安全支柱

AWS Well-Architected 架構

2020 年 7 月

This paper has been archived.

The latest version is now available at:

https://docs.aws.amazon.com/zh_tw/wellarchitected/latest/security-pillar/welcome.html

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。

目錄

摘要

本白皮書重點講述 Well-Architected 架構的安全支柱。文中提供的指導可協助您將最佳實務和目前的建議應用在安全 AWS 工作負載的設計、交付和維護中。

簡介

The AWS Well-Architected 架構可協助您了解在 AWS 上建置工作負載時所做決策的權衡取捨。透過使用該架構，您將了解在雲端設計和操作可靠、安全、有效率且經濟實惠的工作負載的最新架構最佳實務。該架構可讓您根據最佳實務一致地量測工作負載，並找出需要改進的方面。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。

此架構以五大支柱為基礎：

- 卓越營運
- 安全性
- 可靠性
- 效能效率
- 成本最佳化

本白皮書著重於安全支柱。本文可協助您遵循目前的 AWS 建議，以符合業務和法規要求。其適用於擔任技術職務的人員，例如技術長 (CTO)、資安長 (CSO/CISO)、架構師、開發人員和營運團隊成員。

閱讀本白皮書之後，您將了解在考慮安全的情況下，設計雲端架構時應使用的 AWS 目前的建議和策略。本文並未提供實作細節或架構模式，但包含有關這些資訊的適當資源參考。透過採用本文中的實務，您可以建置保護資料和系統、控制存取並自動回應安全事件的架構。

安全性

安全支柱說明如何利用雲端技術，以改善安全狀態的方式來保護資料、系統和資產。本白皮書針對在 AWS 上建構安全的工作負載，提供深入的最佳實務指導。

設計原則

在雲端，有一些原則能協助您強化工作負載的安全：

- **實作堅實的身份識別基礎**：實作最低授權原則，並對於每個與 AWS 資源的互動強制執行職責與適當的授權分離。集中化身份管理，旨在消除對長期靜態登入資料的倚賴。
- **啟用可追蹤性**：即時監控、提醒和稽核您環境中發生的動作和變更。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**：透過多個安全控制，套用深度防禦方法。套用至所有層級 (例如，網路邊緣、VPC、負載平衡、每個執行個體和運算服務、作業系統、應用程式和程式碼)。
- **將安全最佳實務自動化**：將基於軟體的安全機制自動化，以提高您安全、快速和以具成本效益的方式擴展的能力。建立安全架構 (包括實作控制) 在版本控制的範本中作為程式碼定義和管理。
- **保護傳輸中和靜態資料**：將您的資料分為不同的敏感性等級，並使用適當的機制，例如加密、權杖化及存取控制。
- **讓人員遠離資料**：使用機制和工具，來降低或消除對直接存取或手動處理資料的需要。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。
- **為安全事件作準備**：為事故做好萬全準備，建立與您組織的要求吻合的事故管理和調查政策與程序。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。

定義

雲端中的安全包括五個方面：

1. Identity and Access Management

2. 偵測
3. 基礎架構保護
4. 資料保護
5. 事件回應

安全與合規是 AWS 與客戶您之間共同的責任。此共用模型有助於為您降低操作負擔。您應該仔細檢查所選擇的服務，因為您的責任取決於所使用的服務、這些服務與 IT 環境的整合，以及適用的法律和法規。此共同責任的性質也提供允許部署的彈性和控制。

安全地操作您的工作負載

若要安全地操作工作負載，您必須將總體最佳實務套用到每個安全領域。採用您在組織和工作負載層級所定義的卓越營運要求和程序，將這些要求和程序套用到所有領域。透過 AWS 和產業建議與威脅情報持續取得最新資訊，可協助您發展威脅模型和控制目標。自動化安全程序、測試和驗證可讓您擴展安全操作。

使用威脅模型識別風險並排定優先順序：使用威脅模型來識別和維護潛在威脅的最新登錄資料。排定威脅的優先順序並調整安全控制，以防止、偵測和回應威脅。在不斷演變的安全形勢下，重 新審視和維護此事項。

識別並驗證控制目標：根據合規需求以及從威脅模型識別的風險，衍生並驗證您需要套用到工作負載的控制目標和控制。對控制目標與控制持續進行驗證，可協助您測量風險降低的有效性。

掌握安全威脅的最新資訊：透過隨時得知最新安全威脅來辨識攻擊向量，協助您定義並實作適當的控制。

收到安全建議的最新資訊：隨時取得 AWS 和產業安全建議的最新資訊，以發展工作負載的安全狀態。

定期評估和實作新的安全服務和功能：評估和實作 AWS 和 APN 合作夥伴提供的安全服務和功能，讓您發展工作負載的安全狀態。

將管道中安全控制的測試和驗證自動化：為安全機制建立安全基準和範本，在您的建置、管道和程序中接受測試和驗證。使用工具和自動化，持續測試和驗證所有安全控制。例如，掃描機器圖像和基礎架構即程式碼範本，檢查是否有安全漏洞、異常和偏離各階段既定基準。

減少引入生產環境中的錯誤安全組態的數量至關重要；因此，在建置過程中最好能夠執行更多品質控制，並儘可能減少缺陷。應設計持續整合和持續部署 (CI/CD) 管道，在可能的情況下檢測安全問題。CI/CD 管道提供為建置和交付之每個階段增強安全的機會。CI/CD 安全工具也必須持續更新，以緩解不斷演變的威脅。

資源

請參閱以下資源，以進一步了解如何安全地操作工作負載。

影片

- 以 Well-Architected 方式提供安全最佳實務
- 透過自動化和管控大規模採用 AWS
- AWS Security Hub：管理安全提醒與使合規自動化
- 在 AWS 上使您的安全功能自動化

文件

- 安全程序概觀
- 安全公告
- 安全部落格
- AWS 最新消息
- AWS 安全稽核指導方針
- 在 AWS 上設定 CI/CD 管道

AWS 帳戶管理和區隔

我們建議您根據功能、合規需求或一組常用的控制項，在個別帳戶和群組帳戶中整理工作負載，而不是鏡像處理組織的報告結構。在 AWS 中，帳戶是您資源的硬邊界、零信任容器。例如，強 烈建議進行帳戶層級的區隔，以便將生產工作負載與開發和測試工作負載隔離。

使用帳戶區隔工作負載：先從安全與基礎架構開始，讓您的組織隨著工作負載的成長設定常見的防護機制。該方法提供工作負載之間的邊界和控制。強烈建議進行帳戶層級的區隔，以便將生產工作負載與開發和測試工作負載隔離，或在依照外部合規要求 (例如 PCI-DSS 或 HIPAA) 所定義之不同敏感性等級處理資料的工作負載，與未如此做的工作負載之間提供強大的邏輯邊界。

安全的 AWS 帳戶：在多個層面保護 AWS 帳戶，包括保護 (而非使用根使用者)，以及使聯絡資訊保持在最新狀態。隨著您增長和擴展工作負載，可以使用 AWS Organizations 集中管理和管控帳戶。AWS Organizations 可協助您跨帳戶管理帳戶、設定控制及設定服務。

集中管理帳戶：AWS Organizations 可自動化 AWS 帳戶的建立和管理，並在建立帳戶之後控制這些帳戶。當您透過 AWS Organizations 建立帳戶時，請務必考量所使用的電子郵件地址，因為這會允許重設密碼的根使用者。Organizations 可讓您將帳戶分組為 組織單位 (OU)，這些單位可根據工作負載的需求和用途代表不同的環境。

集中設定控制：僅允許適當層級的特定服務、區域和服務動作，以控制您的 AWS 帳戶可以執行的操作。AWS Organizations 讓您能夠使用服務控制政策 (SCP) 在組織、組織單位或帳戶層級套用許可防護，這適用於所有 AWS Identity and Access Management (IAM) 使用者和角色。例如，您可以套用 SCP，限制使用者在您未明確允許的區域中啟動資源。AWS Control Tower 提供一種簡化的方式來設定和管控多個帳戶。它會自動設定 AWS Organization 中的帳戶、自動化佈建、套用防護機制 (包括預防和偵測)，以及為您提供可視性的儀表板。

集中設定服務和資源：AWS Organizations 可協助您設定適用於所有帳戶的 AWS 服務。例如，您 可以使用 AWS CloudTrail，為組織內執行的所有動作設定集中日誌記錄，並阻止成員帳戶停用日誌記錄。此外，您還可以集中彙總使用 AWS Config 定義的規則資料，讓您能夠稽核工作負載的合規性，並快速對變更做出反應。AWS CloudFormation StackSets 可讓您跨帳戶和組織單位集中管理組織中的 AWS CloudFormation 堆疊。這讓您能夠自動佈建新帳戶以符合您的安全需求。

資源

請參閱以下資源，以進一步了解對於部署和管理多個 AWS 帳戶，AWS 提出的建議。

影片

- 使用 AWS Organizations 管理和管控多帳戶 AWS 環境
- AXA：透過全球登陸區域擴展採用
- 使用 AWS Control Tower 管控多帳戶 AWS 環境

文件

- 建立您的最佳實務 AWS 環境
- AWS Organizations
- AWS Control Tower
- 使用 AWS CloudFormation StackSets
- 如何使用服務控制政策在 AWS Organizations 中的各個帳戶之間設定權限保護欄

實作

- 實驗室：AWS 帳戶和根使用者

Identity and Access Management

若要使用 AWS 服務，您必須授予使用者和應用程式存取您 AWS 帳戶中的資源。當您在 AWS 上執行更多工作負載時，需要穩固的身份管理和許可，以確保相應人員在適當條件下存取正確的資源。AWS 提供多種功能選項，協助您管理人類和機器身份及其許可。這些功能的最佳實務分為兩個主要領域：

- 身份管理
- 許可管理

身份管理

處理操作安全的 AWS 工作負載時，您需要管理兩種身份類型。

人員身份：管理員、開發人員、操作人員和應用程式取用者需要身份才能存取您的 AWS 環境和應用程式。這些人可能是組織的成員，或與您協作的外部使用者，以及透過 Web 瀏覽器、用戶端應用程式、行動應用程式或互動式命令列工具與 AWS 資源互動的使用者。

機器身份：您的工作負載應用程式、操作工具和元件需要身份才能向 AWS 服務發出請求，例如讀取資料。這些身份包括在 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部人員管理機器身份。此外，您可能也有在 AWS 外部，需要存取 AWS 環境的機器。

倚賴集中化的身份供應商

若是人力身份，請倚賴可讓您在集中位置管理身份的身份供應商。因為您從單一位置建立、管理和撤銷存取權，因此這可讓您更輕鬆地管理多個應用程式和服務之間的存取。例如，若有人離開您的組織，您在一個位置，即可撤銷所有應用程式和服務 (包括 AWS) 的存取權。這可減少多個登入資料的需求，並提供與現有人力資源 (HR) 程序整合的機會。

針對與個別 AWS 帳戶的聯合，您可以透過 SAML 2.0 供應商使用 AWS 的集中化身份，並搭配 AWS IAM。您可以使用與 SAML 2.0 通訊協定相容的任何供應商，無論是由 AWS 外部託管，還是由 AWS 合作夥伴網路 (APN) 提供。您可以使用 AWS 帳戶與所選供應商之間的聯合，透過使用

SAML 聲明取得臨時安全登入資料，授予使用者或應用程式叫用 AWS API 操作的存取權。此外還支援 Web 型單一登入，讓使用者能夠從您的登入入口網站登入 AWS 管理主控台。

針對與 AWS Organization 中多個帳戶的聯合，您可以在 AWS Single Sign-On (AWS SSO) 中設定您的身份來源，並指定使用者和群組的存放位置。設定好之後，您的身份供應商即真實來源，而資訊可以使用跨網域身份管理系統 (SCIM) v2.0 通訊協定來同步。然後，您可以查詢使用者或群組，並授予他們對 AWS 帳戶、雲端應用程式或兩者的單一登入存取權。

AWS SSO 與 AWS Organizations 整合，讓您只需設定身份供應商一次，然後即可將存取權授予組織中管理的現有及新帳戶。AWS SSO 為您提供預設存放區，這可用於管理使用者和群組。若您選擇使用 AWS SSO 存放區，則建立使用者和群組，並將其存取層級指派給您的 AWS 帳戶和應用程式，並記住最低權限的最佳實務。或者，您可以選擇使用 SAML 2.0 連線至您的外部身份供應商，或使用 AWS Directory Service 連線至您的 Microsoft AD 目錄。設定好之後，您可以透過中央身份供應商進行身份驗證，登入 AWS 管理主控台、命令列界面或 AWS 行動應用程式。

若要管理工作負載的最終使用者或取用者，例如行動應用程式，您可以使用 Amazon Cognito。它可為您的 Web 和行動應用程式提供身份驗證、授權和使用者管理。您的使用者可以憑使用者名稱和密碼直接登入，或透過第三方 (例如 Amazon、Apple、Facebook 或 Google) 登入。

利用使用者群組和屬性

隨著您管理的使用者人數增加，您需要確定整理使用者的方式，以便大規模管理使用者。將具有共同安全需求的使用者放在身分供應商定義的群組中，並設置機制，以確保可用於存取控制的使用者屬性 (例如，部門或位置) 正確並已更新。使用這些群組和屬性 (而非個別使用者) 來控制存取權。這 可讓您透過許可集合一次變更使用者的群組成員資格或屬性集中管理存取權，而不是在使用者存取需求變更時更新許多個別政策。您可以使用 AWS SSO 來管理使用者群組和屬性。AWS SSO 支援最常用的屬性，無論是在使用者建立期間手動輸入，還是使用同步引擎自動佈建，例如 System for Cross-Domain Identity Management (SCIM) 規格中所定義。

使用強式登入機制

強制執行密碼長度下限，並教育使用者避免使用常見密碼或重複使用密碼。透過軟體或硬體機制強制使用 Multi-Factor Authentication (MFA)，以提供額外的驗證保護層。例如，使用 AWS SSO

作為身份來源時，請進行 MFA 的「內容感知」或「永遠啟用」設定，並允許使用者註冊自己的 MFA 裝置以加速採用。使用外部身份提供者 (IdP) 時，設定您的 MFA 的 IdP。

使用臨時登入資料

需要身份才能動態取得臨時登入資料。若是人力身份，請使用 AWS SSO 或與 IAM 的聯合身份來存取 AWS 帳戶。針對機器身份，例如 EC2 執行個體或 Lambda 函數，需要使用 IAM 角色，而不是具有長期存取金鑰的 IAM 使用者。

針對使用 AWS 管理主控台的人類身份，需要使用者取得臨時登入資料並聯合至 AWS。您可以使用 AWS SSO 使用者入口網站，或設定與 IAM 的聯合來執行此動作。針對需要 CLI 存取權的使用者，請確定他們使用 支援與 AWS Single Sign-On (AWS SSO) 直接整合的 AWS CLI v2。使用者可以建立連結至 AWS SSO 帳戶和角色的 CLI 描述檔。CLI 會自動從 AWS SSO 擷取 AWS 登入資料，並代您重新整理。這樣就無需從 AWS SSO 主控台複製並貼上臨時 AWS 登入資料。針對 SDK，使用者應倚賴 AWS STS 來擔任角色，以接收臨時登入資料。在某些情況下，臨時登入資料可能並不實用。您應注意存放存取金鑰的風險，經常輪換這些金鑰，並盡可能要求 MFA 作為條件。

若您需要授予取用者存取 AWS 資源，請使用 Amazon Cognito 身份集區，並為其指派一組臨時、有限權限的登入資料來存取您的 AWS 資源。每個使用者的許可都是透過您建立的 IAM 角色 來控制。您可以定義規則，根據使用者 ID 字符中的宣告，為每個使用者選擇角色。您可以對已驗證使用者定義預設角色。您還可以對未驗證訪客使用者定義具有限制許可的 IAM 角色。

若是機器身份，您應倚賴 IAM 角色來授予 AWS 存取權。若是 EC2 執行個體，您可以使用適用於 Amazon EC2 的角色。您可以將 IAM 角色連接至 EC2 執行個體，讓在 Amazon EC2 上執行的應用程式能夠使用 AWS 自動建立、分發和輪換的臨時安全登入資料。若要使用金鑰或密碼存取 EC2 執行個體，AWS Systems Manager 是一種更安全的方式，可使用預先安裝的代理程式存取和管理執行個體，而無須使用存放的密碼。此外，AWS Lambda 等其他 AWS 服務可讓您設定 IAM 服務角色，授予使用臨時登入資料執行 AWS 動作的服務許可。

定期稽核和輪換登入資料

定期驗證 (最好是透過自動化工具) 是確認強制執行正確的控制項的必要項目。若是人類身份，您 應要求使用者定期變更密碼，並使用臨時登入資料淘汰存取金鑰。我們也建議您持續監控身份

供應商中的 MFA 設定。您可以設定 AWS Config Rules 來監控這些設定。若是機器身份，您應倚賴使用 IAM 角色的臨時登入資料。在無法執行此操作的情況下，需要頻繁稽核和輪換存取金鑰。

安全地存放和使用機密

針對與 IAM 無關的登入資料，例如資料庫登入，請使用專為處理機密管理而設計的服務，例如 AWS Secrets Manager。AWS Secrets Manager 讓您能夠使用支援的服務輕鬆管理、輪換和安全地存放加密機密。為了稽核目的，存取機密的叫用會記錄在 CloudTrail 中，而 IAM 許可能夠授予對這些機密的最低存取權。

資源

請參閱以下資源，進一步了解保護 AWS 登入資料的 AWS 最佳實務。

影片

- 在每一層都能掌握身份
- 使用 AWS SSO 大規模管理使用者許可
- 大規模管理、擷取和輪換密碼的最佳實務

文件

- AWS 帳戶根使用者
- AWS 帳戶根使用者登入資料與 IAM 使用者登入資料
- IAM 最佳實務
- 為 IAM 使用者設定帳戶密碼政策
- AWS Secrets Manager 入門
- 使用執行個體描述檔
- 臨時安全登入資料
- 身份提供者與聯合

許可管理

管理許可，以控制對需要存取 AWS 和工作負載的人員和機器身份的存取。許可控制誰可以在何種條件下存取哪些內容。將許可設定為特定的人類和機器身份，以授予對特定資源執行特定服務動作的存取權。此外，指定必須為 true 才能授予存取的條件。例如，您可以允許開發人員建立新的 Lambda 函數，但僅限於特定區域。大規模管理您的 AWS 環境時，請遵循下列最佳實務，以 確保這些人員身份僅擁有各自所需的存取權。

為您的組織定義許可防護機制

隨著您的工作負載在 AWS 中成長而需要加以管理，應該使用帳戶區隔這些工作負載，並使用 AWS Organizations 管理這些帳戶。我們建議您建立常見的許可防護機制，限制對組織中所有身份的存取權。例如，您可以限制對特定 AWS 區域的存取權，或防止團隊刪除常見資源，例如中央安全團隊使用的 IAM 角色。您可以透過實作範例服務控制政策來開始使用，例如防止使用者停用金鑰服務。

您可以使用 AWS Organizations 來對帳戶分組，並對每組帳戶設定常用控制。若要設定這些常用控制，您可以使用與 AWS Organizations 整合的服務。具體而言，您可以使用服務控制政策 (SCP) 來限制對帳戶群組的存取權。SCP 使用 IAM 政策語言，並讓您能夠建立所有 IAM 主體 (使用者和角色) 遵循的控制。您可以根據特定條件限制對特定服務動作、資源的存取，以滿足您組織的存取控制需求。如有必要，您可以為您的防護措施定義例外狀況。例如，您可以限制帳戶中所有 IAM 實體的服務動作，但特定管理員角色除外。

授予最低權限存取權

建立 最低權限原則可確保在平衡可用性和效率的同時，僅允許身份執行完成特定任務所需的最少量功能。依此原則操作會限制非預期存取，並協助確保您可以稽核誰有權存取哪些資源。在 AWS 中，除了根使用者之外，身份預設沒有許可，應僅適用於幾個特定任務。

您可以使用政策明確授予連接至 IAM 或資源實體的許可，例如聯合身份或機器或資源 (例如 S3 儲存貯體) 使用的 IAM 角色。當您建立和連接政策時，您可以指定必須為 true 的服務動作、資源和條件以便 AWS 允許存取權。AWS 支援各種條件，以協助您縮小存取權。例如，使用 `PrincipalOrgID` 條件金鑰，AWS Organizations 的識別符經過驗證，以便在您的 AWS 組織

內授予存取權。此外，您還可以控制 AWS 服務代您發出的請求，例如 AWS CloudFormation 使用 `CalledVia` 條件金鑰建立 AWS Lambda 函數。這讓您能夠針對 AWS 中的人類和機器身份設定精細許可。

AWS 還提供可讓您擴展許可管理並遵守最低權限的功能。

許可邊界：您可以使用許可邊界來設定管理員可設定的最大許可。這讓您能夠將建立和管理許可的功能委派給開發人員，例如建立 IAM 角色，但限制其可以授予的許可，讓他們無法利用自己建立的內容提升權限。

屬性型存取控制 (ABAC)：AWS 可讓您根據屬性授予許可。在 AWS 中，這些稱為標籤。標籤可以連接至 IAM 主體 (使用者或角色) 和 AWS 資源。使用 IAM 政策，管理員可以建立可重複使用的政策，根據 IAM 主體的屬性套用許可。例如，作為管理員，您可以使用單一 IAM 政策，授予組織中的開發人員存取符合開發人員專案標籤的 AWS 資源。隨著開發人員團隊將資源新增至專案，會根據屬性自動套用許可。因此，無須為每個新資源更新政策。

分析公有和跨帳戶存取

在 AWS 中，您可以授予另一個帳戶中資源的存取權。您可以使用連接至資源的政策 (例如 S3 儲存貯體政策) 來授予直接跨帳戶存取權，或允許身份擔任另一個帳戶中的 IAM 角色。使用資源政策時，您希望確保授予組織中身份的存取權，並有意在將資源設為公有時發生。應謹慎使用將資源設為公有，因為此動作可讓任何人存取資源。IAM Access Analyzer 採用數學方法 (即可證明的安全)，來識別從其帳戶外部存取資源的所有路徑。它會持續檢閱資源政策，並報告公有和跨帳戶存取的結果，讓您輕鬆分析可能的廣泛存取。

安全地共用資源

當您使用個別帳戶管理工作負載時，有時您需要在這些帳戶之間共用資源。建議您使用 AWS Resource Access Manager (AWS RAM) 共用資源。此服務可讓您輕鬆、安全地在 AWS 組織和組織單位內共用 AWS 資源。使用 AWS RAM，當帳戶移入和移出共用它們的組織或組織單位時，會自動授予或撤銷共用資源的存取權。這可協助您確保資源只與您的預期帳戶共用。

持續減少許可

有時，當團隊和專案剛開始時，您可以選擇授予廣泛存取權來激發創新和靈活性。我們建議您持續評估存取權，並將存取權限制為僅必要許可及達到最低權限。AWS 提供存取權分析功能，以協助您識別未使用的存取權。為了協助您識別未使用的使用者和角色，AWS 會分析存取活動，並提供存取金鑰和角色上次使用的資訊。您可以使用上次存取的時間戳記來識別未使用的使用者和角色，並將其移除。此外，您可以檢閱服務和動作上次存取的資訊，以識別和 加強特定使用者和角色的許可。例如，您可以使用上次存取的資訊來識別您的應用程式角色所需的特定 S3 動作，並限制只能存取這些動作。這些功能可在主控台中透過程式設計方式提供，讓您能夠將這些功能併入基礎架構工作流程和自動化工具中。

建立緊急存取程序

在極少數的狀況下，自動化程序或管道發生問題時，您應有允許緊急存取工作負載的程序，尤其是您的 AWS 帳戶。該程序可以包含不同功能的組合，例如，用於存取的緊急 AWS 跨帳戶角色，或管理員需遵循以驗證和核准緊急請求的特定程序。

資源

請參閱以下資源，進一步了解精細授權的 AWS 目前最佳實務。

影片

- 在 60 分鐘內精通 IAM 政策
- 責任區隔、最低權限、委派和 CI/CD

文件

- 授予最低權限
- 制定政策
- 委派許可以管理 IAM 使用者、群組和登入資料
- IAM Access Analyzer
- 移除不需要的登入資料

- 在具有 MFA 的 CLI 中承擔角色
- 許可邊界
- 屬性型存取控制 (ABAC)

實作

- 實驗室：IAM 許可邊界委派角色建立
- 實驗室：EC2 的 IAM 標籤型存取控制
- 實驗室：Lambda 跨帳戶 IAM 角色擔任

偵測

偵測可讓您識別潛在的安全組態錯誤、威脅或未預期的行為。這是安全生命週期的重要部分，可用來支援品質程序、法律或合規義務，以及用於識別威脅和回應工作。有不同類型的偵測機制。例如，您可以分析工作負載的日誌，了解是否有正在被利用的漏洞。您應該定期檢閱與工作負載相關的偵測機制，以確保符合內部和外部的政策和要求。自動提醒和通知應根據已定義的條件，讓您的團隊或工具能夠進行調查。這些機制是重要的反應式因素，可以幫助您的組織識別和了解異常活動的範圍。

在 AWS 中，處理偵測機制時有多種方法可用。以下幾節介紹如何使用這些方法：

- 設定
- 調查

設定

設定服務和應用程式記錄：基本實務是在帳戶層級建立一套偵測機制。這組基本機制旨在記錄和偵測對您帳戶中所有資源的各種動作。可讓您建立完整的偵測功能，其中包含自動修復的選項，以及新增功能的合作夥伴整合。

在 AWS 中，此基本套組中的服務包括：

- AWS CloudTrail 提供 AWS 帳戶活動的事件歷史記錄，包括透過 AWS 管理主控台、AWS 開發套件、命令列工具及其他 AWS 服務所採取的動作。
- AWS Config 可監控和記錄 AWS 資源組態，並讓您根據所需的組態自動評估和修復。
- Amazon GuardDuty Amazon GuardDuty 是威脅偵測服務，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。
- AWS Security Hub 提供以單一位置從多個 AWS 服務和選用的第三方產品將安全提醒或發現結果加以彙總、組織和排列優先順序，為您提供安全提醒和合規狀態的全面檢視。

建立在帳戶層級的基礎上，許多核心 AWS 服務 (例如 Amazon Virtual Private Cloud (VPC) 提供服務層級的記錄功能。VPC Flow Logs 可讓您擷在網路介面取傳入和傳出之 IP 流量的相關資訊，可提供關於連線歷史記錄的寶貴洞見，並能根據異常行為觸發自動動作。

對於不是源自 AWS 服務的 EC2 執行個體和應用程式日誌記錄，可以使用 Amazon CloudWatch Logs 存放和分析日誌。代理程式會從作業系統和執行中的應用程式收集日誌，並且自動存放。日 誌在 CloudWatch Logs 中可用之後，您可以即時處理，或使用 Insights 深入分析。

對於收集和彙總日誌而言，同等重要的是從複雜架構產生的大量日誌和事件資料中，提取有意義見解的能力。如需更多詳細資訊，請參閱可靠性 支柱白皮書的*監控*部分。日誌本身可能包含視為敏感的資料，無論是當應用程式資料錯誤地進入 CloudWatch Logs 代理程式擷取的日誌檔時，或 是為了日誌彙總設定跨區域記錄時，而且在於跨邊界運送特定類型的資訊有法令方面的考量。

其中一種方法是使用 Lambda 函數 (在交付日誌時應事件而觸發)，在轉送到集中記錄位置 (例如 S3 儲存貯體) 之前篩選和修訂日誌資料。未修訂的日誌可以保留在本機儲存貯體中，直到「合理時間」(由法規和法律團隊決定) 過去，屆時 S3 生命週期規則即能自動刪除。使用 S3 Object Lock 可 進一步保護 Amazon S3 中的日誌，您可以使用單寫多讀 (WORM) 模型存放物件。

集中分析日誌、發現結果和指標：安全營運團隊倚賴日誌的收集和使用搜尋工具來探索感興趣的潛在事件，這類事件可能是未經授權的活動或無意間的變更。但是，僅分析收集的資料並手動處理資訊，不足以應付繁複架構之中流通的資訊量。單靠分析和報告並不能幫助分配合適的資源，以及時處理事件。

建立成熟安全營運團隊的最佳實務是：將安全事件和結果流深入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。如此能使工作流程擺脫電子郵件和靜態報告，讓您能夠路由、向上呈報和管理事件或結果。許多組織也正在將安全提醒整合到其聊天/協作和開發人員生產力平台中。對於開始自動化的組織，以 API 驅動的低延遲票證系統在規劃「要先自動化什麼」時能夠提供相當大的彈性。

此最佳實務不僅適用於從描述使用者活動或網路事件的日誌訊息所產生的安全事件，也適用於從基礎架構本身偵測到的變更所產生的安全事件。能夠偵測變更、判斷變更是否適當，然後將該資訊路由到正確的修復工作流程，這對於維護和驗證安全架構至關重要；在變更的環境中，其不甚理想的性質足夠細微，以致目前無法透過 IAM 和 Organizations 組態的組合來阻止執行。

GuardDuty 和 Security Hub 為也會透過其他 AWS 服務提供給您的日誌記錄提供彙總、重複資料刪除和分析機制。特別是 GuardDuty 能導入、彙總和分析來自 VPC DNS 服務的資訊，以及您可以透過 CloudTrail 和 VPC Flow Logs 查看的資訊。Security Hub 可以導入、彙總和分析來自 GuardDuty、AWS Config、Amazon Inspector、Macie、AWS Firewall Manager 的輸出，以及 AWS Marketplace 提供的大量第三方安全產品；如果照著建置，也包括您自己的程式碼。GuardDuty 和 Security Hub 都有主要成員模型，可跨多個帳戶彙總發現結果和洞見，其中使用 Security Hub 的客戶通常以內部部署的 SIEM 做為 AWS 端日誌，並有提醒預處理器和彙總器，藉以經由 Lambda 處理器和轉寄站導入 Amazon EventBridge。

資源

請參閱以下資源，以進一步了解擷取和分析日誌的目前 AWS 建議。

影片

- 雲端威脅管理：Amazon GuardDuty 與 AWS Security Hub
- 集中監控資源組態與合規

文件

- 設定 Amazon GuardDuty
- AWS Security Hub
- 入門：Amazon CloudWatch Logs
- Amazon EventBridge
- 設定 Athena 以分析 CloudTrail 日誌
- Amazon CloudWatch
- AWS Config
- 在 CloudTrail 中建立軌跡
- 將記錄解決方案集中化

實作

- 實驗室：啟用 Security Hub

- 實驗室：偵測控制的自動部署
- 實驗室：Amazon GuardDuty 實作

調查

實作可採取行動的安全事件：對於您擁有的每個偵測機制，您也應該設置一套程序 (採取 Runbook 或手冊的形式) 以進行調查。例如，當您啟用 Amazon GuardDuty 時，就會產生不同的問題清單。每種發現結果類型都應該在 Runbook 有一個輸入項目，例如，如果發現木馬程式，您的 Runbook 會有簡單的指示，指示某人進行調查和修復。

自動回應事件：在 AWS 中，您可以使用 Amazon EventBridge 來調查感興趣的事件，以及自動化工作流程中潛在意外變更的相關資訊。該服務能提供可擴展的規則引擎，旨在代理原生 AWS 事件格式 (例如 CloudTrail 事件) 以及您可從應用程式產生的自訂事件。Amazon EventBridge 也可讓您將事件路由到建立事件回應系統的工作流程系統 (Step Functions)，或路由到中央安全帳戶，或路由到儲存貯體供進一步分析。

也可以使用 AWS Config 規則偵測變更，並將此資訊路由到正確的工作流程。AWS Config 會偵測範圍內服務發生的變更 (雖然延遲高於 Amazon EventBridge)，並產生可使用 AWS Config 規則加以剖析的事件，以進行轉返、強制執行合規政策，以及將資訊轉送到系統 (例如變更管理平台和營運售票系統)。除了編寫自己的 Lambda 函數來回應 AWS Config 事件，您還可以利用 AWS Config Rules 開發套件和開放原始碼庫 AWS Config Rules。

資源

請參閱以下資源，進一步了解將稽核控制與通知和工作流程整合的目前 AWS 最佳實務。

影片

- Amazon Detective
- 補救 Amazon GuardDuty 和 AWS Security Hub 問題清單
- Managing Security Operations on AWS 的最佳實務
- 使用 AWS Config 實現持續合規

文件

- Amazon Detective
- Amazon EventBridge
- AWS Config 規則
- AWS Config 規則資料儲存器 (開放原始碼)
- AWS Config Rules 開發套件

實作

- 解決方案：AWS 帳戶活動的即時洞見
- 解決方案：集中式日誌記錄

基礎架構保護

基礎架構保護包括符合最佳實務和組織或監管義務所必需的控制方法，例如深度防禦。這些方法的使用對於雲端的成功持續營運至關重要。

基礎架構保護是資訊安全計劃的關鍵部分。它可以確保工作負載中的系統和服務受到保護，以防止意外和未經授權的存取以及潛在漏洞。例如，您將定義信任邊界 (例如，網路和帳戶邊界)、系統安全組態和維護 (例如，強化、最小化和修補)、作業系統身份驗證和授權 (例如，使用者、金鑰和存取層級)，以及其他適當的政策強制執行點 (例如，Web 應用程式防火牆和/或 API 閘道)。

在 AWS 中，有多種方法可用於基礎架構保護。以下幾節介紹如何使用這些方法：

- 保護網路
- 保護運算

保護網路

仔細規劃和管理網路設計，可奠定如何為工作負載內的資源提供隔離和邊界的基礎。由於工作負載中的許多資源在 VPC 中運作並繼承安全屬性，因此自動化支援的檢測和保護機制適用於設計非常重要。同樣地，對於在 VPC 外部操作的工作負載，使用純邊緣服務和/或無伺服器，最佳實務

適用於更簡化的方法。如需無伺服器安全的特定指導，請參閱 AWS Well-Architected 無伺服器式應用程式聚焦。

建立網路層：EC2 執行個體、RDS 資料庫叢集等元件，以及共用連線能力要求的 Lambda 函數可分成子網路所組成的層級。例如，不需存取網際網路的 VPC 中的 RDS 資料庫叢集，應放置在沒有往返網際網路路由的子網路中。此控制項的分層方法可減輕單一層組態錯誤所造成的影響，這可能會允許意外存取。對於 AWS Lambda，您可以在 VPC 中執行函數，以預先進行 VPC 控制。

對於可以包含數千個 VPC、AWS 帳戶和內部部署網路的網路連線，您應該使用 AWS Transit Gateway。它可作為中樞，控制流量在所有連線網路之間路由的方式，其作用就像輪輻。Amazon VPC 和 AWS Transit Gateway 之間的流量仍保存在 AWS 私有網路，可減少外部威脅向量，例如分散式拒絕服務 (DDoS) 攻擊和常見入侵程式，例如 SQL 插入、跨網站指令碼、跨網站偽造請求或濫用不完整的身份驗證碼。AWS Transit Gateway 區域間對等也可為區域間的流量加密，不會有單一故障點或頻寬瓶頸。

控制所有層級的流量：建構網路拓撲時，您應該檢查每個元件的連線需求。例如，如果元件需要網際網路可存取性 (傳入和傳出)、連線至 VPC、邊緣服務和外部資料中心。

VPC 可讓您定義橫跨 AWS 區域的網路拓撲，使用您所設定的私有 IPv4 位址範圍，或 AWS 選取的 IPv6 位址範圍。您應該對傳入和傳出流量採用深度防禦方法的多個控制，包括使用安全群組 (狀態檢測防火牆)、網路 ACL、子網路和路由表。在 VPC 內，您可以在可用區域中建立子網路。每個子網都有一個關聯的路由表，定義路由規則，以管理子網路內流量所經過的路徑。您可以透過讓路由前往連接到 VPC 的網際網路或 NAT 閘道，或透過另一個 VPC 來定義網際網路可路由子網路。

當執行個體、RDS 資料庫或其他服務在 VPC 內啟動時，每個網路介面都有自己的安全群組。此防火牆位於作業系統層之外，可用來定義允許傳入和傳出流量的規則。您還可以定義安全群組之間的關係。例如，資料庫層安全群組內的執行個體，藉由參照套用至所涉及執行個體的安全群組，僅接受來自應用程式層內執行個體的流量。除非您使用非 TCP 通訊協定，否則應該不需要從網際網路直接存取 EC2 執行個體 (即使連接埠受安全群組限制)，無須使用負載平衡器或 CloudFront。這有助於防止透過作業系統或應用程式問題意外受到存取。子網路也可以連接著網路 ACL，做為無狀態的防火牆。您應該設定網路 ACL 以縮小層級之間允許的流量範圍，並請注意，需要同時定義傳入和傳出規則。

雖然部分 AWS 服務需要元件能存取網際網路以進行 API 呼叫 (這是 AWS API 端點所在的位置)，但其他服務則使用您 VPC 內的端點。許多 AWS 服務 (包括 Amazon S3 和 DynamoDB) 都支援 VPC 端點，而這項技術已廣泛應用於 AWS PrivateLink 中。對於需要對網際網路進行對外連線的 VPC 資產，這些資產可以透過 AWS 受管 NAT 閘道、僅對外網際網路閘道或您建立和管理的 Web 代理進行僅對外 (單向)。

實作檢查和保護：檢查和篩選每個層級的流量。對於透過 HTTP 通訊協定進行交易的元件，Web 應用程式防火牆可協助防止常見的攻擊。AWS WAF 是一種 Web 應用程式防火牆，可讓您監控和封鎖符合可設定規則的 HTTP 請求；這些請求會轉送到 Amazon API Gateway API、Amazon CloudFront 或 Application Load Balancer。要開始使用 AWS WAF，您可以將 AWS Managed Rules 結合自己的規則，或使用現有的合作夥伴整合。

若要跨 AWS Organizations 管理 AWS WAF、AWS Shield Advanced 保護和 Amazon VPC 安全群組，您可以使用 AWS Firewall Manager。它可讓您集中設定和管理所有帳戶和應用程式的防火牆規則，使得共同規則的擴展強制執行更為輕鬆。它也可讓您使用 AWS Shield Advanced 或可自動封鎖對 Web 應用程式不必要請求的解決方案，快速地回應攻擊。

將網路保護自動化：將保護機制自動化，以根據威脅情報和異常偵測提供自我防禦網路。例如，可以適應目前威脅並降低其影響的入侵偵測和預防工具。Web 應用程式防火牆即為可將網路保護自動化的範例；例如可使用 AWS WAF Security Automations 解決方案 (https://github.com/awslabs/aws-waf-security-automations) 以自動封鎖來自已知威脅者相關 IP 位址的請求。

資源

請參閱以下資源，進一步了解保護網路的 AWS 最佳實務。

影片

- 適用於許多 VPC 的 AWS Transit Gateway 參考架構
- 使用 Amazon CloudFront、AWS WAF 和 AWS Shield 的應用程式加速和保護
- 大規模偵測 DDoS 攻擊

文件

- Amazon VPC 文件
- AWS WAF 入門
- 網路存取控制清單
- VPC 安全群組
- VPC 推薦網路 ACL 規則
- AWS Firewall Manager
- AWS PrivateLink
- VPC 端點
- Amazon Inspector

實作

- 實驗室：VPC 的自動部署
- 實驗室：Web 應用程式防火牆的自動部署

保護運算

執行漏洞管理：經常掃描和修補程式碼、相依性和基礎架構中的漏洞，以協助防禦新的威脅。

使用建置和部署管道，您可以將漏洞管理的許多部分自動化：

- 使用第三方靜態程式碼分析工具來識別常見的安全問題，例如未檢查的函數輸入界限，以 及較新的 CVE。您可以使用 Amazon CodeGuru 取得支援的語言版本。
- 使用第三方相依性檢查工具，判斷您的程式碼連結的程式庫是否為最新版本、本身是否不使用 CVE，以及是否具有符合您軟體政策要求的授權條件。

- 使用 Amazon Inspector，您可以對已知的常見漏洞和披露 (CVE) 的執行個體執行組態評定、根據安全基準進行評估，和將缺陷通知完全自動化。Amazon Inspector 在生產執行個體上或建置管道中執行，並在結果出現時通知開發人員和工程師。您可以透過程式設計方式存取結果，並將您的團隊引導至待辦項目和錯誤追蹤系統。EC2 映像產生器可透過自動修補、AWS 提供的安全政策強制執行以及其他自訂項目來維護伺服器映像 (AMI)。
- 使用容器時，會在您的建置管道中定期對照映像儲存庫執行 ECR 映像掃描，以在容器中尋找 CVE。
- 雖然 Amazon Inspector 和其他工具可以有效地識別現有的組態和任何 CVE，但還需要其他方法來測試應用程式層級的工作負載。Fuzzing 是一種利用自動化尋找錯誤的知名方法，能將格式不正確的資料注入輸入欄位和應用程式的其他區域。

這類函數有些可以使用 AWS 服務、AWS Marketplace 中的產品或開放原始碼工具來執行。

減少攻擊面：透過強化作業系統、盡量降低使用中的元件、程式庫和外部消耗性服務來減少攻擊面。為了減少攻擊面，您需要以威脅模型來識別進入點和可能遇到的潛在威脅。減少攻擊面的一種常見做法是首先減少未使用的元件，無論是作業系統套件、應用程式等 (適用於 EC2 工作負載) 或程式碼中的外部軟體模組 (適用於所有工作負載)。有許多強化和安全組態指南適用於常見的作業系統和伺服器軟體，例如來自 Center for Internet Security，可以做為起點和反覆查看使用。

讓人員能夠遠距離執行動作：移除互動式存取功能可降低人為錯誤的風險，並降低手動設定或管理的可能性。例如，可以採行變更管理工作流程以使用 AWS Systems Manager 這類工具來管理 EC2 執行個體，而不允許直接存取或透過堡壘主機存取。AWS Systems Manager 可使用例如自動化工作流程、文件 (手冊) 和執行命令等功能，自動化各種維護和部署任務。AWS CloudFormation 堆疊會從管道建立，而且可為您將基礎架構的部署和管理任務自動化，無須直接使用 AWS 管理主控台或 API。

實作受管服務：實作管理資源的服務 (例如 Amazon RDS、AWS Lambda 和 Amazon ECS)，為您減少共同的責任模型中的安全維護任務。例如，Amazon RDS 可協助您設定、操作和擴展關聯式資料庫，並使諸如硬體佈建、資料庫設定、修補和備份等管理任務自動化。這表示您有更多空閒時間可以專心用 AWS Well-Architected 架構中所述的其他方式來保護應用程式。AWS Lambda 可讓您執行程式碼時無須佈建或管理伺服器，您可專注在程式碼層級的連線、叫用和安全等事項，無須擔心基礎架構或作業系統。

驗證軟體完整性：實作機制 (例如程式碼簽署) 以驗證工作負載中使用的軟體、程式碼和程式庫是否來自信任的來源，且未遭到篡改。例如，您應該驗證二進位程式碼和指令碼的程式碼簽署憑證，以確認作者，並確保自作者建立後並未遭到篡改。此外，相較於供應商的檢查總和，您所下載軟體的檢查總和有助於確保該軟體並未遭到竄改。

將運算保護自動化：將保護性運算機制自動化，包括漏洞管理、減少攻擊面和資源管理。自動化可協助您將時間花在保護工作負載的其他層面，並降低人為錯誤的風險。

資源

請參閱以下資源，進一步了解保護運算的 AWS 最佳實務。

影片

- Amazon EC2 執行個體中繼資料服務的安全最佳實務
- 保護 AWS 上的區塊儲存安全
- 保護無伺服器和容器服務的安全
- 在 Amazon EKS 上執行高安全的工作負載
- 在 Amazon EKS 中透過政策防護機制架構安全

文件

- AWS Lambda 安全概觀
- Amazon EC2 中的安全
- AWS Systems Manager
- Amazon Inspector
- 編寫自己的 AWS Systems Manager 文件
- 以 Amazon EC2 Systems Manager 取代堡壘主機

實作

- 實驗室：EC2 Web 應用程式的自動部署

資料保護

在建構任何工作負載之前，應先制訂有影響安全的基礎實務。例如，資料分類可基於敏感性等級將資料分類，加密則能對未經授權的存取將資料呈現為無法辨識，以保護資料。這些方法之所以重要，因為能支持例如防止處理不當，或遵循法規義務等目標。

在 AWS 中，進行資料保護時有多種不同的方法可供使用。以下一節介紹如何使用這些方法：

- 資料分類
- 保護靜態資料
- 保護傳輸中的資料

資料分類

資料分類可讓您根據關鍵性和敏感度將組織資料分類，協助判定適當的保護和保留控制。

識別工作負載內的資料：您需要了解工作負載所處理的資料類型和類別、相關的商業程序、資料擁有者、適用的法律和合規要求、存放的位置，以及因而需要強制執行的控制項。這可能包括分類以指出資料是否打算供公開取得；資料是否僅供內部使用，例如客戶的個人識別資訊 (PII)；資料是否用於更受限制的存取，例如智慧財產、依法特權或標示為敏感資料等等。透過仔細管理適當的資料分類系統，並搭配每個工作負載的保護等級要求，您可以規劃適合資料的控制項和存取/保護等級。例如，公開的內容可供任何人存取，然而重要內容則以受保護的方式進行加密和儲存，需要授權取得金鑰才能將內容解密。

定義資料保護控制項：使用資源標籤、根據敏感度 (也可能根據警告/群體/關注的社群)、IAM 政策、組織 SCP、AWS KMS 和 AWS CloudHSM 將 AWS 帳戶做出區隔，您可以定義和實作資料分類和加密保護的政策。例如，假設您有一個專案用到存放高度關鍵資料的 S3 儲存貯體，或處理機密資料的 EC2 執行個體，則可以使用「Project=ABC」標籤進行標記。只有您的直屬團隊知道專案代號的意義，同時也可作為使用屬性型存取控制的方式。您可以透過金鑰政策和授權，定義對 AWS KMS 加密金鑰的存取等級，以確保僅限相應的服務能透過安全機制存取敏感內容。如果要根據標籤做出授權決策，您應該確保在 AWS Organizations 中使用標籤政策，正確地定義標籤上的許可。

定義資料生命週期管理：您已定義的生命週期策略應以敏感性等級以及法律和組織的要求作為依據。您應考慮保留資料的期間、資料銷毀程序、資料存取管理、資料轉換和資料共享等方面。在選擇資料分類方法時，應在使用性與存取之間取得平衡。也應採納存取權的多個等級，並且耐心依照各等級分別實作安全又兼顧使用方便的方法。一律使用深度防禦方法，並減少為了轉換、刪除或複製資料，對資料與機制的手動存取。例如，要求使用者對應用程式進行強式驗證，並給予應用程式(而非使用者) 必要的存取許可，以執行「遠距離動作」。 此外，確保使用者來自受信任的網路路徑，並要求存取解密金鑰。應使用儀表板或自動報告之類的工具為使用者提供來自資料的資訊，而 不是讓使用者直接存取資料。

將識別和分類自動化：將資料的識別和分類自動化，可協助您實作正確的控制方法。針對此目的使用自動化而非由人員直接存取，可降低人為錯誤和外洩的風險。您應該使用 Amazon Macie 這類工具進行評估，該工具會使用機器學習自動探索、分類和保護 AWS 中的敏感資料。Amazon Macie 可辨識個人識別資訊 (PII) 或智慧財產權等敏感資料，並提供儀表板和提醒，讓您深入了解資料的存取或移動方式。

資源

若要進一步了解資料分類，請參閱以下資源。

文件

- 資料分類白皮書
- 標記您的 Amazon EC2 資源
- Amazon S3 物件標記

保護靜態資料

靜態資料代表您在工作負載中的任何期間，保留在非揮發性儲存體中的任何資料。其中包括：長 期存放資料的區塊儲存體、物件儲存體、資料庫、封存、IoT 裝置和任何其他儲存媒介。實作加密和適當的存取控制，保護靜態資料能將未經授權存取的風險降低。

加密和權杖化是兩種重要但截然不同的資料保護機制。

*權杖化*是一種過程，可讓您定義權杖來表示敏感資訊 (例如，用權杖來表示客戶的信用卡號)。權杖本身必須毫無意義，而且不可衍生自權杖化的資料，因此，密碼編譯摘要無法作為權杖使用。透過仔細地規劃權杖化的方法，您可以為內容提供額外的保護，並確保滿足合規要求。例如，如果您善用權杖而非使用信用卡號碼，則可以縮小信用卡處理系統的合規範圍。

*加密*是一種轉換內容的方式，若沒有將內容解密回純文字所需的私密金鑰，就無法讀取。權杖化和加密都可以用來適當地保護資訊。此外，遮罩這種技術也允許將資料片段修訂成為剩餘的資料不視為敏感的狀態。例如，PCI-DSS 允許超出合規範圍邊界，保留卡號的後四碼以編製索引。

實作安全金鑰管理：透過定義加密方法 (包含金鑰的儲存、輪換和存取控制)，可以協助保護您的內容，免於未經授權的使用者和不必要的向授權使用者透露。AWS KMS 可幫助您管理加密金鑰，並與許多 AWS 服務整合。該服務為您的主要金鑰提供耐用、安全和冗餘的儲存。您可以定義金鑰別名以及金鑰層級的政策。這些政策可幫助您定義金鑰管理員和金鑰使用者。此外，AWS CloudHSM 是雲端硬體安全模組 (HSM)，讓您能夠在 AWS 雲端上輕鬆產生和使用自己的加密金鑰。透過使用 FIPS 140-2 3 級驗證的 HSM，它可以幫助您滿足公司、合同和法規對資料安全的合規要求。

強制靜態加密：您應該確保存放資料的唯一方法是使用加密。AWS KMS 與許多 AWS 服務無縫整合，讓您更輕鬆地為所有靜態資料加密。例如，在 Amazon S3 中，您可以在儲存貯體上設定預設加密，以便將所有新物件自動加密。此外，Amazon EC2 支援透過設定預設加密選項，為整個區域強制執行加密。

強制存取控制：各種控制，包括存取 (使用最低權限)、備份 (請參閱「可靠性」白皮書)、隔離和版本控制，都有助於保護您的靜態資料。對資料的存取應使用本白皮書稍早涵蓋的偵測機制進行稽核，包括 CloudTrail 和服務層級日誌 (例如 S3 存取日誌)。您應該清查哪些資料可公開存取，並規劃如何隨著時間減少可用的資料量。Amazon S3 Glacier 文件庫鎖定和 S3 Object Lock 提供強制存取控制的功能，一旦文件庫政策被合規選項鎖定，在鎖定過期之前，就連根使用者也無法變更。此機制符合 SEC、CFTC 和 FINRA 的書籍和記錄管理要求。如需詳細資訊，請參閱此白皮書。

稽核加密金鑰的使用：請確定您了解並稽核加密金鑰的使用，以驗證金鑰的存取控制機制是否正確實作。例如，任何使用 AWS KMS 金鑰的 AWS 服務，都會將每次的使用記錄在 AWS CloudTrail 中。然後，您可以使用 Amazon CloudWatch Insights 這類工具來查詢 AWS CloudTrail，以確保金鑰的所有使用都是有效的。

使用機制讓人員遠離資料：在正常運作情況下，讓所有使用者始終無法直接存取敏感資料和系統。例如，使用變更管理工作流程來使用工具管理 EC2 執行個體，而不允許直接存取或堡壘主機存取。這可使用 AWS Systems Manager Automation 來達成，其使用自動化文件，內有您用來執行任務的步驟。這些文件可以存放在原始檔控制中、在執行前接受對等審查，並經過徹底測試，以盡量降低與 shell 存取相比的風險。商業使用者可以擁有儀表板，而不是直接存取資料存放區來執行查詢。未使用 CI/CD 管道時，請判斷需要哪些控制和程序，才能充分提供一般停用時的緊急存取機制。

將靜態資料保護自動化：使用自動化工具以持續驗證並強制執行靜態資料控制，例如，驗證以確認只有加密的儲存資源。您可以使用 AWS Config 規則自動驗證所有 EBS 磁碟區是否加密。AWS Security Hub 也可以透過符合安全標準的自動化檢查來驗證多種不同的控制。此外，您的 AWS Config 規則可以自動修復不合規的資源。

資源

請參閱以下資源，進一步了解保護靜態資料的 AWS 最佳實務。

影片

- 在 AWS 中加密如何運作
- 保護 AWS 上的區塊儲存安全
- 使用 AWS CloudHSM 達成安全目標
- 實作 AWS Key Management Service 的最佳實務
- 深入研究 AWS 加密服務

文件

- 使用加密保護 Amazon S3 資料
- Amazon EBS 加密
- 加密 Amazon RDS 資源
- 利用加密保護資料
- AWS 服務如何使用 AWS KMS

- Amazon EBS 加密
- AWS Key Management Service
- AWS CloudHSM
- AWS KMS 加密詳細資訊白皮書
- 在 AWS KMS 中使用金鑰政策
- 使用儲存貯體政策和使用者政策
- AWS 加密工具

保護傳輸中的資料

傳輸中的資料是指從一個系統傳送到另一個系統的任何資料。這包括工作負載內資源之間的通訊，以及其他服務與最終使用者之間的通訊。為傳輸中的資料提供適度的保護，意味著您保護工作負載中資料的機密性和完整性。

實作安全金鑰和憑證管理：安全地存放加密金鑰和憑證，並依適當的時間間隔，以嚴格的存取控制進行輪換。達成此目標的最佳方式是使用受管服務，例如 AWS Certificate Manager (ACM)。它可讓您輕鬆佈建、管理和部署可與 AWS 服務和您的內部連線資源搭配使用的公有和私有 Transport Layer Security (TLS) 憑證。TLS 憑證可用來保護網路通訊，和建立網際網路中的網站和私有網路中資源的身份。ACM 與 AWS 資源整合，例如 Elastic Load Balancer、Amazon CloudFront 分發以及 API Gateway 上的 API，也會處理自動憑證更新。如果您使用 ACM 部署私有根 CA，則它可以提供憑證和私有金鑰兩者，用於 EC2 執行個體、容器內等。

強制傳輸中的加密：根據適當的標準和建議強制執行已定義的加密要求，協助您符合組織、法律和合規上的要求。AWS 服務提供使用 TLS 進行通訊的 HTTPS 端點，從而在與 AWS API 通訊時提供傳輸中加密。不安全的通訊協定 (例如 HTTP) 可以在 VPC 中透過使用安全群組加以稽核和封鎖。在 Amazon CloudFront 或 Application Load Balancer 中，HTTP 請求也可以自動重新導向至 HTTPS。您可以完全控制您的運算資源，以在各個服務中實作傳輸中加密。此外，還可以從外部網路使用 VPN 連線功能進入 VPC，實現流量加密。如果您有特殊需求，AWS Marketplace 備有第三方解決方案。

驗證網路通訊：使用支援身份驗證的網路通訊協定，可讓雙方之間建立信任。此法可增加通訊協定中使用的加密，降低通訊遭到更改或攔截的風險。實作身份驗證的常見通訊協定包括許多 AWS 服務中使用的 Transport Layer Security (TLS)，以及在 AWS Virtual Private Network (AWS VPN) 中使用的 IPsec。

將意外資料存取的偵測自動化：您可使用 Amazon GuardDuty 這類工具，根據資料分類層級，自動偵測將資料移到所定義邊界以外的嘗試；例如使用 DNS 通訊協定，偵測出將資料複製到未知或不信任網路的木馬程式。除了 Amazon GuardDuty，可擷取網路流量資訊的 Amazon VPC Flow Logs, 還可與 Amazon EventBridge 搭配使用，以觸發異常連線偵測，其中成功和拒絕兩者皆包含在內。S3 Access Analyzer 可協助評估您的 S3 儲存貯體中誰可以存取哪些資料。

資源

請參閱以下資源，進一步了解保護傳輸中資料的 AWS 最佳實務。

影片

- 如何使用 AWS Certificate Manager 將網站的憑證新增到 ELB
- 深入探討 AWS Certificate Manager Private CA

文件

- AWS Certificate Manager
- Application Load Balancer 的 HTTPS 接聽程式
- AWS VPN
- API Gateway 邊緣最佳化

事件回應

即使採用了非常成熟的預防和偵測控制，您的組織仍應實作機制，以回應並緩和安全事故的潛在影響。您的準備工作會大大地影響團隊在事件發生時有效運作、隔離並控制問題影響範圍，以及將操作恢復為已知良好狀態的能力。在安全事件發生前先備妥工具和存取功能，然後在演練日期間定期練習事件回應，有助於確保您能夠復原，同時盡量減少業務中斷。

Cloud Response 的設計目標

雖然事件回應的一般程序和機制，例如 NIST SP 800-61 Computer Security Incident Handling Guidehttps://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final 中所定義的仍然可行，但我們鼓勵您評估在雲端環境中回應安全事件方面的下列特定設計目標：

- **建立回應目標**：與您的利害關係人、法律顧問和組織領導階層合作，訂定回應事件的目標。一些常見目標包括遏制和減輕問題、復原受影響的資源、保留鑑識資料，以及歸因。
- **文件計劃**：建立計劃以協助您回應、在事件期間進行溝通，以及從事件中復原。
- **使用雲端回應**：在事件發生和資料之處實作回應模式。
- **了解您擁有和需求的是哪些**：將日誌、快照和其他證據複製到集中的安全雲端帳戶加以保留。運用標籤、中繼資料和機制，強制執行保留政策。例如，您可以選擇使用 Linux dd 命令或相當的 Windows 命令，製作完整的資料複本，以用於調查。
- **使用重新部署機制**：如果安全異常可能歸因於組態錯誤，修復的方法可能就是透過使用適當的組態，重新部署資源以移除變異那麼簡單。請盡可能讓您的回應機制在狀態不明的環境中安然地執行多次。
- **盡可能自動化**：當您發現問題或事件重複時，請建置機制，以程式設計方式分類並回應常見的情況。對於獨一無二、新和敏感的事件，請以人力回應。
- **選擇可擴展的解決方案**：努力符合組織雲端運算方法的可擴展性，並縮短偵測和回應之間的時間。

- **了解並改善程序**：當您找出程序、工具或人員中的缺口時，請實作計劃來修正這些缺口。模擬是找出缺口和改善流程的安全方法。

在 AWS 中，進行事故回應時有多種不同的方法可使用。以下一節介紹如何使用這些方法：

- **教育**您的安全操作和事件回應人員，說明雲端技術以及您的組織預備如何使用這些技術。
- **準備**好您的事件回應團隊，以便在雲端偵測和回應事件、啟用偵測功能，並確保能妥善存取必要的工具和雲端服務。此外，請準備必要的 Runbook (包括手動和自動)，以確保做出可靠且一致的回應。與其他團隊合作建立預期的基準操作，並使用該知識來識別與正常操作偏離的部分。
- **模擬**雲端環境中預期和意外的安全事件，以了解準備工作的效果。
- **反覆查看**模擬結果，以改善回應態勢的規模、縮短創造價值的時間，並進一步降低風險。

教育

自動化程序可讓組織有更多時間可以專心提高工作負載安全的措施。自動化事件回應也讓人力能夠用於建立事件關聯性、演練模擬、設計新的回應程序、執行研究、開發新的技能，以及測試或建立新的工具。雖然自動化程度提高，但您的團隊、專家和安全組織內的回應人員仍需要持續接受教育。

除了一般雲端體驗之外，您還需要大量投資在人員上才能獲得成功。您的組織可透過為員工提供額外的培訓來學習程式設計技能、開發程序 (包括版本控制系統和部署實務) 以及基礎架構自動化，而獲益良多。學習的最佳方式是藉由事件回應演練日的機會際操作。這可讓團隊中的專家在教導他人的同時也對於工具和技術更加精進。

準備

在事件發生期間，您的事件回應團隊必須能夠存取事件涉及的各種工具和工作負載資源。在事件發生之前，請確定您的團隊擁有適當的預先佈建存取權，以執行其職責。所有工具、存取和計劃都應在事件發生之前記錄和測試，確保有能力及時回應。

識別重要人員和外部資源：當您在雲端定義回應事件的方法時，與其他團隊 (例如您的法律顧問、領導階層、業務利害關係人、AWS Support Services 等等) 共同合作時，您必須識別關鍵人員、利害關係人和相關聯絡人。為了減少相依性並縮短回應時間，請確保您的團隊、專業安全團隊和回應人員受過您所使用服務的教育訓練，並有機會實際操作。

我們鼓勵您找出可提供外部專業知識和不同觀點，為您增強回應能力的外部 AWS 安全合作夥伴。您信任的安全合作夥伴可協助您識別您可能不熟悉的潛在風險或威脅。

開發事件管理計劃：建立計劃以協助您回應、在事件期間進行溝通，以及從事件中復原。例如，您可以從工作負載和組織最可能發生的情境，開始建立事件回應計劃。包括您在內部和外部進行溝通和向上呈報的流程。從工作負載和組織最可能發生的情境開始，以手冊的形式建立事故回應計劃。例如可以是目前產生的事件。若您需要起點，應該查看 AWS Trusted Advisor 和 Amazon GuardDuty 問題清單。 請使用簡單的格式 (例如 Markdown)，因此易於維護；但應確保包含重要的命令或程式碼片段，以便無須查詢其他文件即可執行。

從簡單開始，並反覆查看。請與您的安全專家和合作夥伴密切合作，找出確保程序可行所需的任務。請訂定所執行程序的手冊描述。在此之後，請測試程序並反覆查看 Runbook 的模式，以改善您所作回應的核心邏輯。應判斷例外狀況，以及這些情境的其他解決方案有哪些。例如，在開發環境中，不妨終止組態錯誤的 Amazon EC2 執行個體。但是，如果生產環境中發生相同的事件，與其終止執行個體，您可以停止執行個體，向利害關係人確認重要資料不會遺失，並且可接受終止。包括您在內部和外部進行溝通和向上呈報的流程。當您對程序的手動回應感到滿意時，請將其自動化以縮短解決時間。

預先佈建存取權：確保已在 AWS 和其他相關系統中預先佈建事件回應人員的正確存取權，以縮短調查直至復原的時間。在事故期間確定如何為有關的人員獲取存取權會延遲回應時間，並且如果存取權共用，或在壓力之下未正確提供，還會帶來其他安全漏洞。您必須知道團隊成員需要何種存取權層級 (例如，他們可能採取哪種動作)，而且您必須提前佈建存取權。以專為回應安全事件的角色或使用者為形式所建立的存取權通常具有特殊權限，以提供足夠的存取權。因此，這類使用者帳戶應限制使用、不宜用於日常活動，並且開啟使用量提醒。

預先部署工具：確保安全人員已預先部署到 AWS 中的適當工具，以縮短調查直至復原的時間。

若要將安全工程和操作功能自動化，您可以使用 AWS 提供的完整 API 和工具集。您可以將身份管理、網路安全、資料保護和監控功能完全自動化，並使用現有的熱門軟體開發方法遞送這些功

能。建置安全自動化時，您的系統可以監控、檢閱和啟動回應，而不是讓人員監控您的安全地位並手動回應事件。

若您的事件回應團隊持續以相同方式回應警示，可能會形成警示疲勞的風險。隨著時間的推移，團隊可能會變得對收到提醒不敏感，而且在處理一般情況時可能會犯錯，或是錯過不尋常的警示。自動化使用能夠處理重複和一般提醒的功能，讓人員處理敏感和獨特的事件，有助於避免發生提醒疲倦的情形。

您可以透過程式設計方式將程序中的步驟自動化，以改善手動程序。定義事件的補救模式之後，您可以將該模式分解為可行的邏輯，並撰寫程式碼來執行該邏輯。回應人員接著可以執行該程式碼來修正問題。隨著時間的推移，您可以將越來越多的步驟自動化，最終自動處理整個類別的常見事件。

對於在 EC2 執行個體的作業系統內執行的工具，您應該使用 AWS Systems Manager 執行命令進行評估，這可讓您使用在 Amazon EC2 執行個體作業系統上安裝的代理程式，從遠端安全地管理執行個體。這需要 AWS Systems Manager Agent (SSM 代理程式)；此代理程式預設安裝在許多 Amazon Machine Image (AMI) 上。不過請注意，執行個體一旦遭侵害，對於在其上執行的工具或代理程式發出的回應都不應視為可信任。

準備鑑識功能：識別和準備適合的鑑識調查功能，包括外部專家、工具和自動化。部分事件回應活動可能包括分析磁碟映像、檔案系統、RAM 傾印或事件涉及的其他成品。請建置自訂的鑑識工作站，供其用來掛載任何受影響資料磁碟區的副本。由於鑑識調查技術需要專業培訓，您可能需要聘請外部專家。

模擬

舉辦演練日：演練日也稱為模擬或練習，是內部舉辦的活動，提供有條理的機會，供您在寫實情境下演練事件管理計劃和程序。演練日基本上就是用來準備和反覆改善您的回應能力。對於進行演練日的活動，您可能會發現有價值的原因包括：

- 驗證整備
- 培養信心 – 從模擬和培訓員工得到學習
- 遵守合規或合約義務

- 產生用於認證的成品
- 靈活 – 增量改進
- 加速並改善工具
- 精簡溝通和上報
- 培養安然面對罕見和意外情形的能力

基於上述原因，參與 SIRS 活動所衍生的價值，會在壓力事件期間提高組織發揮的效用。開發既實際又有益的 SIRS 活動可能是艱鉅的作業。雖然測試處理熟知事件的程序或自動化具有某些優勢，但參與創造性的 SIRS 活動，以考驗自己面對意外和持續改善的能力，同樣也有價值。

反覆

將阻隔與復原功能自動化：將事件範圍侷限與復原自動化，以縮短回應時間與對組織的影響。

一旦您依照手冊建立和操演程序和工具，就可以將邏輯解構成為以程式碼為基礎的解決方案，許多回應人員可將其做為工具使用，以做到自動回應，並免除回應人員面對的變通或猜測。如此可以加速回應的生命週期。下一個目標是透過提醒或事件本身 (而不是由回應人員) 叫用，讓此程式碼能夠完全自動化，以建立事件驅動的回應。

使用事件驅動的回應系統，偵測機制會觸發回應機制，以自動修復事件。您可以使用事件驅動的回應功能，減少偵測機制與回應機制之間體現價值的時間。若要建立此事件驅動架構，您可以使用 AWS Lambda；這是一種無伺服器運算服務，可執行程式碼以回應事件，並自動為您管理基礎運算資源。例如，假設您有一個已啟用 AWS CloudTrail 服務的 AWS 帳戶。如果 AWS CloudTrail 發生停用 (透過 `cloudtrail:StopLogging` API 呼叫)，您可以使用 Amazon EventBridge 監控特定的 `cloudtrail:StopLogging` 事件，並叫用 AWS Lambda 函數以呼叫 `cloudtrail:StartLogging` 以重新啟動記錄。

資源

請參閱以下資源，進一步了解事故回應的 AWS 目前最佳實務。

影片

- 準備和回應 AWS 環境中的安全事件
- 自動化事故回應和鑑識
- Runbook、事件報告和事件回應的 DIY 指南

文件

- AWS 事件回應指南
- AWS Step Functions
- Amazon EventBridge
- CloudEndure Disaster Recovery

實作

- 實驗室：使用 AWS 主控台和 CLI 處理事件回應
- 實驗室：使用 Jupyter 事件回應手冊 – AWS IAM
- 部落格：以 AWS Step Functions 協調安全事件回應

結論

安全是一項持續的工作。發生事故時，應將其視為提高架構安全的機會。擁有強大的身份控制、自動化對安全事件的回應、在多個層級保護基礎架構，並且使用加密管理妥善分類的資料，可提供每個組織皆應實作的深度防禦。歸功於本白皮書所討論的程式設計功能和 AWS 功能及服務，這項工作輕鬆不少。

AWS 致力於幫助您建置和營運可在提供商業價值的同時，保護資訊、系統和資產的架構。

作者群

協力完成本文件的個人與組織如下：

- Ben Potter，Amazon Web Services Well-Architected 首席安全主管
- Bill Shinn，Amazon Web Services CISO 資深辦公室主任
- Brigid Johnson，Amazon Web Services AWS Identity 資深軟體開發經理
- Byron Pogson，Amazon Web Services 資深解決方案架構師
- Darran Boyd，Amazon Web Services 金融服務首席安全解決方案架構師
- Dave Walker，Amazon Web Services 安全與合規首席專業解決方案架構師
- Paul Hopkins，Amazon Web Services 資深安全策略師
- Sam Elmalak，Amazon Web Services 資深技術主管

深入閱讀

如需其他協助，請參考以下資源：

- AWS Well-Architected 架構白皮書

文件修訂

日期	描述
2020 年 7 月	更新帳戶、身份和許可管理的指導方針。
2020 年 4 月	更新以擴展每個領域的建議、新的最佳實務、服務和功能。
2018 年 7 月	更新以反映新的 AWS 服務和功能以及更新的參考。
2017 年 5 月	更新了「系統安全組態和維護」部分，以反映新的 AWS 服務和功能。
2016 年 11 月	首次出版