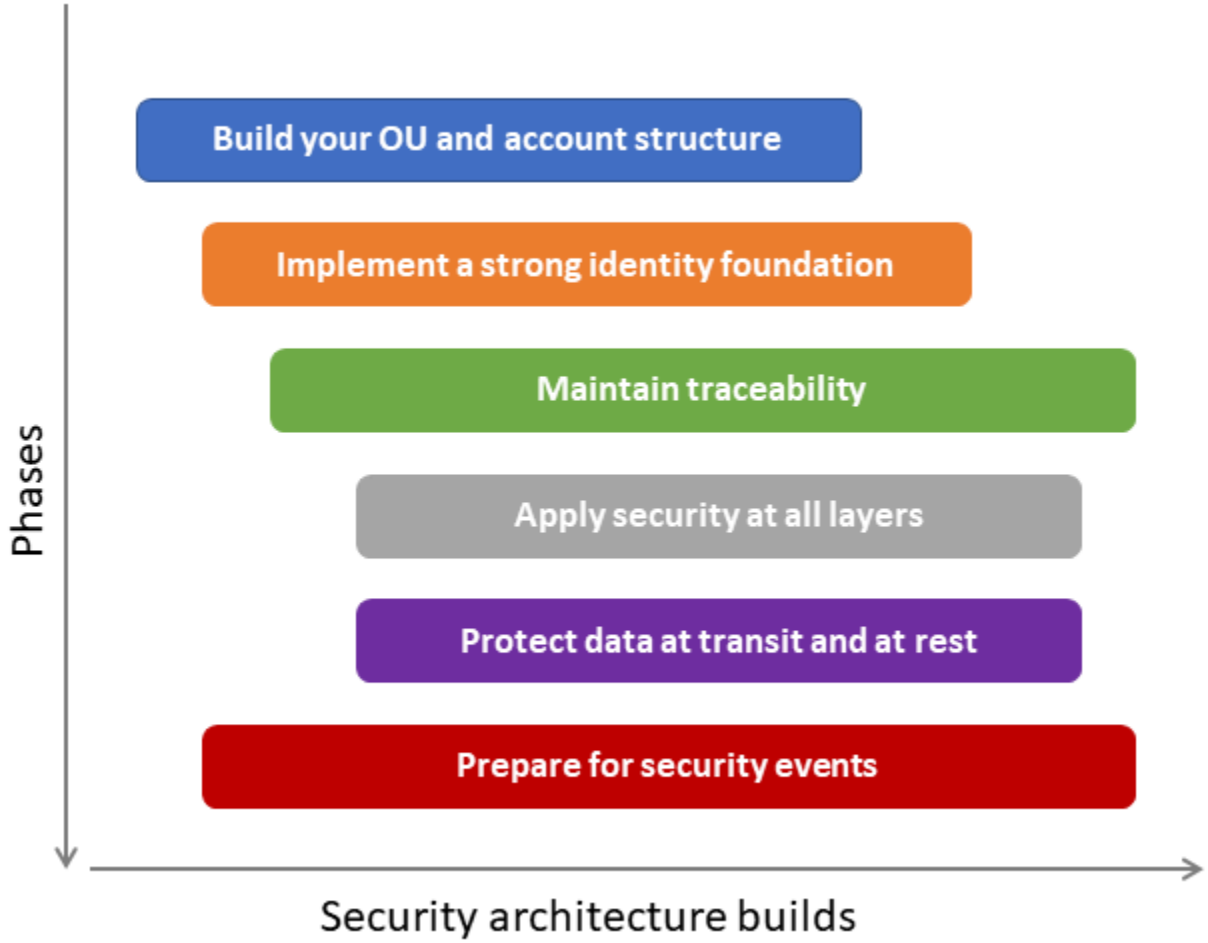
當您操作 IT 環境時，將會遇到安全事件，這是 IT 環境日常操作的變更，表示可能違反安全政策或無法安全控制。適當的可追蹤性至關重要，以便您盡快知道安全事件。同樣重要的是，請準備好分類和回應此類安全事件，以便在安全事件升級之前採取適當動作。準備可協助您快速分類安全事件，以了解其潛在影響。

AWS SRA 透過設計 安全工具帳戶 和 在所有範圍內部署常見的安全服務 AWS 帳戶，可讓您偵測整個 AWS 組織的安全事件。安全工具帳戶中的 Amazon Detective 可協助您分類安全事件並識別根本原因。在安全調查期間，您必須能夠檢閱相關日誌，以記錄並了解事件的完整範圍和時間表。當特定感興趣的動作發生時，產生警示也需要日誌。 AWS SRA 建議使用中央 Log Archive 帳戶 來儲存所有安全性和操作日誌。您可以使用 CloudWatch Logs Insights 查詢儲存在 CloudWatch 日誌群組中的資料，以及使用 Amazon Athena 和 Amazon OpenSearch Service 查詢儲存在 Amazon S3 中的資料。使用 Amazon Security Lake 自動集中來自 AWS 環境、軟體即服務 (SaaS) 提供者、內部部署和其他雲端提供者的安全資料。在安全工具帳戶或任何專用帳戶中設定訂閱者，如 AWS SRA 所述，以查詢這些日誌以進行調查。

AWS 安全事件應變 可協助您自動化安全事件回應、調查和修復。它提供預先建置的手冊和工作流程，協助您快速一致地回應安全事件。啟用主動回應功能時，安全事件回應會與 Security Hub CSPM 和 GuardDuty 整合，以便在偵測到安全調查結果時自動觸發回應工作流程。此服務可協助您將整個 AWS 組織的事件回應程序標準化並自動化。如果您需要其他協助，您可以開啟服務支援案例，以與客戶事件回應團隊 AWS (CIRT) 互動。

設計考量

- 您應該從雲端旅程的一開始就開始準備偵測和回應安全事件。為了更好地利用有限的資源，請將資料和業務關鍵性指派給您的 AWS 資源，以便在偵測到安全事件時，您可以根據涉及的資源關鍵性來排定分類和回應的優先順序。
- 如本節所述，建置雲端安全架構的階段本質上是循序的。不過，您不需要等待一個階段的完整完成，即可開始下一個階段。我們建議您採用反覆方法，開始平行處理多個階段，並在您發展雲端安全狀態時發展每個階段。隨著您經歷不同的階段，您的設計將會演進。請考慮根據您的特定需求，量身打造下圖所示的建議序列。



實作範例

AWS SRA 程式碼庫提供 Detective Organization 的範例實作，透過將管理委派給帳戶（例如，稽核或安全工具）來自動啟用 Amazon Detective，並為現有和未來的 AWS Organizations 帳戶設定 Detective。

AWS SRA 最佳實務檢查清單

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

本節會將本指南中詳述的 AWS SRA 最佳實務分割成檢查清單，供您在建置安全架構版本時遵循 AWS。使用此清單做為參考點，而不是用來取代檢閱指南。檢查清單會依 分組 AWS 服務。如果您想要根據 AWS SRA 最佳實務檢查清單以程式設計方式驗證現有 AWS 環境，您可以使用 SRA Verify。

SRA Verify 是一種安全評估工具，可協助您評估組織跨多個 AWS 帳戶 和 區域的 AWS SRA 一致性。它透過提供根據 AWS SRA 指引驗證實作的自動檢查，直接映射到 AWS SRA 建議。此工具可協助您驗證您的安全服務是否已根據參考架構正確設定。它提供詳細的調查結果和可行的修補步驟，以協助確保您的 AWS 環境遵循安全最佳實務。SRA Verify 旨在組織稽核（安全工具）帳戶中的 AWS CodeBuild 中執行。您也可以在本機執行它，或使用 SRA Verify 程式庫將其擴展。

> **Note**
>
> SRA Verify 包含多項服務的檢查，但可能不會包含 AWS SRA 每個考量的檢查。如需詳細資訊，請參閱 AWS SRA 程式庫中的指南。

AWS Organizations

- AWS Organizations 已啟用所有 功能。
- 服務控制政策 SCPs) 用於定義 IAM 主體的存取控制準則。
- 資源控制政策 RCPs) 用於定義 AWS 資源的存取控制準則。
- 宣告政策用於集中宣告和強制執行整個組織中指定 AWS 服務 所需的組態。
- 建立三個基礎 OUs（安全性、基礎設施和工作負載），以將提供基礎服務的成員帳戶分組。
- 安全工具帳戶是在安全 OU 下建立。此帳戶提供 AWS 安全服務和其他第三方安全工具的集中式管理。
- Log Archive 帳戶是在安全 OU 下建立。此帳戶提供 AWS 服務 和應用程式日誌的嚴格控制中央日誌儲存庫。
- 網路帳戶是在基礎設施 OU 下建立。此帳戶會管理應用程式與更廣泛的網際網路之間的閘道。它將網路服務、組態和操作與個別應用程式工作負載、安全性和其他基礎設施隔離。

- 共用服務帳戶是在基礎設施 OU 下建立。此帳戶支援多個應用程式和團隊用來交付其結果的服務。
- 應用程式帳戶是在工作負載 OU 下建立。此帳戶託管主要基礎設施和服務，以執行和維護企業應用程式。本指南提供了一個表示法，但在現實世界中，應用程式、開發環境和其他安全考量將隔離多個 OUs 和成員帳戶。
- 已設定所有成員帳戶的帳單、操作和安全性的替代聯絡資訊。

AWS CloudTrail

- 已設定組織線索，可啟用管理帳戶和組織中所有成員帳戶中的 CloudTrail AWS 管理事件交付。
- 組織線索設定為多區域線索。
- 組織線索已設定為從全域資源擷取事件。
- 用於擷取特定資料事件的其他線索會視需要設定，以監控敏感 AWS 資源活動。
- 安全工具帳戶設定為組織追蹤的委派管理員。
- 組織線索已設定為為所有新成員帳戶自動啟用。
- 組織線索設定為將日誌發佈至在 Log Archive 帳戶中託管的集中式 S3 儲存貯體。
- 組織追蹤已啟用日誌檔案驗證，以驗證日誌檔案的完整性。
- 組織追蹤與 CloudWatch Logs 整合，以保留日誌。
- 使用客戶受管金鑰來加密組織追蹤。
- 用於 Log Archive 帳戶中日誌儲存庫的中央 S3 儲存貯體會使用客戶受管金鑰加密。
- 用於 Log Archive 帳戶中日誌儲存庫的中央 S3 儲存貯體已設定為 S3 物件鎖定，以實現不可變性。
- 對於日誌存檔帳戶中用於日誌儲存庫的中央 S3 儲存貯體，已啟用版本控制。
- 用於 Log Archive 帳戶中日誌儲存庫的中央 S3 儲存貯體具有定義的資源政策，只能透過資源 Amazon Resource Name (ARN) 依組織追蹤限制物件上傳。

AWS Security Hub CSPM

- 所有成員帳戶和管理帳戶都已啟用 Security Hub CSPM。
- AWS Config 已啟用所有成員帳戶作為 Security Hub CSPM 的先決條件。
- Security Tooling 帳戶設定為 Security Hub CSPM 的委派管理員。
- Amazon GuardDuty 和 Amazon Detective 具有與 Security Hub CSPM 相同的委派管理員帳戶，以實現順暢的服務整合。

- 中央組態用於跨多個 和 設定和管理 Security Hub CSPM AWS 帳戶 AWS 區域。
- 所有 OU 和成員帳戶都由 Security Hub CSPM 的委派管理員指定為集中管理。
- 所有新成員帳戶都會自動啟用 Security Hub CSPM。
- Security Hub CSPM 會自動啟用以設定新標準。
- 來自所有區域的 Security Hub CSPM 調查結果會彙總到單一主區域。
- 來自所有成員帳戶的 Security Hub CSPM 調查結果會在 Security Tooling 帳戶中彙總。
- Security Hub CSPM 中的AWS 基礎最佳實務 (FSBP) 標準已啟用所有成員帳戶。
- Security Hub CSPM 中的 CIS AWS Foundation Benchmark 標準已啟用所有成員帳戶。
- 其他 Security Hub CSPM 標準會依適用情況啟用。
- Security Hub CSPM 自動化規則用於充實具有資源內容的問題清單。
- Security Hub CSPM 自動化回應和修復功能用於建立自訂 EventBridge 規則，以對特定調查結果採取自動動作。

AWS Config

- 所有成員帳戶和管理帳戶都會啟用 AWS Config 記錄器。
- 已為所有區域啟用 AWS Config 記錄器。
- AWS Config 交付管道 S3 儲存貯體集中在 Log Archive 帳戶中。
- AWS Config 委派管理員帳戶已設定為安全工具帳戶。
- AWS Config 已設定組織彙整工具。彙總工具包含所有區域。
- AWS Config 一致性套件會從委派管理員帳戶統一部署到所有成員帳戶。
- AWS Config 規則調查結果會自動傳送至 Security Hub CSPM。

Amazon GuardDuty

- 已為所有成員帳戶和管理帳戶啟用 GuardDuty 偵測器。
- 已為所有區域啟用 GuardDuty 偵測器。
- GuardDuty 偵測器會自動為所有新成員帳戶啟用。
- GuardDuty 委派管理設定為安全工具帳戶。
- GuardDuty 基礎資料來源已啟用，例如 CloudTrail 管理事件、VPC 流程日誌和 Route 53 Resolver DNS 查詢日誌。

- GuardDuty S3 保護已啟用。
- 已啟用 EBS 磁碟區的 GuardDuty 惡意軟體防護。
- S3 的 GuardDuty 惡意軟體防護已啟用。
- GuardDuty RDS 保護已啟用。
- GuardDuty Lambda 保護已啟用。
- GuardDuty EKS 保護已啟用。
- GuardDuty EKS 執行期監控已啟用。
- GuardDuty 延伸威脅偵測已啟用。
- GuardDuty 調查結果會匯出至 Log Archive 帳戶中的中央 S3 儲存貯體以進行保留。

IAM

- 不會使用 IAM 使用者。
- 強制執行成員帳戶的根存取權的集中管理。
- 管理帳戶的集中式特殊權限根使用者任務會從委派管理員強制執行。
- 集中式根存取管理會委派給 Security Tooling 帳戶。
- 所有成員帳戶根登入資料都會移除。
- 所有成員和管理 AWS 帳戶 密碼政策都根據組織的安全標準設定。
- IAM 存取顧問用於檢閱 IAM 群組、使用者、角色和政策的上次使用資訊。
- 許可界限用於限制 IAM 角色的最大可能許可。

IAM Access Analyzer

- 已為所有成員帳戶和管理帳戶啟用 IAM Access Analyzer。
- IAM Access Analyzer 委派管理員設定為安全工具帳戶。
- IAM Access Analyzer 外部存取分析器是以每個區域中的信任組織區域進行設定。
- IAM Access Analyzer 外部存取分析器是以每個區域中的信任帳戶區域進行設定。
- IAM Access Analyzer 內部存取分析器是以每個區域中的信任組織區域進行設定。
- IAM Access Analyzer 內部存取分析器是以每個區域中的信任帳戶區域設定。
- 為目前帳戶建立 IAM Access Analyzer 未使用的存取分析器。

- 為目前組織建立 IAM Access Analyzer 未使用的存取分析器。

Amazon Detective

- 為所有成員帳戶啟用 Detective。
- Detective 會自動為所有新成員帳戶啟用。
- 所有 區域都已啟用 Detective。
- Detective 委派管理員設定為安全工具帳戶。
- Detective、GuardDuty 和 Security Hub CSPM 委派管理員設定為相同的安全工具帳戶。
- Detective 與 Security Lake 整合，用於儲存和分析原始日誌。
- Detective 與 GuardDuty 整合以擷取問題清單。
- Detective 正在擷取 Amazon EKS 稽核日誌進行分析。
- Detective 正在擷取 Security Hub CSPM 日誌進行分析。

AWS Firewall Manager

- 已設定 Firewall Manager 安全政策。
- Firewall Manager 委派管理員設定為安全工具帳戶。
- AWS Config 已啟用 做為先決條件。
- 每個 OU、帳戶和區域設定多個 Firewall Manager 管理員的限制範圍。
- 已定義 Firewall Manager AWS WAF 安全政策。
- 已定義 Firewall Manager AWS WAF 集中式記錄政策。
- 已定義 Firewall Manager Shield Advanced 安全政策。
- 已定義 Firewall Manager 安全群組安全政策。

Amazon Inspector

- Amazon Inspector 已為所有成員帳戶啟用。
- Amazon Inspector 會自動為任何新的成員帳戶啟用。
- Amazon Inspector 委派管理員設定為安全工具帳戶。
- Amazon Inspector EC2 漏洞掃描已啟用。

- Amazon Inspector ECR 映像漏洞掃描已啟用。
- Amazon Inspector Lambda 函數和層漏洞掃描已啟用。
- Amazon Inspector Lambda 程式碼掃描已啟用。
- Amazon Inspector 程式碼安全掃描已啟用。

Amazon Macie

- Macie 已針對適用的成員帳戶啟用。
- Macie 會自動為適用的新成員帳戶啟用。
- Macie 委派管理員設定為安全工具帳戶。
- Macie 調查結果會匯出至日誌封存帳戶中的中央 S3 儲存貯體。
- 存放 Macie 調查結果的 S3 儲存貯體會使用客戶受管金鑰加密。
- Macie 政策和分類政策會發佈至 Security Hub CSPM。

Amazon Security Lake

- Security Lake 組織組態已啟用。
- Security Lake 委派管理員設定為 Security Tooling 帳戶。
- 新成員帳戶已啟用 Security Lake 組織組態。
- 安全工具帳戶設定為資料存取訂閱者，以執行日誌分析。
- Security Tooling 帳戶設定為資料查詢訂閱者，以進行日誌分析。
- 已啟用所有或指定作用中成員帳戶中 Security Lake 的 CloudTrail 管理日誌來源。
- 已啟用所有或指定作用中成員帳戶中 Security Lake 的 VPC 流量日誌來源。
- 在所有或指定的作用中成員帳戶中，Security Lake 都會啟用 Route 53 日誌來源。
- S3 日誌來源的 CloudTrail 資料事件已啟用所有或指定作用中成員帳戶中的 Security Lake。
- 已啟用所有或指定作用中成員帳戶中 Security Lake 的 Lambda 執行日誌來源。
- Amazon EKS 稽核日誌來源已啟用所有或指定作用中成員帳戶中的 Security Lake。
- 在所有或指定的作用中成員帳戶中，Security Hub 調查結果日誌來源已啟用 Security Lake。
- 在所有或指定的作用中成員帳戶中，Security Lake 都會啟用 AWS WAF 日誌來源。
- 委派管理員帳戶中的 Security Lake SQS 佇列會使用客戶受管金鑰加密。
- 委派管理員帳戶中的 Security Lake SQS 無效字母佇列會使用客戶受管金鑰加密。

- Security Lake S3 儲存貯體使用客戶受管金鑰加密。
- Security Lake S3 儲存貯體具有資源政策，僅限制 Security Lake 的直接存取。

AWS WAF

- 所有 CloudFront 分佈都與 相關聯 AWS WAF。
- 所有與 相關聯的 Amazon API Gateway REST APIs AWS WAF。
- 所有 Application Load Balancer 都與 相關聯 AWS WAF。
- All AWS AppSync GraphQL APIs 會與 建立關聯 AWS WAF。
- 所有與 相關聯的 Amazon Cognito 使用者集區 AWS WAF。
- 所有 AWS App Runner 服務都與 相關聯 AWS WAF。
- 所有 AWS Verified Access 執行個體都會與 建立關聯 AWS WAF。
- 所有 AWS Amplify 應用程式都與 相關聯 AWS WAF。
- AWS WAF 記錄已啟用。
- AWS WAF 日誌會集中在 Log Archive 帳戶中的 S3 儲存貯體中。

AWS Shield Advanced

- Shield Advanced 訂閱已啟用，並針對具有公開資源的所有應用程式帳戶設定為自動續約。
- Shield Advanced 已針對所有 CloudFront 分佈設定。
- Shield Advanced 已針對所有 Application Load Balancer 設定。
- Shield Advanced 已針對所有 Network Load Balancer 設定。
- Shield Advanced 已針對所有 Route 53 託管區域設定。
- Shield Advanced 已針對所有彈性 IP 地址設定。
- Shield Advanced 已針對所有 Global Accelerator 設定。
- CloudWatch 警示會針對受 Shield Advanced 保護的 CloudFront 和 Route 53 資源進行設定。
- 已設定 Shield Response Team (SRT) 存取。
- Shield Advanced 主動參與已啟用。
- 已設定 Shield Advanced 主動參與聯絡人。
- Shield Advanced 受保護的資源已設定自訂 AWS WAF 規則。
- Shield Advanced 受保護的資源已啟用自動應用程式層 DDoS 緩解。

AWS 安全事件回應

- AWS 已針對整個 AWS 組織啟用安全事件回應。
- AWS 安全事件回應委派管理員設定為安全工具帳戶。
- 主動回應和警示分類工作流程已啟用。
- AWS 客戶事件回應團隊 (CIRT) 遏制動作已獲得授權。

AWS Audit Manager

- 所有成員帳戶都已啟用 Audit Manager。
- Audit Manager 會自動為新成員帳戶啟用。
- Audit Manager 委派管理員設定為安全工具帳戶。
- AWS Config 已啟用 做為 Audit Manager 的先決條件。
- 客戶受管金鑰用於儲存在 Audit Manager 中的資料。
- 已設定預設評估報告目的地。

IAM 資源

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

雖然 AWS Identity and Access Management (IAM) 不是包含在傳統架構圖中的服務，它觸及 AWS 組織的各個層面 AWS 帳戶，以及 AWS 服務。 AWS 服務 您必須先建立 IAM 實體並授予許可，才能部署任何 。IAM 的完整說明超出本文件的範圍，但本節提供最佳實務建議和其他資源指標的重要摘要。

- 如需 IAM 最佳實務，請參閱 AWS 文件中的 IAM 安全最佳實務、安全部落格中的 IAM 文章，以及 AWS re：Invent 簡報。 AWS
- AWS Well-Architected 安全支柱概述許可管理程序中的關鍵步驟：定義許可護欄、授予最低權限存取、分析公有和跨帳戶存取、安全地共用資源、持續減少許可，以及建立緊急存取程序。
- 下表及其隨附的備註提供有關可用 IAM 許可政策類型的建議指引，以及如何在安全架構中使用它們的高階概觀。若要進一步了解，請參閱 AWS re：Invent 2020 影片，了解選擇正確的 IAM 政策組合。

使用案例或政策	效果	管理者	用途	與 相關	影響	在 中部署
服務控制政策 (SCP)	Restrict	中央團隊，例如平台或安全團隊 【1】	護欄、控管	Organization、OU、帳戶	Organization、OU 和帳戶中的所有主體	組織管理帳戶 【2】
資源控制政策 RCPs)	Restrict	中央團隊，例如平台或安全團隊 【1】	護欄、控管	Organization、OU、帳戶	成員帳戶中的資源 【12】	組織管理帳戶 【2】
基準帳戶自動化政策（平台用來操作帳戶的 IAM 角色）	授予和限制	中央團隊，例如平台、安全或 IAM 團隊 【1】	（基準）非工作負載自動化角色的許可 【3】	單一帳戶 【4】	自動化在成員帳戶中使用的委託人	成員帳戶

基準人工政策（授予使用者執行其工作的許可的 IAM 角色）	授予和限制	中央團隊，例如平台、安全或 IAM 團隊 【1】	人類角色的許可 【5】	單一帳戶 【4】	聯合主體 【5】 和 IAM 使用者 【6】	成員帳戶
許可界限（授權開發人員可指派給另一個委託人的許可上限）	Restrict	中央團隊，例如平台、安全或 IAM 團隊 【1】	應用程式角色的護欄（必須套用）	單一帳戶 【4】	此帳戶中應用程式或工作負載的個別角色 【7】	成員帳戶
應用程式（連接至開發人員所部署基礎設施的角色）的機器角色政策	授予和限制	委派給開發人員 【8】	應用程式或工作負載的許可 【9】	單一帳戶	此帳戶中的委託人	成員帳戶
資源政策	授予和限制	委派給開發人員 【8，10】	資源的許可	單一帳戶	帳戶中的委託人 【11】	成員帳戶
中央根使用者管理	授予和限制	中央團隊，例如平台、安全或 IAM 團隊 【1】	大規模集中管理成員帳戶根使用者	組織	成員帳戶中的所有根使用者	組織管理帳戶、委派管理員帳戶

資料表的備註：

1. 企業有許多集中式團隊（例如雲端平台、安全操作或身分和存取管理團隊），這些團隊會劃分這些獨立控制的責任，並對彼此的政策進行對等審核。資料表中的範例為預留位置。您需要為企業確定最有效的職責分離。
2. 若要使用 SCPs，您必須啟用其中的所有功能 AWS Organizations。

3. 啟用自動化通常需要常見的基準角色和政策，例如管道的許可、部署工具、監控工具（例如 AWS Lambda 和 AWS Config 規則) 和其他許可。此組態通常會在佈建帳戶時傳送。
4. 雖然這些與單一帳戶中的資源（例如角色或政策）有關，但可以使用 AWS CloudFormation StackSets 複寫或部署到多個帳戶。
5. 定義由中央團隊（通常在帳戶佈建期間）部署到所有成員帳戶的核心一組基準人工角色和政策。範例包括平台團隊的開發人員、IAM 團隊和安全稽核團隊。
6. 盡可能使用聯合身分（而非本機 IAM 使用者）。
7. 委派管理員會使用許可界限。此 IAM 政策會定義最大許可，並覆寫其他政策（包括允許對資源執行所有動作"*:*"的政策）。基準人工政策中應該需要許可界限，作為建立角色（例如工作負載效能角色）和連接政策的條件。SCPs等其他組態會強制執行許可界限的連接。
8. 這會假設已部署足夠的護欄（例如 SCPs和許可界限）。
9. 這些選用政策可以在帳戶佈建期間或應用程式開發程序中交付。建立和連接這些政策的許可將由應用程式開發人員自己的許可管理。
10. 除了本機帳戶許可之外，集中式團隊（例如雲端平台團隊或安全操作團隊）通常會管理一些以資源為基礎的政策，讓跨帳戶存取能夠操作帳戶（例如，提供 S3 儲存貯體的存取以進行記錄）。
11. 以資源為基礎的 IAM 政策可以參考任何帳戶中的任何委託人，以允許或拒絕對其資源的存取。它甚至可以參考匿名主體來啟用公開存取。
12. RCPs適用於 子集的資源 AWS 服務。如需詳細資訊，請參閱 文件中的 AWS Organizations AWS 服務 支援 RCPs 清單。

確保 IAM 身分只有明確描述任務集所需的許可，對於降低惡意或無意濫用許可的風險至關重要。建立和維護最低權限模型需要有深思熟慮的計劃，才能持續更新、評估和緩解超額權限。以下是該計畫的一些其他建議：

- 使用組織的控管模型和已建立的風險偏好來建立特定的護欄和許可界限。
- 透過持續反覆運算程序實作最低權限。這不是一次性練習。
- 使用 SCPs來降低可行的風險。這些旨在作為廣泛的護欄，而不是窄度目標控制。
- 使用許可界限，以更安全的方式委派 IAM 管理。
  - 確定委派管理員將適當的 IAM 界限政策連接到他們建立的角色和使用者。
- 作為defense-in-depth（結合以身分為基礎的政策），請使用以資源為基礎的 IAM 政策來拒絕廣泛存取資源。
- 使用 IAM Access Advisor AWS CloudTrail、IAM Access Analyzer 和相關工具定期分析授予的歷史用量和許可。立即修復明顯的超額許可。

- 在適用的情況下，將廣泛的動作範圍涵蓋在特定資源，而不是使用星號做為萬用字元來表示所有資源。
- 實作機制，根據請求快速識別、檢閱和核准 IAM 政策例外狀況。

AWS SRA 範例的程式碼儲存庫

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

為了協助您開始建置和實作 AWS SRA 中的指引，位於 https：//https://github.com/aws-samples/aws-security-reference-architecture-examples 的基礎設施即程式碼 (IaC) 儲存庫隨附於本指南。此儲存庫包含程式碼，可協助開發人員和工程師部署本文件中呈現的一些指引和架構模式。此程式碼取自 AWS Professional Services 顧問與客戶的第一手經驗。這些範本本質上是一般的，其目標是說明實作模式，而不是提供完整的解決方案。 AWS 服務 組態和資源部署刻意非常嚴格。您可能需要修改和量身打造這些解決方案，以符合您的環境和安全需求。

AWS SRA 程式碼儲存庫提供具有 AWS CloudFormation 和 Terraform 部署選項的程式碼範例。解決方案模式支援兩個環境：一個需要 AWS Control Tower ，另一個 AWS Organizations 不使用 AWS Control Tower。此儲存庫中需要 的解決方案 AWS Control Tower 已在AWS Control Tower環境中使用和 Customizations for AWS Control Tower (CfCT) 部署 AWS CloudFormation和測試。不需要 的解決方案 AWS Control Tower 已在 AWS Organizations環境中使用 進行測試 AWS CloudFormation。CfCT 解決方案可協助客戶根據 AWS 最佳實務快速設定安全的多帳戶 AWS 環境。透過自動設定環境以執行安全且可擴展的工作負載，同時透過建立帳戶和資源來實作初始安全基準，有助於節省時間。 AWS Control Tower 還提供基準環境，以開始使用多帳戶架構、身分和存取管理、控管、資料安全、網路設計和記錄。 AWS SRA 儲存庫中的解決方案提供額外的安全組態，以實作本文件中所述的模式。

以下是 AWS SRA 儲存庫中解決方案的摘要。每個解決方案都包含包含詳細資訊`README.md`的檔案。

- CloudTrail Organization 解決方案會在組織管理帳戶中建立組織追蹤，並將管理委派給成員帳戶，例如稽核或安全工具帳戶。此追蹤會使用安全工具帳戶中建立的客戶受管金鑰進行加密，並將日誌交付至日誌封存帳戶中的 S3 儲存貯體。或者，可為 Amazon S3 和 AWS Lambda 函數啟用資料事件。組織追蹤會記錄組織中所有 的事件 AWS 帳戶 ， AWS 同時防止成員帳戶修改組態。
- GuardDuty Organization 解決方案透過將管理委派給安全工具帳戶來啟用 Amazon GuardDuty。它會針對所有現有和未來的 AWS 組織帳戶，在安全工具帳戶中設定 GuardDuty。GuardDuty 調查結果也會使用 KMS 金鑰加密，並傳送至 Log Archive 帳戶中的 S3 儲存貯體。
- Security Hub CSPM Organization 解決方案透過將管理委派給 Security Tooling 帳戶來設定 Security Hub CSPM。它會為所有現有和未來的 AWS 組織帳戶設定 Security Tooling 帳戶中的 Security Hub CSPM。解決方案也提供跨所有帳戶和區域同步已啟用安全標準的參數，以及在安全工具帳戶中設定區域彙總工具。在 Security Tooling 帳戶中集中 Security Hub CSPM 提供安全標準合規性的跨帳戶檢視，以及來自 AWS 服務 和第三方 AWS Partner 整合的問題清單。

- Inspector 解決方案會針對組織下的所有帳戶和受管區域，在委派的管理員（安全工具）帳戶中設定 AWS Amazon Inspector。
- Firewall Manager 解決方案透過將管理委派給安全工具帳戶，並使用 AWS Firewall Manager 安全群組政策和多個 AWS WAF 政策設定 Firewall Manager 來設定安全政策。安全群組政策需要 VPC（由解決方案現有或建立）內允許的最大安全群組，該 VPC 由解決方案部署。
- Macie Organization 解決方案透過將管理委派給安全工具帳戶來啟用 Amazon Macie。它會為所有現有和未來的 AWS 組織帳戶設定安全工具帳戶中的 Macie。Macie 進一步設定為將其探索結果傳送至使用 KMS 金鑰加密的中央 S3 儲存貯體。
- AWS Config:
  - Config Aggregator 解決方案透過將管理委派給 Security Tooling AWS Config 帳戶來設定彙總工具。然後，解決方案會針對 AWS 組織中所有現有和未來的帳戶，在安全工具帳戶中設定 AWS Config 彙總工具。
  - 透過將管理 AWS Config 規則 委派給 安全工具帳戶來部署一致性套件組織規則解決方案。然後，它會在委派管理員帳戶中為組織中的所有現有和未來帳戶建立 AWS 組織一致性套件。解決方案已設定為部署加密和金鑰管理一致性套件範例範本的操作最佳實務。
  - AWS Config Control Tower 管理帳戶解決方案 AWS Config 會在 AWS Control Tower 管理帳戶中啟用 AWS Config ，並相應地更新安全工具帳戶中的彙總工具。解決方案使用 AWS Control Tower CloudFormation 範本來啟用 AWS Config 做為參考，以確保與 AWS 組織中其他 帳戶的一致性。
- IAM：
  - Access Analyzer 解決方案透過將管理委派給 安全工具帳戶來啟用 IAM Access Analyzer。然後，它會為組織中的所有現有和未來帳戶，在安全工具帳戶中設定 AWS 組織層級的 IAM Access Analyzer。解決方案也會將 IAM Access Analyzer 部署到所有成員帳戶和區域，以支援分析帳戶層級許可。
  - IAM 密碼政策解決方案會 AWS 帳戶 更新 AWS 組織中所有帳戶中的密碼政策。解決方案提供設定密碼政策設定的參數，協助您符合產業合規標準。
- EC2 預設 EBS 加密解決方案 AWS 區域 會在 AWS 組織中的每個 AWS 帳戶 和 內啟用帳戶層級的預設 Amazon EBS 加密。它強制加密您建立的新 EBS 磁碟區和快照。例如，Amazon EBS 會加密啟動執行個體時建立的 EBS 磁碟區，以及從未加密快照複製的快照。
- S3 封鎖帳戶公開存取解決方案 AWS 帳戶 會在 AWS 組織中的每個 內啟用 Amazon S3 帳戶層級設定。Amazon S3 封鎖公開存取功能可提供存取點、儲存貯體和帳戶的設定，以協助您管理對 Amazon S3 資源的公開存取。依預設，新的儲存貯體、存取點和物件不允許公開存取。不過，使用者可以修改儲存貯體政策、存取點政策或物件許可，以允許公開存取。Amazon S3 封鎖公開存取設定會覆寫這些政策和許可，讓您可以限制對這些資源的公開存取。

- Detective Organization 解決方案會將管理委派給 帳戶 （例如 Audit 或 Security Tooling 帳戶），並為所有現有和未來的 AWS Organizations 帳戶設定 Detective，以自動化啟用 Amazon Detective。
- Shield Advanced 解決方案可自動部署 AWS Shield Advanced ，為您的應用程式提供增強的 DDoS 保護 AWS。
- AMI Bakery Organization 解決方案有助於自動化建置和管理標準強化 Amazon Machine Image (AMI) 映像的程序。這可確保 AWS 執行個體的一致性和安全性，並簡化部署和維護任務。
- 修補程式管理員解決方案有助於簡化跨多個 的修補程式管理 AWS 帳戶。您可以使用此解決方案更新所有受管執行個體上的 AWS Systems Manager Agent (SSM Agent)，並在 Windows 和 Linux 標記的執行個體上掃描和安裝關鍵和重要的安全修補程式和錯誤修正。解決方案也會設定預設主機管理組態設定，以偵測新 的建立， AWS 帳戶 並自動將解決方案部署到這些帳戶。

貢獻者

主要作者：

- Avik Mukherjee， AWS 資深安全 SA

貢獻者：

- Jason Hurst， AWS CIRT 資深安全調查人員
- Abhishek Panday， AWS 首席產品經理 – 技術
- Itay Meller， AWS 資深專員 SA
- Jonathan VanKim， AWS 委託人安全 SA
- Josh Du Lac， AWS Enterprise 安全策略師
- James Thompson， AWS 資深解決方案架構師
- Jeremy Girven， AWS 專員 SA
- Rodney Underkoffler， AWS 資深 SA 專家
- Farhan Farooq， AWS 資深解決方案架構師
- Prashob Krishnan， AWS 技術客戶經理
- Meg Peddada， AWS 資深安全顧問
- Ashwin Phadke， AWS 資深解決方案架構師
- Sowjanya Rajavaram， AWS 資深安全 SA
- Tomek Jakubowski， AWS 資深顧問
- Arun Thomas， AWS 資深解決方案架構師
- Ross Warren， AWS 產品解決方案架構師
- Scott Conklin， AWS 資深顧問
- Ilya Epshteyn， Identity Solutions AWS 資深經理
- Michael Haken， AWS 首席技術專家
- Mehial Mendrin， AWS 資深顧問
- Christopher Evensen， AWS 資深技術客戶經理

檢閱：

- Eric Rose，AWS 委託人安全 SA
- Manoj Kumar，AWS 交付顧問

技術撰寫：

- Handan Selamoglu，AWS 資深技術作者

附錄： AWS 安全性、身分和合規服務

進行簡短的問卷，以影響 AWS 安全參考架構 (AWS SRA) 的未來。

如需簡介或重新整理，請參閱 AWS 網站上的安全、身分和合規 AWS，以取得 AWS 服務 可協助您保護雲端工作負載和應用程式安全的 清單。這些服務分為五個類別：資料保護、身分與存取管理、網路與應用程式保護、威脅偵測與持續監控，以及合規與資料隱私權。

資料保護 – AWS 提供的服務可協助您保護資料、帳戶和工作負載免於未經授權的存取。

- Amazon Macie – 透過採用機器學習的安全功能探索、分類和保護敏感資料。
- AWS KMS – 建立和控制用於加密資料的金鑰。
- AWS CloudHSM– 在 中管理您的硬體安全模組 (HSMs) AWS 雲端。
- AWS Certificate Manager – 佈建、管理和部署 SSL/TLS 憑證，以搭配 使用 AWS 服務。
- AWS Secrets Manager – 輪換、管理和擷取資料庫登入資料、API 金鑰和其他秘密的整個生命週期。

Identity & Access Management – AWS Identity Services 可讓您大規模安全地管理身分、資源和許可。

- IAM – 安全地控制對 AWS 服務 和資源的存取。
- IAM Identity Center – 集中管理對多個 AWS 帳戶 和商業應用程式的 SSO 存取。
- Amazon Cognito – 將使用者註冊、登入和存取控制新增至您的 Web 和 行動應用程式。
- AWS Directory Service – 在 中使用受管 Microsoft Active Directory AWS 雲端。
- AWS RAM – 簡單且安全地共用 AWS 資源。
- AWS Organizations – 實作多個 的政策型管理 AWS 帳戶。
- Amazon Verified Permissions – 在自訂應用程式中管理可擴展、精細的許可和授權。

網路和應用程式保護 – 這些類別的服務可讓您在整個組織的網路控制點強制執行精細的安全政策。AWS 服務 可協助您檢查和篩選流量，以協助防止在主機層級、網路層級和應用程式層級界限進行未經授權的資源存取。

- AWS Shield – AWS 使用受管 DDoS 保護來保護在 上執行的 Web 應用程式。
- AWS WAF – 保護您的 Web 應用程式免受常見的 Web 入侵，並確保可用性和安全性。

- AWS Firewall Manager – 從中央位置設定和管理跨 AWS 帳戶 和應用程式的 AWS WAF 規則。
- AWS Systems Manager – 設定和管理 Amazon EC2 和內部部署系統，以套用作業系統修補程式、建立安全系統映像，以及設定安全作業系統。
- Amazon VPC – 佈建邏輯上隔離的 區段 AWS ，讓您可以在定義的虛擬網路中啟動 AWS 資源。
- AWS Network Firewall – 部署 VPCs 的基本網路保護。
- Amazon Route 53 DNS 防火牆 – 保護您的 VPCs傳出 DNS 請求。
- AWS Verified Access – 提供對應用程式的安全存取，而不需要虛擬私有網路 VPNs)。
- Amazon VPC Lattice – 簡化service-to-service連線、安全性和監控。

威脅偵測和持續監控 – AWS 監控和偵測服務提供指引，以協助識別您 AWS 環境中的潛在安全事件。

- AWS Security Hub CSPM – 從中央位置檢視和管理安全提醒並自動化合規檢查。
- AWS Security Hub – 關聯和豐富安全調查結果，以排定您帳戶和 之間重大安全問題的優先順序 AWS 區域。
- Amazon GuardDuty – 透過智慧型威脅偵測 AWS 帳戶 和持續監控來保護您的 和工作負載。
- Amazon Inspector – 自動化安全評估，以協助改善所部署應用程式的安全性和合規性 AWS。
- AWS Config – 記錄和評估 AWS 資源的組態，以啟用合規稽核、資源變更追蹤和安全性分析。
- AWS Config 規則 – 建立自動採取行動以回應環境中變更的規則，例如隔離資源、使用其他資料擴充事件，或將組態還原為已知良好狀態。
- AWS 安全事件應變 – 使用預先建置的手冊和工作流程，自動化安全事件回應、調查和修復。
- AWS CloudTrail – 追蹤使用者活動和 API 用量，以啟用對您 的控管、操作和風險稽核 AWS 帳戶。
- Amazon Detective – 分析和視覺化安全資料，以快速找到潛在安全問題的根本原因。
- AWS Lambda – 在不佈建或管理伺服器的情況下執行程式碼，讓您可以擴展對事件的程式設計、自動化回應。

合規與資料隱私權 – AWS 可讓您全面檢視合規狀態，並根據業務遵循的 AWS 最佳實務和產業標準，使用自動化合規檢查來持續監控您的環境。

- AWS Artifact – 使用免費的自助式入口網站，即可隨需存取 AWS 安全與合規報告，並選取線上協議。
- AWS Audit Manager – 持續稽核您的 AWS 用量，以簡化您評估風險的方式，以及是否符合法規和業界標準。

文件歷史記錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
內容重組和更新	• 新增 Security Hub 和 AWS Nitro Enclaves 的指引。 • 重組 AWS SRA 以專注於核心架構，並將深入探討章節移至單獨的身分管理、周邊安全性、網路鑑識、生成式 AI 和 IoT 指南。 • 更新現有指引，納入 AWS CloudTrail、AWS Config、Amazon Detective、 AWS Firewall Manager、Amazon GuardDuty、IAM Access Analyzer AWS Shield Advanced、Amazon Security Lake 和 的其他詳細資訊 AWS Audit Manager。	2025 年 12 月 22 日
主要更新	• 新增有關新的 IAM 集中式根使用者存取管理、資源控制政策 (RCPs) 和宣告政策的資訊。 • 更新 Security Hub CSPM 對新 Security Hub CSPM 的參考。 • 包含 Amazon GuardDuty 和 Security Hub CSPM 的新服務功能。	2025 年 8 月 29 日

	• 新增AWS 安全事件應變 服務指引。 • 更新了 IAM 深入探討指引，以納入用於machine-to-machine身分管理的 VPC Lattice。 • 新增了新的深入探討指引：適用於 IoT 的 SRA。	
新增和釐清	• 在安全工具帳戶區段中 AWS KMS ， 已更新指引。 • 在客戶身分管理區段中， 擴充了授權 API Gateway 的相關資訊。 • 更新了生成式 AI 章節，以新增 OU 和帳戶設計的設計考量。 • 在 AWS SRA 程式碼儲存庫區段中，新增有關新修補程式管理解決方案的資訊。	2024 年 9 月 12 日

主要更新	• 為深入探討架構指引新增了兩個區段：使用 Amazon Bedrock 和身分管理的生成式 AI。 • 使用新的服務功能更新 AWS Identity and Access Management Access Analyzer、Amazon Detective、Amazon Inspector、AWS ArtifactAWS Config、、Amazon Security LakeAWS Security Hub CSPM、 和 Amazon CloudFront 區段。 • 更新 AWS SRA 程式碼儲存庫區段，以包含新的 Terraform 部署選項，以及新增 AWS Shield Advanced 和 AMI Bakery 解決方案。	2024 年 6 月 7 日
主要更新	• 更新網路帳戶和應用程式帳戶區段，以新增 Amazon Verified Permissions AWS Verified Access和 Amazon VPC Lattice 的架構指引。 • 根據安全功能新增深入探討架構指引。 • 新增 AWS 服務 如何使用 AI/ML 提供更佳安全結果的新指引。 • 新增如何分階段規劃安全架構的指引。	2023 年 11 月 4 日

Security Lake 新增	更新 Security Tooling 帳戶和 Log Archive 帳戶區段，以新增與 Amazon Security Lake 相關的設計指南。	2023 年 9 月 22 日
次要更新	• 更新現有指引，以反映新 AWS 服務 功能和最佳實務。 • 更新 AWS CloudTrail AWS IAM Identity Center、 和 邊緣安全性的架構指引。	2023 年 5 月 10 日
調查	新增了簡短的問卷，以進一步了解您在組織中如何使用 AWS SRA。	2022 年 12 月 14 日
參考架構圖的來源檔案	在AWS 安全參考架構區段中，新增了下載檔案，以可編輯的 PowerPoint 格式提供本指南的架構圖。	2022 年 11 月 17 日
安全性基礎章節的更新	在安全基礎區段中，更新了 Well-Architected Framework 支柱和安全設計原則的相關資訊。	2022 年 9 月 27 日

主要新增和更新	• 新增如何使用 AWS SRA 和金鑰實作指導方針的相關資訊。 • 新增其他 的架構指引， AWS 服務 例如 AWS Artifact、Amazon Inspector AWS RAM、Amazon Route 53、 AWS Control Tower AWS Audit Manager、Directory Service、Amazon Cognito 和 Network Access Analyzer。 • 更新現有指引，以反映新 AWS 服務 功能和最佳實務。	2022 年 7 月 25 日
一	初次出版	2021 年 6 月 23 日

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。