AWS 決策指南

# 選擇 AWS 安全、身分和控管服務

# 選擇 AWS 安全、身分和控管服務: AWS 決策指南

# Table of Contents

# 選擇 AWS 安全、身分和控管服務

採取第一步

| | | |
|---|---|---|
| 讀取時間 | 27 分鐘 | |
| 用途 | 協助您判斷哪些 AWS 安全、身分和控管服務最適合您的組織。 | |
| 上次更新 | 2024 年 12 月 30 日 | |
| 涵蓋的服務 | • AWS Artifact<br>• AWS Audit Manager<br>• AWS Certificate Manager<br>• AWS CloudHSM<br>• AWS CloudTrail<br>• Amazon Cognito<br>• AWS Config<br>• AWS Control Tower<br>• Amazon Detective<br>• AWS Firewall Manager<br>• Amazon GuardDuty<br>• AWS IAM<br>• AWS IAM Identity Center<br>• Amazon Inspector | • AWS KMS<br>• Amazon Macie<br>• AWS Network Firewall<br>• AWS Organizations<br>• AWS Payment Cryptography<br>• AWS Private CA<br>• AWS RAM<br>• AWS Secrets Manager<br>• AWS Security Hub<br>• Amazon Security Lake<br>• AWS 安全事件回應<br>• AWS Shield<br>• AWS WAF |

## 簡介

雲端的安全、身分和控管是實現和維護資料和服務完整性和安全性的重要元件。隨著更多企業遷移到 Amazon Web Services () 等雲端供應商，這尤其重要AWS。

本指南可協助您選取最符合您的需求和組織 AWS 的安全性、身分和控管服務和工具。

首先，讓我們來探索安全性、身分和控管的含義：

- 雲端安全性是指使用 措施和實務來保護數位資產免受威脅。這包括資料中心的實體安全性和網路安全措施，以防止線上威脅。 透過加密的資料儲存、網路安全和持續監控潛在威脅來 AWS 優先考慮安全性。
- 身分服務可協助您以可擴展的方式安全地管理身分、資源和許可。 AWS 提供專為人力資源和面向客戶的應用程式設計的身分服務，以及管理工作負載和應用程式的存取。
- 雲端控管是一組規則、程序和報告，可引導您的組織遵循最佳實務。您可以跨 AWS 資源建立雲端控管、使用內建的最佳實務和標準，以及自動化合規和稽核程序。雲端https://aws.amazon.com/compliance/合規是指遵守管理資料保護和隱私權的法律和法規。AWS 合規計劃提供有關符合的認證、法規和架構 AWS 的資訊。

此 one-and-a-half 分鐘影片摘要說明 如何在我們的核心 AWS 建置強大的安全性。

# 了解 AWS 安全、身分和控管服務

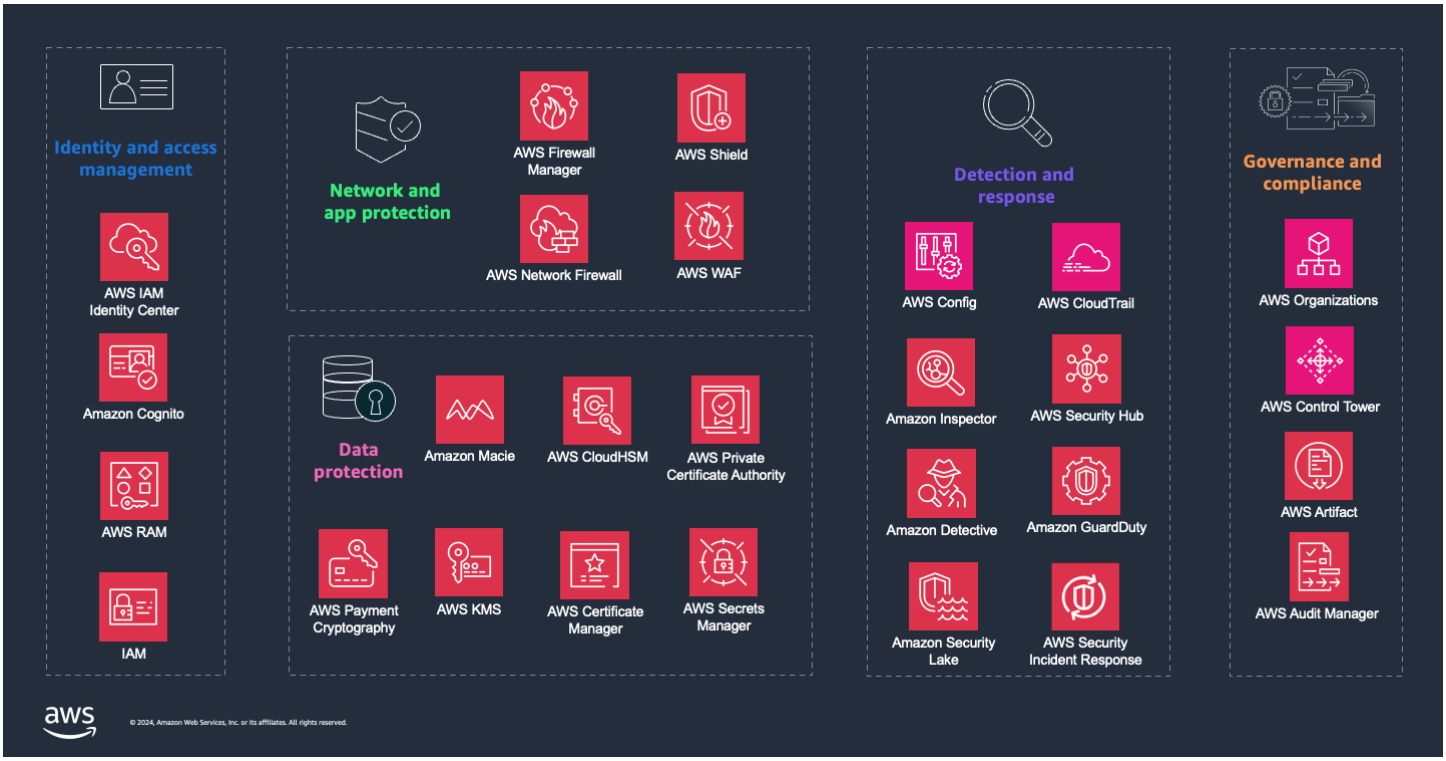
## 安全與合規是共同的責任

在選擇您的 AWS 安全、身分和控管服務之前，請務必了解安全與合規是您和 之間的共同責任 AWS。

此共同責任的性質有助於減輕您的營運負擔，並為您提供彈性和對部署的控制。這種責任差異通常稱為「雲端」安全性和「雲端」安全性。

透過了解此模型，您可以了解可用的選項範圍，以及適用的 AWS 服務 如何結合在一起。

# 您可以結合 AWS 工具和服務，協助保護您的工作負載




如上圖所示， 跨五個網域 AWS 提供工具和服務，協助您在雲端中實現和維護強大的安全性、身分管理和控管。您可以使用 AWS 服務 這五個網域中的 來協助您執行下列動作：

- 形成多層方法來保護您的資料和環境
- 強化您的雲端基礎設施，防範不斷演變的威脅
- 遵守嚴格的法規標準

若要進一步了解 AWS 安全性，包括 的安全性文件 AWS 服務，請參閱 AWS 安全性文件。

在下列各節中，我們會進一步檢查每個網域。

## 了解 AWS 身分和存取管理服務

在 AWS 安全性的中心是最低權限原則：個人和服務只有他們所需的存取權。 AWS IAM Identity Center 是 AWS 服務 管理使用者存取 AWS 資源的建議。您可以使用此服務來管理對帳戶和這些帳戶中許可的存取，包括來自外部身分提供者的身分。

下表摘要說明本指南討論的身分和存取管理方案：

AWS IAM Identity Center

AWS IAM Identity Center 可協助您連接身分來源，或建立使用者。您可以集中管理對多個 AWS 帳戶 和應用程式的人力資源存取。

Amazon Cognito

Amazon Cognito 為 Web 和行動應用程式提供身分工具，以驗證和授權來自內建使用者目錄、您的企業目錄和消費者身分提供者的使用者。

AWS RAM

AWS RAM 可協助您安全地跨組織 AWS 帳戶、組織內以及與 IAM 角色和使用者共用資源。

IAM

IAM 可對 AWS 工作負載資源的存取進行安全、精細的控制。

## 了解 AWS 資料保護服務

資料保護在雲端至關重要， AWS 並提供可協助您保護資料、帳戶和工作負載的服務。例如，加密傳輸中和靜態資料有助於保護資料免於暴露。使用 AWS Key Management Service(AWS KMS) AWS CloudHSM 和 ，您可以建立和控制用來保護資料的密碼編譯金鑰。

下表摘要說明本指南討論的資料保護方案：

Amazon Macie

Amazon Macie 使用機器學習和模式比對來探索敏感資料，並啟用自動化保護來防範相關風險。

AWS KMS

AWS KMS 會建立和控制您用來保護資料的密碼編譯金鑰。

AWS CloudHSM

AWS CloudHSM 提供高可用性的雲端型硬體安全模組 HSMs)。

AWS Certificate Manager

AWS Certificate Manager 處理建立、儲存和續約公有和私有 SSL/TLS X.509 憑證和金鑰的複雜性。

AWS Private CA

AWS Private CA 可協助您建立私有憑證授權單位階層，包括根憑證授權單位和次級憑證授權單位 (CAs)。

AWS Secrets Manager

AWS Secrets Manager 可協助您管理、擷取和輪換資料庫登入資料、應用程式登入資料、OAuth 權杖、API 金鑰和其他秘密。

AWS Payment Cryptography

AWS Payment Cryptography 根據支付卡產業 (PCI) 標準，提供用於付款處理的密碼編譯函數和金鑰管理的存取權。

## 了解 AWS 網路和應用程式保護服務

AWS 提供多種 服務來保護您的網路和應用程式。 AWS Shield為您提供防範分散式阻斷服務 (DDoS) 攻擊的保護，並AWS WAF協助您保護 Web 應用程式免受常見的 Web 入侵攻擊。

下表摘要說明本指南中討論的網路和應用程式保護方案：

AWS Firewall Manager

AWS Firewall Manager 簡化跨多個帳戶和資源的管理和維護任務，以提供保護。

AWS Network Firewall

AWS Network Firewall 為您的 VPC 提供具狀態的受管網路防火牆和入侵偵測和預防服務。

AWS Shield

AWS Shield 為網路、傳輸和應用程式層 AWS 的資源提供防範 DDoS 攻擊的保護。

AWS WAF

AWS WAF 提供 Web 應用程式防火牆，讓您可以監控轉送到受保護 Web 應用程式資源的 HTTP(S) 請求。

## 了解 AWS 偵測和回應服務

AWS 提供工具，協助您簡化整個 AWS 環境的安全操作，包括多帳戶環境。例如，您可以使用 Amazon GuardDuty 進行智慧威脅偵測，也可以使用 Amazon Detective 透過收集日誌資料來識別和分析安全調查結果。 AWS Security Hub支援多個安全標準，並提供 安全提醒和合規狀態的概觀 AWS 帳戶。 會AWS CloudTrail追蹤使用者活動和應用程式程式設計界面 (API) 使用情況，這對於了解和回應安全事件至關重要。

下表摘要說明本指南討論的偵測和回應方案：

AWS Config

AWS Config 提供 中 AWS 資源組態的詳細檢視 AWS 帳戶。

AWS CloudTrail

AWS CloudTrail 會記錄使用者、角色或 採取的動作 AWS 服務。

AWS Security Hub

AWS Security Hub 提供 中安全狀態的完整檢視 AWS。

Amazon GuardDuty

Amazon GuardDuty 會持續監控您的 AWS 帳戶、工作負載、執行時間活動和資料是否有惡意活動。

Amazon Inspector

Amazon Inspector 會掃描您的 AWS 工作負載是否有軟體漏洞和意外的網路暴露。

Amazon Security Lake

Amazon Security Lake 會自動將來自 AWS 環境、SaaS 提供者、內部部署環境、雲端來源和第三方來源的安全資料集中到資料湖中。

Amazon Detective

Amazon Detective 會協助您分析、調查並快速識別安全調查結果或可疑活動的根本原因。

AWS Security Incident Response

AWS 安全事件回應

協助您快速準備、回應和接收指引，以協助從安全事件中復原。

## 了解 AWS 控管和合規服務

AWS 提供的工具可協助您遵守安全、營運、合規和成本標準。例如，您可以使用 AWS Control Tower 來設定和管理具有方案控制的多帳戶環境。使用 AWS Organizations，您可以為組織內的多個帳戶設定以政策為基礎的管理。

AWS 也可讓您全面檢視合規狀態，並根據組織的 AWS 最佳實務和業界標準，使用自動化合規檢查來持續監控您的環境。例如， AWS Artifact可讓您隨需存取合規報告，並AWS Audit Manager自動化證據收集，讓您更輕鬆地評估控制項是否有效運作。

下表摘要說明本指南討論的控管和合規方案：

AWS Organizations

AWS Organizations 可協助您將多個 合併 AWS 帳戶 到您建立並集中管理的組織。

AWS Control Tower

AWS Control Tower 可協助您設定和管理以最佳實務為基礎的 AWS 多帳戶環境。

AWS Artifact

AWS Artifact 提供隨需下載 AWS 的安全與合規文件。

AWS Audit Manager

AWS Audit Manager

協助您持續稽核 AWS 用量，以簡化評估風險與合規的方式。

# 考慮 AWS 安全性、身分和控管條件

在 上選擇正確的安全、身分和控管服務 AWS ，取決於您的特定需求和使用案例。決定採用 AWS 安全服務可提供決策樹，協助您決定 AWS 服務 採用安全、身分和控管是否適合您的組織。此外，以下是決定要使用哪些 服務時需要考慮的一些條件。

Security requirements and threat landscape

對組織的特定漏洞和威脅進行全面評估。這包括識別您處理的資料類型，例如個人客戶資訊、財務記錄或專屬商業資料。了解與每個 相關的潛在風險。

評估您的應用程式和基礎設施架構。判斷您的應用程式是否公開，以及它們處理的 Web 流量類型。這將影響您對 等服務的需求 AWS WAF ，以防止 Web 入侵。對於內部應用程式，請考慮使用 Amazon GuardDuty 進行內部威脅偵測和持續監控的重要性，這可以識別不尋常的存取模式或未經授權的部署。

最後，請考慮現有安全狀態的複雜性，以及安全團隊的專業知識。如果您的團隊資源有限，選擇提供更多自動化和整合的服務可以為您提供有效的安全增強功能，而不會讓您的團隊負擔過重。範例服務包括 AWS Shield DDoS 保護和 AWS Security Hub 集中式安全監控。

Compliance and regulatory requirements

識別您產業或地理區域的相關法律和標準，例如一般資料保護法規 (GDPR)、1996 年美國健康保險流通與責任法案 (HIPAA) 或支付卡產業資料安全標準 (PCI DSS)。

AWS 提供 AWS Config 和 AWS Artifact 等服務，協助您管理各種標準的合規性。透過 AWS Config，您可以評估、稽核和評估 AWS 資源的組態，讓您更輕鬆地確保符合內部政策和法規要求。 AWS Artifact 提供隨需存取 AWS 合規文件，協助您進行稽核和合規報告。

選擇符合您特定合規需求的服務，可協助您的組織符合法律要求，並為您的資料建立安全且值得信賴的環境。探索AWS 合規計劃以進一步了解。

Scalability and flexibility

考慮您的組織將如何成長，以及速度有多快。選擇 AWS 服務 可協助您的安全措施與基礎設施無縫成長，並適應不斷變化的威脅。

為了協助您快速擴展， AWS Control Tower 會協調其他數個 的功能AWS 服務，包括 AWS Organizations 和 AWS IAM Identity Center，在不到一小時的時間內建置登陸區域。Control Tower 會代表您設定和管理資源。

AWS 也會設計許多 服務，以根據應用程式的流量和使用模式自動擴展，例如 Amazon GuardDuty 用於威脅偵測和 AWS WAF 保護 Web 應用程式。隨著您的業務擴展，這些服務會隨之擴展，而不需要手動調整或造成瓶頸。

此外，您可以自訂安全控制以符合您的業務需求和威脅態勢至關重要。請考慮使用 管理您的帳戶 AWS Organizations，讓您可以跨多個帳戶管理 40 多個 服務的資源。這為個別應用程式團隊提供彈性和可見性，以管理工作負載特定的安全需求，同時為集中式安全團隊提供控管和可見性。

考量可擴展性和靈活性，有助於確保您的安全狀態強大、回應能力高且能夠支援動態商業環境。

Integration with existing systems

考慮增強而不是中斷您目前操作的安全措施。例如，請考慮下列事項：

- 透過彙總來自 的安全資料和警示 AWS 服務 ，以及與現有安全資訊和事件管理 (SIEM) 系統一起分析它們，簡化您的工作流程。
- 建立跨 和內部部署環境的安全威脅 AWS 和漏洞的統一檢視。
- AWS CloudTrail 與現有的日誌管理解決方案整合，以全面監控 AWS 基礎設施和現有應用程式的使用者活動和 API 用量。
- 檢查您可以最佳化資源使用率的方式，並一致地跨環境套用安全政策。這可協助您降低安全涵蓋範圍漏洞的風險。

Cost and budget considerations

檢閱您考慮的每個服務的定價模型。 AWS 通常根據用量收費，例如 API 呼叫次數、處理的資料量或儲存的資料量。例如，Amazon GuardDuty 會根據針對威脅偵測分析的日誌資料量收費，而 AWS WAF 帳單是根據部署的規則數目和收到的 Web 請求數目。

估計您的預期用量，以準確預測成本。同時考慮目前需求和潛在的成長或需求激增。例如，可擴展性是 的主要功能 AWS 服務，但如果不小心管理，也可能會導致成本增加。使用 AWS 定價計算工具建立不同案例的模型，並評估其財務影響。

評估總體擁有成本 (TCO)，其中包括直接成本和間接成本，例如管理和維護所需的時間和資源。選擇受管服務可以降低營運開銷，但價格可能更高。

最後，根據風險評估排定安全投資的優先順序。並非所有安全服務對您的基礎設施都同樣重要，因此請將您的預算集中在對降低風險和確保合規有最重要影響的領域。在成本效益與您需要的安全層級之間取得平衡，是成功 AWS 安全策略的關鍵。

Organizational structure and access needs

評估組織的結構和運作方式，以及您的存取需求可能因團隊、專案或位置而有所不同。這會影響您如何管理和驗證使用者身分、指派角色，以及在整個 AWS 環境中強制執行存取控制。實作最佳實務，例如套用最低權限許可和需要多重要素驗證 (MFA)。

大多數組織都需要多帳戶環境。檢閱此類型環境的最佳實務，並考慮使用 AWS Organizations 和 AWS Control Tower 來協助您實作。

您應該考慮的另一個層面是管理登入資料和存取金鑰。考慮使用 IAM Identity Center 集中管理多個 AWS 帳戶 和商業應用程式的存取，這可提高安全性和使用者便利性。為了協助您順暢管理組織帳戶的存取權，IAM Identity Center 會與 整合 AWS Organizations。

此外，請評估這些身分和存取管理服務如何與您現有的目錄服務整合。如果您有現有的身分提供者，您可以使用 SAML 2.0 或 OpenID Connect (OIDC) 將其與 IAM Identity Center 整合。IAM Identity Center 也支援跨網域身分管理 (SCIM) 佈建，以協助保持目錄同步。這有助於您在存取 AWS 資源時確保無縫且安全的使用者體驗。

# 選擇 AWS 安全、身分和控管服務

現在您知道評估安全選項的條件，您已準備好選擇哪些 AWS 安全服務可能非常適合您的組織需求。

下表重點介紹針對哪些情況最佳化哪些服務。使用 資料表來協助判斷最適合您組織和使用案例的服務。

Note

[1] 與 整合 AWS Security Hub (完整清單)
[2] 與 Amazon GuardDuty 整合 (完整清單)
[3] 與 Amazon Security Lake 整合 (完整清單)

## 選擇 AWS 身分和存取管理服務

授予適當的個人適當的存取層級，以存取系統、應用程式和資料。

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 安全性、身分和控管服務 |
| --- | --- | --- |
| 使用這些服務可協助您安全地管理和控管客戶、人力和工作負載的存取。 | 協助您連接身分來源或建立使用者。您可以集中管理對多個 AWS 帳戶和應用程式的人力資源存取。 | AWS IAM Identity Center |
| | 針對 Web 和行動應用程式的身分驗證和授權使用者進行最佳化。 | Amazon Cognito |
| | 已針對內部安全共用資源進行最佳化 AWS。 | AWS RAM |
| | 對 AWS 工作負載資源的存取進行安全、精細的控制。 | IAM [1] |

## 選擇 AWS 資料保護服務

自動化並簡化資料保護和安全任務，範圍從金鑰管理和敏感資料探索到憑證管理。

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 資料保護服務 |
| --- | --- | --- |
| 使用這些服務來協助您實現和維護 AWS 環境中存放和處理 | 針對探索敏感資料進行最佳化。 | Amazon Macie [1] |

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 資料保護服務 |
| --- | --- | --- |
| 的敏感資料的機密性、完整性和可用性。 | 針對密碼編譯金鑰最佳化。 | AWS KMS |
| | 針對 HSMs最佳化。 | AWS CloudHSM |
| | 針對私有 SSL/TLS X.509 憑證和金鑰進行最佳化。 | AWS Certificate Manager |
| | 已針對建立私有憑證授權單位階層進行最佳化。 | AWS Private CA |
| | 針對資料庫登入資料、應用程式登入資料、OAuth 權杖、API 金鑰和其他秘密進行最佳化。 | AWS Secrets Manager |
| | 根據 PCI 標準，針對提供用於付款處理的密碼編譯函數和金鑰管理的存取權進行最佳化。 | AWS Payment Cryptography |

## 選擇 AWS 網路和應用程式保護服務

集中保護您的網際網路資源，防範常見的 DDoS 和應用程式攻擊。

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 網路和應用程式保護服務 |
| --- | --- | --- |
| 使用這些服務可協助您在每個網路控制點強制執行詳細的安全政策。 | 針對集中設定和管理防火牆規則進行最佳化。 | AWS Firewall Manager [1] |
| | 針對提供具狀態的受管網路防火牆和入侵偵測和預防服務進行最佳化。 | AWS Network Firewall |
| | 針對網路、傳輸和應用程式層 AWS 的資源，針對防範 DDoS 攻擊進行最佳化。 | AWS Shield |

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 網路和應用程式保護服務 |
| --- | --- | --- |
| | 針對提供 Web 應用程式防火牆進行最佳化。 | AWS WAF |

## 選擇 AWS 偵測和回應服務

持續識別安全風險並排定優先順序，同時及早整合安全最佳實務。

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 偵測和回應服務 |
| --- | --- | --- |
| 使用這些服務可協助您偵測和回應帳戶的安全風險，以便大規模保護您的工作負載。 | 針對使用 和第三方整合自動化安全檢查 AWS 和集中安全提醒進行最佳化。 | AWS Security Hub [2、3] |
| | 針對評估、稽核和評估 資源的組態進行最佳化。 | AWS Config [1] |
| | 針對將其他 的事件記錄 AWS 服務 為稽核線索進行最佳化。 | AWS CloudTrail |
| | 針對智慧型威脅偵測和詳細報告進行最佳化。 | Amazon GuardDuty [1] |
| | 針對漏洞管理進行最佳化。 | Amazon Inspector [1] |
| | 針對集中安全資料進行最佳化。 | Amazon Security Lake [1] |
| | 針對彙整和摘要潛在安全問題進行最佳化。 | Amazon Detective [1、2、3] |
| | 針對協助您分類問題清單、呈報安全事件和管理需要您立即注意的案例進行最佳化。 | AWS 安全事件回應 |

## 選擇 AWS 控管和合規服務

建立跨 資源的雲端控管，並自動化合規和稽核程序。

| 您應該何時使用它？ | 它針對什麼進行最佳化？ | 治理和合規服務 |
| --- | --- | --- |
| 使用這些服務可協助您實作最佳實務，並在使用 時符合業界標準 AWS。 | 針對集中管理多個帳戶和合併帳單進行最佳化。 | AWS Organizations |
| | 針對提供隨需下載 AWS 的安全性和合規文件進行最佳化。 | AWS Artifact |
| | 已針對稽核 AWS 用量進行最佳化。 | AWS Audit Manager [1] |
| | 針對設定和管理 AWS 多帳戶環境進行最佳化。 | AWS Control Tower |

# 使用 AWS 安全、身分和控管服務

您現在應該清楚了解每個 AWS 安全、身分和控管服務 （以及支援 AWS 工具和服務） 的功能，以及哪些可能適合您。

為了探索如何使用和進一步了解每個可用的 AWS 安全、身分和控管服務，我們提供了探索每個服務運作方式的途徑。下列各節提供深入文件、實作教學課程和資源的連結，協助您開始使用。

## 使用 AWS 身分和存取管理服務

下表顯示一些有用的身分和存取管理資源，依服務組織，以協助您開始使用。

AWS IAM Identity Center

- 啟用 AWS IAM Identity Center

  啟用 IAM Identity Center 並開始將其與 搭配使用 AWS Organizations。

  探索指南

- 使用預設 IAM Identity Center 目錄設定使用者存取權

  使用預設目錄做為您的身分來源，並設定和測試使用者存取權。

  教學課程入門

- 使用 Active Directory 做為身分來源

  完成使用 Active Directory 做為 IAM Identity Center 身分來源的基本設定。

  教學課程入門

- 使用 Okta 和 IAM Identity Center 設定 SAML 和 SCIM

  設定與 Okta 和 IAM Identity Center 的 SAML 連線。

  教學課程入門

Amazon Cognito

- Amazon Cognito 入門

  了解最常見的 Amazon Cognito 任務。

  探索指南

- 教學課程：建立使用者集區

  建立使用者集區，以允許使用者登入您的 Web 或行動應用程式。

  教學課程入門

- 教學課程：建立身分集區

  建立身分集區，這可讓您的使用者取得暫時 AWS 登入資料以進行存取 AWS 服務。

  教學課程入門

- Amazon Cognito 研討會

  練習使用 Amazon Cognito 為假設性寵物商店建置身分驗證解決方案。

  教學課程入門

AWS RAM

- 入門 AWS RAM

  了解 AWS RAM 術語和概念。

  探索指南

- 使用共用 AWS 資源

  共用您擁有 AWS 的資源，並存取與您共用 AWS 的資源。

  探索指南

- 在 RAM AWS 中管理許可

  了解兩種類型的受管許可：受 AWS 管許可和客戶受管許可。

  探索指南

- 設定使用 RAM AWS 共用之資源的詳細存取權

  使用客戶受管許可來自訂您的資源存取，並實現最低權限的最佳實務。

  閱讀部落格

IAM

- IAM 入門

  使用 建立 IAM 角色、使用者和政策 AWS Management Console。

  教學課程入門

- AWS 帳戶 使用角色委派跨 的存取權

  使用角色委派存取您擁有的不同 AWS 帳戶 中的資源，稱為Production andDevelopment。

  教學課程入門

- 建立客戶受管政策

  使用 AWS Management Console 建立客戶受管政策，然後將該政策連接到您 中的 IAM 使用者 AWS 帳戶。

教學課程入門

- 根據標籤定義存取 AWS 資源的許可

  建立和測試政策，允許具有主體標籤的 IAM 角色存取具有相符標籤的資源。

  教學課程入門

- IAM 中的安全最佳實務

  使用 IAM 最佳實務協助保護您的 AWS 資源。

  探索指南

## 使用 AWS 資料保護服務

下一節提供您描述 AWS 資料保護的詳細資源連結。

Macie

- Amazon Macie 入門

  為您的 啟用 Macie AWS 帳戶、評估您的 Amazon S3 安全狀態，並設定金鑰設定和資源，以探索和報告 S3 儲存貯體中的敏感資料。

  探索指南

- 使用 Amazon Macie 監控資料安全和隱私權

  使用 Amazon Macie 監控 Amazon S3 資料安全並評估您的安全狀態。

  探索指南

- 分析 Amazon Macie 調查結果

  檢閱、分析和管理 Amazon Macie 調查結果。

  探索指南

- 使用 Amazon Macie 調查結果擷取敏感資料範例

  使用 Amazon Macie 擷取和顯示個別問題清單報告的敏感資料範例。

  探索指南

- 使用 Amazon Macie 探索敏感資料

  自動化探索、記錄和報告 Amazon S3 資料資產中的敏感資料。

  探索指南

AWS KMS

- 入門 AWS KMS

  管理從建立到刪除的對稱加密 KMS 金鑰。

  探索指南
- 特殊用途金鑰

  了解 AWS KMS 支援的不同類型的金鑰，以及對稱加密 KMS 金鑰。

  探索指南
- 使用 擴展靜態加密功能 AWS KMS

  了解 中可用的靜態加密選項 AWS。

  探索研討會

AWS CloudHSM

- 入門 AWS CloudHSM

  建立、初始化和啟用 AWS CloudHSM 叢集。

  探索指南
- 管理 AWS CloudHSM 叢集

  連線至您的 AWS CloudHSM 叢集，以及管理叢集的各種管理任務。

  探索指南
- 在 中管理 HSM 使用者和金鑰 AWS CloudHSM

  在叢集的 HSMs上建立使用者和金鑰。

探索指南

- 在 CloudHSM 中使用 Amazon ECS 搭配 TLS 卸載來自動化 NGINX Web 服務的部署

  使用 AWS CloudHSM 來存放託管於雲端之網站的私有金鑰。

  閱讀部落格

AWS Certificate Manager

- 請求公有憑證

  使用 AWS Certificate Manager (ACM) 主控台或 AWS CLI 請求公有 ACM 憑證。

  探索指南
- 的最佳實務 AWS Certificate Manager

  根據目前 ACM 客戶的真實體驗，了解最佳實務。

  探索指南
- 如何使用 AWS Certificate Manager 強制執行憑證發行控制

  使用 IAM 條件金鑰，確保您的使用者根據組織的準則發行或請求 TLS 憑證。

  閱讀部落格

AWS Private CA

- 規劃您的 AWS Private CA 部署

  建立私有憑證授權機構之前， AWS Private CA 請先準備使用 。

  探索指南
- AWS Private CA 管理

  建立根和次級憑證授權單位的完全 AWS 託管階層，以供組織內部使用。

  探索指南
- 憑證管理

使用 執行基本憑證管理任務 AWS Private CA，例如發行、擷取和列出私有憑證。

探索指南

- AWS Private CA 研討會

  開發私有憑證授權單位各種使用案例的實作體驗。

  探索研討會

- 如何使用 簡化 Active Directory 中的憑證佈建 AWS Private CA

  使用 AWS Private CA 可更輕鬆地為 Microsoft Active Directory 環境中的使用者和機器佈建憑證。

  閱讀部落格

- 如何在 中強制執行 DNS 名稱限制 AWS Private CA

  使用 AWS Private CA 服務將 DNS 名稱限制條件套用至次級 CA。

  閱讀部落格

AWS Secrets Manager

- AWS Secrets Manager 概念

  使用 執行基本憑證管理任務 AWS Private CA，例如發行、擷取和列出私有憑證。

  探索指南

- 設定 的交替使用者輪換 AWS Secrets Manager

  為包含資料庫登入資料的秘密設定交替使用者輪換。

  探索指南

- 搭配 Kubernetes 使用 AWS Secrets Manager 秘密

  使用 Secrets and Configuration Provider (ASCP)，將 Secrets Manager 的 AWS 秘密顯示為掛載在 Amazon EKS Pod 中的檔案。

  探索指南

AWS Payment Cryptography

- 入門 AWS Payment Cryptography

  建立金鑰，並在各種密碼編譯操作中使用它們。

  探索指南
- AWS Payment Cryptography FAQs

  了解 的基本概念 AWS Payment Cryptography。

  探索FAQs

## 使用 AWS 網路和應用程式保護服務

下表提供說明 AWS 網路和應用程式保護的詳細資源連結。

AWS Firewall Manager

- AWS Firewall Manager 政策入門

  使用 AWS Firewall Manager 啟用不同類型的安全政策。

  探索指南
- 如何使用 持續稽核和限制安全群組 AWS Firewall Manager

  使用 AWS Firewall Manager 限制安全群組，確保僅開啟必要的連接埠。

  閱讀部落格
- 使用 AWS Firewall Manager 大規模部署保護 AWS Organizations

  使用 AWS Firewall Manager 跨 來部署和管理安全政策 AWS Organizations。

  閱讀部落格

AWS Network Firewall

- 入門 AWS Network Firewall

  為具有基本網際網路閘道架構的 VPC 設定和實作 AWS Network Firewall 防火牆。

探索指南

- AWS Network Firewall 研討會

  使用基礎設施做為程式碼 AWS Network Firewall 來部署 。

  探索研討會

- AWS Network Firewall 彈性規則引擎的實作演練 – 第 1 部分

  在 AWS Network Firewall 中部署 的示範 AWS 帳戶 ，以與其規則引擎互動。

  閱讀部落格

- AWS Network Firewall 彈性規則引擎的實作演練 – 第 2 部分

  建立具有嚴格規則順序的防火牆政策，並設定一或多個預設動作。

  閱讀部落格

- 的部署模型 AWS Network Firewall

  了解您可以新增至 AWS Network Firewall 流量路徑的常見使用案例的部署模型。

  閱讀部落格

- AWS Network Firewall 具有 VPC 路由增強功能的 部署模型

  使用增強型 VPC 路由基本概念，在相同 VPC 的不同子網路中的工作負載 AWS Network Firewall 之間插入 。

  閱讀部落格

AWS Shield

- AWS Shield 運作方式

  了解 AWS Shield Standard 和 如何為網路和傳輸層 （第 3 層和第 4 層） 和應用程式層 （第 7 層） 上的 AWS 資源 AWS Shield Advanced 提供 DDoS 攻擊防護。

  探索指南

- 入門 AWS Shield Advanced

  AWS Shield Advanced 使用 Shield Advanced 主控台開始使用 。

探索指南

- AWS Shield Advanced 研討會

  保護網際網路暴露的資源免受 DDoS 攻擊、監控對基礎設施的 DDoS 攻擊，並通知適當的團隊。

  探索研討會

AWS WAF

- 入門 AWS WAF

  設定 AWS WAF、建立 Web ACL，並透過新增規則和規則群組來篩選 Web 請求來保護 Amazon CloudFront。

  教學課程入門

- 分析 Amazon CloudWatch AWS WAF Logs 中的日誌

  設定 Amazon CloudWatch logs的原生 AWS WAF 記錄，並將日誌中的資料視覺化和分析。

  閱讀部落格

- 使用 Amazon CloudWatch 儀表板視覺化 AWS WAF 日誌

  使用 Amazon CloudWatch 透過 CloudWatch 指標、Contributor Insights 和 Logs Insights 來監控和分析 AWS WAF 活動。

  閱讀部落格

## 使用 AWS 偵測和回應服務

下表提供詳細資源的連結，說明 AWS 偵測和回應服務。

AWS Config

- 入門 AWS Config

  設定 AWS Config 和使用 AWS SDKs。

  探索指南

- 風險與合規研討會

使用 AWS Config 和 AWS 受管 Config 規則來自動化控制項。

探索研討會

- AWS Config 規則開發套件程式庫：大規模建置和操作規則

  使用規則開發套件 (RDK) 來建置自訂 AWS Config 規則，並使用 RDKLib 部署它。

  閱讀部落格

AWS CloudTrail

- 檢視事件歷史記錄

  檢閱 中支援 CloudTrail AWS 帳戶 之服務的 AWS API 活動。

  教學課程入門

- 建立追蹤以記錄管理事件

  建立追蹤以記錄所有區域中的管理事件。

  教學課程入門

AWS Security Hub

- 啟用 AWS Security Hub

  在獨立帳戶中 AWS Security Hub 啟用 AWS Organizations 或 。

  探索指南

- 跨區域彙總

  將 AWS Security Hub 問題清單從多個彙總 AWS 區域 到單一彙總區域。

  探索指南

- AWS Security Hub 研討會

  了解如何使用 AWS Security Hub 和 來管理和改善 AWS 環境的安全狀態。

  探索研討會

- 三種重複的 Security Hub 使用模式以及如何部署它們

  了解三種最常見的 AWS Security Hub 使用模式，以及如何改善識別和管理問題清單的策略。

  閱讀部落格

Amazon GuardDuty

- Amazon GuardDuty 入門

  啟用 Amazon GuardDuty、產生範例問題清單，以及設定提醒。

  探索教學課程

- Amazon GuardDuty 中的 EKS 保護

  使用 Amazon GuardDuty 監控 Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌。

  探索指南

- Amazon GuardDuty 中的 Lambda 保護

  當您叫用 AWS Lambda 函數時，識別潛在的安全威脅。

  探索指南

- GuardDuty Amazon RDS 保護

  使用 Amazon GuardDuty 來分析和描述 Amazon Relational Database Service (Amazon RDS) 登入活動，以找出對 Amazon Aurora 資料庫的潛在存取威脅。

  探索指南

- Amazon GuardDuty 中的 Amazon S3 保護 Amazon GuardDuty

  使用 GuardDuty 監控 CloudTrail 資料事件，並識別 S3 儲存貯體內的潛在安全風險。

  探索指南

- Amazon GuardDuty 和 Amazon Detective 的威脅偵測和回應

  了解 Amazon GuardDuty 和 Amazon Detective 的基本概念。

  探索研討會

Amazon Inspector

- Amazon Inspector 入門

  啟用 Amazon Inspector 掃描以了解 主控台中的問題清單。

  教學課程入門

- 使用 Amazon Inspector 進行漏洞管理

  使用 Amazon Inspector 掃描 Amazon Elastic Container Registry (Amazon ECR) 中的 Amazon EC2 執行個體和容器映像是否有軟體漏洞。

  探索研討會

- 如何使用 Amazon Inspector 掃描 EC2 AMIs

  使用多個 AWS 服務 來掃描 AMIs是否有已知漏洞，以建置解決方案。

  閱讀部落格

Amazon Security Lake

- Amazon Security Lake 入門

  啟用並開始使用 Amazon Security Lake。

  探索指南

- 使用 管理多個帳戶 AWS Organizations

  從多個 收集安全日誌和事件 AWS 帳戶。

  探索指南

- 擷取、轉換和交付 Amazon Security Lake 發佈至 Amazon OpenSearch Service 的事件

  擷取、轉換 Amazon Security Lake 資料並將其交付至 Amazon OpenSearch Service，以供您的 SecOps 團隊使用。

  閱讀部落格

- 如何使用 QuickSight 視覺化 Amazon Security Lake 調查結果

  使用 Amazon AthenaandQuickSight 從 Amazon Security Lake 查詢和視覺化資料。 QuickSight

閱讀部落格

Amazon Detective

- Amazon Detective 術語和概念

  了解 Amazon Detective 及其運作方式的重要關鍵術語和概念。

  探索指南
- 設定 Amazon Detective

  從 Amazon Detective 主控台、Amazon Detective API 或 啟用 Amazon Detective AWS CLI。

  探索指南
- Amazon GuardDuty 和 Amazon Detective 的威脅偵測和回應

  了解 Amazon GuardDuty 和 Amazon Detective 的基本概念。

  探索研討會

## 使用 AWS 控管和合規服務

下表提供詳細資源的連結，說明控管和合規。

AWS Organizations

- 建立和設定組織

  建立您的組織，並使用兩個 AWS 成員帳戶進行設定。

  教學課程入門
- 使用 的服務 AWS Organizations

  了解 AWS 服務 您可以搭配哪些 使用， AWS Organizations 以及在全組織層級使用每項服務的優點。

  探索指南
- 使用多個帳戶來組織您的 AWS 環境

實作最佳實務和目前的建議，以組織您的整體 AWS 環境。

閱讀白皮書

AWS Artifact

- 入門 AWS Artifact

  下載安全與合規報告、管理法律協議和管理通知。

  探索指南

- 在 中管理協議 AWS Artifact

  使用 AWS Management Console 來檢閱、接受和管理您帳戶或組織的協議。

  探索指南

- 第 1 AWS 部分 – AWS 稽核管理員 AWS Config和 AWS 成品中的稽核準備工作

  使用 AWS 服務 來協助您自動收集稽核中使用的證據。

  閱讀部落格

AWS Audit Manager

- 啟用 AWS Audit Manager

  使用 AWS Management Console、Audit Manager API 或 啟用 Audit Manager AWS CLI。

  探索指南

- 稽核擁有者教學課程：建立評估

  使用 Audit Manager 範例架構建立評估。

  探索指南

- 委派代表的教學課程：檢閱控制集

  檢閱 Audit Manager 中稽核擁有者與您共用的控制集。

  探索指南

AWS Control Tower

- 入門 AWS Control Tower

  設定並啟動符合規範最佳實務的多帳戶環境，稱為登陸區域。

  探索指南
- 使用 Amazon Bedrock 和 現代化帳戶管理 AWS Control Tower

  佈建安全工具帳戶，並利用生成式 AI 來加速 AWS 帳戶 設定和管理程序。

  閱讀部落格
- 使用 建置架構良好的 AWS GovCloud (US) 環境 AWS Control Tower

  在 AWS GovCloud (US) 區域中設定您的管理，包括使用組織單位 (OUs) 和 來管理 AWS 工作負載 AWS 帳戶。

  閱讀部落格

# 探索 AWS 安全、身分和控管服務

Editable architecture diagrams

參考架構圖

探索參考架構圖，協助您開發安全性、身分和控管策略。

探索安全性、身分和管理參考架構

Ready-to-use code

精選解決方案

上的安全洞見 AWS

部署 AWS建置的程式碼可協助您將 Amazon Security Lake 中的資料視覺化，以更快速地調查和回應安全事件。

探索此解決方案

AWS 解決方案

探索由 建置的預先設定、可部署的解決方案及其實作指南 AWS。

探索所有 AWS 安全性、身分和控管解決方案

Documentation

### 安全性、身分和管理白皮書

探索白皮書，進一步了解選擇、實作和使用最適合您組織的安全性、身分和控管服務時的洞見和最佳實務。

探索安全性、身分和管理白皮書

### AWS 安全部落格

探索解決特定安全使用案例的部落格文章。

探索 AWS 安全部落格

# 文件歷史紀錄

下表說明此決策指南的重要變更。如需有關本指南更新的通知，您可以訂閱 RSS 摘要。

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| re：Invent 更新 | 新增有關 AWS 安全事件回應和 的資訊 AWS Payment Cryptography。已更新 AWS Identity and Access Management 和 的服務資訊 AWS IAM Identity Center。 | 2024 年 12 月 30 日 |
| 影片更新 | 使用 re：Inforce 2024 的最新閃電對談更新簡介影片。 | 2024 年 6 月 25 日 |
| 新增控管服務 | 擴大文件的範圍以包含控管，包括新增 AWS CloudTrail AWS Control Tower、 和 AWS Organizations。更新圖形以反映新的範圍。釐清身分的最佳實務。整體的編輯變更。 | 2024 年 6 月 7 日 |
| 初次出版 | 指南首先發佈。 | 2024 年 3 月 21 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。