AWS Well-Architected Framework

安全支柱

安全支柱: AWS Well-Architected Framework

Table of Contents

安全支柱 – AWS Well Architected Framework

出版日期： 2023 年 12 月 6 日 (文件修訂)

本白皮書的重點是 AWS Well-Architected Framework。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

此 AWS Well-Architected Framework 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，您將了解關於在雲端設計和操作可靠、安全、有效率、經濟實惠且永續的工作負載的現有架構最佳實務。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。

此架構以六大支柱為基礎：

- 卓越營運
- 安全性
- 可靠性
- 效能達成效率
- 成本最佳化
- 永續性

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。

安全基礎

安全支柱說明如何利用雲端技術，採取能夠提升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引。

設計原則

雲端中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。集中進行身分管理，旨在消除對長期靜態憑證的倚賴。
- 維持可追溯性： 即時監控、警示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。
- 保護傳輸中資料和靜態資料：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

雲端中的安全包括七個層面：

- 安全基礎
- 身分和存取管理
- 偵測
- 基礎設施保護
- 資料保護
- 事故回應

- 應用程式安全

共同的責任

安全與合規是 AWS 與客戶之間共同的責任。這種共同模式有助減輕客戶的運作負擔，因為 AWS 會深入服務運作所在設施的實體安全性，操作、管理並控制主機作業系統及虛擬化層的元件。客戶應承擔相關責任並負責管理訪客作業系統 (包括更新與安全性修補程式)，以及其他相關應用程式軟體，還有設定 AWS 提供的安全群組防火牆。客戶應審慎思考所選的服務，因為使用的服務、服務與客戶 IT 環境的整合情形，以及適用的法律與法規不同，客戶應承擔的責任也會不同。此共同責任的性質也提供允許部署的彈性和客戶控制。如下圖所示，這種責任區分通常被稱為「雲端安全性」與「雲端中的安全性」。

AWS 責任「雲端安全性」 – AWS 會負責保護執行 AWS 雲端中所有服務的全球基礎設施。此基礎設施由硬體、軟體、聯網以及執行 AWS 雲端服務的設施所組成。

客戶責任「雲端中的安全性」 – 客戶責任將由客戶選取的 AWS 雲端服務決定。這也決定了客戶在履行其安全性責任的過程中，必須執行的設定工作量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 等服務會分類為基礎設施即服務 (IaaS)，因此會要求客戶執行所有必要的安全設定和管理任務。部署 Amazon EC2 執行個體的客戶負責管理訪客作業系統 (包括更新和安全性修補程式)、客戶在執行個體上安裝的任何應用程式軟體或公用程式，以及設定每個執行個體上由 AWS 提供的防火牆 (稱為安全群組)。對於 Amazon S3 和 Amazon DynamoDB 等抽象服務，AWS 會操作基礎設施層、作業系統和平台，而且客戶會存取端點以儲存和擷取資料。客戶負責管理其資料 (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。

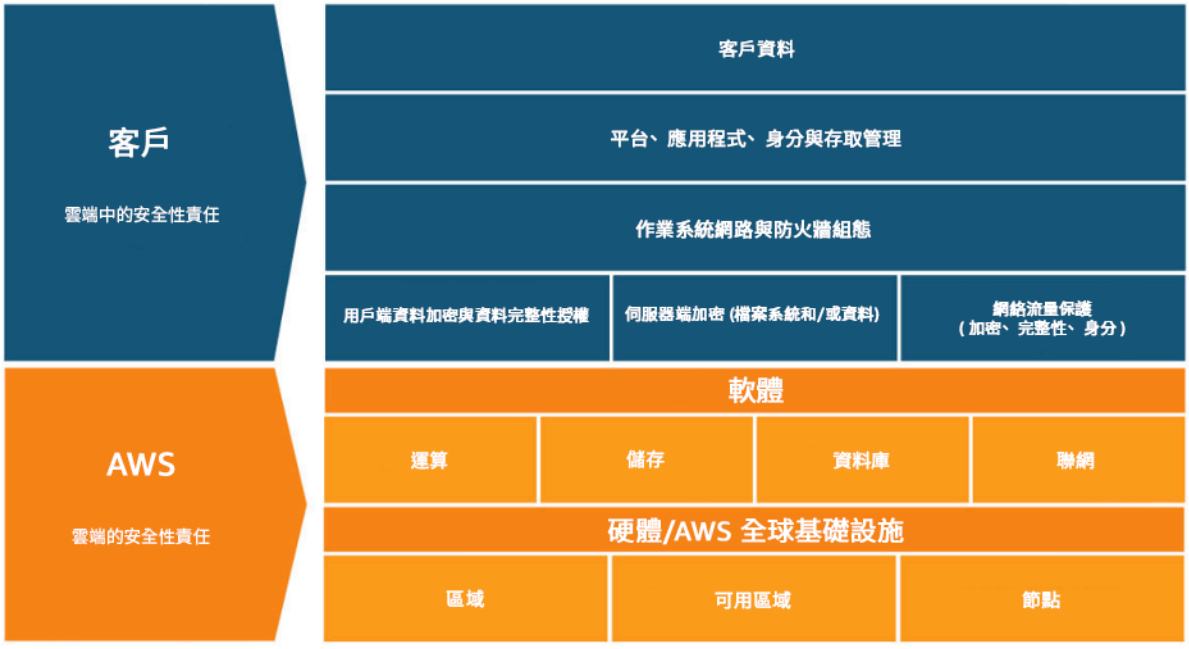


圖 1：AWS 共同的責任模型

這種客戶/AWS 共同的責任模式也擴大到 IT 控制。一如 AWS 和客戶共同承擔 IT 環境的操作責任，IT 控制的管理、操作和驗證，也是由雙方共同承擔責任。AWS 可以藉由管理與 AWS 環境中所部署的實體基礎設施相關聯的那些控制，來協助減輕客戶操作控制的負擔，而上述控制先前已由客戶管理。由於每個客戶在 AWS 中的部署方式均不同，因此客戶可將特定 IT 控制的管理工作轉移給 AWS，以產生 (新的) 分散式控制環境。客戶可以使用其可取得之 AWS 控制與合規文件，視需要執行控制評估與驗證程序。以下範例控制是由 AWS、AWS 客戶或兩者共同管理。

繼承的控制 – 客戶完全繼承自 AWS 的控制。

- 實體與環境控制

共用的控制 – 同時適用於基礎設施層和客戶層的控制，但在不同的內容或觀點中。在共用的控制中，AWS 提供基礎設施的需求，而且客戶必須在他們使用的 AWS 服務內提供自己的控制實作。這些範例包括：

- 修補程式管理 – AWS 負責修補和修正基礎設施中的瑕疵，但客戶負責修補其客體作業系統和應用程式。
- 組態管理 – AWS 維護其基礎設施裝置的組態，但客戶負責設定其自己的客體作業系統、資料庫和應用程式。
- 認知與培訓 – AWS 負責培訓 AWS 員工，但客戶必須培訓其自己的員工。

客戶特有 – 根據客戶在 AWS 服務內部署的應用程式而定，客戶須全權負責的控制。這些範例包括：

- 服務和通訊保護或區域安全，客戶可能須在特定安全環境內路由或區分資料。

管控

安全管控作為整體方法的子集，旨在藉由定義政策和控制目標來協助管理風險，以支援業務目標。藉由遵循分層方法安全地控制目標來實現風險管理 - 每一層都建立在前一層之上。了解 AWS 共同責任模型是您的基礎層。這點清楚地說明了您在客戶端的責任，以及您從 AWS 繼承的責任。有益的資源是 AWS Artifact，可讓您隨需存取 AWS 安全和合規報告，以及選取線上協議。

滿足下一層的大部分控制目標。這就是全平台的能力所在。例如，這一層包括 AWS 帳戶銷售流程、與身分供應商 (例如 AWS IAM Identity Center 單一登入) 的整合，以及常見的偵測控制。這裡也會列出一些平台管控流程輸出。當您想要開始使用新的AWS 服務時，請更新 AWS Organizations 服務中的服

務控制政策 (SCP)，為服務的初始使用提供防護機制。您可以使用其他 SCP 來實現常見的安全控制目標，通常稱為安全不變量。這些是您套用至多個帳戶、組織單位或整個 AWS 組織的控制目標或組態。典型範例是限制基礎設施執行所在的區域或防止停用偵測控制。此中間層還包含編碼政策，例如管道中的組態規則或檢查。

最上層是產品團隊符合控制目標的地方。因為這個實作是由產品團隊所控制應用程式進行完成。過程中可能是在應用程式中實作輸入驗證，或確保身分在微型服務之間正確傳遞。即使產品團隊擁有組態，他們仍可能繼承中間層的一些功能。

無論您在何處實作控制，目標都是管理風險。一系列適用於特定產業、區域或技術的風險管理架構。您的主要目標：根據可能性和後果來找出風險。這是 固有風險。您可以接著定義一個控制目標，以降低可能性或後果，或同時降低兩者。然後，配合適當的控制，您就能預見可能產生的風險。這是 剩餘風險。控制目標適用於一個或多個工作負載。下圖顯示典型的風險矩陣。可能性以先前發生的頻率為依據，而後果以事件的財務、信譽和時間成本為依據。

可能性	風險等級				
非常可能	低	中	高	嚴重	嚴重
有可能	低	中	中	高	嚴重
可能	低	低	中	中	高
不太可能	低	低	中	中	高
非常不可能	低	低		中	高
結果	最低	低	中	高	嚴重

圖 2：風險等級可能性矩陣

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，將個別帳戶和群組帳戶中的工作負載分門別類，而不要複製組織的報告結構。在 AWS 中，帳戶是硬性界限。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。

集中管理帳戶： AWS Organizations 可自動建立和管理 AWS 帳戶，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機制，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)，以及提供儀表板方便您深入檢視。

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，並防止成員帳戶停用記錄。此外，您還可以集中彙總使用 AWS Config定義的規則資料，如此就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。

使用安全服務的委託管理功能將用於管理的帳戶與組織計費 (管理) 帳戶分開。數個 AWS 服務 (例如 GuardDuty、Security Hub 和 AWS Config) 支援與 AWS Organizations 的整合，包括為管理功能指定特定帳戶。

最佳實務

- SEC01-BP01 使用帳戶區隔工作負載
- SEC01-BP02 保護帳戶根使用者和屬性

SEC01-BP01 使用帳戶區隔工作負載

透過多帳戶策略在環境 (例如生產、開發和測試) 與工作負載之間建立共通的防護機制和隔離。強烈建議帳戶層級的區隔，因為這在安全性、帳單和存取方面提供了有力的隔離界限。

預期成果：將雲端作業、不相關的工作負載和環境隔離成不同帳戶的帳戶結構，以提高雲端基礎設施間的安全性。

常見的反模式：

- 將多個具有不同資料敏感度等級且不相關的工作負載置於相同的帳戶中。
- 定義不良的組織單位 (OU) 結構。

建立此最佳實務的優勢：

- 若工作負載遭到意外存取，縮小影響範圍。
- 集中管控對 AWS 服務、資源和區域的存取。
- 利用政策以及集中管理安全服務，維護雲端基礎設施的安全性。
- 自動化帳戶建立和維護流程。
- 集中稽核您的基礎設施以滿足合規性和法規需求。

未建立此最佳實務時的風險暴露等級：高

實作指引

AWS 帳戶 在以不同的敏感度等級操作的工作負載或資源之間提供安全隔離界限。AWS 提供工具透過多帳戶策略大規模管理您的雲端工作負載，以利用此隔離界限。如需有關 AWS 上多帳戶策略的概念、模式和實作的指引，請參閱使用多個帳戶管理您的 AWS 環境。

當您集中管理多個 AWS 帳戶 時，應該將您的帳戶組織成由組織單位 (OU) 層定義的階層。接著可以組織安全控制並套用至 OU 和成員帳戶，在組織內的成員帳戶上建立一致的預防性控制。安全控制是繼承的，讓您能夠篩選位於 OU 階層較低層級的成員帳戶可用的許可。良好的設計可利用此繼承關係來降低必要的安全政策數目和複雜度，達成每個成員帳戶預期的安全控制。

您可以使用 AWS Organizations 和 AWS Control Tower 這兩個服務來實作和管理在 AWS 環境中的多帳戶結構。AWS Organizations 可讓您將帳戶組織成由一或多個 OU 層所定義的階層，各個 OU 包含數個成員帳戶。服務控制政策 (SCP) 可讓組織管理員於成員帳戶建立細微的預防性控制，而 AWS Config 可用來於成員帳戶建立主動式和偵測控制。許多 AWS 服務皆與 AWS Organizations 整合以提供委派的管理控制，並跨組織內的所有成員帳戶執行服務特定的工作。

位於 AWS Organizations 分層之上的 AWS Control Tower 透過登陸區域為多帳戶 AWS 環境提供了一鍵式最佳實務設定。該登陸區域是通往由 Control Tower 所建立之多帳戶環境的進入點。Control Tower 提供數項優於 AWS Organizations 的優點。提供改進的帳戶管控的三個優點是：

- 整合式強制性安全防護機制，會自動套用至獲准加入組織的帳戶。
- 選擇性防護機制，可針對指定 OU 集合開啟或關閉。
- AWS Control Tower Account Factory 提供帳戶的自動化部署，當中包含組織內部預先核准的基準和設定選項。

實作步驟

1. 設計組織單位結構：設計妥善的組織單位結構可減輕建立和維護服務控制政策及其他安全控制所需的管理負擔。您的組織單位結構應該與您的業務需求、資料敏感度和工作負載結構協調一致。
2. 為您的多帳戶環境建立登陸區域：登陸區域提供一致的安全和基礎設施，您的組織可以從該基礎迅速開發、啟動和部署工作負載。您可以使用定製的登陸區域或 AWS Control Tower 來協調您的環境。
3. 建立防護機制：透過您的登陸區域為您的環境實作一致的安全性防護機制。AWS Control Tower 提供可部署的強制性和選擇性控制清單。實作 Control Tower 時會自動部署強制性控制。檢閱強烈建議和選擇性控制清單，並實作符合您需求的控制。
4. 限制對新增區域的存取：對於新的 AWS 區域，IAM 資源 (例如使用者和角色) 只會傳播到您指定的區域。當使用 Control Tower 時可以透過主控台，或透過調整 AWS Organizations 中的 IAM 許可政策執行此動作。
5. 考慮 AWS CloudFormation StackSets：StackSets 可幫助您將資源 (包括 IAM 政策、角色和群組) 從核准的範本部署到不同的 AWS 帳戶 和區域中。

資源

相關的最佳實務：

- SEC02-BP04 利用集中式身分提供者

相關文件：

- AWS Control Tower
- AWS 安全稽核指導方針
- IAM 最佳實務
- 使用 CloudFormation StackSets 跨多個 AWS 帳戶 和區域佈建資源
- 組織常見問答集
- AWS Organizations 術語和概念
- 在 AWS Organizations 多帳戶環境中服務控制政策的最佳實務
- AWS 帳戶管理參考指南
- 使用多個帳戶整理您的 AWS 環境

相關影片：

- 透過自動化和管控大規模採用 AWS
- 以 Well-Architected 方式提供安全最佳實務
- 使用 AWS Control Tower 建立和管控多個帳戶
- 為現有組織啟用 Control Tower

相關研討會：

- Control Tower Immersion Day

SEC01-BP02 保護帳戶根使用者和屬性

根使用者是 AWS 帳戶 中最具特權的使用者，對帳戶內的所有資源具備完整的管理存取權，並且在某些情況下，不受安全政策的限制。停用對根使用者的程式設計存取，為根使用者建立適當的控制，以及避免例行使用根使用者，可降低意外暴露根憑證及後續危及雲端環境的風險。

預期成果：保護根使用者有助於降低因誤用根使用者憑證而可能發生的意外或有意傷害的可能性。建立偵測控制也能在當使用根使用者採取動作時警告適當的人員。

常見的反模式：

- 將根使用者用於需要根使用者憑證以外的工作。
- 疏於定期測試緊急應變計劃以確認重大基礎設施、程序和人員在緊急情況下的運作情形。
- 僅考慮一般帳戶登入流程而疏於考慮或測試替代帳戶復原方法。
- 未將 DNS、電子郵件伺服器和電話提供者作為重要安全周邊的一部分來處理，因為其會用於帳戶復原流程。

建立此最佳實務的優勢：保護對根使用者的存取可建立信心，讓您知道帳戶中的動作受到控制和稽核。

未建立此最佳實務時的風險暴露等級：高

實作指引

AWS 提供眾多工具來協助保護您的帳戶。然而，由於不會啟用當中部分的措施預設，您必須採取直接的行動加以實作。考慮將這些建議作為保護 AWS 帳戶 的基本步驟。實作這些步驟時，務必建立程序以持續評估和監視安全控制。

首次建立 AWS 帳戶 時，您是從一個對帳戶中所有 AWS 服務和資源具有完全存取權的身分開始。此身分就是所謂的 AWS 帳戶 根使用者。您可以使用您建立該帳戶所用的電子郵件地址和密碼，以根使用者的身分登入。由於 AWS 根使用者獲得的已提升存取權，您必須將 AWS 根使用者限用於執行特別需要它的工作。根使用者登入憑證必須受嚴密防護，並且您應該一律為 AWS 帳戶 根使用者啟用多重要素驗證 (MFA)。

除了一般驗證流程 (使用使用者名稱、密碼和多重要素驗證 (MFA) 裝置登入根使用者) 之外，還有帳戶復原流程會登入 AWS 帳戶 根使用者，而其能夠存取與您的帳戶相關聯的電子郵件地址和電話號碼。因此，保護傳送復原電子郵件的根使用者電子郵件帳戶以及與帳戶相關聯的電話號碼同樣也很重要。另外，對於與根使用者相關聯的電子郵件地址託管在相同 AWS 帳戶的電子郵件伺服器或網域名稱服務 (DNS) 資源上的情況，也要考慮可能的循環相依性。

使用 AWS Organizations 時，會有多個 AWS 帳戶，各自都有根使用者。將一個帳戶指定為管理帳戶，接著可以在該管理帳戶之下新增數層成員帳戶。優先保護您的管理帳戶根使用者後，再來處理成員帳戶根使用者。保護管理帳戶根使用者的策略可不同於成員帳戶根使用者，而且您可以對成員帳戶根使用者設立預防性安全控制。

實作步驟

以下是為根使用者建立控制的建議實作步驟。適用時，可交互參考 CIS AWS Foundations 基準版本 1.4.0 建議。除了這些步驟之外，請諮詢 AWS 最佳實務指導方針來保護您的 AWS 帳戶 和資源。

預防性控制

1. 為帳戶設定準確的聯絡資訊。
    a. 此資訊會用於遺失密碼復原流程、遺失 MFA 裝置帳戶復原流程，以及與您的團隊進行重大安全相關通訊。
    b. 使用由您的企業網域所託管的電子郵件地址 (最好是使用分發清單) 作為根使用者的電子郵件地址。使用分發清單而不是個人的電子郵件帳戶可對長期存取根帳戶提供額外的備援和持續性。
    c. 聯絡資訊上所列的電話號碼應該是針對此用途的專用安全電話。不應公布或與他人共用電話號碼。
2. 請勿為根使用者建立存取金鑰。若存在存取金鑰，請將其移除 (CIS 1.4)。
    a. 去除根使用者任何長期存留的程式設計憑證 (存取和秘密金鑰)。
    b. 若根使用者存取金鑰已存在，您應該將使用這些金鑰的程序轉換為從 AWS Identity and Access Management (IAM) 角色使用暫時存取金鑰，然後刪除根使用者存取金鑰。
3. 確定您是否需要儲存根使用者的憑證。

a. 如果您使用 AWS Organizations 建立新成員帳戶，則成員帳戶上的根使用者的初始密碼會設為隨機值，並且不會向您公開。必要時，考慮使用 AWS 組織管理帳戶的密碼重設程序獲取對成員帳戶的存取權。

b. 對於獨立 AWS 帳戶 或管理 AWS 組織帳戶，請考慮建立根使用者的憑證並安全存放。為根使用者啟用 MFA。

4. 在 AWS 多帳戶環境中為成員帳戶根使用者啟用預防性控制。

a. 考慮為成員帳戶啟用不允許建立根使用者的根存取金鑰預防性防護機制。

b. 考慮為成員帳戶啟用不允許根使用者的動作預防性防護機制。

5. 如果您需要根使用者的憑證：

a. 使用複雜密碼。

b. 為根使用者啟用多重要素驗證 (MFA)，尤其是 AWS Organizations 管理 (付款人) 帳戶 (CIS 1.5)。

c. 考慮硬體 MFA 裝置以獲得彈性和安全性，因為一次性裝置可減少包含 MFA 代碼的裝置重複用於其他用途的可能性。確認定期更換使用電池的硬體 MFA 裝置。(CIS 1.6)

- 若要為根使用者設定 MFA，請遵循啟用虛擬 MFA 或硬體 MFA 裝置的指示。

d. 考慮註冊多個 MFA 裝置以備用。 每個帳戶最多允許 8 個 MFA 裝置。

- 請注意，為根使用者註冊一個以上的 MFA 裝置會自動停用 MFA 裝置遺失時復原帳戶的流程。

e. 請將密碼妥善保管，如果以電子方式儲存密碼，請考慮循環相依性。儲存密碼時，請勿以需要存取相同的 AWS 帳戶 來取得密碼的方式儲存。

6. 選擇性：考慮為根使用者建立定期密碼輪流排程。

- 憑證管理最佳實務取決於您法規和政策需求。受 MFA 保護的根使用者不依賴把密碼當作單一驗證要素。
- 定期變更根使用者密碼可降低意外洩露的密碼可能遭到誤用的可能性。

偵測控制

- 建立警示以偵測根憑證的使用 (CIS 1.7)。啟用 Amazon GuardDuty 將透過 RootCredentialUsage 發現結果監控並發出關於根使用者 API 憑證使用的通知。
- 評估並實作適用於 AWS Config 的 AWS Well-Architected 安全支柱合規套件中包含的偵測控制，或者若是使用 AWS Control Tower，Control Tower 內有提供強烈建議的控制。

操作指導

- 確定組織內誰應該存取根使用者憑證。
  - 使用雙人規則，如此沒有單獨一人可以存取所有必要的憑證和 MFA 來取得根使用者存取權。
  - 確認組織而不是單一個人持有對與帳戶相關聯的電話號碼和電子郵件別名 (用於密碼重設和 MFA 重設程序) 的控制權。
- 只在特殊情況下使用根使用者 (CIS 1.7)。
  - AWS 根使用者不可用於日常任務，即使管理任務也一樣。僅以根使用者身分登入執行需要根使用者的 AWS 任務。所有其他動作都應該由其他擔任適當角色的使用者執行。
- 定期檢查根使用者的存取權操作正常，以便在發生需要使用根使用者憑證的緊急情況之前，測試相關程序。
- 定期檢查與帳戶相關聯的電子郵件地址，以及替代聯絡人下所列的電子郵件地址有效。監控這些電子郵件收件匣，查看您可能接收的安全通知 <abuse@amazon.com>。另外確保與帳戶相關聯的任何電話號碼都有效。
- 準備事件回應程序以回應根帳戶誤用的情況。請參考 AWS 安全事件應變指南和安全支柱白皮書的事件應變一節中的最佳實務，取得更多有關為您的 AWS 帳戶 建立事件應變策略的資訊。

資源

相關的最佳實務：

- SEC01-BP01 使用帳戶區隔工作負載
- SEC02-BP01 使用強式登入機制
- SEC03-BP02 授予最低權限存取權
- SEC03-BP03 建立緊急存取程序
- SEC10-BP05 預先佈建存取權

相關文件：

- AWS Control Tower
- AWS 安全稽核指導方針
- IAM 最佳實務
- Amazon GuardDuty – 根憑證使用警示
- 透過 CloudTrail 監控根憑證使用的逐步指引

- 經核准可與 AWS 搭配使用的 MFA 權杖
- 在 AWS 上實作緊急存取
- 改進 AWS 帳戶中 10 大安全性項目
- 如果我發現 AWS 帳戶 中有未授權的活動該怎麼辦？

相關影片：

- 透過自動化和管控大規模採用 AWS
- 以 Well-Architected 方式提供安全最佳實務
- 限制使用 AWS 根憑證，取自 AWS re:inforce 2022 – 使用 AWS 的安全最佳實務 IAM

相關範例和實驗室：

- 實驗室：AWS 帳戶 和根使用者

安全操作工作負載

操作工作負載安全地涵蓋了工作負載的整個生命週期，從設計、建置、執行到持續改善。改善在雲端中安全操作能力的方法之一，就是採用組織方法進行管控。管控是一致地指引決策的方式，而不是僅依賴相關人員的良好判斷。您的管控模型和流程是您回答「我如何知道是否達到給定工作負載的控制目標，並且這些目標是否適合於該工作負載？」問題的方式。 採用一致方法做出決策，可以加快工作負載的部署，並有助於提高組織中安全能力的標準。

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。自動化安全流程、測試和驗證可協助您擴展安全操作。

自動化讓流程得以維持一致性和可重複性。人員或許擅長做很多事情，但卻不包括一直重複同一件事而能不出錯。即使執行手冊撰寫得再完整，仍難免發生人員未能始終如一地執行重複任務的風險。尤其當人員承擔不同的責任，而必須回應不熟悉的警示時，更是如此。然而，自動化每次都會以相同的方式回應。部署應用程式的最佳方式就是透過自動化。執行部署的程式碼可以進行測試，然後用來執行部署。這可在變更過程中增加信心，並降低變更失敗的風險。

若要驗證組態是否達到您的控制目標，請先在非生產環境中測試自動化和部署的應用程式。如此一來，您可以測試自動化以證明它已正確地執行所有步驟。您也可以在開發和部署週期中獲得早期意見回饋，

從而減少返工。若要減少部署錯誤的機會，請透過程式碼而不是人員來進行組態變更。如果您需要重新部署應用程式，自動化會使這個動作容易得多。當定義其他控制目標時，您可以輕鬆地將它們新增到所有工作負載的自動化。

與其讓個別工作負載擁有者投資於其工作負載特有的安全性，不如透過使用常用功能和共用元件來節省時間。多個團隊可以取用的一些服務範例包括 AWS 帳戶建立流程、集中式人員身分、常用的記錄組態，以及 AMI 和容器基礎映像建立。這種方法可以協助建立者縮短工作負載週期時間，並始終如一地達到安全控制目標。當團隊更加一致時，您可以驗證控制目標，並向利害關係人更好地報告您的控制態勢和風險位置。

最佳實務

- SEC01-BP03 識別和驗證控制目標
- SEC01-BP04 掌握安全威脅的最新資訊
- SEC01-BP05 及時了解安全建議的最新資訊
- SEC01-BP06 將管道中安全控制的測試和驗證自動化
- SEC01-BP07 使用威脅模型識別威脅並優先考慮緩解措施
- SEC01-BP08 定期評估和實作新的安全服務和功能

SEC01-BP03 識別和驗證控制目標

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。

若未建立此最佳實務，暴露的風險等級： 高

實作指引

- 識別合規要求：發現您的工作負載務必遵守的組織、法律和合規要求。
- 識別 AWS 合規資源：識別 AWS 可用於協助您達成合規的資源。
  - https://aws.amazon.com/compliance/
  - https://aws.amazon.com/artifact/

資源

相關文件：

- AWS 安全稽核指導方針
- 安全公告

相關影片：

- AWS Security Hub：管理安全提醒與使合規自動化
- 以 Well-Architected 方式提供安全最佳實務

SEC01-BP04 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，以協助您定義並實作適當的控制。取用 AWS Managed Services 可讓您更輕鬆地接收 AWS 帳戶中非預期或異常行為的通知。使用 AWS 合作夥伴工具或第三方威脅資訊摘要，做為安全資訊流程的一部分進行調查。AWS Well-Architected 通用漏洞披露 (CVE) 清單 此清單包含公開揭露的網路安全漏洞，您可以使用這些漏洞來保持最新狀態。

若未建立此最佳實務，暴露的風險等級為： 高

實作指引

- 訂閱威脅情報來源：定期從多個來源檢閱與工作負載中使用的技術相關的威脅情報。
  - 通用漏洞披露清單
- 考慮 AWS Shield Advanced 服務：如果您的工作負載可透過網際網路存取，它可提供近乎即時的情報來源可見性。

資源

相關文件：

- AWS 安全稽核指導方針
- AWS Shield
- 安全公告

相關影片：

- 以 Well-Architected 方式提供安全最佳實務

SEC01-BP05 及時了解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。AWS 安全公告 包含有關安全和隱私權通知的重要資訊。

若未建立此最佳實務，暴露的風險等級： 高

實作指引

- 關注 AWS 更新：訂閱或定期查看新的建議、秘訣和技巧。
  - AWS Well-Architected 實驗室
  - AWS 安全部落格
  - AWS 服務文件
- 訂閱產業新聞：定期在多個來源檢閱與工作負載中使用技術相關的新聞摘要。
  - 範例：通用漏洞披露清單

資源

相關文件：

- 安全公告

相關影片：

- 以 Well-Architected 方式提供安全最佳實務

SEC01-BP06 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設施即程式碼範本，檢查是否有安全漏洞、異常和偏離各階段既定基準。AWS CloudFormation Guard 可以協助您驗證 CloudFormation 範本是否安全、為您節省時間，以及減少組態錯誤的風險。

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。

追蹤對您工作負載組態的變更，以協助進行合規稽核、變更管理，以及可能適用於您的調查。您可以使用 AWS Config，來記錄並評估 AWS 和第三方資源。它可讓您使用規則和一致性套件持續稽核和評估整體合規，這些規則和一致性套件是具有修復動作的規則集合。

變更追蹤應該包括規劃的變更，這是組織變更控制程序的一部分 (有時稱為 MACD—移動、新增、變更、刪除)，也包括非規劃的變更，以及非預期的變更，例如事故。基礎設施上可能會發生變更，但它們也可能與其他類別相關，例如程式碼儲存庫中的變更、機器映像和應用程式庫存變更、程序和政策變更，或文件變更。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

- 自動化組態管理：透過使用組態管理服務或工具，來自動執行和驗證安全組態。
  - AWS Systems Manager
  - AWS CloudFormation
  - 在 AWS 上設定 CI/CD 管道

資源

相關文件：

- 如何使用服務控制政策在 AWS Organizations 中的各個帳戶之間設定許可防護機制

相關影片：

- 使用 AWS Organizations 管理多帳戶 AWS 環境
- 以 Well-Architected 方式提供安全最佳實務

SEC01-BP07 使用威脅模型識別威脅並優先考慮緩解措施

執行威脅建模，為您的工作負載識別並保有潛在威脅及相關緩解措施的最新記錄。排定威脅的優先順序並調整安全控制緩解措施，以防止、偵測和回應威脅。就您的工作負載的情況，以及不斷演變的安全形勢，重新檢視和維護此工作。

未建立此最佳實務時的風險暴露等級：高

實作指引

什麼是威脅建模？

「威脅建模以保護有價值物為目標，識別、溝通和了解威脅及緩解措施。」– 開放 Web 應用程式安全專案 (OWASP) 應用程式威脅建模

為何使用威脅模型？

系統本身錯綜複雜，並且隨時間變得更形複雜且更具能力，而實現更大的商業價值及更高的客戶滿意度和參與度。這表示 IT 設計決策需要考慮不斷增加的使用案例數量。這種複雜性和使用案例數量的排列通常使得非結構化方法無法有效尋找和緩解威脅。反之，您需要一套系統化方法來列舉對系統的潛在威脅，以及策畫緩解措施，並以這些緩解措施為優先來確保組織的有限資源能在改善系統整體安全形勢上發揮最大的影響力。

威脅建模旨在提供這套系統化方法，目的是要在設計過程中及早尋找和解決問題，此時進行緩解的成本和精力與生命週期稍後相比要來得低。此方法與往前移安全性的業界原則相一致。威脅建模最終會與組織的風險管理程序整合，透過使用威脅驅動的方法，協助推動要實作哪些控制措施的決策。

何時執行威脅建模？

在工作負載的生命週期中及早開始威脅建模，可給予您更大的彈性來決定要如何處理所識別的威脅。就跟軟體錯誤一樣，越早識別威脅，就能以越具成本效益的方式加以解決。威脅模型是不斷更新的文件，並且應該持續隨著工作負載的變更而演進。隨時間重新檢視您的威脅模型，包括當有重大變更、威脅形勢有變化，或是採用新功能或服務時。

實作步驟

我們能如何執行威脅建模？

執行威脅建模的方式有很多種。就跟程式設計語言一樣，各有優缺點，而您應該選擇最適合您的方式。其中一個方法是從 Shostack 針對威脅建模的 4 個問題框架開始著手，當中提出自由回答的問題會為您的威脅建模練習提供結構：

1. 目前正在做什麼？

   此問題的目的是幫助您了解正在建置的系統並對之取得一致的意見，以及該系統與安全相關的細節。建立模型或圖表是回答此問題最受歡迎的方法，因為這可幫助您將正在建置的東西視覺化，例如使用資料流程圖。寫下關於您的系統的假設和重要細節也有助您定義涵蓋的範圍。這使得所有參與威脅模型的人能夠專注於相同的事物，並避免偏離至與主題無關的話題 (包括過時的系統版本) 而

耗費時間。舉例來說，如果您正在建置 Web 應用程式，可能不值得花時間為瀏覽器用戶端建立作業系統信任開機順序的模型，因為您無法透過您的設計對此產生影響。

2. 什麼可能出錯？

   這是您識別對系統的威脅之處。威脅是意外或有意的動作或事件，會帶來不必要的衝擊，並且可能影響系統安全。對可能出錯之處沒有清楚的了解，便無法對症下藥。

   對於什麼可能出錯，您並沒有標準的清單可循。建立此清單需要團隊內的每個人與涉及的相關角色在威脅建模練習中集思廣益和共同協作。您可以使用識別威脅的模型來協助集思廣益，例如 STRIDE，這會建議不同的類別以進行評估：詐騙、竄改、否認性、資訊洩露、拒絕服務和提升權限。此外，您可能會想要檢閱現有的清單並研究以獲得靈感來協助集思廣益，包括 OWASP 前十大、HiTrust 威脅目錄，以及您組織本身的威脅目錄。

3. 我們要做何處理？

   就跟前一個問題一樣，對於所有可能的緩解措施並沒有標準的清單可循。此步驟的輸入是前一步驟識別的威脅、動作和改進之處。

   安全與合規是您與 AWS 之間的共同責任。了解當您提出「我們要做何處理？」時，也是在問「誰要對其負責？」，這一點很重要。了解您與 AWS 之間的責任制衡有助您將威脅建模練習的範圍定在您控制之下的緩解措施，這通常是 AWS 服務組態選項與您自身的系統特定緩解措施的組合。

   對於共同責任的 AWS 部分，您將發現 AWS 服務在許多合規計畫的範圍之內。這些計畫會幫助您了解 AWS 在維護雲端安全和合規方面設立的強大控制措施。來自這些計畫的稽核報告可供 AWS 客戶從 AWS Artifact 下載。

   無論您使用何種 AWS 服務，其始終涉及客戶責任，而您的威脅模型中應該包含與這些責任一致的緩解措施。對於 AWS 服務本身的安全控制緩解措施，您應該考慮跨領域實作安全控制，包括身分和存取管理 (驗證和授權)、資料保護 (靜態和傳輸中)、基礎結構安全、記錄和監控等領域。每個 AWS 服務的文件都有專屬的安全章節，提供將安全控制視為緩解措施的指引。重要的是，考慮您正在編寫的程式碼及其程式碼相依性，並思考您可以設立以解決該些威脅的控制措施。這些控制措施可以是輸入驗證、工作階段處理和界限處理等事項。大多數漏洞通常是在自訂程式碼中引入，因此請專注於此區域。

4. 我們處理得當嗎？

   目標是讓您的團隊與組織改進威脅模型的品質以及隨時間執行威脅建模的速度。這些改進出自練習、學習、教導和評量的組合。若要更加深入並實際操作，建議您與您的團隊完成建置人員建立威脅模型的正確方式訓練課程或研討會。此外，如果您正在尋找有關如何將威脅建模整合至您組織的應用程式開發生命週期，請參閱 AWS 安全部落格上的如何進行威脅建模。

威脅編寫器

為了協助並指導您執行威脅建模，請考慮使用威脅編寫器工具，該工具旨在縮短威脅建模實現價值的時間。該工具可幫助您執行以下操作：

- 撰寫與威脅文法相符、可在自然非線性工作流程中使用的有用威脅陳述式
- 產生人類可讀的威脅模型
- 產生機器可讀的威脅模型，以便您能將威脅模型視為程式碼
- 使用洞察儀表板協助您快速識別品質和涵蓋範圍有所改進的領域

如需進一步的參考，請造訪「威脅編寫器」，並切換到系統定義的範例工作區。

資源

相關的最佳實務：

- SEC01-BP03 識別和驗證控制目標
- SEC01-BP04 掌握安全威脅的最新資訊
- SEC01-BP05 及時了解安全建議的最新資訊
- SEC01-BP08 定期評估和實作新的安全服務和功能

相關文件：

- 如何進行威脅建模 (AWS 安全部落格)
- NIST：以資料為中心的系統威脅建模指南

相關影片：

- AWS Summit ANZ 2021 - 如何進行威脅建模
- AWS Summit ANZ 2022 - 擴展安全性 – 針對快速和安全交付進行最佳化

相關訓練：

- 建置人員建立威脅模型的正確方式 – AWS Skill Builder 虛擬自訂進度訓練課程
- 建置人員建立威脅模型的正確方式 – AWS 研討會

相關工具：

- 威脅編寫器

SEC01-BP08 定期評估和實作新的安全服務和功能

評估和實作 AWS 和 AWS 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。AWS 安全部落格強調新的 AWS 服務和功能、實作指南和一般安全指引。AWS 最新消息？ 是及時了解所有新的 AWS 功能、服務和公告的最佳方式。

若未建立此最佳實務，暴露的風險等級： 低

實作指引

- 規劃定期審查：建立一個審查活動行事曆，其中包含合規要求、對新的 AWS 安全功能和服務的評估以及最新的產業新聞。
- 探索 AWS 服務與功能：探索可用於您正在使用的服務的安全功能，並在新功能發佈時審查這些功能。
  - AWS 安全部落格
  - AWS 安全公告
  - AWS 服務文件
- 定義 AWS 服務的採用程序：定義採用新 AWS 服務的程序。包含您如何評估新 AWS 服務的功能，以及工作負載的合規要求。
- 測試新的服務和功能：在緊密複寫生產服務的非生產環境中發佈新服務和功能時，請對其進行測試。
- 實作其他防禦機制：實作自動化機制以保護您的工作負載，探索可用的選項。
  - 依 AWS Config 規則 修補不合規的 AWS 資源

資源

相關影片：

- 以 Well-Architected 方式提供安全最佳實務

身分和存取管理

若要使用 AWS 服務，您必須授權您的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，需要穩固的身分管理和許可，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分及其許可。這些功能的最佳實務分為兩個主要領域。

主題

身分管理

處理操作安全的 AWS 工作負載時，您需要管理兩種身分類型。

- 人員身分：管理員、開發人員、操作人員和應用程式取用者需要身分才能存取您的 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。
- 機器身分：您的工作負載應用程式、操作工具和元件需要身分才能向 AWS 服務發出請求，例如讀取資料。這些身分包括在 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分。此外，您可能也有在 AWS 外部，需要存取 AWS 環境的機器。

最佳實務

- SEC02-BP01 使用強式登入機制
- SEC02-BP02 使用臨時憑證
- SEC02-BP03 安全地存放和使用機密
- SEC02-BP04 利用集中式身分提供者
- SEC02-BP05 定期稽核和輪換憑證
- SEC02-BP06 利用使用者群組和屬性

SEC02-BP01 使用強式登入機制

登入 (使用登入憑證進行驗證) 可預防當沒有使用多重要素驗證 (MFA) 等機制時的風險，尤其是在登入憑證遭到意外洩露或輕易被猜出的情況下。使用強式登入機制透過要求 MFA 和強式密碼政策來降低這些風險。

預期成果：透過對 AWS Identity and Access Management (IAM) 使用者、AWS 帳戶根使用者、AWS IAM Identity Center (AWS 單一登入的後繼者) 和協力廠商身分提供者使用強式登入機制，來降低 AWS 中意外存取憑證的風險。這意味著要求使用 MFA，強制強式密碼政策，以及偵測異常的登入行為。

常見的反模式：

- 沒有為您的身分強制強式密碼政策，包括複雜密碼和 MFA。
- 在不同使用者之間共用相同的憑證。
- 沒有針對可疑的登入使用偵測控制。

未建立此最佳實務時的風險暴露等級：高

實作指引

人類身分登入 AWS 的方法有很多。AWS 最佳實務是仰賴使用聯合 (直接聯合或使用 AWS IAM Identity Center) 的集中式身分提供者向 AWS 進行驗證。在這種情況下，您應該以您的身分提供者或 Microsoft Active Directory 建立安全的登入程序。

當您第一次開啟 AWS 帳戶 時，是從 AWS 帳戶 根使用者開始。您應該只使用帳戶根使用者來設定使用者的存取權 (以及需要根使用者的任務)。請務必在開啟 AWS 帳戶 後使用 AWS 最佳實務指南立即為帳戶根使用者啟用 MFA。

如果您在 AWS IAM Identity Center 中建立使用者，請保護該服務中的登入程序。對於消費者身分，您可以使用 Amazon Cognito user pools 並保護該服務中的登入程序，或使用 Amazon Cognito user pools 支援的其中一個身分提供者。

如果您使用的是 AWS Identity and Access Management (IAM) 使用者，請使用 IAM 保護登入程序。

無論登入方法為何，強制強式登入政策必不可少。

實作步驟

以下是一般的強式登入建議。您設定的實際設定應由貴公司政策來規定，或使用如 NIST 800-63 的標準。

- 要求 MFA。IAM 最佳實務是對人類身分和工作負載要求 MFA。啟用 MFA 可提供多一層安全防護，要求使用者提供登入憑證和一次性密碼 (OTP)，或是從硬體裝置以密碼編譯方式驗證和產生的字串。
- 強制密碼長度下限，此為密碼強度的要素。
- 強制密碼複雜性，使密碼更難猜測。
- 允許使用者變更自己的密碼。
- 建立個別身分，而不是共用憑證。透過建立個別身分，您可以為每個使用者提供一組獨一無二的安全憑證。個別使用者可讓您稽核每個使用者的活動。

IAM Identity Center 建議：

- 當使用預設目錄來建立密碼長度、複雜性和重複使用需求時，IAM Identity Center 提供預先定義的密碼政策。
- 當身分來源為預設目錄、AWS Managed Microsoft AD 或 AD Connector 時，啟用 MFA 並為 MFA 設定內容感知或永遠開啟設定。
- 允許使用者註冊自己的 MFA 裝置。

Amazon Cognito user pools 目錄建議：

- 設定密碼強度設定。
- 對使用者要求 MFA。
- 針對調適性驗證 (這可封鎖可疑登入) 等功能使用 Amazon Cognito user pools 進階安全性設定。

IAM 使用者建議：

- 在理想情況下，您使用 IAM Identity Center 或直接聯合。然而，您可能需要 IAM 使用者。在這種情況下，請為 IAM 使用者設定密碼政策。您可以使用密碼政策來定義需求，例如最短長度或是密碼是否需要非字母字元等。
- 建立 IAM 政策以強制 MFA 登入，允許使用者管理自己的密碼和 MFA 裝置。

資源

相關的最佳實務：

- SEC02-BP03 安全地存放和使用機密
- SEC02-BP04 利用集中式身分提供者

- SEC03-BP08 在組織內安全地共用資源

相關文件：

- AWS IAM Identity Center (AWS 單一登入的後繼者) 密碼政策
- IAM 使用者密碼政策
- 設定 AWS 帳戶根使用者密碼
- Amazon Cognito 密碼政策
- AWS 憑證
- IAM 安全最佳實務

相關影片：

- 使用 AWS IAM Identity Center 大規模管理使用者許可
- 在每一層都能掌握身分

SEC02-BP02 使用臨時憑證

當進行任何類型的驗證時，最好是使用臨時憑證，而不是長期憑證，以降低或消除風險，例如憑證遭到意外洩露、共用或遭竊。

預期成果：為了降低長期憑證的風險，對於人員和機器身分，請盡可能使用臨時憑證。長期憑證會產生許多風險，例如，可能在程式碼中將它們上傳至公有 GitHub 儲存庫。透過使用臨時憑證，您可大幅降低憑證遭到入侵的可能性。

常見的反模式：

- 開發人員使用取自 IAM users 的長期存取金鑰，而不是使用聯合從 CLI 取得臨時憑證。
- 開發人員將長期存取金鑰內嵌在程式碼中，並將該程式碼上傳到公有 Git 儲存庫。
- 開發人員將長期存取金鑰內嵌在行動應用程式中，之後在應用程式商店中提供該行動應用程式。
- 使用者與其他使用者共用長期存取金鑰，或是擁有長期存取金鑰的離職員工仍持有金鑰。
- 對機器身分可以使用臨時憑證時，卻使用長期存取金鑰。

未建立此最佳實務時的風險暴露等級：高

實作指引

對所有 AWS API 和 CLI 請求使用臨時安全憑證，而不是長期憑證。幾乎在任何情況下，對 AWS 服務的 API 和 CLI 請求都必須使用 AWS 存取金鑰簽署。您可以使用臨時或長期憑證簽署這些請求。您唯一應該使用長期憑證 (又稱為長期存取金鑰) 的時候是在使用 IAM 使用者或 AWS 帳戶 根使用者時。當您聯合至 AWS 或透過其他方法擔任 IAM 角色時，系統會產生臨時憑證。每當您使用登入憑證存取 AWS Management Console 時，系統會為您產生臨時憑證以呼叫 AWS 服務。在幾種情況下，您將需要長期憑證，並能夠使用臨時憑證完成幾乎所有任務。

避免使用長期憑證而改用臨時憑證，同時實行減少使用 IAM 使用者並支持聯合和 IAM 角色的策略。雖然對人類和機器身分過去以來都是使用 IAM 使用者，我們現在建議不要使用它們以避免使用長期存取金鑰的風險。

實作步驟

對於人類身分，例如員工、管理員、開發人員、操作員和客戶：

- 您應該仰賴集中式身分提供者並要求人類使用者以聯合搭配身分提供者，使用臨時憑證存取 AWS。您可以直接聯合至各個 AWS 帳戶 或使用 AWS IAM Identity Center (AWS IAM Identity Center 的後繼者) 和自選的身分提供者，為您的使用者進行聯合。與使用 IAM 使用者相比，聯合除了可消除長期憑證外，還提供一些優勢。您的使用者也可以從命令列進行直接聯合，或使用 IAM Identity Center 請求臨時憑證。這表示有少數使用案例會需要 IAM 使用者，或使用者需要長期憑證。
- 當授權讓第三方 (例如軟體即服務 (SaaS) 提供者) 存取 AWS 帳戶中的資源時，您可以使用跨帳戶角色和以資源為基礎的政策。
- 如果您需要授權應用程式供消費者或客戶存取您的 AWS 資源，您可以使用 Amazon Cognito 身分集區或 Amazon Cognito user pools 來提供臨時憑證。憑證的許可透過 IAM 角色設定。 您還可以對未驗證的訪客使用者另外定義一個具有限制許可的 IAM 角色。

對於機器身分，您可能需要使用長期憑證。在這些情況下，您應該要求工作負載使用臨時憑證，並以 IAM 角色存取 AWS。

- 對於 Amazon Elastic Compute Cloud (Amazon EC2)，您可以使用適用於 Amazon EC2 的角色。
- AWS Lambda 可讓您設定 Lambda 執行角色，授予服務許可以使用臨時憑證執行 AWS 動作。有許多其他類似的模型可供 AWS 服務使用 IAM 角色授予臨時憑證。
- 對於 IoT 裝置，您可以使用 AWS IoT Core 憑證提供者來請求臨時憑證。

- 對於內部部署系統或是在 AWS 之外執行並需要存取 AWS 資源的系統，您可以使用 IAM Roles Anywhere。

有些情況無法使用臨時憑證，而您可能需要使用長期憑證。在這些情況下，定期稽核和輪換憑證並針對需要長期憑證的使用案例定期輪換存取金鑰。有些可能需要長期憑證的例子包括 WordPress 外掛程式和第三方 AWS 用戶端。在您必須使用長期憑證的情況下，或是對於 AWS 存取金鑰以外的憑證，例如資料庫登入，您可以使用專為管理機密而設計的服務，例如 AWS Secrets Manager。Secrets Manager 方便您使用支援的服務管理、輪換和安全地儲存加密的機密。如需有關輪換長期憑證的詳細資訊，請參閱輪換存取金鑰。

資源

相關的最佳實務：

- SEC02-BP03 安全地存放和使用機密
- SEC02-BP04 利用集中式身分提供者
- SEC03-BP08 在組織內安全地共用資源

相關文件：

- 臨時安全憑證
- AWS 憑證
- IAM 安全最佳實務
- IAM 角色
- IAM Identity Center
- 身分提供者與聯合
- 輪換存取金鑰
- 安全合作夥伴解決方案：存取與存取控制
- AWS 帳戶根使用者

相關影片：

- 使用 AWS IAM Identity Center (AWS IAM Identity Center 的後繼者) 大規模管理使用者許可
- 在每一層都能掌握身分

SEC02-BP03 安全地存放和使用機密

工作負載需要能夠自動向資料庫、資源和第三方資源證明其身分。這需使用私密存取憑證來完成，例如 API 存取金鑰、密碼和 OAuth 權杖。使用專用服務來儲存、管理和輪換這些憑證有助於降低該些憑證遭到入侵的可能性。

預期成果：實施一種安全管理應用程式憑證的機制並達到以下目標：

- 識別工作負載需要何種機密。
- 盡可能以短期憑證取代長期憑證，來減少所需的長期憑證數目。
- 建立安全的存放區並自動輪換其餘的長期憑證。
- 稽核對存在於工作負載中的機密的存取。
- 持續監控以確認原始程式碼在開發過程中沒有內嵌機密。
- 降低憑證遭意外洩露的可能性。

常見的反模式：

- 沒有輪換憑證。
- 將長期憑證存放在原始程式碼或設定檔中。
- 未加密儲存靜態憑證。

建立此最佳實務的優勢：

- 已加密儲存靜態和傳輸中的機密。
- 透過 API 限制憑證的存取 (把這想成是憑證自動販賣機)。
- 稽核並記錄對憑證的存取 (包括讀寫)。
- 區隔顧慮：由不同的元件執行憑證輪換，而該元件可與其餘的架構分離。
- 自動將機密隨需散發到軟體元件並集中進行輪換。
- 可以精細的方式控制對憑證的存取。

未建立此最佳實務時的風險暴露等級：高

實作指引

以往，憑證用於向資料庫進行驗證，而第三方 API、權杖和其他機密可能內嵌在原始程式碼或環境檔案中。AWS 提供數種機制以安全存放這些憑證，自動輪換並稽核它們的使用情況。

著手機密管理的最佳方法是遵循移除、取代和輪換的指引。最安全的憑證是您不用存放、管理或處理的憑證。有些憑證對於工作負載的運作不再是必要的，故能夠安全移除。

對於工作負載適當運作仍舊是必要的憑證，可能有機會以臨時或短期憑證取代長期憑證。例如，與其對 AWS 私密存取金鑰進行硬式編碼，考慮使用 IAM 角色以臨時憑證取代長期憑證。

部分長期存留的機密可能無法移除或取代。可將這些機密存放在 AWS Secrets Manager 之類的服務中，進行集中存放、管理和定期輪換。

對工作負載的原始程式碼和設定檔的稽核，可能顯現多種類型的憑證。下表概述處理常見憑證類型的策略：

Credential type	Description	Suggested strategy
IAM access keys	AWS IAM access and secret keys used to assume IAM roles inside of a workload	Replace: Use IAM 角色 assigned to the compute instances (such as Amazon EC2 or AWS Lambda) instead. For interoperability with third parties that require access to resources in your AWS 帳戶, ask if they support AWS 跨帳戶存取權. For mobile apps, consider using temporary credentials through Amazon Cognito 身分集區 (聯合身分). For workloads running outside of AWS, consider IAM Roles Anywhere or AWS Systems Manager 混合式啟用.
SSH keys	Secure Shell private keys used to log into Linux EC2	Replace: Use AWS Systems Manager or EC2 執行個體連

Credential type	Description	Suggested strategy
	instances, manually or as part of an automated process	線 to provide programmatic and human access to EC2 instances using IAM roles.
Application and database credentials	Passwords – plain text string	Rotate: Store credentials in AWS Secrets Manager and establish automated rotation if possible.
Amazon RDS and Aurora Admin Database credentials	Passwords – plain text string	Replace: Use the Secrets Manager 與 Amazon RDS 整合 or Amazon Aurora. In addition, some RDS database types can use IAM roles instead of passwords for some use cases (for more detail, see IAM 資料庫身分驗證).
OAuth tokens	Secret tokens – plain text string	Rotate: Store tokens in AWS Secrets Manager and configure automated rotation.
API tokens and keys	Secret tokens – plain text string	Rotate: Store in AWS Secrets Manager and establish automated rotation if possible.

常見的反模式是將 IAM 存取金鑰內嵌在原始程式碼、設定檔或行動應用程式內。當需要 IAM 存取金鑰與 AWS 服務通訊時，請使用臨時 (短期) 安全憑證。這些短期憑證可以透過 IAM 角色 (用於 EC2 執行個體)、執行角色 (用於 Lambda 函數)、Cognito IAM 角色 (用於行動使用者存取)，以及 IoT Core 政策 (用於 IoT 裝置) 提供。當與第三方互動時，偏好委派 IAM 角色的存取權，包含對帳戶資源的必要存取權，而不是設定 IAM 使用者並將其的私密存取金鑰傳送給該第三方。

在很多情況下，工作負載需要儲存機密才能與其他服務和資源相互操作。AWS Secrets Manager 是專為安全管理這些憑證所打造的，可儲存和輪換 API 權杖、密碼和其他憑證。

AWS Secrets Manager 提供五項重要功能以確保敏感憑證的安全存放和處理：靜態加密、傳輸中加密、 全面性稽核、精細存取控制，以及可擴充的憑證輪換。來自 AWS 合作夥伴的其他機密管理服務，或本機開發並提供類似功能和保證的解決方案也可接受。

實作步驟

1. 使用 Amazon CodeGuru 等自動工具識別包含硬式編碼憑證的程式碼路徑。
   - 使用 Amazon CodeGuru 掃描您的程式碼儲存庫。審閱完成後，在 CodeGuru 中篩選 `Type=Secrets` 以尋找有問題的程式碼行。
2. 識別可移除或取代的憑證。
   a. 識別不再需要的憑證並標示以進行移除。
   b. 對於內嵌在原始程式碼中的 AWS 機密金鑰，請使用與必要資源相關聯的 IAM 角色加以取代。如果您部分的工作負載位於 AWS 之外但需要 IAM 憑證存取 AWS 資源，請考慮 IAM Roles Anywhere 或 AWS Systems Manager 混合式啟用。
3. 對於其他第三方長期存留且需要使用輪換策略的機密，將 Secrets Manager 整合至程式碼中以在執行時間擷取第三方機密。
   a. CodeGuru 主控台可以使用已探索的憑證自動在 Secrets Manager 中建立機密。
   b. 將 Secrets Manager 的機密擷取整合至您的應用程式程式碼中。
      - 無伺服器 Lambda 函數可以使用語言中立的 Lambda 延伸。
      - 對於 EC2 執行個體或容器，AWS 提供範例用戶端程式碼，可以數種熱門的程式設計語言從 Secrets Manager 擷取機密。
4. 定期審閱您的程式碼基底並重新掃描，以確認程式碼中未加入新的機密。
   - 考慮使用 git-secrets 之類的工具以防將新機密認可到您的原始程式碼儲存庫。
5. 監控 Secrets Manager 活動以尋找非預期使用、不當私密存取或嘗試刪除機密的跡象。
6. 減少對憑證的人員接觸。將讀寫和修改憑證的存取權限於專門用於此用途的 IAM 角色，並且只將擔任該角色的存取權提供給一小組可操作的使用者子集。

資源

相關的最佳實務：

- SEC02-BP02 使用臨時憑證
- SEC02-BP05 定期稽核和輪換憑證

相關文件：

- AWS Secrets Manager 入門
- 身分提供者與聯合
- Amazon CodeGuru 推出機密偵測器
- AWS Secrets Manager 如何使用 AWS Key Management Service
- Secrets Manager 中的機密加密和解密
- Secrets Manager 部落格文章
- Amazon RDS 宣布與 AWS Secrets Manager 整合

相關影片：

- 大規模管理、擷取和輪換密碼的最佳實務
- 使用 Amazon CodeGuru 機密偵測器
- 使用 AWS Secrets Manager 保護混合式工作負載的機密

相關研討會：

- 在 AWS Secrets Manager 中儲存、擷取和管理敏感憑證
- AWS Systems Manager 混合式啟用

SEC02-BP04 利用集中式身分提供者

人力身分 (員工和承包商) 可利用身分供應商來集中管理身分。由於您是從單一位置建立、指派、管理、撤銷和稽核存取權，因此這樣一來可以更好管理多個應用程式和系統中的存取權。

預期成果： 擁有集中式身分提供者，可集中管理員工使用者、身分驗證政策 (例如，要求多重要素驗證 (MFA))，以及對系統和應用程式進行授權 (例如，根據使用者的群組成員資格或屬性指派存取權)。您的員工使用者登入集中身分提供者並聯合 (單一登入) 至內部和外部應用程式，如此一來，使用者就不需記住多個憑證。您的身分提供者與您的人力資源 (HR) 系統整合，因此人事變更會自動同步至您的身分提供者。例如，若有人離開您的組織，您可以自動撤銷聯合應用程式和系統 (包括 AWS) 的存取權。您已在身分提供者中啟用詳細稽核記錄，並監控這些日誌以找出不尋常的使用者行為。

常見的反模式：

- 您未使用聯合和單一登入。您的員工使用者在多個應用程式和系統中建立了不同的使用者帳戶和憑證。
- 您尚未將員工使用者的身分生命週期自動化，例如透過整合身分提供者與您的 HR 系統。使用者離開您的組織或變更職務時，您採取手動程序在多個應用程式和系統中刪除或更新記錄。

建立此最佳實務的優勢： 透過使用集中式身分提供者，您就可以從單一位置管理員工使用者身分和政策，而且能夠將應用程式存取權指派給使用者和群組，並監控使用者登入活動。透過與您的人力資源 (HR) 系統整合，使用者變更職務時，這些變更就會同步至身分提供者，並自動更新指派的應用程式和許可。使用者離開您的組織時，系統會自動停用他們在身分提供者中的身分，並撤銷他們對聯合應用程式和系統的存取權。

未建立此最佳實務時的曝險等級：高

實作指引

員工使用者存取 AWS 的指引

員工使用者 (例如組織中的員工和承包商) 可能需要使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI) 存取 AWS 來執行其工作職能。您可以透過從集中式身分提供者，在兩個層級聯合至 AWS 的方式，將 AWS 存取權授與員工使用者：直接聯合至各個 AWS 帳戶，或聯合至您的 AWS 組織中的多個帳戶。

- 若要將您的員工使用者直接與各個 AWS 帳戶 聯合，您可以使用集中式身分提供者來聯合至該帳戶中的 AWS Identity and Access Management 。IAM 的彈性可讓您啟用單獨的 SAML 2.0 或 Open ID Connect (OIDC) 身分提供者用於各個 AWS 帳戶，並使用聯合身分使用者屬性進行存取控制。您的員工使用者將透過提供憑證 (例如密碼和 MFA 權杖代碼) 的方式，使用自己的 Web 瀏覽器登入身分提供者。身分提供者會向其瀏覽器發出 SAML 判斷提示，並提交至 AWS Management Console 登入 URL，以允許使用者藉由 承擔 IAM 角色對 AWS Management Console 進行單一登入。您的使用者也可以取得臨時 AWS API 憑證，以便在 AWS CLI 或 AWS SDK (從 AWS STS) 中使用，方法是 使用來自身分提供者的 SAML 判斷提示承擔 IAM 角色 。
- 若要將您的員工使用者與 AWS 組織中的多個帳戶聯合，您可以使用 AWS IAM Identity Center 集中管理員工使用者對 AWS 帳戶 和應用程式的存取權。您可以為組織啟用 Identity Center，並設定您的身分來源。IAM Identity Center 提供了預設身分來源目錄，您可以使用此目錄來管理您的使用者和群組。或者，您可以選擇外部身分來源，方法是 使用 SAML 2.0 連線至您的 外部身分提供者，並 使用 SCIM 自動佈建 使用者和群組， 或是 使用 AWS Directory Service連線至您的 Microsoft AD 目錄。身分來源設定完成後，您就可以透過在您的許可集中定義最低許可政策的方式，指派使用者和群組對 AWS 帳戶 的 存取權。您的員工使用者可以進行身分驗證的方式包括：透過您的集中身分提供者登入 AWS 存取入口網站 以及對 AWS 帳戶 和指派給他們的雲端應用程式進行單一登入。

您的使用者可以設定 AWS CLI v2 以透過 Identity Center 進行身分驗證，並取得憑證來執行 AWS CLI 命令。Identity Center 也允許透過單一登入方式存取 AWS 應用程式，例如 Amazon SageMaker Studio 和 AWS IoT Sitewise Monitor 入口網站。

依照上述指引進行後，您的員工使用者在 AWS 上管理工作負載時，將不再需要使用 IAM users 和群組，可直接正常操作。您的使用者和群組會改為在 AWS 外部進行管理，而且使用者能夠以聯合身分存取 AWS 資源。聯合身分會使用您的集中式身分提供者所定義的群組。您應該找出並移除您的 AWS 帳戶 中不再需要的 IAM 群組、IAM users 和長期存在的使用者憑證 (密碼和存取金鑰)。您可以 藉由 使用 IAM 憑證報告找到未使用的憑證， 刪除相應的 IAM users 和 刪除 IAM 群組。 您可以對組織套用 服務控制政策 (SCP) 以協助防止建立新的 IAM users 和群組，並強制透過聯合身分存取 AWS。

應用程式使用者的指引

您可以使用 Amazon Cognito 做為您的集中式身分提供者來管理應用程式 (例如行動應用程式) 使用者的身分。Amazon Cognito 可為您的 Web 和行動應用程式啟用身分驗證、授權和使用者管理功能。Amazon Cognito 提供了可擴展到數百萬使用者的身分存放區、可支援社交與企業聯合身分，並且提供進階安全功能來協助保護您的使用者和業務。您可以將自訂 Web 或行動應用程式與 Amazon Cognito 整合，在幾分鐘內就能在應用程式中加入使用者身分驗證和存取控制。Amazon Cognito 是以 SAML 和 Open ID Connect (OIDC) 等開放身分標準為基礎所建置，可支援各種不同的合規法規，並與前端和後端開發資源整合。

實作步驟

員工使用者存取 AWS 的步驟

- 使用下列其中一種方法，透過集中式身分提供者將您的員工使用者聯合至 AWS：
  - 使用 IAM Identity Center 透過與您的身分提供者聯合，對您的 AWS 組織中的多個 AWS 帳戶 啟用單一登入。
  - 使用 IAM 將您的身分提供者直接連接到各個 AWS 帳戶，以實現聯合的精細存取。
- 找出並移除已由聯合身分取代的 IAM users 和群組。

應用程式使用者的步驟

- 使用 Amazon Cognito 做為應用程式的集中式身分提供者。
- 使用 OpenID Connect 和 OAuth 將您的自訂應用程式與 Amazon Cognito 整合。您可以使用 Amplify 程式庫來開發自訂應用程式，這些程式庫提供了簡單的介面，可與各種不同的 AWS 服務進行整合，例如用於身分驗證的 Amazon Cognito。

資源

相關 Well-Architected 的最佳實務：

- SEC02-BP06 利用使用者群組和屬性
- SEC03-BP02 授予最低權限存取權
- SEC03-BP06 根據生命週期管理存取

相關文件：

- AWS 中的聯合身分
- IAM 中的安全最佳實務
- AWS Identity and Access Management 最佳實務
- 開始使用 IAM Identity Center 委派管理
- 如何在 IAM Identity Center 中針對進階使用案例使用客戶管理的政策
- AWS CLI v2：IAM Identity Center 憑證提供者

相關影片：

- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) 深入剖析
- AWS re:Invent 2022 - 使用 IAM Identity Center 簡化現有的員工存取權
- AWS re:Invent 2018：在每一層都能掌握身分

相關範例：

- 研討會：使用 AWS IAM Identity Center 實現強大的身分管理
- 研討會：無伺服器身分

相關工具：

- AWS 安全能力合作夥伴：身分和存取管理
- saml2aws

SEC02-BP05 定期稽核和輪換憑證

定期稽核和輪換憑證以限制憑證可用來存取資源的時限。長期憑證會產生許多風險，而透過定期輪換長期憑證可以降低這些風險。

預期成果：實施憑證輪換以幫助降低與使用長期憑證相關聯的風險。定期稽核和修正不符合憑證輪換政策的情況。

常見的反模式：

- 沒有稽核憑證的使用。
- 不必要地使用長期憑證。
- 使用長期憑證並且未定期輪換。

未建立此最佳實務時的風險暴露等級：中

實作指引

當您無法倚賴臨時憑證且需要長期憑證時，請稽核憑證以確保已強制定義的控制 (例如多重要素驗證 (MFA))，定期輪換並且具備適當的存取層級。

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。對於人類身分，您應要求使用者定期變更密碼，並淘汰存取金鑰而改用臨時憑證。隨著您從 AWS Identity and Access Management (IAM) 使用者移向集中式身分，您可以產生憑證報告以稽核您的使用者。

我們也建議您在身分提供者中強制和監控 MFA。您可以設定 AWS Config 規則 或使用 AWS Security Hub 安全標準來監視使用者是否已啟用 MFA。請考慮使用 IAM Roles Anywhere 為機器身分提供臨時憑證。在無法使用 IAM 角色和臨時憑證的情況下，必須經常稽核和輪換存取金鑰。

實作步驟

- 定期稽核憑證：稽核身分提供者和 IAM 中設定的身分有助於確保只有已授權的身分能存取您的工作負載。此類身分可能包括但不限於 IAM 使用者、AWS IAM Identity Center 使用者、Active Directory 使用者，或不同上游身分提供者中的使用者。例如，移除離職的人員和移除不再需要的跨帳戶角色。設立程序以定期稽核由 IAM 實體存取之服務的許可。這有助您識別需要修改的政策，以移除任何不使用的許可。使用憑證報告和 AWS Identity and Access Management Access Analyzer 來稽核 IAM 憑證和許可。您可以使用 Amazon CloudWatch 來設定對特定 API 呼叫 (在 AWS 環境中呼叫) 的警示。Amazon GuardDuty 也可以向您通知未預期的活動，這可指出對 IAM 憑證過於寬鬆的存取或意外存取。

- 定期輪換憑證：當您無法使用臨時憑證時，定期輪換長期 IAM 存取金鑰 (最長每 90 天)。如果在您不知情的情況下意外洩漏了存取金鑰，這可限制憑證可用來存取資源的時限。如需有關輪換 IAM 使用者的存取金鑰的詳細資訊，請參閱輪換存取金鑰。
- 檢閱 IAM 許可：為了改善 AWS 帳戶 的安全，請定期檢閱和監控每個 IAM 政策。確認政策遵守最低權限的原則。
- 考慮自動化 IAM 資源建立和更新： IAM Identity Center 會自動執行許多 IAM 任務，例如角色和政策管理。或者，可以使用 AWS CloudFormation 自動化 IAM 資源 (包括角色和政策) 的部署，以減少人為錯誤，因為可針對範本進行驗證和版本控制。
- 對於機器身分，使用 IAM Roles Anywhere 取代 IAM 使用者： IAM Roles Anywhere 可讓您在傳統上無法使用角色的區域中 (例如內部部署伺服器) 使用角色。IAM Roles Anywhere 使用可信的 X.509 憑證向 AWS 進行驗證及接收臨時憑證。使用 IAM Roles Anywhere 讓您無需輪換這些憑證，因為長期憑證不再儲存於內部部署環境中。請注意，您將需要監視 X.509 憑證，並在快到期時輪換。

資源

相關的最佳實務：

- SEC02-BP02 使用臨時憑證
- SEC02-BP03 安全地存放和使用機密

相關文件：

- AWS Secrets Manager 入門
- IAM 最佳實務
- 身分提供者與聯合
- 安全合作夥伴解決方案：存取與存取控制
- 臨時安全憑證
- 取得 AWS 帳戶 的憑證報告

相關影片：

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

相關範例：

- Well-Architected 實驗室 - 自動化 IAM 使用者清理
- Well-Architected 實驗室 - 自動化 IAM 群組和角色的部署

SEC02-BP06 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 IAM Identity Center (IAM Identity Center) 來管理使用者群組和屬性。IAM Identity Center 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。

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) 來控制存取情形。這可讓您透過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。

若未建立此最佳實務，暴露的風險等級為： 低

實作指引

- 如果您是使用 AWS IAM Identity Center (IAM Identity Center)，請設定群組：IAM Identity Center 可讓您設定使用者群組，並將所需的許可層級指派給群組。
  - AWS 單一登入 - 管理身分
- 了解屬性型存取控制 (ABAC)：ABAC 是一種授權策略，可根據屬性定義許可。
  - 什麼是 ABAC for AWS？
  - 實驗室：EC2 的 IAM 標籤型存取控制

資源

相關文件：

- AWS Secrets Manager 入門
- IAM 最佳實務

- 身份提供者與聯合
- AWS 帳戶根使用者

相關影片：

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

相關範例：

- 實驗室：EC2 的 IAM 標籤型存取控制

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分的存取。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，以確保這些人員身分僅擁有各自所需的存取權。

有多種方法可以授予對不同類型資源的存取權。其中一種方法是使用不同的政策類型。

IAM 中以身分為基礎的政策是受管或內嵌的政策，並連接到 IAM 身分，包括使用者、群組或角色。這些政策可讓您指定該身分可以做什麼 (其許可)。可以進一步將身分型政策分類。

受管政策 – 您可以附加到 AWS 帳戶中多個使用者、群組和角色的獨立身分型政策。有兩種類型的受管政策：

- AWS 受管政策 – 由 AWS 建立和管理的受管政策。
- 客戶受管政策 – 您在 AWS 帳戶中建立和管理的受管政策。客戶受管政策比 AWS 受管政策更能精確地控制您的政策。

受管政策是套用許可的慣用方法。不過，您也可以使用內嵌政策，直接將其新增到單一使用者、群組或角色。內嵌政策會在政策和身分之間維持嚴格的一對一關係。刪除身分時也會刪除內嵌政策。

在大多數情況下，您應該建立自己的客戶受管政策，並遵循最低權限原則。

以資源為基礎的政策會附加至資源。例如，S3 儲存貯體是資源型政策。這些政策會將許可授予與資源位於同一帳戶的主體，或位於另一個帳戶的主體。如需支援以資源為基礎的政策的服務清單，請參閱可搭配 IAM 運作的 AWS 服務。

許可界限使用受管政策，設定管理員可以設定的最大許可。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許可。

屬性型存取控制 (ABAC) 可讓您根據屬性授予許可。在 AWS 中，這些稱為標籤。標籤可以附加至 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。

組織服務控制政策 (SCP) 為組織或組織單位 (OU) 的帳戶成員定義最大許可。SCP 會限制以身分為基礎的政策或以資源為基礎的政策授予帳戶內實體 (使用者或角色) 的許可，但不會授予許可。

工作階段政策會擔任角色或聯合身分使用者。在使用 AWS CLI 或 AWS API 工作階段政策時傳遞工作階段政策，以限制角色或使用者的身分型政策授予工作階段的許可。這些政策會限制已建立工作階段的許可，但不會授予許可。如需詳細資訊，請參閱工作階段政策。

最佳實務

- SEC03-BP01 定義存取需求
- SEC03-BP02 授予最低權限存取權
- SEC03-BP03 建立緊急存取程序
- SEC03-BP04 持續減少許可
- SEC03-BP05 為您的組織定義許可防護機制
- SEC03-BP06 根據生命週期管理存取
- SEC03-BP07 分析公有和跨帳戶存取權
- SEC03-BP08 在組織內安全地共用資源
- SEC03-BP09 安全地與第三方共用資源

SEC03-BP01 定義存取需求

工作負載的每個組成部分或資源都需要由管理員、最終使用者或其他組成部分存取。您需要清楚定義哪些人或哪些項目應該可以存取每個組成部分，然後選擇適當的身分類型與身分驗證和授權方法。

常見的反模式：

- 將機密硬式編碼或存放在應用程式中。
- 為每名使用者授予自訂許可。
- 使用長期憑證。

若未建立此最佳實務，暴露的風險等級： 高

實作指引

工作負載的每個組成部分或資源都需要由管理員、最終使用者或其他組成部分存取。您需要清楚定義哪些人或哪些項目應該可以存取每個組成部分，然後選擇適當的身分類型與身分驗證和授權方法。

應提供組織中對 AWS 帳戶 的定期存取 (使用 聯合存取 或集中式的身分提供者)。 您應集中進行身分管理，並確保有既定的實務，可將 AWS 存取整合至員工的存取生命週期。例如，當員工改為擔任具有不同存取層級的任務角色時，其群組成員資格也應變更，以反映新的存取需求。

為非人類身分定義存取需求時，請判斷哪些應用程式和組成部分需要存取權，以及如何授予許可。使用透過最低權限存取模型建置的 IAM 角色是建議的方法。AWS 受管政策 提供預先定義的 IAM 政策，其中涵蓋最常見的使用案例。

AWS 服務，例如 AWS Secrets Manager 和 AWS Systems Manager 參數存放區，可以協助在無法使用 IAM 角色的情況下，將機密從應用程式或工作負載中安全地分離。在 Secrets Manager 中，您可以為憑證建立自動輪換。您可以使用 Systems Manager 來參考指令碼、命令、SSM 文件、組態和自動化工作流程中的參數，方法是使用您在建立參數時指定的唯一名稱。

您可以使用 AWS Identity and Access Management Roles Anywhere 來取得 IAM 中的臨時安全憑證，該憑證適用於在 AWS 以外執行的工作負載。您的工作負載可以使用相同的 IAM 政策 和 IAM 角色 ，您可以將這些政策和角色與 AWS 應用程式搭配使用，來存取 AWS 資源。

可能的話，請選擇短期暫時憑證，而不是長期靜態憑證。對於您希望 IAM 使用者具備程式設計存取權和長期憑證的情況，請使用 存取金鑰前次使用的資訊 來輪換和移除存取金鑰。

資源

相關文件：

- 屬性型存取控制 (ABAC)
- AWS IAM Identity Center

- IAM Roles Anywhere
- IAM Identity Center 的 AWS 受管政策
- AWSIAM 政策條件
- IAM 使用案例
- 移除不需要的憑證
- 制定政策
- 如何根據 AWS 帳戶、OU 或組織控制對 AWS 資源的存取權
- 使用 AWS Secrets Manager 中增強的搜尋功能來輕鬆識別、安排和管理機密

相關影片：

- 在 60 分鐘內精通 IAM 政策
- 責任區隔、最低權限、委派和 CI/CD
- 簡化身分和存取管理，以促進創新

SEC03-BP02 授予最低權限存取權

最佳實務是僅授與身分在特定情況下對特定資源執行特定動作所需的存取權。使用群組和身分屬性大規模動態設定許可，而不是定義個別使用者的許可。例如，您可以允許一組開發人員的存取權，以只管理其專案的資源。如此，當開發人員退出專案時，其存取權將自動被撤銷，而無須變更基礎存取政策。

預期成果：使用者應該只擁有完成其工作所需的許可。使用者只應獲得在有限時間內執行特定任務的生產環境存取權，且任務完成後，存取權就應該被撤銷。許可不再需要時就應撤銷，包括當使用者移至不同的專案或工作性質。管理員特權只應授予給一小部分受信任的管理員。並應定期檢查許可，避免許可滲透的問題。電腦或系統帳戶應被授予完成其任務所需的最小許可集。

常見的反模式：

- 預設授予使用者管理員許可。
- 使用根使用者來處理每日活動。
- 建立過於寬鬆的政策，但不具完整的管理員權限。
- 不檢閱許可，無法確定是否符合最低權限存取權。

未建立此最佳實務時的風險暴露等級：高

實作指引

最低權限原則指出，只應允許身分執行完成特定任務所需的最小動作集。這平衡了可用性、效率和安全性。根據此原則運作有助於限制意外存取，也有助於追蹤誰有權存取哪些資源。IAM 使用者和角色在預設情況下沒有任何許可。根使用者預設擁有完整存取權，應該受到嚴格監控，並僅用於需要根存取權的任務。

IAM 政策用於明確授予許可給 IAM 角色或特定資源。例如，以身分為基礎的政策可以連接到 IAM 群組，而 S3 儲存貯體可由以資源為基礎的政策控制。

建立 IAM 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 允許或拒絕存取。AWS 支援各種條件，以協助您縮減存取權範圍。例如，透過使用 `PrincipalOrgID` 條件鍵，如果請求者不屬於您的 AWS 組織，您可以拒絕動作。

此外，您還可以使用 `CalledVia` 條件金鑰控制 AWS 服務代您發出的請求，例如建立 AWS Lambda 函數的 AWS CloudFormation。您應該將不同的政策類型分層，以便建立深度防禦並限制使用者的整體許可。您還可以限制在什麼條件下，可以授予哪些許可。例如，您可以允許應用程式團隊為他們建置的系統建立自己的 IAM 政策，但也必須同時套用許可界限來限制系統可以接受的最大許可。

實作步驟

- 實作最低權限政策：將具有最低權限的存取政策指派給 IAM 群組和角色，以反映您已定義的使用者角色或職能。
  - API 使用方式的基本政策：決定所需許可的一個方法是檢查 AWS CloudTrail 日誌。這種檢查可讓您根據使用者在 AWS 中實際執行的動作，建立適合的許可。IAM Access Analyzer 可根據活動自動產生 IAM 政策。您可以在組織或帳戶層級使用 IAM Access Advisor 來追蹤特定政策的最後存取資訊。
- 考慮使用適用於各工作性質的 AWS 受管政策。 開始建立精細的許可政策時，可能不知道從何處開始。AWS 提供常見職務的受管政策，例如帳單、資料庫管理員和資料科學家。這些政策可協助縮小使用者的存取權，同時決定如何實施最低權限政策。
- 移除不需要的許可：移除不需要的許可，並削減過於寬鬆的政策。IAM Access Analyzer 政策產生可協助微調許可政策。
- 確保使用者對生產環境具有有限的存取權：使用者應該只能存取具有有效使用案例的生產環境。在使用者執行完需要生產存取權的特定任務後，就應撤銷存取權。限制對生產環境的存取，有助於防止發生會影響生產的意外事件，也能降低意外存取的影響範圍。
- 考慮使用許可界限：許可界限是使用受管政策的功能，可設定以身分為基礎的政策可授與 IAM 實體的最大許可。實體的許可界限只允許執行其以身分為基礎的政策和許可界限同時允許的動作。

- 考慮許可的資源標籤：使用資源標籤的屬性型存取控制模型，可讓您根據資源用途、擁有者、環境或其他條件來授予存取許可。例如，您可以使用資源標籤來區分開發環境和生產環境。使用這些標籤，您可以將開發人員限制在開發環境中。結合標記和許可政策，您可以實現精細的資源存取，無需為每個工作性質定義複雜的自訂政策。
- 使用 AWS Organizations 的服務控制政策。 服務控制政策可集中控制組織中成員帳戶的最大可用許可。重要的是，服務控制政策還能讓您限制成員帳戶中的根使用者許可。此外，還可以考慮使用 AWS Control Tower，它提供規範性受管控制，可以豐富 AWS Organizations。您也可以在 Control Tower 中定義自己的控制項。
- 為您的組織制定使用者生命週期政策：使用者生命週期政策定義了當使用者上線至 AWS、變更職務或範圍或不再需要存取 AWS 時要執行的任務。應在使用者生命週期的每個步驟中進行許可審查，以驗證許可是否受到適當限制並避免許可滲透的問題。
- 建立定期檢查許可的排程，並移除任何不需要的許可：您應該定期檢查使用者存取權，確認使用者沒有過度寬鬆的存取權。AWS Config 和 IAM Access Analyzer 可以在稽核使用者許可時提供幫助。
- 建立職務矩陣：職務矩陣會以視覺化的方式顯示您 AWS 據點內所需的各種角色和存取層級。使用職務矩陣，您可以根據組織內的使用者職責定義和區分許可。使用群組，而不是將許可直接套用至個別使用者或角色。

資源

相關文件：

- 授予最低權限
- IAM 實體的許可界限
- 寫入最低權限 IAM 政策的技巧
- IAM Access Analyzer 透過根據存取活動產生 IAM 政策，來輕鬆實作最低權限許可
- 使用 IAM 許可界限，將許可管理委託給開發人員
- 使用上次存取的資訊以精簡許可
- IAM 政策類型以及何時使用這些政策
- 使用 IAM 政策模擬器測試 IAM 政策
- AWS Control Tower 中的防護機制
- 零信任架構：AWS 觀點
- 如何使用 CloudFormation StackSets 實作最低權限原則
- 屬性型存取控制 (ABAC)
- 透過查看使用者活動來縮小政策範圍

- 檢視角色存取
- 使用標記來組織環境並提高責任心
- AWS 標記策略
- 標記 AWS 資源

相關影片：

- 下一代許可管理
- 零信任：AWS 觀點
- 我如何使用許可界限，來限制使用者和角色避免權限升級？

相關範例：

- 實驗室：IAM 許可界限委派角色建立
- 實驗室：EC2 的 IAM 標籤型存取控制

SEC03-BP03 建立緊急存取程序

建立一項程序，在集中式身分提供者發生問題時，緊急存取您的工作負載。

您必須針對可能導致緊急事件發生的不同故障模式設計不同的程序。例如，正常情況下，您的員工使用者會使用集中式身分提供者 (SEC02-BP04) 聯合至雲端，以管理其工作負載。不過，如果您的集中式身分提供者發生錯誤，或是雲端中聯合的組態經過修改，則您的員工使用者可能無法連至雲端。緊急存取程序可讓授權的管理員透過替代方式 (例如聯合或直接使用者存取的替代形式) 存取您的雲端資源，以修正聯合組態或工作負載的問題。緊急存取程序會持續使用，直到恢復正常聯合機制為止。

預期成果：

- 您已定義並記載可視為緊急情況的故障模式：請考慮正常情況以及使用者用來管理工作負載的系統。考慮這些相依性如何發生錯誤並導致緊急情況。您可以在 可靠性支柱 中找到問題與最佳實務，有助於識別故障模式並架構更具彈性的系統，以盡量降低故障的可能性。
- 您已記載確認故障為緊急情況須遵循的步驟。例如，您可以要求身分管理員檢查主要和待命身分提供者的狀態，如果兩者都無法使用，則發布身分提供者發生錯誤緊急事件。
- 您已針對每一種緊急或故障模式類型定義了緊急存取程序。明確定義可減少部分使用者過度使用一般程序，來處理所有類型的緊急情況。您的緊急存取程序描述了各個程序應在何種情況下使用，以及不應在哪些情況下使用，並指出可能適用的替代程序。

- 您的程序完整記載了詳細指示和程序手冊，可快速有效地遵循。請記住，緊急事件對使用者來說可能會非常緊張，他們可能面對極大的時間壓力，因此程序的設計應盡可能簡單。

常見的反模式：

- 您沒有詳細記載且經過充分測試的緊急存取程序。您的使用者未準備好面對緊急情況，而在緊急事件發生時只能隨機應變。
- 您的緊急存取程序與正常存取機制依賴相同的系統 (例如集中式身分提供者)。這表示，一旦這類系統發生故障，就可能同時影響您的正常和緊急存取機制，並損及您從故障復原的能力。
- 您的緊急存取程序用在非緊急情況。例如，您的使用者經常濫用緊急存取程序，因為他們發現直接進行變更透過管道提交變更容易。
- 您的緊急存取程序未產生足夠的日誌來稽核程序，或是日誌未受監控，無法在發生可能濫用程序的情況時發出警示。

建立此最佳實務的優勢：

- 只要有詳細記載且經充分測試的緊急存取程序，就能縮短使用者回應和解決緊急事件所花的時間。這樣就能進一步減少停機時間，並為客戶帶來更高的服務可用性。
- 您可以追蹤每一項緊急存取請求，以及偵測未經授權的人士試圖濫用程序來處理非緊急事件的情況，並發出警示。

未建立此最佳實務時的曝險等級：中

實作指引

本節提供建立緊急存取程序的指引，用於處理與 AWS 上部署的工作負載相關的數種故障模式，一開始先介紹適用於所有故障模式的通用指引，接著再根據故障模式類型說明特定指引。

適用所有故障模式的通用指引

為故障模式設計緊急存取程序時，請考慮下列事項：

- 記載程序的前提和假設：應該和不應該使用程序的時機。這樣做有助於詳細說明故障模式並記載假設，例如其他相關系統的狀態。舉例來說，故障模式 2 的程序假設身分提供者可以使用，但 AWS 上的組態已經過修改或已過期。
- 預先建立緊急存取程序所需的資源 (SEC10-BP05)。例如，在所有工作負載帳戶中預先建立具有 IAM users 和角色的緊急存取 AWS 帳戶，以及跨帳戶 IAM 角色。這樣就可確定這些資源在緊急事件發生

時立即可用。透過預先建立資源，您就不必依賴 AWS 控制平面 API (用來建立和修改 AWS 資源)，因為它們在緊急情況下可能無法使用。此外，預先建立 IAM 資源就不需考慮 因最終一致性而可能發生的延遲。

- 請將緊急存取程序納入您的事件管理計畫當中 (SEC10-BP02)。記載緊急事件的追蹤方式，並傳達給組織中的其他人，例如同儕團隊、您的領導階層，以及適時向外傳達給您的客戶和業務合作夥伴。
- 在您現有的服務請求工作流程系統 (若有的話) 中定義緊急存取請求程序。一般來說，這類工作流程系統可讓您建立接收表單來收集有關請求的資訊、在工作流程的每個階段追蹤請求，以及新增自動和手動核准步驟。將每一個請求與事件管理系統中追蹤的對應緊急事件建立關聯。採用統一的緊急存取系統，可讓您在單一系統中追蹤這些請求、分析使用趨勢並改善程序。
- 確認您的緊急存取程序只能由經授權的使用者啟動，並且視情況要求使用者同儕或管理層的核准。核准程序在營業時間內外都要能夠有效運作。定義在主要核准者沒有空的情況下，如何由次要核准者核准請求，以及如何在您的管理鏈中向上呈報，直到請求獲得核准。
- 確認程序會同時針對成功和失敗的嘗試產生詳細的稽核日誌和事件，以便取得緊急存取權。同時監控請求程序和緊急存取機制，以偵測濫用或未經授權存取的情況。將活動與事件管理系統中正在發生的緊急事件相互關聯，並且在動作於預期時間之外發生時發出警示。例如，您應該監控緊急存取 AWS 帳戶 中的活動並發出警示，因為這不應該用於正常操作。
- 定期測試緊急存取程序，以確認步驟是否清楚，並且快速有效地授予正確的存取層級。您的緊急存取程序應在事故回應模擬的過程中 (SEC10-BP07) 和災難恢復測試中 (REL13-BP03) 進行測試。

故障模式 1：用於聯合至 AWS 的身分提供者無法使用

如 SEC02-BP04 利用集中式身分提供者中所述，我們建議您利用集中式身分提供者來聯合您的員工使用者，以授予 AWS 帳戶 的存取權。您可以使用 IAM Identity Center 聯合至您 AWS 組織中的多個 AWS 帳戶，或是使用 IAM 聯合至個別 AWS 帳戶。在這兩種情況下，員工使用者都會先透過集中式身分提供者進行身分驗證，然後才重新導向至 AWS 登入端點進行單一登入。

萬一您的集中式身分提供者無法使用，您的員工使用者就無法聯合至 AWS 帳戶 或管理其工作負載。在此緊急事件中，您可以提供緊急存取程序讓一小群管理員存取 AWS 帳戶，以便執行無法等到集中式身分提供者恢復連線後才處理的重要工作。例如，您的身分提供者停擺了 4 小時，而在此期間，您需要修改生產帳戶中 Amazon EC2 Auto Scaling 群組的上限，以處理客戶流量意外暴增的情況。您的緊急管理員應遵循緊急存取程序，才能獲得特定生產 AWS 帳戶 的存取權並進行必要的變更。

緊急存取程序依賴預先建立的緊急存取 AWS 帳戶，該帳戶單純用於緊急存取，並擁有 AWS 資源 (例如 IAM 角色和 IAM users) 可支援緊急存取程序。在正常操作期間，任何人都不應該存取緊急存取帳戶，而且您必須監控濫用此帳戶的情況並發出警示 (如需詳細資訊，請參閱前一節「通用指引」)。

緊急存取帳戶具有緊急存取 IAM 角色，有權在需要緊急存取的 AWS 帳戶 中擔任跨帳戶角色。這些 IAM 角色會預先建立並設定信任政策，以便信任緊急帳戶的 IAM 角色。

緊急存取程序可以使用下列其中一種方法：

- 您可以預先建立一組 IAM users 並包含相關的強式密碼和 MFA 權杖，以供緊急存取帳戶中的緊急管理員使用。這些 IAM users 有權承擔 IAM 角色，且後續可在需要緊急存取時跨帳戶存取 AWS 帳戶。我們建議這類使用者的數量越少越好，並且將每一位使用者指派給單一緊急管理員。在緊急情況下，緊急管理員使用者會使用其密碼和 MFA 權杖代碼登入緊急存取帳戶，切換到緊急帳戶中的緊急存取 IAM 角色，最後再切換到工作負載帳戶中的緊急存取 IAM 角色，以執行緊急變更動作。這種方法的優點是，每個 IAM user 都會指派給一名緊急管理員，而且您可以透過檢閱 CloudTrail 事件得知登入的使用者。缺點是，您必須維護多個 IAM users 及其相關聯的長期存在密碼和 MFA 權杖。
- 您可以使用緊急存取 AWS 帳戶 根使用者 來登入緊急存取帳戶、擔任緊急存取的 IAM 角色，並且在工作負載帳戶中擔任跨帳戶角色。我們建議您為根使用者設定強式密碼和多個 MFA 權杖。同時也建議您，將密碼和 MFA 權杖儲存在強制執行強式身分驗證和授權的安全企業憑證保存庫中。您應確保密碼和 MFA 權杖重設要素的安全性：將帳戶的電子郵件地址設定為受到您的雲端安全管理員監控的電子郵件分發清單，並將帳戶的電話號碼設定為同樣受到安全管理員監控的共用電話號碼。這種方法的優點是，只需管理一組根使用者憑證。缺點是，由於這是共用使用者，因此有多個管理員能夠以根使用者的身分登入。您必須稽核企業保存庫日誌事件，以確定哪個管理員簽出了根使用者密碼。

故障模式 2：AWS 上的身分提供者組態已經過修改或已過期

若要讓您的員工使用者聯合至 AWS 帳戶，您可以使用外部身分提供者設定 IAM Identity Center，或建立 IAM 身分提供者 (SEC02-BP04)。一般來說，您可以匯入身分提供者提供的 SAML 中繼資料 XML 文件來進行這些設定。中繼資料 XML 文件包含一個 X.509 憑證，對應於身分提供者用來簽署其 SAML 判斷提示的私密金鑰。

AWS 端的這些組態可能遭到管理員誤改或誤刪。另一種情況是，匯入 AWS 中的 X.509 憑證可能過期，而具有新憑證的新中繼資料 XML 尚未匯入 AWS 中。這兩種情況都可能使員工使用者的 AWS 聯合中斷，導致緊急情況發生。

在這類緊急事件中，您可以提供 AWS 的存取權給身分管理員，以修正聯合問題。例如，您的身分管理員使用緊急存取程序登入緊急存取 AWS 帳戶、切換為 Identity Center 管理員帳戶中的角色，並透過從您的身分提供者匯入最新的 SAML 中繼資料 XML 文件來更新外部身分提供者組態，以重新啟用聯合。聯合修復後，您的員工使用者繼續使用正常操作程序來聯合至其工作負載帳戶。

您可以依照先前「故障模式 1」中詳述的方法來建立緊急存取程序。您可以將最低權限許可授予身分管理員，以限制他們只能存取 Identity Center 管理員帳戶以及在該帳戶中對 Identity Center 執行動作。

故障模式 3：Identity Center 中斷

萬一發生 IAM Identity Center 或 AWS 區域 中斷的情況，建議您設定一個可用來臨時存取 AWS Management Console 的組態。

緊急存取程序會在緊急帳戶中，使用您的身分提供者對 IAM 的直接聯合。如需有關程序和設計考量的詳細資訊，請參閱 設定 AWS Management Console 的緊急存取。

實作步驟

適用所有故障模式的通用步驟

- 建立緊急存取程序專用的 AWS 帳戶。在帳戶中預先建立所需的 IAM 資源，例如 IAM 角色或 IAM users，也可以選擇建立 IAM 身分提供者。此外，在工作負載 AWS 帳戶 中預先建立跨帳戶 IAM 角色，並與緊急存取帳戶中對應的 IAM 角色建立信任關係。您可以使用 AWS CloudFormation StackSets 搭配 AWS Organizations 在組織的成員帳戶中建立此類資源。

- 建立 AWS Organizations 服務控制政策 (SCP) 以拒絕刪除和修改成員 AWS 帳戶 中的跨帳戶 IAM 角色。
- 為緊急存取 AWS 帳戶 啟用 CloudTrail，並將軌跡事件傳送到日誌收集 AWS 帳戶 中的中央 S3 儲存貯體。如果您使用 AWS Control Tower 來設定和管控您的 AWS 多帳戶環境，則您使用 AWS Control Tower 建立或在 AWS Control Tower 中註冊的每個帳戶都會預設啟用 CloudTrail，並傳送至專用日誌封存 AWS 帳戶 中的 S3 儲存貯體。
- 透過建立在主控台登入時比對的 EventBridge 規則來監控活動的緊急存取帳戶，以及透過緊急 IAM 角色監控 API 活動。當活動於事件管理系統中追蹤的持續緊急事件之外發生時，傳送通知給您的安全營運中心。

適用「故障模式 1：用於聯合至 AWS 的身分提供者無法使用」及「故障模式 2：AWS 上的身分提供者組態已經過修改或已過期」的其他步驟

- 根據您選擇的緊急存取機制預先建立資源：
  - 使用 IAM users： 預先建立 IAM users 並設定強式密碼和相關聯的 MFA 裝置。
  - 使用緊急帳戶根使用者： 設定根使用者使用強式密碼，並將密碼儲存在您的企業憑證保存庫中。將多個實體 MFA 裝置與根使用者建立關聯，並將裝置儲存在您的緊急管理員小組成員可快速存取的位置。

適用「故障模式 3：Identity Center 中斷」的其他步驟

- 如 設定 AWS Management Console 的緊急存取中所述，在緊急存取 AWS 帳戶 中，建立 IAM 身分提供者，以從您的身分提供者啟用直接 SAML 聯合。
- 在 IdP 中建立緊急操作群組，但不新增任何成員。
- 在緊急存取帳戶中建立對應於緊急操作群組的 IAM 角色。

資源

相關 Well-Architected 的最佳實務：

- SEC02-BP04 利用集中式身分提供者
- SEC03-BP02 授予最低權限存取權
- SEC10-BP02 制定事件管理計畫
- SEC10-BP07 執行演練日

相關文件：

- 設定 AWS Management Console 的緊急存取
- 讓 SAML 2.0 聯合身分使用者存取 AWS Management Console
- 緊急存取

相關影片：

- AWS re:Invent 2022 - 使用 IAM Identity Center 簡化現有的員工存取權
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) 深入剖析

相關範例：

- AWS 緊急存取角色
- AWS 客戶程序手冊架構
- AWS 事故應變程序手冊範例

SEC03-BP04 持續減少許可

在團隊確定所需的存取權時，請移除不需要的許可，並建立檢閱程序以達最低權限許可。持續監控人類和機器存取權，並移除不使用的身分和許可。

預期成果：許可政策應該遵守最低權限原則。隨著工作職責和角色的定義變得更具體，您需要檢閱許可政策以移除不必要的許可。若憑證遭到意外洩露或以其他方式在未經授權下遭存取，此方法可縮小影響範圍。

常見的反模式：

- 預設為使用者授予管理員許可。
- 建立過於寬鬆的政策，但不具完整的管理員權限。
- 保留不再需要的許可政策。

未建立此最佳實務時的風險暴露等級：中

實作指引

在團隊和專案剛開始時，可使用寬鬆的許可政策來激發創新和敏捷性。例如，在開發或測試環境中，可以讓開發人員存取廣泛的 AWS 服務。我們建議您持續評估存取權，並將存取權限於完成目前工作所需的該些服務和服務動作。我們建議對人類和機器身分進行此項評估。機器身分有時候稱為系統或服務帳戶，是提供 AWS 存取權給應用程式或伺服器的身分。此存取權在生產環境中尤為重要，因為過於寬鬆的許可可能影響廣大而且可能暴露客戶資料。

AWS 提供多種方法可幫助識別未使用的使用者、角色、許可和憑證。AWS 也有助於分析 IAM 使用者和角色的存取活動，包括相關聯的存取金鑰，以及對 AWS 資源的存取，例如 Amazon S3 儲存貯體中的物件。AWS Identity and Access Management Access Analyzer 政策產生可協助您根據某主體進行互動的實際服務和動作來建立限制性許可。屬性型存取控制 (ABAC) 可以幫助簡化許可管理，因為您可以使用使用者的屬性提供許可給他們，而不是將許可證測直接附加到每個使用者。

實作步驟

- 使用 AWS Identity and Access Management Access Analyzer：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 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 IAM 角色。
- 使用 IAM Access Analyzer 政策產生： IAM Access Analyzer 政策產生可協助您根據 IAM 使用者或角色的存取活動建立精細的許可政策。
- 為 IAM 使用者和角色確定可接受的時間範圍和使用政策：使用上次存取的時間戳記以識別未使用的使用者和角色並將其移除。檢閱服務和動作上次存取的資訊，以識別和設定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 Amazon S3 動作，並將該角色的存取權僅限於該些動作。AWS Management Console 中有提供「上次存取的資訊」功能，並且您可透過程式設計的方式將這些功能併入基礎設施工作流程和自動化工具中。

- 考慮在 AWS CloudTrail 中記錄資料事件：在預設情況下，CloudTrail 不會記錄資料事件，例如 Amazon S3 物件層級活動 (如 `GetObject` 和 `DeleteObject`) 或 Amazon DynamoDB 資料表活動 (如 `PutItem` 和 `DeleteItem`)。考慮為這些事件啟用記錄功能以確定哪些使用者和角色需要存取特定 Amazon S3 物件或 DynamoDB 資料表項目。

資源

相關文件：

- 授予最低權限
- 移除不需要的憑證
- 什麼是 AWS CloudTrail？
- 制定政策
- 記錄和監控 DynamoDB
- 為 Amazon S3 儲存貯體和物件啟用 CloudTrail 事件記錄
- 取得 AWS 帳戶的憑證報告

相關影片：

- 在 60 分鐘內精通 IAM 政策
- 責任區隔、最低權限、委派和 CI/CD
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) 深入剖析

SEC03-BP05 為您的組織定義許可防護機制

建立通用控制項，限制對組織中所有身分的存取權。比方說，您可以限制對特定 AWS 區域 的存取權，或防止操作人員刪除常見資源，例如用於中央安全團隊的 IAM 角色。

常見的反模式：

- 在組織管理員帳戶中執行工作負載。
- 在相同帳戶中執行生產和非生產工作負載。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

隨著工作負載在 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 管理那些帳戶。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分的存取權。比方說，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重要服務。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) 都遵循的控制項。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，您可以為防護機制定義例外狀況。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。

我們建議您在管理帳戶中避免執行工作負載。應使用管理帳戶來管控和部署會對成員帳戶造成影響的安全防護機制。某些 AWS 服務支援使用委派的管理員帳戶。當委派的帳戶可用時，您應使用該帳戶，而不是管理帳戶。您應嚴格限制組織管理員帳戶的存取權。

使用多帳戶策略，可讓您在將防護機制套用到工作負載時享有更大的彈性。AWS 安全性參考架構提供規範性指引，其中說明如何設計帳戶結構。AWS Control Tower 之類的 AWS 服務提供的功能，可同時集中管理組織中的預防性和偵測性控制項。清楚定義每個帳戶或組織中 OU 的用途，並根據該用途限制控制項。

資源

相關文件：

- AWS Organizations
- 服務控制政策 (SCP)
- 在多帳戶環境中充分利用服務控制政策
- AWS 安全性參考架構 (AWS SRA)

相關影片：

- 使用服務控制政策來強制執行預防性防護機制
- 使用 AWS Control Tower 大規模建立管控
- 深入探討 AWS 身分和存取管理

SEC03-BP06 根據生命週期管理存取

將存取控制與操作員和應用程式之生命週期以及集中化的聯合身分供應商相整合。例如，在使用者離職或變動職務時移除其存取權。

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)。此服務可讓您輕鬆、安全地在 AWS Organizations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。

若未建立此最佳實務，暴露的風險等級： 低

實作指引

使用者存取生命週期：為加入的新使用者、工作職能變更和離開的使用者，實作使用者存取生命週期的政策，以便只有目前的使用者擁有存取權。

資源

相關文件：

- 屬性型存取控制 (ABAC)
- 授予最低權限
- IAM Access Analyzer
- 移除不需要的登入資料
- 制定原則

相關影片：

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

SEC03-BP07 分析公有和跨帳戶存取權

持續監控突顯公有和跨帳戶存取權的發現結果。減少公有存取權和跨帳戶存取權，僅限於需要此類存取的特定資源。

預期成果：知道您共用了哪些 AWS 資源以及共用的對象。持續監控和稽核您共用的資源以確認這些資源僅與已授權主體共用。

常見的反模式：

- 沒有維持共用資源的詳細目錄。
- 未遵循程序來核准跨帳戶或資源的公有存取權。

未建立此最佳實務時的風險暴露等級：低

實作指引

如果您的帳戶位於 AWS Organizations 中，您可以將資源的存取權授予整個組織、特定組織單位或個別帳戶。如果您的帳戶不是組織的成員，您可以與個別帳戶共用資源。您可以使用以資源為基礎的政策 (例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策) 來授予直接跨帳戶存取權，或允許另一個帳戶中的主體擔任您帳戶中的 IAM 角色。當使用資源政策時，確認僅將該存取權授予已授權的主體。定義程序，來核准所有需要公開提供的資源。

AWS Identity and Access Management Access Analyzer 採用可證明的安全性來找出從其帳戶外部存取資源的所有路徑。它會持續審查資源政策，並報告公有和跨帳戶存取權的發現結果，讓您輕鬆分析潛在的各種存取。考慮使用 AWS Organizations 設定 IAM Access Analyzer，以確認您對所有帳戶具有能見度。IAM Access Analyzer 也允許您在部署資源許可之前預覽發現結果。這可讓您驗證政策變更僅授予您資源預期的公有和跨帳戶存取權。設計多帳戶存取權時，您可以使用信任政策來控制可以擔任角色的情況。例如，您可以使用 `PrincipalOrgId` 條件金鑰來拒絕嘗試從 AWS Organizations 外部擔任角色的動作。

AWS Config 可以報告設定不當的資源，並可透過 AWS Config 政策檢查來偵測已設定公開存取的資源。諸如 AWS Control Tower 和 AWS Security Hub 的服務可簡化在 AWS Organizations 間部署控制和防護機制的作業，以識別和修正公開暴露的資源。例如，AWS Control Tower 具備受管的防護機制，可偵測是否有任何可由 AWS 帳戶 還原的 Amazon EBS 快照。

實作步驟

- 考慮為 AWS Organizations 啟用 AWS Config：AWS Config 可讓您將 AWS Organizations 內來自多個帳戶的發現結果彙總到一個委派的管理員帳戶。這提供了全面性檢視並讓您在帳戶間部署 AWS Config 規則 以偵測公開可存取的資源。
- 設定 AWS Identity and Access Management Access Analyzer 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 Amazon S3 儲存貯體或 IAM 角色。

- 使用 AWS Config 中的自動矯正以回應 Amazon S3 儲存貯體的公開存取設定中的變更：您可以自動重新啟用 Amazon S3 儲存貯體的封鎖公開存取設定。
- 實作監控和警示以識別 Amazon S3 儲存貯體是否已變為公有：您必須設立監控與警示以識別何時停用 Amazon S3 封鎖公開存取，以及 Amazon S3 儲存貯體是否變為公有。此外，如果您正在使用 AWS Organizations，可以建立服務控制政策來防止對 Amazon S3 公開存取政策進行變更。AWS Trusted Advisor 會檢查具有公開存取許可的 Amazon S3 儲存貯體。將上傳或刪除存取權授予每個人的儲存貯體許可，可讓任何人在儲存貯體中新增、修改或移除項目，進而產生潛在的安全問題。Trusted Advisor 檢查會分析明確的儲存貯體許可，以及可能覆寫儲存貯體許可的相關儲存貯體政策。您也可以使用 AWS Config 來監控 Amazon S3 儲存貯體的公開存取。如需詳細資訊，請參閱如何使用 AWS Config 來監控及回應允許公開存取的 Amazon S3 儲存貯體。檢閱存取權時，請務必考慮 Amazon S3 儲存貯體中包含何種類型的資料。Amazon Macie 有助於探索和保護敏感資料，例如 PII、PHI 憑證 (如私有或 AWS 金鑰)。

資源

相關文件：

- 使用 AWS Identity and Access Management Access Analyzer
- AWS Control Tower 控制程式庫
- AWS 基礎安全最佳實務標準
- AWS Config 受管規則
- AWS Trusted Advisor 檢查參考
- 使用 Amazon EventBridge 監控 AWS Trusted Advisor 檢查結果
- 管理組織內所有帳戶間的 AWS Config 規則
- AWS Config 與 AWS Organizations

相關影片：

- 保護多帳戶環境的最佳實務
- 深入了解 IAM Access Analyzer

SEC03-BP08 在組織內安全地共用資源

隨著工作負載數量增加，您可能需要在這些工作負載內共用資源的存取權，或在多個帳戶間多次佈建資源。您可能具備劃分環境 (例如擁有開發、測試和生產環境) 的建構模組。然而，擁有分隔建構模組並

不會限制您安全共用的能力。透過共用重疊的元件，您可以降低營運負擔並允許一致的體驗，而不用猜測在多次建立相同的資源時可能錯過了什麼。

預期成果：使用安全方法在組織內共用資源，藉此充分減少意外存取，並協助您的資料外洩防護計畫。減輕與管理個別元件相較下的營運負擔，減少多次手動建立相同元件的錯誤，以及增加工作負載的可擴展性。您可以從多點失敗案例中更短的解決時間獲益，並更有信心確定何時不再需要某元件。如需有關分析外部共用的資源的規範指引，請參閱SEC03-BP07 分析公有和跨帳戶存取權。

常見的反模式：

- 缺乏可持續監控和自動發出意外外部共用通知的程序。
- 對於應該和不應該共用的內容缺乏基準。
- 預設採用廣泛的開放政策而不是在必要時明確共用。
- 必要時手動建立重疊的基礎資源。

未建立此最佳實務時的風險暴露等級：中

實作指引

建構您的存取控制和模式來管控安全地取用共用資源並只與信任的實體共用。監控共用資源並持續審查共用資源存取，在不當或意外共用時獲得警示。檢閱分析公開和跨帳戶存取權協助您確立管控能力以減少外部存取，而僅限於需要存取的資源，以及確立程序持續監控並自動提供警示。

在 AWS Organizations 內跨帳戶共用受到數個 AWS 服務的支援，例如 AWS Security Hub、Amazon GuardDuty 和 AWS Backup。這些服務允許將資料共用到中央帳戶，從中央帳戶存取，或從中央帳戶管理資源和資料。例如，AWS Security Hub 可以將發現結果從個別帳戶轉移到中央帳戶，讓您能夠檢視所有發現結果。AWS Backup 可以對資源進行備份並在帳戶之間共用。您可以使用 AWS Resource Access Manager (AWS RAM) 來共用其他常見的資源，例如 VPC 子網路和 Transit Gateway 附件、AWS Network Firewall 或 Amazon SageMaker 管道。

若要將您的帳戶限制為僅共用組織內的資源，請使用服務控制政策 (SCP) 防止存取外部主體。當共用資源時，結合身分型控制和網路控制為您的組織建立資料周邊，以幫助預防意外存取。資料周邊是一組預防性防護機制，可協助確認只有可信的身分從預期的網路存取可信的資源。這些控制項應適當限制可以共用哪些資源，並防止共用或公開不應該允許的資源。例如，做為資料周邊的一部分，您可以使用 VPC 端點政策和 `AWS:PrincipalOrgId` 條件來確保存取 Amazon S3 儲存貯體的身分屬於您的組織。需要注意的是，SCP 不適用於連結服務的角色 (LSR) 或 AWS 服務主體。

當使用 Amazon S3 時，請停用 Amazon S3 儲存貯體的 ACL 並使用 IAM 政策來定義存取控制。若要限制從 Amazon CloudFront 對 Amazon S3 原點的存取，請從原始存取身分 (OAI) 遷移至原始存取控制 (OAC)，後者支援額外的功能，包括使用 AWS Key Management Service 的伺服器端加密。

在某些情況下，您可能會想要允許在組織外部共用資源或將資源的存取權授予第三方。如需有關管理許可以在外部共用資源的規範指引，請參閱許可管理。

實作步驟

1. 使用 AWS Organizations。

   AWS Organizations 是一項帳戶管理服務，可讓您將多個 AWS 帳戶 合併至您建立且集中管理的組織中。您可以將帳戶編組成組織單位 (OU) 並將不同的政策附加到各個 OU，以協助滿足您的預算、安全和合規需求。您也可以控制 AWS 人工智慧 (AI) 和機器學習 (ML) 服務收集和儲存資料的方式，並使用與 Organizations 整合的 AWS 服務的多帳戶管理功能。

2. 整合 AWS Organizations 與 AWS 服務。

   當您啟用 AWS 服務代表您在組織的成員帳戶中執行任務時，AWS Organizations 會在每個成員帳戶中為該服務建立一個連結 IAM 服務的角色。您應該使用 AWS Management Console、AWS API 或 AWS CLI 來管理可信存取。如需有關啟用可信存取的規範指引，請參閱使用 AWS Organizations 與其他 AWS 服務以及您可以搭配 Organizations 使用的 AWS 服務。

3. 建立資料周邊。

   AWS 周邊一般表示為由 AWS Organizations 管理的組織。許多人將存取 AWS 資源與內部部署網路和系統一同視為「我的 AWS」的周邊。周邊的目標是要確認若身分可信、資源可信且是預期的網路，則允許存取。

   a. 定義並實作周邊。

      遵循《在 AWS 上建置資料周邊》白皮書的周邊實作中所述的步驟，了解各個授權條件。如需有關保護網路層的規範指引，請參閱保護網路。

   b. 持續監控與警示。

      AWS Identity and Access Management Access Analyzer 可協助您識別組織中與外部實體共用的資源。您可以將 IAM Access Analyzer 與 AWS Security Hub 整合，並將資源的發現結果從 IAM Access Analyzer 傳送並彙總到 Security Hub，以協助分析您環境的安全態勢。若要啟用整合，請在每個帳戶的每個區域中同時啟用 IAM Access Analyzer 和 Security Hub。您還可以使用 AWS Config 規則 來稽核設定，並使用 AWS Chatbot 與 AWS Security Hub 警告適當的一方。您接著可以使用 AWS Systems Manager 自動化文件來修復不合規的資源。

c. 如需有關持續監控與警示外部共用的資源的規範指引，請參閱分析公開和跨帳戶存取權。

4. 使用 AWS 服務中的資源共用並適當限制。

   許多 AWS 服務都允許您與另一個帳戶共用資源，或鎖定另一個帳戶中的資源，例如 Amazon Machine Images (AMI) and AWS Resource Access Manager (AWS RAM)。限制 `ModifyImageAttribute` API 以指定可信帳戶來共用 AMI。當使用 AWS RAM 來限制僅共用至您的組織時，指定 `ram:RequestedAllowsExternalPrincipals` 條件來協助防止不受信任的身分的存取。相關規範指引和考量，請參閱資源共用和外部目標。

5. 使用 AWS RAM 在帳戶中或與其他 AWS 帳戶 安全地共用。

   AWS RAM 可幫助您安全地將您使用帳戶中的角色和使用者所建立的資源與 AWS 帳戶 共用。在多帳戶環境中，AWS RAM 可讓您建立資源一次並與其他帳戶共用。這個方法有助於降低營運負擔，同時透過與 Amazon CloudWatch 和 AWS CloudTrail 的整合提供一致性、能見度和可稽核性，這是在使用跨帳戶存取權時所沒有的。

   如果您擁有之前使用以資源為基礎的政策共用的資源，可以使用 `PromoteResourceShareCreatedFromPolicy` API 或同等項目將資源共用升級到完整 AWS RAM 資源共用。

   在某些情況下，您可能需要採取額外步驟來共用資源。例如，要共用加密快照，您需要共用 AWS KMS 金鑰。

資源

相關的最佳實務：

- SEC03-BP07 分析公有和跨帳戶存取權
- SEC03-BP09 安全地與第三方共用資源
- SEC05-BP01 建立網路層

相關文件：

- 儲存貯體擁有者將跨帳戶許可授予非其擁有的物件
- 如何使用信任政策搭配 IAM
- 在 AWS 上建置資料周邊
- 向第三方授予對 AWS 資源的存取權限時如何使用外部 ID

- 您可以搭配 AWS Organizations 使用的 AWS 服務
- 在 AWS 上建立資料周邊：僅允許可信身分存取公司資料

相關影片：

- 使用 AWS Resource Access Manager 進行精密的存取
- 使用 VPC 端點確保資料周邊的安全
- 在 AWS 上建立資料周邊

相關工具：

- 資料周邊政策範例

SEC03-BP09 安全地與第三方共用資源

您雲端環境的安全並不止於您的組織。您的組織可能仰賴第三方來管理您的部分資料。針對第三方管理的系統的許可管理應該遵循即時存取的做法，採用最低權限的原則搭配臨時憑證。透過與第三方密切合作，您可以同時減少影響範圍以及意外存取的風險。

預期成果：只要憑證有效且作用中，任何人都可以使用與使用者相關聯的長期 AWS Identity and Access Management (IAM) 憑證、IAM 存取金鑰和機密金鑰。使用 IAM 角色和臨時憑證可透過減輕維護長期憑證的工作 (包括管理這些敏感詳細資料的營運負擔)，協助改善您的整體安全態勢。透過在 IAM 信任政策中針對外部 ID 使用通用唯一識別符，以及控制附加到 IAM 角色的 IAM 政策，您可以稽核並確認授予第三方的存取權未過於寬鬆。如需有關分析外部共用的資源的規範指引，請參閱SEC03-BP07 分析公有和跨帳戶存取權。

常見的反模式：

- 無條件地使用預設 IAM 信任政策。
- 使用 IAM 憑證和存取金鑰。
- 重複使用外部 ID。

未建立此最佳實務時的風險暴露等級：中

實作指引

您可能會想要允許在 AWS Organizations 之外共用資源或將帳戶存取權授予第三方。例如，第三方可能提供監控解決方案，而該解決方案需要存取您帳戶中的資源。在該些情況下，僅以第三方需要的權限來建立 IAM 跨帳戶角色。此外，請使用外部 ID 條件定義信任政策。當使用外部 ID 時，您或第三方可以為每個客戶、第三方或租用戶產生唯一 ID。在建立唯一 ID 後，其不應該受除了您之外的任何人控制。第三方必須實作程序，以安全、可稽核且可重新產生的方式將外部 ID 與客戶關聯。

您還可以使用 IAM Roles Anywhere 為 AWS 之外使用 AWS API 的應用程式管理 IAM 角色。

如果第三方不再需要存取您的環境，請移除該角色。避免為第三方提供長期憑證。掌握對其他支援共用的 AWS 服務的狀態。例如，AWS Well-Architected Tool 允許與其他 AWS 帳戶 共用工作負載，而 AWS Resource Access Manager 有助您安全地與其他帳戶共用您擁有的 AWS 資源。

實作步驟

1. 使用跨帳戶角色提供存取權給外部帳戶。

   跨帳戶角色可減少外部帳戶和第三方為了服務客戶所儲存的敏感資訊量。跨帳戶角色允許您在帳戶中將 AWS 資源的存取權安全地授予第三方，例如 AWS Partner 或組織內的其他帳戶，同時維持管理和稽核該存取權的能力。

   第三方可能從混合式基礎設施為您提供服務，或將資料提取至異地。IAM Roles Anywhere 可幫助您啟用第三方工作負載，以安全地與您的 AWS 工作負載進行互動，並進一步減少使用長期憑證的需要。

   您不應該使用與使用者相關聯的長期憑證或存取金鑰來提供外部帳戶存取權。反而應該使用跨帳戶角色來提供跨帳戶存取權。

2. 對第三方使用外部 ID。

   使用外部 ID 可讓您指定誰可以擔任在 IAM 信任政策中的角色。信任政策可以要求擔任該角色的使用者聲明他們操作的條件和目標，還提供方法讓客戶擁有者允許只能在特定情況下擔任角色。外部 ID 的主要功能是解決和防止混淆代理人問題。

   如果您是 AWS 帳戶 擁有者並且已為存取您的帳戶以及其他 AWS 帳戶 的第三方設定角色，或是當您代表不同客戶擔任角色時，請使用外部 ID。與您的第三方或 AWS Partner 合作建立要納入 IAM 信任政策中的外部 ID 條件。

3. 使用通用唯一外部 ID。

實作為外部 ID 產生隨機唯一值的程序，例如通用唯一識別符 (UUID)。在不同客戶間重複使用外部 ID 的第三方並不會解決混淆代理人的問題，因為客戶 A 可能能夠使用客戶 B 的角色 ARN 搭配重複的外部 ID 來檢視客戶 B 的資料。在多租用戶環境中，第三方支援使用不同 AWS 帳戶 的多個客戶，因此第三方必須為各個 AWS 帳戶 使用不同的唯一 ID 作為外部 ID。第三方負責偵測重複的外部 ID 並安全地將各個客戶對應到其個別的外部 ID。第三方應該測試以確認他們只能在指定外部 ID 時擔任該角色。在要求使用外部 ID 之前，第三方不應該儲存客戶角色 ARN 和外部 ID。

外部 ID 不會被視為機密，但外部 ID 不能是容易猜測的值，例如電話號碼、名稱或帳戶 ID。將外部 ID 設為唯讀欄位，而使外部 ID 不能為了冒充設定的目的而遭到變更。

您或第三方可以產生外部 ID。定義程序以決定由誰負責產生 ID。無論建立外部 ID 的實體為何，第三方都要在客戶間一致地強制唯一性和格式。

4. 棄用客戶提供的長期憑證。

   棄用長期憑證並使用跨帳戶角色或 IAM Roles Anywhere。如果您必須使用長期憑證，請制定計畫以遷移至角色型存取。如需有關管理金鑰的詳細資訊，請參閱身分管理。另外也與您的 AWS 帳戶 團隊和第三方合作建立風險緩解執行手冊。如需有關回應和緩解潛在安全事件的衝擊的規範指引，請參閱事件回應。

5. 確認該設定具有規範指引且已自動化。

   您的帳戶中為跨帳戶存取權建立的政策必須遵循最低權限原則。第三方必須提供角色政策文件，或使用 AWS CloudFormation 範本或對您來說同等的自動設定機制。這可減少發生與手動政策建立相關聯之錯誤的機率，並提供可稽核的記錄。如需有關使用 AWS CloudFormation 範本來建立跨帳戶角色的詳細資訊，請參閱跨帳戶角色。

   第三方應該提供自動化、可稽核的設定機制。然而，透過使用概述所需存取權的角色政策文件，您應該可自動設定角色。使用 AWS CloudFormation 範本或同等項目，您應該透過偏移偵測來監控變更，以作為稽核實務的一部份。

6. 將變更列入考量。

   您的帳戶結構、對第三方的需求或他們提供的服務方案可能發生變更。您應該預期變更和失敗，並透過合適的人員、程序和技術相應進行規劃。定期稽核您提供的存取層級，並實作偵測方法以在發生意外變更時通知您。監控和稽核角色和外部 ID 資料儲存的使用。您應該準備好在發生意外變更或存取模式時撤銷第三方存取權，無論是暫時或永久撤銷。另外，衡量撤銷作業的衝擊，包括執行所花的時間、牽涉的人員、成本，以及對其他資源的衝擊。

   如需有關偵測方法的規範指引，請參閱偵測最佳實務。

資源

相關的最佳實務：

- SEC02-BP02 使用臨時憑證
- SEC03-BP05 為您的組織定義許可防護機制
- SEC03-BP06 根據生命週期管理存取
- SEC03-BP07 分析公有和跨帳戶存取權
- SEC04 偵測

相關文件：

- 儲存貯體擁有者將跨帳戶許可授予非其擁有的物件
- 如何使用信任政策搭配 IAM 角色
- 使用 IAM 角色在 AWS 帳戶間委派存取權
- 如何使用 IAM 存取另一個 AWS 帳戶中的資源？
- IAM 中的安全最佳實務
- 跨帳戶政策評估邏輯
- 如何在向第三方授予對您的 AWS 資源的存取權時使用外部 ID
- 從在外部帳戶中使用自訂資源建立的 AWS CloudFormation 資源收集資訊
- 安全地使用外部 ID 存取其他人擁有的 AWS 帳戶
- 使用 IAM Roles Anywhere 將 IAM 角色擴展到 IAM 之外的工作負載

相關影片：

- 如何允許不同 AWS 帳戶中的使用者或角色存取我的 AWS 帳戶？
- AWS re:Invent 2018：在 60 分鐘內精通 IAM 政策
- AWS 知識中心直播：IAM 最佳實務和設計決策

相關範例：

- Well-Architected 實驗室 - Lambda 跨帳戶 IAM 角色擔任 (Level 300)
- 設定 Amazon DynamoDB 跨帳户存取權
- AWS STS 網路查詢工具

偵測

偵測由兩部分組成：偵測意外或不需要的組態變更，以及偵測意外行為。第一個部分可以發生在應用程式交付生命週期中的多個位置。使用基礎設施即程式碼 (例如，CloudFormation 範本)，您可以透過在 CI/CD 管道或來源控制中實作檢查，在部署工作負載之前檢查是否有不需要的組態。然後，將工作負載部署到非生產和生產環境時，您可以使用原生 AWS、開放原始碼或 AWS 合作夥伴工具檢查組態。這些檢查可以針對不符合安全原則或最佳實務的組態，或者針對在所測試組態和所部署組態之間進行的變更。對於執行中應用程式，您可以檢查組態是否以意外方式變更，包括在已知部署或自動擴展事件之外。

對於偵測的第二部分 (意外行為)，您可以使用工具，或在特定類型的 API 呼叫增加時發出提醒。使用 Amazon GuardDuty，您可以在您的 AWS 帳戶內發生意外且可能未經授權或惡意的活動時收到提醒。您還應該明確地監控您不期望在工作負載中使用的變異 API 呼叫，以及變更安全態勢的 API 呼叫。

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：

最佳實務

- SEC04-BP01 設定服務和應用程式記錄
- SEC04-BP02 集中分析日誌、問題清單和指標
- SEC04-BP03 自動回應事件
- SEC04-BP04 實作可採取行動的安全事件

SEC04-BP01 設定服務和應用程式記錄

保留服務和應用程式的安全事件日誌這是稽核、調查和操作使用案例的基礎原則，以及由管控、風險和合規 (GRC) 標準、政策和程序所推動的常見安全需求。

預期成果：組織應該能夠在需要執行內部程序或義務時，例如安全事件回應，以可靠且一致的方式及時從 AWS 服務和應用程式擷取安全事件日誌。考慮集中日誌以達到更佳的營運成果。

常見的反模式：

- 日誌存放太久或太早刪除。
- 每個人都能存取日誌。
- 日誌的管控和使用完全仰賴手動程序。
- 儲存每一種日誌以備不時之需。
- 只在必要時檢查日誌完整性。

建立此最佳實務的優勢：對安全事件和證據來源實作根本原因分析 (RCA) 機制，以履行管控、風險和合規義務。

未建立此最佳實務時的風險暴露等級：高

實作指引

根據您的需求進行安全調查或其他使用案例期間，您需要能夠審查相關日誌以記錄和了解該事件的全部範圍和時間表。產生警示也需要日誌，以指出特定關注的動作已發生。選擇、啟用、儲存和設定查詢與擷取機制和警示至關重要。

實作步驟

- 選擇和啟用日誌來源。 在安全調查之前，您需要擷取相關日誌以追溯的方式重新建構 AWS 帳戶 中的活動。選擇並啟用與您的工作負載相關的日誌來源。

  日誌來源選擇條件應該根據您的業務所需的使用案例。使用 AWS CloudTrail 或 AWS Organizations 線索為每個 AWS 帳戶 建立線索，以及為其設定 Amazon S3 儲存貯體。

  AWS CloudTrail 是一種記錄服務，會追蹤對 AWS 帳戶 的 API 呼叫以擷取 AWS 服務活動。預設啟用時，此服務會保留 90 天的管理活動，而其能以 AWS Management Console、AWS CLI 或 AWS SDK 透過 CloudTrail 事件歷史記錄擷取。如需較長的保留期間和資料事件的能見度，可建立 CloudTrail 線索並將其與 Amazon S3 儲存貯體建立關聯，也可以選擇與 Amazon CloudWatch 日誌群組相關聯。或者，您可以建立 CloudTrail Lake，這會將 CloudTrail 日誌保留長達七年，並提供以 SQL 為基礎的查詢設施。

  AWS 建議使用 VPC 的客戶分別使用 VPC Flow Logs 和 Amazon Route 53 解析器查詢日誌來啟用網路流量和 DNS 日誌，並將它們串流處理到 Amazon S3 儲存貯體或 CloudWatch 日誌群組。您可以為 VPC、子網路或網路介面建立 VPC 流程日誌。對於 VPC Flow Logs，您可以選擇何時何地使用 Flow Logs 來降低成本。

  AWS CloudTrail 日誌、VPC Flow Logs 和 Route 53 解析器查詢日誌是在 AWS 中支援安全調查的基本記錄來源。您還可以使用 Amazon Security Lake 以 Apache Parquet 格式和 Open Cybersecurity

Schema Framework (OCSF) 收集、正規化並儲存此日誌資料，此種格式隨時可供查詢。Security Lake 還支援其他 AWS 日誌以及來自第三方來源的日誌。

AWS 服務可產生基本日誌來源未擷取的日誌，例如 Elastic Load Balancing 日誌、AWS WAF 日誌、AWS Config 記錄器日誌、Amazon GuardDuty 發現結果、 Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌和 Amazon EC2 執行個體作業系統及應用程式日誌。如需記錄和監控選項的完整清單，請參閱《AWS 安全事件回應指南》的附錄 A：雲端功能定義 – 記錄和事件。

- 每個 AWS 服務和應用程式的研究記錄功能： 每個 AWS 服務和應用程式都為您提供日誌儲存的選項，而其各自有自己的保留和生命週期功能。兩個最常見的日誌儲存服務是 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch。如需長期保留，建議使用具成本效益和彈性生命週期功能的 Amazon S3。若主要的記錄選項是 Amazon CloudWatch 日誌，您應該考慮將較不常存取的日誌封存到 Amazon S3，作為一種選項。
- 選擇日誌儲存：日誌儲存的選擇通常與您使用的查詢工具、保留功能、熟悉度和成本有關。日誌儲存的主要選項是 Amazon S3 儲存貯體或 CloudWatch 日誌群組。

  Amazon S3 儲存貯體提供符合成本效益、耐用的儲存方式，並且具備可選擇的生命週期政策。存放在 Amazon S3 儲存貯體的日誌可使用 Amazon Athena 之類的服務進行查詢。

  CloudWatch 日誌群組透過 CloudWatch Logs Insights 提供耐用的儲存方式和內建查詢設施。
- 識別適當的日誌保留時間 ：當您使用 Amazon S3 儲存貯體或 CloudWatch 日誌群組來存放日誌時，您必須為每個日誌來源建立充分的生命週期，以最佳化儲存和擷取成本。客戶一般擁有三個月到一年的時間使日誌隨時可供查詢，並且最長可保留七年。可用性和保留時間的選擇應該配合您的安全需求與各種法令、法規和業務規定。
- 依照適當的保留和生命週期政策為每個 AWS 服務和應用程式啟用記錄功能：對於組織內的每個 AWS 服務或應用程式，尋找特定的記錄設定指引：
  - 設定 AWS CloudTrail 線索
  - 設定 VPC Flow Logs
  - 設定 Amazon GuardDuty 發現結果匯出
  - 設定 AWS Config 記錄
  - 設定 AWS WAF Web ACL 流量
  - 設定 AWS Network Firewall 網路流量日誌
  - 設定 Elastic Load Balancing 存取日誌
  - 設定 Amazon Route 53 解析器查詢日誌
  - 設定 Amazon RDS 日誌
  - 設定 Amazon EKS 控制平面日誌

  - 為 Amazon EC2 執行個體和內部部署伺服器設定 Amazon CloudWatch 代理程式
- 為日誌選擇並實作查詢機制：對於日誌查詢，您可以使用 CloudWatch Logs Insights (適用於存放在 CloudWatch 日誌群組中的資料) 以及 Amazon Athena 和 Amazon OpenSearch Service (適用於存放在 Amazon S3 中的資料)。您還可以使用第三方查詢工具，例如安全資訊和事件管理 (SIEM) 服務。

  選擇日誌查詢工具的過程中應該考慮安全營運的人員、程序和技術層面。選擇符合營運、業務和安全需求的工具，並且可供存取和長期維護。請記住，將要掃描的日誌數目維持在日誌查詢工具限制之內，以便以最佳狀態運作。因為成本或技術限制的關係，擁有多個查詢工具十分常見。

  例如，您可能使用第三方安全資訊和事件管理 (SIEM) 工具對過去 90 天的資料執行查詢，但基於 SIME 的日誌擷取成本，而使用 Athena 來執行超過 90 天的查詢。無論實作方式為何，請確認您的方法將所需的工具數量最小化以最大化營運效率，尤其是在安全事件調查期間。
- 使用日誌提供警示：AWS 透過數種安全服務提供警示功能：
  - 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 是威脅偵測服務，會持續監控惡意活動和未授權行為以保護 AWS 帳戶 和工作負載。GuardDuty 會擷取、彙總和分析來自如 AWS CloudTrail 管理和資料事件、DNS 日誌、VPC Flow Logs 和 Amazon EKS 稽核日誌等來源的資訊。GuardDuty 會直接從 CloudTrail、VPC Flow Logs、DNS 查詢日誌和 Amazon EKS 提取獨立資料串流。您不需要管理 Amazon S3 儲存貯體或修改您收集和儲存日誌的方式。仍舊建議您保留這些日誌，供自身調查和合規用途。
  - 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警示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。

  您還可以使用自訂警示產生引擎，取得這些服務未涵蓋的安全警示或與您的環境相關的特定警示。如需有關建立這些警示和偵測的資訊，請參閱《AWS 安全事件回應指南》中的偵測。

資源

相關的最佳實務：

- SEC04-BP02 集中分析日誌、問題清單和指標
- SEC07-BP04 定義資料生命週期管理
- SEC10-BP06 預先部署工具

相關文件：

- AWS 安全事件應變指南
- Amazon Security Lake 入門
- 入門：Amazon CloudWatch Logs
- 安全合作夥伴解決方案：記錄與監控

相關影片：

- AWS re:Invent 2022 - Amazon Security Lake 簡介

相關範例：

- Assisted Log Enabler for AWS
- AWS Security Hub 發現結果歷史匯出

相關工具：

- Snowflake for Cybersecurity

SEC04-BP02 集中分析日誌、問題清單和指標

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。

建立成熟的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、錯誤或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或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，也適用於從基礎設施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 AWS Identity and Access Management (IAM) 和 AWS Organizations 組態的組合來阻止執行。

Amazon GuardDuty 和 AWS Security Hub 針對也會透過其他 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。GuardDuty 會從 AWS CloudTrail 管理和資料事件、VPC DNS 日誌和 VPC 流程日誌等來源擷取、彙總和分析資訊。Security Hub 可從 GuardDuty、AWS Config、Amazon Inspector、Amazon Macie、AWS Firewall Manager，以及可在 AWS Marketplace 取得的眾多第三方安全產品擷取、彙總和分析輸出，而且如果照著建置，也會從您自己的程式碼這樣做。GuardDuty 和 Security Hub 都有管理員-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 AWS Lambda 處理器和轉寄站導入 Amazon EventBridge。

若未建立此最佳實務，暴露的風險等級： 高

實作指引

- 評估日誌處理能力：評估可用於處理日誌的選項。
  - 使用 Amazon OpenSearch Service 記錄和監控 (幾乎) 一切
  - 尋找一個專門從事記錄和監控解決方案的合作夥伴
- 若要開始分析 CloudTrail 日誌，請測試 Amazon Athena。
  - 設定 Athena 來分析 CloudTrail 日誌
- 在 AWS 中實作集中記錄：請參閱下列 AWS 範例解決方案，來集中多個來源記錄。
  - 將記錄解決方案集中化
- 透過合作夥伴實作集中記錄：APN 合作夥伴提供的解決方案可協助您集中分析日誌。
  - 記錄和監控

資源

相關文件：

- AWS Answers：集中式記錄
- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge
- 入門：Amazon CloudWatch Logs
- 安全合作夥伴解決方案：記錄與監控

相關影片：

- 集中監控資源組態與合規
- 修補 Amazon GuardDuty 和 AWS Security Hub 發現結果
- 雲端中的威脅管理：Amazon GuardDuty 和 AWS Security Hub

SEC04-BP03 自動回應事件

使用自動化來調查和修復事件可減少人工作業和人為錯誤，還可讓您擴展調查功能。定期檢閱將協助您調整自動化工具並持續反覆運算。

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 AWS CloudTrail 事件) 以及您可從應用程式產生的自訂事件。Amazon GuardDuty 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 (AWS 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。

也可以偵測變更，並將此資訊路由到正確的工作流程，方法為使用 AWS Config 規則 和 合規套件。AWS Config 偵測範圍內服務的變更 (但延遲比 EventBridge 高)，並產生可使用 AWS Config 規則剖析的事件，用於還原、執行合規政策以及將資訊轉發到系統 (例如變更管理平台和營運票證系統)。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 規則 開發套件和開放原始碼庫 AWS Config 規則。合規套件是 AWS Config 規則 和修補動作的集合，其會部署為以 YAML 範本撰寫的單一實體。路由層 範例合規套件範本 適用於 Well-Architected 安全支柱。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

- 使用 GuardDuty 實作自動提醒：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。啟用 GuardDuty 並設定自動提醒。
- 自動化調查程序：開發可調查事件並向管理員報告相關資訊的自動化程序，以節省時間。
  - 實驗室：Amazon GuardDuty 實作

資源

相關文件：

- AWS Answers：集中式記錄

- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge
- 入門：Amazon CloudWatch Logs
- 安全合作夥伴解決方案：記錄與監控
- 設定 Amazon GuardDuty

相關影片：

- 集中監控資源組態與合規
- 修補 Amazon GuardDuty 和 AWS Security Hub 發現結果
- 雲端中的威脅管理：Amazon GuardDuty 和 AWS Security Hub

相關範例：

- 實驗室：偵測控制的自動部署

SEC04-BP04 實作可採取行動的安全事件

建立傳送給團隊並能讓團隊據此採取行動的提醒。確保提醒包含讓團隊採取動作的相關資訊。對於您擁有的每個偵測機制，您也應該設置一套程序 (採取 執行手冊 或 程序手冊的形式) 以進行調查。例如，當您啟用 Amazon GuardDuty時，就會產生不同的 發現結果。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 ，您的執行手冊會有簡單的指示，指示某人進行調查和修復。

若未建立此最佳實務，暴露的風險等級為： 低

實作指引

- 探索 AWS 服務可用的指標：針對您所使用的服務，探索透過 Amazon CloudWatch 提供的指標。
  - AWS 服務文件
  - 使用 Amazon CloudWatch 指標
- 設定 Amazon CloudWatch 警示。
  - 使用 Amazon CloudWatch 警示

資源

相關文件：

- Amazon CloudWatch
- Amazon EventBridge
- 安全合作夥伴解決方案：記錄與監控

相關影片：

- 集中監控資源組態與合規
- 修補 Amazon GuardDuty 和 AWS Security Hub 發現結果
- 雲端中的威脅管理：Amazon GuardDuty 和 AWS Security Hub

基礎設施保護

基礎設施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。

基礎設施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)。

區域、可用區域、AWS Local Zones 和 AWS Outposts

確定您熟悉區域、可用區域、AWS Local Zones和 AWS Outposts，這些都是 AWS 安全全球基礎設施的元件。

AWS 具有區域概念，它是我們在全世界將資料中心叢集化的實體位置。我們會將邏輯資料中心的每個群組稱為可用區域 (AZ)。每個 AWS 區域由地理區域內多個隔離且實際上分開的 AZ 組成。如果您有資料落地要求，則可以選擇靠近您所需位置的 AWS 區域。您保留對資料實際所在區域的完全控制和擁有權，這有助於符合您的區域合規和資料落地要求。每個 AZ 都有獨立的電源、冷卻和實體安全性。如果應用程式跨 AZ 分割，則您可以獲得更好的隔離和保護，讓您免於停電、雷擊、龍捲風、地震等問題。AZ 與任何其他 AZ 實際上相距一段有意義的距離 (數公里)，但它們彼此的距離都在 100 公里 (60 英里) 內。AWS 區域中的所有 AZ 都是使用完全冗餘的專用都會光纖 (在 AZ 之間提供高輸送量、低延遲網路)，搭配高頻寬、低延遲網路來互連。AZ 之間的所有流量都是加密的。專注於高可用性的 AWS 客戶可以將其應用程式設計為在多個 AZ 中執行，以實現更高的容錯。AWS 區域符合最高階的安全性、合規和資料保護。

AWS 將運算、儲存、資料庫和其他精選 AWS 服務置於更靠近最終使用者的位置。使用 AWS Local Zones，您可以輕鬆執行要求最終使用者十毫秒延遲的高要求應用程式，例如媒體和娛樂內容創作、即時遊戲、水庫模擬、電子設計自動化和機器學習。每個 AWS Local Zone 位置都是 AWS 區域的延伸，您可以在其中執行對延遲敏感的應用程式，方法為使用地理上接近最終使用者的 Amazon EC2、Amazon VPC、Amazon EBS、Amazon File Storage 和 Elastic Load Balancing 等 AWS 服務。AWS Local Zones 會提供高頻寬、保護本機工作負載與在 AWS 區域中執行的工作負載之間的連線，進而允許您透過相同的 API 和工具集無縫連線到各種區域內服務。

AWS Outposts 將原生 AWS 服務、基礎設施和營運模式帶到幾乎任何資料中心、主機代管空間或內部部署設施。您可以跨內部部署設施和 AWS 雲端使用相同的 AWS API、工具和基礎設施，以提供真正一致的混合體驗。AWS Outposts 專為連線環境而設計，而且可以用來支援由於低延遲或本機資料處理需求而必須保留在內部部署的工作負載。

在 AWS 中，有多種方法可用於基礎設施保護。以下幾節介紹如何使用這些方法。

主題

保護網路

您的員工和客戶中的使用者可以位於任何地方。您需要從傳統模式轉變，這些模式信任可以存取您網路的任何人和任何事物。當您遵循在所有層套用安全性的原則時，您可以使用 零信任 方法。零信任安全是一種模型，其中應用程式元件或微型服務被認為是彼此獨立的，並且沒有任何元件或微型服務信任彼此。

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。如需有關 Web 應用程式後端的建議，請參閱 AWS Well-Architected 無伺服器應用程式聚焦 。

最佳實務

SEC05-BP01 建立網路層

將具有共同敏感度需求的元件編組成不同層，以盡可能縮小未授權存取的潛在影響範圍。例如：不需存取網際網路的虛擬私有雲端 (VPC) 中的資料庫叢集，應放置在沒有往返網際網路路由的子網路中。流量應該流自鄰接的下一個最不敏感的資源。考慮負載平衡器背後的 Web 應用程式。您的資料庫不應該直接從負載平衡器存取，只有商業邏輯或 Web 伺服器能夠直接存取資料庫。

預期成果：建立分層網路。分層網路有助於以邏輯方式編組相似的網路元件，並且可縮小未授權網路存取的潛在影響範圍。適當分層的網路可使未授權使用者更難轉移到 AWS 環境內的其他資源。除了保護內部網路路徑之外，您也應該保護網路邊緣，例如 Web 應用程式和 API 端點。

常見的反模式：

- 將所有資源建立在單一 VPC 或子網路中。
- 使用過於寬鬆的安全群組。
- 未使用子網路。
- 允許直接存取資料存放區，例如資料庫。

未建立此最佳實務時的風險暴露等級：高

實作指引

Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Relational Database Service (Amazon RDS) 資料庫叢集等元件，以及具有共同連線能力需求的 AWS Lambda 函數可分成子網路所組成的層級。考慮將無伺服器工作負載，例如 Lambda 函數，部署在 VPC 內或 Amazon API Gateway 背後。無須網際網路存取權的 AWS Fargate (Fargate) 任務應該放置在沒有往返網際網路路由的子網路中。此分層方法可減輕單層組態錯誤所造成的影響，此類錯誤可能允許意外存取。對於 AWS Lambda，您可以在 VPC 中執行函數，以利用 VPC 型控制。

對於可能包含數千個 VPC、AWS 帳戶 和內部部署網路的網路連線，您應該使用 AWS Transit Gateway。Transit Gateway 可做為中樞，就像輪輻般控制流量在所有連線網路間路由的方式。Amazon Virtual Private Cloud (Amazon VPC) 與 Transit Gateway 之間的流量會保留在 AWS 私有網路上，如此可減少對外暴露於未授權使用者和潛在的安全問題。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。

實作步驟

- 使用 Reachability Analyzer 根據組態來分析來源與目標之間的路徑：Reachability Analyzer 可讓您自動驗證 VPC 連線資源之間的連線能力。請注意，此分析是透過審查組態 (進行分析時不會傳送任何網路封包) 完成的。
- 使用 Amazon VPC 網路存取分析器來識別對資源的意外網路存取：Amazon VPC 網路存取分析器可讓您指定網路存取需求並識別潛在的網路路徑。
- 考慮是否需要將資源置於公有子網路中：請勿將資源置於 VPC 的公有子網路中，除非它們絕對必須從公開來源接收傳入網路流量。
- 在 VPC 中建立子網路：為每個網路層建立子網路 (在包含多個可用區域的群組中) 以增強微分段。另外也確認您已將正確的路由表與您的子網路相關聯，以控制路由和網際網路連線能力。
- 使用 AWS Firewall Manager 來管理您的 VPC 安全群組：AWS Firewall Manager 有助於減輕使用多個安全群組的管理負擔。
- 使用 AWS WAF 來防範常見的網路漏洞：AWS WAF 可透過檢查常見網路漏洞的流量，例如 SQL 隱碼攻擊，幫助加強邊緣安全。它還可讓您限制源自特定國家或地理位置的 IP 地址的流量。

- 使用 Amazon CloudFront 作為內容交付網路 (CDN)：Amazon CloudFront 可透過將資料存放在更靠近使用者的地方而協助加快 Web 應用程式的速度。它還能強制 HTTPS、限制對地理區域的存取，以及確保網路流量僅能在經由 CloudFront 時存取資源，來提升邊緣安全。
- 當建立應用程式設計介面 (API) 時使用 Amazon API Gateway：Amazon API Gateway 有助於發佈、監控和保護 REST、HTTPS 和 WebSocket API。

資源

相關文件：

- AWS Firewall Manager
- Amazon Inspector
- Amazon VPC 安全性
- Reachability Analyzer
- Amazon VPC 網路存取分析器

相關影片：

- 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
- AWS re:Inforce 2022 - 在 AWS 上驗證有效的網路存取控制
- AWS re:Inforce 2022 - 使用 AWS WAF 抵禦機器人的進階保護

相關範例：

- Well-Architected 實驗室 - 自動化 VPC 的部署
- 研討會：Amazon VPC 網路存取分析器

SEC05-BP02 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、Amazon Relational Database Service (Amazon 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 Amazon Elastic Compute Cloud (Amazon 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。

有些 AWS 服務會要求元件存取網際網路以進行 API 呼叫，其中 AWS API 端點 所在位置。其他 AWS 服務會使用 VPC 端點 (在您的 Amazon VPC 內)。許多 AWS 服務 (包括 Amazon S3 和 Amazon DynamoDB) 都支援 VPC 端點，而這項技術已廣泛應用於 AWS PrivateLink。我們建議您使用此方法安全地存取 AWS 服務、第三方服務，以及您在其他 VPC 中託管的專屬服務。AWS PrivateLink 上的所有網路流量都停留在全球 AWS 骨幹網路上，而且永遠不會周遊網際網路。連線只能由服務的消費者啟動，而不能由服務的供應商啟動。使用 AWS PrivateLink 進行外部服務存取可讓您建立沒有網際網路存取的氣隙 VPC，並協助保護您的 VPC 免於外部威脅向量的攻擊。第三方服務可以使用 AWS PrivateLink，允許其客戶透過私有 IP 地址從其 VPC 連線到服務。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)。

若未建立此最佳實務，暴露的風險等級： 高

實作指引

- 控制 VPC 中的網路流量：實作 VPC 最佳實務來控制流量。
  - Amazon VPC 安全性
  - VPC 端點
  - Amazon VPC 安全群組
  - 網路 ACL
- 控制邊緣的流量：實作 Amazon CloudFront 等邊緣服務，以提供多一層的保護和其他功能。
  - Amazon CloudFront 使用案例
  - AWS Global Accelerator
  - AWS Web 應用程式防火牆 (AWS WAF)

  - Amazon Route 53
  - Amazon VPC 輸入路由
- 控制私有網路流量：實作可保護工作負載私有流量的服務。
  - Amazon VPC 對等互連
  - Amazon VPC 端點服務 (AWS PrivateLink)
  - Amazon VPC Transit Gateway
  - AWS Direct Connect
  - AWS 站點對站點 VPN
  - AWS Client VPN
  - Amazon S3 存取點

資源

相關文件：

- AWS Firewall Manager
- Amazon Inspector
- AWS WAF 入門

相關影片：

- 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

相關範例：

- 實驗室：VPC 的自動部署

SEC05-BP03 自動化網路保護

自動化保護機制，以借助威脅情報和異常偵測提供自衛網路。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，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。

若未建立此最佳實務，暴露的風險等級為： 中

實作指引

- 針對以網頁為基礎的流量進行自動保護：AWS 提供的解決方案使用 AWS CloudFormation 自動部署一組 AWS WAF 規則，專門用於篩選常見網頁式攻擊。使用者可從預先設定的保護功能中進行選擇，以定義 AWS WAF Web 存取控制清單 (web ACL) 中包含的規則。
  - AWS WAF 安全自動化
- 考慮 AWS Partner 解決方案：AWS 合作夥伴提供數百種領先業界的產品，這些產品與您內部部署環境中的現有控制項相當、相同或互相整合。這些產品可補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境中部署全方位的安全架構，以及擁有更流暢的體驗。
  - 基礎設施安全

資源

相關文件：

- AWS Firewall Manager
- Amazon Inspector
- Amazon VPC 安全性
- AWS WAF 入門

相關影片：

- 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

相關範例：

- 實驗室：VPC 的自動部署

SEC05-BP04 實作檢查和保護

檢查和篩選每個層級的流量。為了檢查您的 VPC 組態並找出潛在的意外存取，您可以使用 VPC Network Access Analyzer。您可以指定您的網路存取要求，並識別未符合它們的潛在網路路徑。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。若要開始使用 AWS WAF，您可以將 AWS 受管規則 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。Firewall Manager 也會使用 AWS Network Firewall。AWS Network Firewall 是一種託管服務，其會使用規則引擎，讓您精細控制有狀態和無狀態網路流量。它支援 Suricata 相容的 開放原始碼入侵防禦系統 (IPS) 規格，供規則用來協助保護您的工作負載。

若未建立此最佳實務，暴露的風險等級為： 低

實作指引

- 設定 Amazon GuardDuty：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。啟用 GuardDuty 並設定自動提醒。
  - Amazon GuardDuty
  - 實驗室：偵測控制的自動部署
- 設定虛擬私有雲端 (VPC) 流程日誌：VPC 流程日誌讓您可以擷取有關往返 VPC 網路界面 IP 流量的資訊。流程日誌資料可以發佈至 Amazon CloudWatch Logs 和 Amazon Simple Storage Service (Amazon S3)。建立流程日誌後，您可以在選定的目標位置擷取和檢視其資料。
- 考慮 VPC 流量鏡像化：流量鏡像化是一項 Amazon VPC 功能，可用來從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的彈性網路界面複製網路流量，然後將流量傳送到頻外安全與監控設備，以進行內容檢查、威脅監控和故障排除。
  - VPC 流量鏡像化

資源

相關文件：

- AWS Firewall Manager
- Amazon Inspector
- Amazon VPC 安全性
- AWS WAF 入門

相關影片：

- 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

相關範例：

- 實驗室：VPC 的自動部署

保護運算

運算資源包括 EC2 執行個體、容器、AWS Lambda 函數、資料庫服務、IoT 裝置等。這些運算資源類型中的每一種都需要不同的方法來保護它們。不過，它們確實分享您需要考慮的常用策略：深度防禦、漏洞管理、減少受攻擊面、組態和操作的自動化，以及遠距離執行動作。在本節中，您將找到有關保護關鍵服務之運算資源的一般指引。對於使用的每項 AWS 服務，請您務必檢查服務文件中的特定安全建議。

最佳實務

- SEC06-BP01 執行漏洞管理
- SEC06-BP02 減少受攻擊面
- SEC06-BP03 實作受管服務
- SEC06-BP04 自動化運算保護
- SEC06-BP05 讓人員能夠遠距離執行動作
- SEC06-BP06 驗證軟體完整性

SEC06-BP01 執行漏洞管理

經常掃描和修補程式碼、相依性和基礎設施中的漏洞，以協助防禦新的威脅。

預期成果：建立和維護漏洞管理計畫。定期掃描和修補資源，例如 Amazon EC2 執行個體、Amazon Elastic Container Service (Amazon ECS) 容器和 Amazon Elastic Kubernetes Service (Amazon EKS) 工作負載。設定 AWS 受管資源的維護時段，例如 Amazon Relational Database Service (Amazon RDS) 資料庫。使用靜態程式碼掃描來檢查應用程式原始程式碼的常見問題。如果您的組織具有必備技能或是可以雇用外部協助，請考慮 Web 應用程式滲透測試。

常見的反模式：

- 沒有漏洞管理計畫。
- 執行系統修補而不考慮嚴重性或避免風險。
- 使用已過廠商提供的結束生命週期日期的軟體。
- 在分析程式碼的安全問題之前將其部署至生產環境。

建立此最佳實務的優勢：

未建立此最佳實務時的風險暴露等級：高

實作指引

漏洞管理計畫包括安全評定、識別問題、排定優先順序，以及執行修補作業做為解決問題的一部分。持續掃描工作負載，以發現問題和意外網路暴露並執行修正，自動化是關鍵。自動建立和更新資源可節省時間並降低組態錯誤造成進一步問題的風險。設計良好的漏洞管理計畫也應該考慮在軟體生命週期的開發和部署階段進行漏洞測試。在開發和部署期間實作漏洞管理有助於降低漏洞能夠滲入生產環境的可能性。

實作漏洞管理計畫需要對 AWS 共同責任模式有良好的了解，以及它如何與特定工作負載相關。在共同責任模式下，AWS 負責保護 AWS 雲端 的基礎設施。此基礎設施是由硬體、軟體、網路以及執行 AWS 雲端 服務的設施所組成。您負責雲端中的安全，例如實際的資料、安全組態和 Amazon EC2 執行個體的管理工作，以及確認您的 Amazon S3 物件已適當分類和設定。您著手漏洞管理的方法也可能視取用的服務而異。例如，AWS 會管理修補我們受管的關聯式資料庫服務 Amazon RDS，但是您須負責修補自我託管的資料庫。

AWS 擁有可協助您漏洞管理計畫的各種服務。Amazon Inspector 會持續掃描 AWS 工作負載以發現軟體問題和意外的網路存取。AWS Systems Manager Patch Manager 可協助管理 Amazon EC2 執行個體間的修補工作。Amazon Inspector 和 Systems Manager 可供在 AWS Security Hub 中檢視，其是一項雲端安全狀態管理服務，可協助自動化 AWS 安全檢查並集中化安全警示。

Amazon CodeGuru 可協助使用靜態程式碼分析來識別 Java 和 Python 應用程式中的潛在問題。

實作步驟

- 設定 Amazon Inspector：Amazon Inspector 會自動偵測新啟動的 Amazon EC2 執行個體、Lambda 函數和推送到 Amazon ECR 的合格容器映像，並即刻掃描軟體以發現問題、潛在瑕疵和意外的網路暴露。
- 掃描原始碼：掃描程式庫和相依性的問題和瑕疵。Amazon CodeGuru 可以掃描並提供建議來修正 Java 和 Python 應用程式的常見安全問題。OWASP Foundation 發佈了一份原始程式碼分析工具 (也稱為 SAST 工具) 的清單。

- 實作機制以掃描和修補現有環境，並將掃描實作為 CI/CD 管道建置過程的一部分：實作機制來掃描和修補相依性和作業系統中的問題，以協助抵禦新威脅。定期執行該機制。了解您需要在何處套用修補或解決軟體問題，軟體漏洞管理必不可少。透過儘早將漏洞評定嵌入持續整合/持續交付 (CI/CD) 管道，優先修正潛在的安全問題。您的方法可能視您取用的 AWS 服務而異。要檢查在 Amazon EC2 執行個體中執行的軟體的潛在問題，請將 Amazon Inspector 新增到您的管道，在偵測到問題或潛在瑕疵時通知您並停止建置程序。Amazon Inspector 會持續監控資源。您也可以使用開放原始碼產品，例如 OWASP Dependency-Check、Snyk、OpenVAS、封裝管理員和 AWS Partner 工具來進行漏洞管理。
- 使用 AWS Systems Manager：您負責對您的 AWS 資源進行修補程式管理，包括 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Machine Image (AMI) 和其他運算資源。AWS Systems Manager Patch Manager 可自動化透過安全相關及其他更新來修補受管執行個體的流程。您可以使用 Patch Manager 在 Amazon EC2 執行個體上針對作業系統和應用程式套用修補程式，包括 Microsoft 應用程式、Windows Service Pack 和 Linux 型執行個體的次要版本更新。除了 Amazon EC2 之外，Patch Manager 也可以用來修補內部部署伺服器。

  如需支援的作業系統清單，請參閱《Systems Manager 使用者指南》中的受支援作業系統。您可以掃描執行個體而只查看修補程式缺失報告，也可以掃描並自動安裝所有缺失的修補程式。
- 使用 AWS Security Hub：Security Hub 為您在 AWS 中的安全狀態提供全方位檢視。它會收集多個 AWS 服務間的安全資料，並以標準格式提供該些發現結果，讓您能夠跨 AWS 服務排定安全發現結果的優先順序。
- 使用 AWS CloudFormation：AWS CloudFormation 是基礎設施即程式碼 (IaC) 服務，可透過在多個帳戶和環境間自動化資源部署和標準化資源架構，來協助漏洞管理。

資源

相關文件：

- AWS Systems Manager
- AWS Lambda 的安全概觀
- Amazon CodeGuru
- 透過全新的 Amazon Inspector 改進、自動化雲端工作負載的漏洞管理
- 使用 Amazon Inspector 和 AWS Systems Manager 自動化 AWS 中的漏洞管理和矯正 – 第 1 部分

相關影片：

- 保護無伺服器和容器服務的安全

- Amazon EC2 執行個體中繼資料服務的安全最佳實務

SEC06-BP02 減少受攻擊面

透過強化作業系統以及盡量減少使用中的元件、程式庫和外部消耗性服務，來減少意外存取。首先減少未使用的元件，無論它們是作業系統套件或應用程式 (適用於 Amazon Elastic Compute Cloud (Amazon EC2) 型工作負載) 或程式碼中的外部軟體模組 (適用於所有工作負載)。對於常見的作業系統和伺服器軟體，您可以找到許多強化和安全組態指南。例如，您可以從 Center for Internet Security 開始並反覆。

在 Amazon EC2 中，您可以建立自己的 Amazon Machine Image (AMI)，並已對其進行修補和強化，以協助您符合組織的特定安全要求。您在 AMI 上套用的修補程式和其他安全控制，在建立它們的時間點有效—它們不是動態的，除非您在啟動後進行修改，例如，使用 AWS Systems Manager 進行此修改。

您可以使用 EC2 Image Builder 簡化建置安全 AMI 的程序。EC2 Image Builder 會大幅地減少建立和維護黃金映像所需的工作量，而不會編寫和維護自動化。當軟體更新可用時，Image Builder 會自動產生新映像，而無需用戶手動啟動映像構置。EC2 Image Builder 可讓您在生產環境中使用您的映像，搭配 AWS 提供的測試和您自己的測試之前，輕鬆地驗證這些映像的功能和安全性。您也可以套用 AWS 提供的安全設定，以進一步保護您的映像，來符合內部安全準則。例，您可以使用 AWS 提供的範本，產生符合安全技術實作指南 (STIG) 標準的映像。

使用第三方靜態程式碼分析工具，您可以識別常見的安全問題，例如未檢查的函數輸入界限，以及適用的常見漏洞和披露 (CVE)。您可以使用 Amazon CodeGuru 取得支援的語言。相依性檢查工具也可以用來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 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 Image Builder 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 影像掃描 ，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。

若未建立此最佳實務，暴露的風險等級為： 高

實作指引

- 強化作業系統：設定作業系統以符合最佳實務。
  - 保護 Amazon Linux
  - 保護 Microsoft Windows Server
- 強化容器化資源：設定容器化資源以符合安全最佳實務。
- 實作 AWS Lambda 最佳實務。
  - AWS Lambda 最佳實務

資源

相關文件：

- AWS Systems Manager
- 將堡壘主機取代為 Amazon EC2 Systems Manager
- AWS Lambda 的安全概觀

相關影片：

- 在 Amazon EKS 上執行高安全的工作負載
- 保護無伺服器和容器服務的安全
- Amazon EC2 執行個體中繼資料服務的安全最佳實務

相關範例：

- 實驗室：Web 應用程式防火牆的自動部署

SEC06-BP03 實作受管服務

實作管理資源的服務 (例如 Amazon Relational Database Service (Amazon RDS)、AWS Lambda 和 Amazon Elastic Container Service (Amazon ECS))，能為您減少共同責任模式中的安全維護任務。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 Framework 中所述的其他方式來保護應用程式。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，無須擔心基礎設施或作業系統。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

- 探索可用的服務：探索、測試和實作可管理資源的服務，例如 Amazon RDS、AWS Lambda 和 Amazon ECS。

資源

相關文件：

- AWS 網站
- AWS Systems Manager
- 將堡壘主機取代為 Amazon EC2 Systems Manager
- AWS Lambda 的安全概觀

相關影片：

- 在 Amazon EKS 上執行高安全的工作負載
- 保護無伺服器和容器服務的安全
- Amazon EC2 執行個體中繼資料服務的安全最佳實務

相關範例：

- 實驗室：AWS Certificate Manager 請求公有憑證

SEC06-BP04 自動化運算保護

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。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

- 自動化組態管理：透過使用組態管理服務或工具，來自動執行和驗證安全組態。
  - AWS Systems Manager

  - AWS CloudFormation
  - 實驗室：VPC 的自動部署
  - 實驗室：EC2 Web 應用程式的自動部署

- 自動修補 Amazon Elastic Compute Cloud (Amazon EC2)：AWS Systems Manager 修補程式管理員可將管理執行個體在安全相關與其他類型方面的更新修補過程自動化。您可以使用修補程式管理員為作業系統和應用程式套用修補程式。
  - AWS Systems Manager Patch Manager
  - 使用 AWS Systems Manager 自動化進行集中式多帳戶和多區域修補

- 實作入侵偵測和預防：實作入侵偵測和預防工具，以監控和阻止執行個體上的惡意活動。
- 考慮 AWS Partner 解決方案：AWS 合作夥伴提供數百種領先業界的產品，這些產品與您內部部署環境中的現有控制項相當、相同或互相整合。這些產品可補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境中部署全方位的安全架構，以及擁有更流暢的體驗。
  - 基礎設施安全

資源

相關文件：

- AWS CloudFormation
- AWS Systems Manager
- AWS Systems Manager Patch Manager
- 使用 AWS Systems Manager 自動化進行集中式多帳戶和多區域修補
- 基礎設施安全
- 將堡壘主機取代為 Amazon EC2 Systems Manager
- AWS Lambda 的安全概觀

相關影片：

- 在 Amazon EKS 上執行高安全的工作負載
- 保護無伺服器和容器服務的安全
- Amazon EC2 執行個體中繼資料服務的安全最佳實務

相關範例：

- 實驗室：Web 應用程式防火牆的自動部署
- 實驗室：EC2 Web 應用程式的自動部署

SEC06-BP05 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，使用變更管理工作流程，以利用基礎設施即程式碼來部署 Amazon Elastic Compute Cloud (Amazon EC2)，然後 AWS Systems Manager 這類工具來管理 Amazon 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 可以使用 自動化 工作流程，文件 (程序手冊) 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，而且可為您將基礎設施的部署和管理任務自動化，無須直接使用 AWS Management Console或 API。

若未建立此最佳實務，暴露的風險等級： 低

實作指引

- 取代主控台存取：以 AWS Systems Manager Run Command 取代執行個體的主控台存取 (SSH 或 RDP)，以自動化管理任務。

- AWS Systems Manager Run Command

資源

相關文件：

- AWS Systems Manager
- AWS Systems Manager Run Command
- 將堡壘主機取代為 Amazon EC2 Systems Manager
- AWS Lambda 的安全概觀

相關影片：

- 在 Amazon EKS 上執行高安全的工作負載
- 保護無伺服器和容器服務的安全

- Amazon EC2 執行個體中繼資料服務的安全最佳實務

相關範例：

- 實驗室：Web 應用程式防火牆的自動部署

SEC06-BP06 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，確保它們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。AWS Signer 可以集中管理程式碼簽署生命週期 (包括簽署認證和公有和私有金鑰) 來協助確保程式碼的信任和完整性。您可以了解如何使用進階模式和最佳實務，搭配下列項目進行程式碼簽署： AWS Lambda。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。

若未建立此最佳實務，暴露的風險等級： 低

實作指引

- 調查機制：程式碼簽署是用來驗證軟體完整性的一種機制。
  - NIST：程式碼簽署的安全考量

資源

相關文件：

- AWS Signer
- 新增功能 – 程式碼簽署，AWS Lambda 的信任和完整性控制

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。

主題

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。

最佳實務

SEC07-BP01 識別工作負載內的資料

了解您的工作負載正在處理的資料類型和分類、相關聯的業務流程、資料存放在何處以及誰是資料擁有者至關重要。您也應該了解工作負載的適用法律和合規要求，以及需要強制何種資料控制。識別資料是資料分類歷程的第一步。

建立此最佳實務的優勢：

資料分類可讓工作負載擁有者識別存放敏感資料的位置，並決定應該如何存取和共用該資料。

資料分類旨在回答以下問題：

- 您擁有何種類型的資料？

  這可能是如下資料：

  - 智慧財產權 (IP)，例如交易機密、專利或合約協議。
  - 受保護醫療資訊 (PHI)，例如包含與個人相關之醫療歷史資訊的醫療記錄。
  - 個人身分識別資訊 (PII)，例如姓名、地址、出生日期和國民身分證號碼或登記號碼。
  - 信用卡資料，例如主要帳號 (PAN)、持卡人姓名、到期日和服務碼編號。
  - 敏感資料存放於何處？
  - 誰能夠存取、修改和刪除資料？
  - 了解使用者許可對於防止資料可能遭到不當處理必不可少。
- 誰能夠執行建立、讀取、更新和刪除 (CRUD) 操作？
  - 了解誰能夠管理對資料的許可，藉以考量潛在的權限提升。
- 如果資料遭到意外洩露、更改或刪除，可能會導致何種業務影響？
  - 了解若資料遭到修改、刪除或意外洩露的風險後果。

透過知道這些問題的答案，您可以採取以下動作：

- 縮小敏感資料的範圍 (例如敏感資料的位置數量)，以及將對敏感資料的存取僅限為核准使用者。
- 了解不同的資料類型，以便實作適當的資料保護機制和方法，例如加密、資料外洩防護，以及身分和存取管理。
- 針對資料達到適當的控制目標以優化成本。
- 有信心地回答監管機構和稽核人員關於資料類型和數量，以及如何區隔不同敏感度的資料的問題。

未建立此最佳實務時的風險暴露等級：高

實作指引

資料分類是識別資料敏感度的行動，當中可能牽涉標記，使資料方便搜尋和追蹤。資料分類還可減少資料重複，如此有助於降低儲存和備份成本，同時加速搜尋程序。

使用 Amazon Macie 之類的服務可大規模自動化敏感資料的探索和分類。其他像是 Amazon EventBridge 和 AWS Config 等服務可用來自動化資料安全問題的修正作業，例如未加密的 Amazon Simple Storage Service (Amazon S3) 儲存貯體和 Amazon EC2 EBS 磁碟區或未標記的資料資源。如需 AWS 服務整合的完整清單，請參閱 EventBridge 文件。

偵測非結構化資料中的 PII，例如客戶電子郵件、支援票證、產品評論和社交媒體，可使用 Amazon Comprehend 來達成，其是一項自然語言處理 (NLP) 服務，使用機器學習 (ML) 在非結構化文字中尋找洞察和關係，例如如人員、情緒和主題。如需可協助資料識別的 AWS 服務清單，請參閱使用 AWS 服務偵測 PHI 和 PII 的常見方法。

另一種支援資料分類和保護的方法是 AWS 資源標記。標記可讓您將中繼資料指派到您的 AWS 資源，其可用於管理、識別、組織、搜尋和篩選資源。

在某些情況下，您可能選擇標記整個資源 (例如 S3 儲存貯體)，尤其是在特定工作負載或服務應該存放已知資料分類的處理和傳輸時。

適用時，您可以標記 S3 儲存貯體而不是個別的物件，以方便管理和維護安全。

實作步驟

偵測 Amazon S3 內的敏感資料：

1. 開始前，請確定您具備適當的許可，以存取 Amazon Macie 主控台和 API 操作。如需其他詳細資訊，請參閱 Amazon Macie 入門。
2. 當您的敏感資料位於 Amazon S3 中時，使用 Amazon Macie 來執行自動化資料探索。
   - 使用 Amazon Macie 入門指南為敏感資料探索結果設定儲存庫，並為敏感資料建立探索工作。
   - 如何使用 Amazon Macie 預覽 S3 儲存貯體中的敏感資料。

     Macie 預設會使用我們針對自動化敏感資料探索所建議的受管資料識別符集合來分析物件。您可以設定 Macie 在為您的帳戶或組織執行自動化敏感資料探索時使用特定的受管資料識別符、自訂資料識別符和允許清單，藉此將分析客製化。您可以透過排除特定儲存貯體 (例如，一般存放 AWS 記錄資料的 S3 儲存貯體)，來調整分析的範圍。
3. 若要設定和使用自動化敏感資料探索，請參閱使用 Amazon Macie 執行自動化敏感資料探索。
4. 您也應該考慮適用於 Amazon Macie 的自動化資料探索。

偵測 Amazon RDS 內的敏感資料：

如需關於 Amazon Relational Database Service (Amazon RDS) 資料庫中的資料探索的詳細資訊，請參閱使用 Macie 為 Amazon RDS 資料庫啟用資料分類。

偵測 DynamoDB 內的敏感資料：

- 使用 Macie 偵測 DynamoDB 內的敏感資料說明如何使用 Amazon Macie 透過將資料匯出到 Amazon S3 以進行掃描，來偵測 Amazon DynamoDB 資料表中的敏感資料。

AWS 合作夥伴解決方案：

- 考慮使用我們廣大的 AWS Partner Network。AWS 合作夥伴擁有廣泛的工具和合規架構，與 AWS 服務直接整合。合作夥伴可以為您提供客製化的治理和合規解決方案，協助您滿足組織需要。
- 如需資料分類的自訂解決方案，請參閱在法規和合規要求的時代進行資料治理。

您可以使用 AWS Organizations 建立和部署政策，藉此自動強制您的組織採用的標記標準。標籤政策可讓您指定規則，定義有效的金鑰名稱以及每個金鑰的有效值。您可以選擇只進行監控，這讓您有機會評估和清理現有的標籤。在您的標籤符合所選的標準後，您可以開啟標籤政策中的強制實施，以防建立不合規的標籤。如需詳細資訊，請參閱使用 AWS Organizations 中的服務控制政策保護用於授權的資源標籤以及有關預防標籤遭修改 (授權主體除外) 的範例政策。

- 若要開始使用 AWS Organizations 中的標籤政策，強烈建議您先遵循標籤政策入門中的工作流程。再移向更進階的標籤政策。了解將簡單的標籤政策先附加到單一帳戶再擴展到整個組織單位 (OU) 或組織的作用，可讓您在強制遵守標籤政策之前先查看標籤政策的作用。標籤政策入門提供與更進階政策相關的任務之指示連結。
- 考慮評估其他支援資料分類的 AWS 服務和功能，這在資料分類白皮書中有列出。

資源

相關文件：

- Amazon Macie 入門
- 使用 Amazon Macie 自動化資料探索
- 標籤政策入門
- 偵測 PII 實體

相關部落格：

- 如何使用 Amazon Macie 預覽 S3 儲存貯體中的敏感資料。
- 使用 Amazon Macie 執行自動化敏感資料探索。
- 使用 AWS 服務偵測 PHI 和 PII 資料的常見方法
- 使用 Amazon Comprehend 偵測和修訂 PII
- 使用 AWS Organizations 中的服務控制政策保護用於授權的資源標籤
- 使用 Macie 為 Amazon RDS 資料庫啟用資料分類

- 使用 Macie 偵測 DynamoDB 中的敏感資料
-

相關影片：

- 使用 Amazon Macie 的事件驅動資料安全
- Amazon Macie 用於資料保護和治理
- 使用允許清單微調敏感資料問題清單

SEC07-BP02 定義資料保護控制

根據資料的分類層級保護資料。例如：使用相關建議來保護歸類為公有的資料，同時實作額外的控制以保護敏感資料。

使用資源標籤、根據敏感度 (也可能適用於警告、群體或關注的社群)、IAM 政策、AWS Organizations SCP、AWS Key Management Service (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 Amazon Elastic Compute Cloud (Amazon 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。

若未建立此最佳實務，暴露的風險等級： 高

實作指引

- 定義您的資料識別和分類結構描述：對資料進行識別和分類，評估您儲存的資料的潛在影響和類型，以及誰可以存取它。
  - AWS 文件
- 探索可用的 AWS 控制：針對您目前正在使用或計劃使用的 AWS 服務探索安全控制。許多服務在其文件中皆有安全性區段。
  - AWS 文件
- 識別 AWS 合規資源：識別 AWS 可用於協助的資源。
  - https://aws.amazon.com/compliance/

資源

相關文件：

- AWS 文件
- 資料分類白皮書
- Amazon Macie 入門
- 缺少文字

相關影片：

- 介紹新的 Amazon Macie

SEC07-BP03 自動識別和分類

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。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

- 使用 Amazon Simple Storage Service (Amazon S3) 庫存：Amazon S3 庫存是可用來稽核和報告物件複寫與加密狀態的其中一項工具。
  - Amazon S3 庫存
- 考慮 Amazon Macie：Amazon Macie 使用機器學習來自動發現和分類存放在 Amazon S3 中的資料。
  - Amazon Macie

資源

相關文件：

- Amazon Macie

- Amazon S3 庫存
- 資料分類白皮書
- Amazon Macie 入門

相關影片：

- 介紹新的 Amazon Macie

SEC07-BP04 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。

若未建立此最佳實務，暴露的風險等級： 低

實作指引

- 識別資料類型：識別您在工作負載中存放或處理的資料類型。該資料可以是文字、影像、二進位資料庫等。

資源

相關文件：

- 資料分類白皮書
- Amazon Macie 入門

相關影片：

- 介紹新的 Amazon Macie

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。

加密和權杖化是兩個重要但截然不同的資料保護方案。

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。

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 這類工具來查詢 AWS CloudTrail，以確保金鑰的所有使用都是有效的。

最佳實務

- SEC08-BP01 實作安全金鑰管理
- SEC08-BP02 強制靜態加密
- SEC08-BP03 將靜態資料保護自動化
- SEC08-BP04 強制存取控制
- SEC08-BP05 使用限制人員存取資料的機制

SEC08-BP01 實作安全金鑰管理

安全金鑰管理包括儲存、輪替、存取控制及監控保護工作負載的靜態資料所需的金鑰資料。

預期成果： 可擴展、可重複且自動化的金鑰管理機制。此機制應提供對金鑰資料強制執行最低權限存取的能力，並且在金鑰可用性、機密性和完整性之間提供正確的平衡。金鑰存取權應受到監控，而金鑰資料應透過自動化程序輪替。金鑰資料絕不可供真人身分存取。

常見的反模式：

- 真人存取未加密的金鑰資料。
- 建立自訂的加密演算法。
- 存取金鑰資料的許可過於廣泛。

建立此最佳實務的優勢： 透過為工作負載建立安全的金鑰管理機制，就可以協助保護您的內容，防止未經授權的存取。此外，您可能需要依法加密您的資料。有效的金鑰管理解決方案能夠提供符合這些法規的技術機制，以保護金鑰資料。

未建立此最佳實務時的曝險等級： 高

實作指引

許多法規需求和最佳實務都納入了靜態資料加密做為基本的安全控制。為了符合此控制，您的工作負載須採取某種機制，以安全存放和管理用於加密靜態資料的金鑰資料。

AWS 提供 AWS Key Management Service (AWS KMS) 來為 AWS KMS 金鑰提供耐用、安全和冗餘的儲存。 許多 AWS 服務會與 AWS KMS 整合， 以支援資料加密。AWS KMS 使用 FIPS 140-2 3 級驗證的硬體安全模組來保護您的金鑰。沒有任何機制可將 AWS KMS 金鑰匯出為純文字。

使用多帳戶策略部署工作負載時，會採取的 最佳實務 是將 AWS KMS 金鑰與使用金鑰的工作負載保留在相同的帳戶中。在這個分散式模型中，管理 AWS KMS 金鑰的責任會落在應用程式團隊身上。在其他使用案例中，組織可能會選擇將 AWS KMS 金鑰儲存到集中式帳戶中。此集中式結構須實施其他政策來實現跨帳戶存取權，才能讓工作負載帳戶存取儲存在集中式帳戶中的金鑰，但此結構可能較適合跨多個 AWS 帳戶 共用單一金鑰的使用案例。

無論金鑰資料存放在何處，金鑰的存取權都應透過使用 金鑰政策 和 IAM 政策進行嚴格控管。金鑰政策是控制 AWS KMS 金鑰存取權的主要方式。此外，AWS KMS 金鑰授權可提供 AWS 服務的存取權，以代表您加密和解密資料。請安排時間來檢閱 AWS KMS 金鑰存取控制的最佳實務。

最佳實務是監控加密金鑰的使用情況，以偵測不尋常的存取模式。使用存放在 AWS KMS 中 AWS 管理的金鑰和客戶管理的金鑰執行的操作可記錄在 AWS CloudTrail 中，並且應定期檢閱。應特別注意監控金鑰銷毀事件。為了減少意外或惡意銷毀金鑰資料的情況，金鑰銷毀事件並不會立即刪除金鑰資料。嘗試刪除 AWS KMS 中的金鑰會受到 等待期的約束 (預設為 30 天)，讓管理員有時間檢閱這些動作，並在必要時撤回請求。

大多數 AWS 服務會以顯而易見的方式使用 AWS KMS，您唯一要做的就是決定要使用 AWS 管理或客戶管理的金鑰。如果您的工作負載要求直接使用 AWS KMS 來加密或解密資料，則最佳實務是使用 封套加密 來保護您的資料。此 AWS Encryption SDK 可為您的應用程式提供用戶端加密基本類型，以實作封套加密並與 AWS KMS 整合。

實作步驟

1. 確定適當的 金鑰管理選項 (AWS 管理或客戶管理的金鑰)。
   - 為了方便使用，AWS 為大多數服務提供了 AWS 擁有和 AWS 管理的金鑰，其提供靜態加密功能，而不需要管理金鑰資料或金鑰政策。
   - 使用客戶管理的金鑰時，請考慮使用預設金鑰存放區，以便在敏捷性、安全性、資料主權與可用性之間達到最佳平衡。其他使用案例可能會要求使用自訂金鑰存放區搭配 AWS CloudHSM 或 外部金鑰存放區。
2. 檢閱您用於工作負載的服務清單，以了解 AWS KMS 與服務整合的方式。例如，EC2 執行個體可以使用加密的 EBS 磁碟區，因此要確認從這些磁碟區建立的 Amazon EBS 快照同樣是使用客戶管理的金鑰加密，並減少意外洩漏未加密的快照資料。
   - AWS 服務如何使用 AWS KMS
   - 如需有關 AWS 服務所提供加密選項的詳細資訊，請參閱使用者指南中的「靜態加密」主題或服務的開發人員指南。
3. 實作 AWS KMS：AWS KMS 可讓您輕鬆建立和管理金鑰，並控制多種 AWS 服務和應用程式中的加密使用方式。
   - 入門：AWS Key Management Service (AWS KMS)
   - 檢閱 AWS KMS 金鑰存取控制的最佳實務。
4. 考慮 AWS Encryption SDK：當您的應用程式需要在用戶端對資料進行加密時，可使用整合 AWS KMS 的 AWS Encryption SDK。
   - AWS Encryption SDK
5. 啟用 IAM Access Analyzer 以自動檢閱並在發現有過度廣泛的 AWS KMS 金鑰政策時發出通知。
6. 啟用 Security Hub 以在金鑰政策設定錯誤、有排定要刪除的金鑰，或有未啟用自動輪替的金鑰時收到通知。
7. 確定適合 AWS KMS 金鑰的記錄層級。由於 AWS KMS 的呼叫 (包括唯讀事件) 會加以記錄，因此與 AWS KMS 相關聯的 CloudTrail 日誌可能會變得很龐大。
   - 有些組織偏好將 AWS KMS 記錄活動分隔為單獨的軌跡記錄。如需詳細資訊，請參閱「使用 CloudTrail 記錄 AWS KMS API 呼叫」一節 (《AWS KMS 開發人員指南》中)。

資源

相關文件：

- AWS Key Management Service

- AWS 加密服務和工具
- 使用加密保護 Amazon S3 資料
- 封套加密
- 數位主權承諾
- 揭密 AWS KMS 金鑰操作、攜帶自有金鑰、自訂金鑰存放區，以及密文可攜性
- AWS Key Management Service 加密詳細資訊

相關影片：

- 在 AWS 中加密如何運作
- 保護 AWS 上的區塊儲存安全
- AWS 資料保護：使用鎖定、金鑰、簽章和憑證

相關範例：

- 使用 AWS KMS 實作進階存取控制機制

SEC08-BP02 強制靜態加密

您應該對靜態資料強制使用加密。在發生未授權存取或意外洩露的情況時，加密可保持敏感資料的機密性。

預期成果：私有資料應該預設在處於靜態時加密。加密有助於維持資料的機密性，並提供多一層保護以防有意或不慎的資料暴露或外洩。加密的資料必須先解密後才能讀取或存取。任何在未加密下儲存的資料都應該進行清查並加以控制。

常見的反模式：

- 未使用預設加密組態。
- 對解密金鑰提供過於寬鬆的存取權。
- 未監控加密和解密金鑰的使用。
- 在未加密的情況下儲存資料。
- 對所有資料使用相同的加密金鑰，無論資料使用方式、類型和分類。

未建立此最佳實務時的風險暴露等級：高

實作指引

在工作負載中將加密金鑰對應到資料分類。當對資料使用單一或極少數的加密金鑰時，此方法有助於防止過於寬鬆的存取權 (請參閱 SEC07-BP01 識別工作負載內的資料)。

AWS Key Management Service (AWS KMS) 與許多 AWS 服務整合，更方便您加密靜態資料。例如，在 Amazon Simple Storage Service (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。當使用 AWS KMS 時，考慮需要嚴格限制資料的程度。AWS 會代表您管理及使用預設和服務控制的 AWS KMS 金鑰。對於需要對基礎加密金鑰的精細存取權之敏感資料，可考慮客戶自管金鑰 (CMK)。您可全權控制 CMK，包括透過使用金鑰政策進行輪換和存取管理。

此外，Amazon Elastic Compute Cloud (Amazon EC2) 和 Amazon S3 可透過設定預設加密來支援強制加密。您可以使用 AWS Config 規則 自動檢查您是否正對如 Amazon Elastic Block Store (Amazon EBS) 磁碟區、Amazon Relational Database Service (Amazon RDS) 執行個體和 Amazon S3 儲存貯體等使用加密。

AWS 也提供用戶端加密選項，允許您在上傳到雲端之前加密資料。AWS Encryption SDK 提供使用封套加密來加密資料的方法。您提供包裝金鑰，而 AWS Encryption SDK 會為它加密的每個資料物件產生唯一的資料金鑰。如果您需要受管的單一租用戶硬體安全模組 (HSM)，可考慮 AWS CloudHSM。AWS CloudHSM 可讓您在 FIPS 140-2 3 級驗證的 HSM 上產生、匯入和管理加密金鑰。AWS CloudHSM 的一些使用案例包括保護用於核發憑證認證機構 (CA) 的私有金鑰，以及為 Oracle 資料庫啟用透明資料加密 (TDE)。AWS CloudHSM 用戶端 SDK 提供軟體，可讓您在將資料上傳到 AWS 之前，使用儲存在 AWS CloudHSM 內的金鑰加密資料用戶端。Amazon DynamoDB Encryption Client 還允許您在上傳到 DynamoDB 資料表之前，加密和簽署項目。

實作步驟

- 強制對 Amazon S3 執行靜態加密：實作 Amazon S3 儲存貯體預設加密。

  為新的 Amazon EBS 磁碟區設定預設加密：使用 AWS 提供的預設金鑰或您自行建立的金鑰，指定您希望以加密形式建立所有新的 Amazon EBS 磁碟區。

  設定加密的 Amazon Machine Images (AMI)：複製已啟用加密的現有 AMI 會自動加密根磁碟區和快照。

  設定 Amazon RDS 加密：透過使用加密選項，為您的 Amazon RDS 資料庫叢集和靜態快照設定啟用加密。

  使用政策限制對適當主體的存取，為每個資料分類建立和設定 AWS KMS 金鑰：例如，建立一個 AWS KMS 金鑰用於加密生產資料，另一個金鑰用於加密開發或測試資料。您還可以提供金鑰來存取

其他 AWS 帳戶。考慮針對開發和生產環境擁有不同的帳戶。如果您的生產環境需要解密開發帳戶中的成品，您可以編輯用來加密開發成品的 CMK 金鑰，使生產帳戶能夠解密這些成品。生產環境接著可以擷取解密的資料以用於生產。

在其他 AWS 服務中設定加密：對於您使用的其他 AWS 服務，請檢閱該服務的安全文件，以確定該服務的加密選項。

資源

相關文件：

- AWS 加密工具
- AWS 文件
- AWS Encryption SDK
- AWS KMS 加密詳細資訊白皮書
- AWS Key Management Service
- AWS 加密服務和工具
- Amazon EBS 加密
- Amazon EBS 磁碟區的預設加密
- 加密 Amazon RDS 資源
- 如何針對 Amazon S3 儲存貯體啟用預設加密？
- 使用加密保護 Amazon S3 資料

相關影片：

- AWS 中加密的運作方式
- 保護 AWS 上的區塊儲存安全

SEC08-BP03 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 規則資料目錄中。AWS Security Hub 也可以透過符合安全標準的自動化檢查來驗證數種不同的控制。此外，您的 AWS Config 規則 可以自動 修復不合規的資源。

若未建立此最佳實務，暴露的風險等級為： 中

實作指引

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。

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 Simple Storage Service (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 和 Amazon S3 透過設定預設加密來支援強制加密。您可以使用 AWS 受管 Config 規則 ，自動檢查您是否正在將加密用於，例如， EBS 磁碟區，Amazon Relational Database Service (Amazon RDS) 執行個體和 Amazon S3 儲存貯體。

資源

相關文件：

- AWS 加密工具
- AWS 加密開發套件

相關影片：

- 在 AWS 中加密如何運作
- 保護 AWS 上的區塊儲存安全

SEC08-BP04 強制存取控制

若要協助保護您的靜態資料，使用隔離和版本控制等機制來強制存取控制，並套用最低權限原則。防止授予對您資料的公開存取權。

預期成果：確認只有授權使用者能夠在必要時存取資料。透過定期備份和版本控制來保護您的資料以防有意或不慎修改或刪除資料。將重要資料與其他資料分離，以保護其機密性和資料完整性。

常見的反模式：

- 將具有不同敏感度需求或分類的資料存放在一起。
- 對解密金鑰使用過於寬鬆的許可。
- 資料分類不當。

- 未保留重要資料的詳細備份。
- 對生產資料提供持續存取權。
- 未稽核資料存取或定期審查許可。

未建立此最佳實務時的風險暴露等級：低

實作指引

多項控制可協助您保護靜態資料，包括存取 (使用最低權限)、隔離和版本控制。對資料的存取應使用偵測機制進行稽核，例如 AWS CloudTrail 和服務層級日誌 (例如 Amazon Simple Storage Service (Amazon S3) 存取日誌)。您應該清查哪些資料可公開存取，並建立計畫以隨著時間減少可用的資料量。

Amazon S3 Glacier Vault Lock 和 Amazon S3 物件鎖定為 Amazon S3 中的物件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。

實作步驟

- 強制存取控制：強制最低權限存取控制，包括對加密金鑰的存取。
- 根據不同的分類層級分離資料：針對資料分類層級使用不同的 AWS 帳戶，並使用 AWS Organizations 來管理這些帳戶。
- 審查 AWS Key Management Service (AWS KMS) 政策：審查 AWS KMS 政策中授予的存取層級。
- 審查 Amazon S3 儲存貯體和物件許可：定期審查 S3 儲存貯體政策中授予的存取層級。最佳實務是避免使用可公開讀取或寫入的儲存貯體。考慮使用 AWS Config 偵測公開可用的儲存貯體，以及使用 Amazon CloudFront 從 Amazon S3 提供內容。確認不允許公開存取的儲存貯體已正確設定為禁止公開存取。依照預設，所有 S3 儲存貯體皆為私有，只有明確獲得存取權的使用者得以存取。
- 啟用 AWS IAM Access Analyzer： IAM Access Analyzer 會分析 Amazon S3 儲存貯體並在 S3 政策將存取權授予外部實體時產生發現結果。
- 適當時，啟用 Amazon S3 版本控制和物件鎖定。
- 使用 Amazon S3 庫存：Amazon S3 庫存可用來稽核和報告 S3 物件的複寫和加密狀態。
- 審查 Amazon EBS 和 AMI 共用許可：共用許可可以允許將映像和磁碟區與工作負載外部的 AWS 帳戶共用。
- 審查 AWS Resource Access Manager 定期共用以確定是否應該持續共用資源。 Resource Access Manager 可讓您共用 Amazon VPC 內的資源，例如 AWS 網路防火牆政策、Amazon Route 53 解析器規則和子網路。定期稽核共用的資源並停止共用不再需要共用的資源。

資源

相關的最佳實務：

- SEC03-BP01 定義存取需求
- SEC03-BP02 授予最低權限存取權

相關文件：

- AWS KMS 加密詳細資訊白皮書
- 管理對 Amazon S3 資源的存取許可的簡介
- 管理對您 AWS KMS 資源的存取概觀
- AWS Config 規則
- Amazon S3 + Amazon CloudFront：雲端的最佳拍檔
- 使用版本控制
- 使用 Amazon S3 物件鎖定來鎖定物件
- 共用 Amazon EBS 快照
- 共用的 AMI
- 在 Amazon S3 上託管單頁應用程式

相關影片：

- 保護 AWS 上的區塊儲存安全

SEC08-BP05 使用限制人員存取資料的機制

在正常運作情況下，讓所有使用者遠離直接存取敏感資料和系統的權限。例如，使用變更管理工作流程來使用工具管理 Amazon Elastic Compute Cloud (Amazon 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。

若未建立此最佳實務，暴露的風險等級為： 低

實作指引

- 實作限制人員存取資料的機制：這些機制包括使用 Amazon QuickSight 等儀表板向使用者顯示資料，而不是直接查詢。
  - Amazon QuickSight
- 自動化組態管理：透過使用組態管理服務或工具，在遠距離執行動作，並自動執行和驗證安全組態。避免使用堡壘主機或直接存取 EC2 執行個體。
  - AWS Systems Manager
  - AWS CloudFormation
  - AWS 上 AWS CloudFormation 範本的 CI/CD 管道

資源

相關文件：

- AWS KMS 加密詳細資訊白皮書

相關影片：

- 在 AWS 中加密如何運作
- 保護 AWS 上的區塊儲存安全

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。

保護來自 VPC 之間或內部部署位置的資料： 您可以使用 AWS PrivateLink ，在 Amazon Virtual Private Cloud (Amazon VPC) 之間建立安全且私有的網路連線，或建立 AWS 中所託管服務的內部部署連線。您可以存取 AWS 服務、第三方服務，以及其他 AWS 帳戶 中的服務，就像它們是在您的私有網路一樣。使用 AWS PrivateLink，您可以跨具有重疊 IP CIDR 的帳戶存取服務，而不需要網際網路閘道或 NAT。您也不必設定防火牆規則、路徑定義或路由表。流量停留在 Amazon 骨幹網路上，而且不會周遊網際網路，因此您的資料受到保護。您可以遵守產業特定的合規法規，例如 HIPAA 和歐盟/美國隱私保護盾。AWS PrivateLink 無縫使用第三方解決方案，建立簡化的全球網路，讓您可以加速遷移到雲端並利用可用的 AWS 服務。

最佳實務

- SEC09-BP01 實作安全金鑰和憑證管理
- SEC09-BP02 強制傳輸中加密
- SEC09-BP03 自動偵測意外的資料存取
- SEC09-BP04 驗證網路通訊

SEC09-BP01 實作安全金鑰和憑證管理

Transport Layer Security (TLS) 憑證可用來保護網路通訊，和建立網際網路跟私有網路中的網站、資源和工作負載的身份。

預期成果： 能夠在公開金鑰基礎設施 (PKI) 佈建、部署、儲存和更新憑證的安全憑證管理系統。安全金鑰與憑證管理機制可以防止憑證私有金鑰資料外洩，也能定期自動更新憑證。它也能與其他服務整合，為工作負載內的機器資源提供安全的網路通訊和身分識別。金鑰資料絕不可供真人身分存取。

常見的反模式：

- 在憑證部署或更新程序期間執行手動步驟。
- 設計私有 CA 時，請忽略憑證授權單位 (CA) 階層。
- 針對公用資源使用自我簽署憑證。

建立此最佳實務的優勢：

- 透過自動化部署和更新來簡化憑證管理
- 鼓勵使用 TLS 憑證加密傳輸中的資料
- 增加憑證授權單位所採取憑證動作的安全性和可稽核性
- 在 CA 階層中不同層次的管理責任組織

未建立此最佳實務時的曝險等級： 高

實作指引

現代工作負載可透過利用 TLS 等 PKI 通訊協定，來廣泛使用加密網路通訊。PKI 憑證管理可能很複雜，但自動化憑證佈建、部署和更新可以減少憑證管理相關障礙。

AWS 提供兩種管理一般用途 PKI 憑證的服務： AWS Certificate Manager 和 AWS Private Certificate Authority (AWS Private CA)ACM 是客戶在公有和私有 AWS 工作負載中，用來佈建、管理和佈數憑

證的主要服務。ACM 則使用 AWS Private CA 的公有憑證授權單位來發行憑證，並 整合 至許多其他 AWS 受管服務，以提供安全的工作負載 TLS 憑證。

AWS Private CA 可讓您建立自己的根憑證授權單位或下層憑證授權單位，並透過 API 發行 TLS 憑證。在您控制和管理 TLS 連線用戶端信任鏈時，您可以使用這些憑證類型。除了 TLS 使用案例之外，AWS Private CA 可以用來發行憑證給 Kubernetes pods、重要裝置產品證明、程式碼簽署，以及其他使用案例，過程中搭配 自訂範本。您也可以使用 IAM Roles Anywhere 提供臨時 IAM 憑證給具有您私有 CA 簽發 X.509 憑證的內部部署工作負載。

除了 ACM 和 AWS Private CA 之外， AWS IoT Core 也為物聯網裝置提供特別支援，用來佈建、管理和部署 PKI 憑證。AWS IoT Core 提供特別機制給 上線物聯網裝置。 大規模提供特別機制至您的公有金鑰基礎設施。

建立私有 CA 階層時的考量

您要建立私有 CA 時，請務必特別留意，預先正確設計 CA 階層。建立私有 CA 階層時，最佳做法是將 CA 階層的每個層級部署到個別 AWS 帳戶。這個刻意的步驟會減少 CA 階層中每個層級的界面面積，讓您更容易察覺 CloudTrail 日誌資料的異常狀況，並在出現未經授權的帳戶存取動作時降低存取或影響範圍。根 CA 應位於自己的個別帳戶中，且只能用來發行一個或多個中繼 CA 憑證。

接著，請在不同於根 CA 帳戶的其他帳戶中建立一個或多個中繼 CA，為終端使用者、裝置或其他工作負載發行憑證。最後，請將憑證從根 CA 發行至中繼 CA，這個動作會將憑證發行給您的終端使用者或裝置。如需深入了解 CA 部署規畫和 CA 階層設計，包括恢復能力、跨區域複寫、在組織中共用 CA 等規畫，請參閱 規劃您的 AWS Private CA 部署。

實作步驟

1. 決定使用案例所需的相關 AWS 服務：
   - 許多使用案例都可以利用 AWS 的現有公有金鑰基礎設施搭配，過程中使用 AWS Certificate Manager。ACM 可用於為 Web 伺服器、負載平衡器或其他用途部署 TLS 憑證。
   - 考慮 AWS Private CA 何時需要建立自己的私有憑證授權單位階層，或需要存取可匯出憑證的權限。ACM 可以接著用於發行 許多類型的終端實體憑證 過程中會使用 AWS Private CA。
   - 針對必須為嵌入式物聯網 (IoT) 裝置大規模佈建憑證的使用案例，請考慮 AWS IoT Core。
2. 盡可能實施自動憑證續約：
   - 使用 使用 ACM 的受管更新 搭配 ACM 發行的憑證和 AWS 受管服務。
3. 建立日誌和稽核軌跡：
   - 啟用 CloudTrail 日誌 以追蹤對持有憑證授權單位之帳戶的存取權。請考慮在 CloudTrail 中設定日誌檔完整性驗證，以驗證日誌資料的真實性。

- 定期產出稽核報告，其中列出您的私有 CA 發行或撤銷的憑證。這些報告可以匯出到 S3 儲存貯體。
- 部署私有 CA 時，您也需要建立 S3 儲存貯體來儲存憑證撤銷清單 (CRL)。如需詳細了解如何根據工作負載需求設定此 S3 儲存貯體，請參閱規劃憑證撤銷清單 (CRL)。

資源

相關的最佳實務：

- SEC02-BP02 使用臨時憑證
- SEC08-BP01 實作安全金鑰管理
- SEC09-BP04 驗證網路通訊

相關文件：

- 如何在 AWS 中託管和管理整個私有憑證基礎設施
- 如何鞏固用於汽車和製造領域的企業規模 ACM 私有 CA 階層
- 私有 CA 最佳實務
- 如何使用 AWS RAM 共用您的 ACM 私有 CA 跨帳戶

相關影片：

- 啟動 AWS Certificate Manager 私有 CA (研討會)

相關範例：

- 私人 CA 研討會
- IOT Device Management 研討會 (包括裝置佈建)

相關工具：

- 要使用 AWS Private CA 的 Kubernetes cert-manager 外掛程式

SEC09-BP02 強制傳輸中加密

根據您組織的政策、法規義務和標準強制已定義的加密需求，協助滿足組織、法律和合規上的要求。只有在虛擬私有雲端 (VPC) 以外傳輸敏感資料時才使用加密通訊協定。加密有助於保持資料完整性，甚至當資料傳輸於不受信任的網路時。

預期成果：所有資料都應該在傳輸時使用安全的 TLS 通訊協定和密碼套件加密。您的資源與網際網路之間的網路流量必須經過加密以緩解對資料的未授權存取。完全位於您內部 AWS 環境的網路流量應該盡可能使用 TLS 加密。AWS 內部網路會經預設加密，而且 VPC 內的網路流量無法受詐騙或嗅探，除非未授權方獲得對產生流量的資源 (例如 Amazon EC2 執行個體和 Amazon ECS 容器) 的存取權。考慮使用 IPsec 虛擬私有網路 (VPN) 保護網路對網路流量。

常見的反模式：

- 使用 SSL、TLS 和其他套件元件已棄用的版本 (例如，SSL v3.0、1024 位元 RSA 金鑰和 RC4 密碼)。
- 允許未加密的 (HTTP) 流量來往面向公眾的資源。
- 未監控 X.509 憑證並在到期前更換。
- 對 TLS 使用自我簽署的 X.509 憑證。

未建立此最佳實務時的風險暴露等級：高

實作指引

AWS 服務提供使用 TLS 的 HTTPS 端點以進行通訊，在與 AWS API 通訊時提供傳輸中加密。不安全的通訊協定 (如 HTTP) 可以在 VPC 中透過使用安全群組加以稽核和封鎖。HTTP 請求也可以在 Amazon CloudFront 中或 Application Load Balancer 上自動重新導向至 HTTPS 。您可以全權控制您的運算資源，以在各個服務中實作傳輸中加密。此外，還可以從外部網路或 AWS Direct Connect 使用 VPN 連線功能進入 VPC，加速流量加密。確認您的用戶端至少使用 TLS 1.2 對 AWS API 進行呼叫，因為 AWS 將於 2023 年 6 月棄用 TLS 1.0 和 1.1。如果您有特殊需求，AWS Marketplace 備有第三方解決方案。

實作步驟

- 強制傳輸中加密：您定義的加密要求應符合最新標準和最佳實務，並僅允許採用安全協定。例如，設定安全群組，僅允許 HTTPS 協定連至 Application Load Balancer 或 Amazon EC2 執行個體。
- 在邊緣服務中設定安全通訊協定： 使用 Amazon CloudFront 設定 HTTPS並使用適用於您的安全狀態和使用案例的安全設定檔。

- 使用 VPN 進行外部連線：考慮使用 IPsec VPN，保護點對點或網路對網路連線，以協助提供資料隱私和完整性。
- 在負載平衡器中設定安全的通訊協定：選擇安全政策，以提供要連接到接聽程式的用戶端所支援的最強固的密碼套件。為您的 Application Load Balancer 建立 HTTPS 接聽程式.
- 在 Amazon Redshift 中設定安全協定：將您的叢集設定為要求 Secure Socket Layer (SSL) 或 Transport Layer Security (TLS) 連線。
- 設定安全通訊協定：檢閱 AWS 服務文件以確定傳輸中加密功能。
- 設定上傳至 Amazon S3 儲存貯體時的安全存取：使用 Amazon S3 儲存貯體政策控制對資料強制安全存取。
- 考慮使用 AWS Certificate Manager：ACM 可讓您佈建、管理和部署 TLS 憑證與 AWS 服務搭配使用。
- 考慮使用 AWS Private Certificate Authority 滿足私有 PKI 需求：AWS Private CA 可讓您建立私有憑證認證機構 (CA) 階層來核發可用於建立已加密 TLS 管道的終端實體 X.509 憑證。

資源

相關文件：

- AWS 文件
- 搭配 CloudFront 使用 HTTPS
- 使用 AWS Virtual Private Network 將您的 VPC 連接到遠端網路
- 為您的 Application Load Balancer 建立 HTTPS 接聽程式 .
- 教學課程：在 Amazon Linux 2 上設定 SSL/TLS
- 使用 SSL/TLS 加密與資料庫執行個體的連線
- 設定連線的安全性選項

SEC09-BP03 自動偵測意外的資料存取

使用 Amazon GuardDuty 這類工具，自動偵測可疑活動或將資料移到所定義邊界之外的嘗試。例如，GuardDuty 可以偵測異常的 Amazon Simple Storage Service (Amazon S3) 讀取活動，發現結果為 Exfiltration:S3/AnomalousBehavior。除了 GuardDuty，擷取網路流量資訊的 Amazon VPC 流程日誌還可與 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。Amazon S3 Access Analyzer 可協助評估您的 Amazon S3 儲存貯體中誰可以存取哪些資料。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

- 自動偵測意外的資料存取：使用工具或偵測機制自動偵測將資料移出定義邊界的嘗試；例如，偵測將資料複製到無法識別之主機的資料庫系統。
  - VPC Flow Logs
- 考慮 Amazon Macie：Amazon Macie 是一項全受管的資料安全和資料隱私服務，它使用機器學習和模式比對來探索和保護 AWS 中的敏感資料。
  - Amazon Macie

資源

相關文件：

- VPC Flow Logs
- Amazon Macie

SEC09-BP04 驗證網路通訊

使用支援身份驗證的通訊協定 (Transport Layer Security (TLS) 或 IPsec) 來驗證通訊的身分。

設計工作負載，以在每當服務、應用程式或使用者之間進行通訊時，使用安全、經驗證的網路通訊協定。使用支援驗證和授權的網路通訊協定可提供更強大的網路流量控制能力，並減少未經授權存取所造成的影響。

預期成果：設計出工作負載，讓其有明確定義的服務間資料平面和控制平面流量。在技術允許的情況下，流量要使用經過驗證和加密的網路通訊協定。

常見的反模式：

- 工作負載內有未經加密或驗證的流量。
- 在多個使用者或實體之間重複使用驗證憑證。
- 僅依賴網路控制作為存取控制機制。
- 建立自訂驗證機制，而非依賴業界標準的驗證機制。
- 服務元件或 VPC 中的其他資源之間有過於寬鬆的流量。

建立此最佳實務的優勢：

- 將未經授權存取所造成的影響範圍限制在工作負載的某個部分。
- 提供只會由已驗證實體執行動作的更高層級保證。
- 透過清楚地定義並強制執行預期的資料傳輸介面來改善服務的去耦。
- 透過請求歸因和明確定義的通訊介面，增強監控、記錄和事件應變。
- 結合網路控制與驗證和授權控制，為您的工作負載提供深度防禦。

未建立此最佳實務時的風險暴露等級：低

實作指引

您工作負載的網路流量模式可分為兩個類別：

- 東西流量代表構成工作負載的服務之間的流量。
- 南北流量代表工作負載和取用者之間的流量。

加密南北流量是常見的做法，使用經過驗證的通訊協定來保護東西流量則較不常見。現代安全實務的建議是，單靠網路設計並無法讓兩個實體之間建立信任的關係。當兩個服務可能位於一個共通的網路邊界內時，最佳做法仍是對這些服務之間的通訊進行加密、驗證和授權。

舉例來說，無論請求來自哪個網路，AWS 服務 API 都會使用 AWS 第 4 版簽署程序 (SigV4) 簽署通訊協定來驗證呼叫者。此驗證可確保 AWS API 可以驗證發出動作請求的身分，該身分接著可與政策結合來作出授權決策，決定是否應允許該動作。

Amazon VPC Lattice 和 Amazon API Gateway 等服務可讓您使用相同的 SigV4 簽署通訊協定，為自己的工作負載中的東西流量新增驗證和授權功能。如果 AWS 環境以外的資源需要與要求進行 SigV4 型驗證和授權的服務進行通訊，您可以在非 AWS 資源上使用 AWS Identity and Access Management (IAM) Roles Anywhere 來取得臨時的 AWS 憑證。使用這些憑證，便可透過 SigV4 簽署服務請求以授權存取。

用於驗證東西流量的另一種常見機制是 TLS 相互驗證 (mTLS)。許多物聯網 (IoT)、企業對企業應用程式和微服務都使用 mTLS，透過使用用戶端和伺服器端 X.509 憑證來驗證 TLS 通訊兩端的身分。這些憑證可由 AWS Private Certificate Authority (AWS Private CA) 核發。您可以使用 Amazon API Gateway 和 AWS App Mesh 等服務，為工作負載之間或工作負載內部的通訊提供 mTLS 驗證。mTLS 會為 TLS 通訊的兩端提供驗證資訊，但不提供授權機制。

最後，OAuth 2.0 和 OpenID Connect (OIDC) 是兩種常用於控制使用者對服務存取行為的通訊協定，但現在也變成服務對服務流量的熱門通訊協定。API Gateway 會提供 JSON Web 權杖 (JWT) 授權器，

可讓工作負載使用 OIDC 或 OAuth 2.0 身分提供者所核發的 JWT 來限制 API 路由的存取。OAuth2 的範圍可作為基本授權決策的來源，但仍需要在應用程式層實作授權檢查，而且單靠 OAuth2 範圍並無法支援更複雜的授權需求。

實作步驟

- 定義並記錄您的工作負載網路流量：實作深度防禦策略的第一步是定義工作負載的流量。
  - 建立可清楚定義構成工作負載的不同服務間資料傳輸方式的資料流程圖。此圖是透過已驗證的網路通道強制執行這些流程的第一步。
  - 在開發和測試階段檢測您的工作負載，以驗證資料流程圖是否準確反映工作負載在執行期的行為。
  - 資料流程圖在執行威脅建模練習時也很有用，如 SEC01-BP07 使用威脅模型識別威脅並優先考慮緩解措施中所述。
- 建立網路控制：考慮用來建立與資料流程一致的網路控制的 AWS 功能。網路邊界不應成為唯一的安全控制，但其可在深度防禦策略中提供一個保護層，以保護您的工作負載。
  - 使用安全群組建立定義和限制資源之間的資料流程。
  - 考慮使用 AWS PrivateLink 與支援 AWS PrivateLink 的 AWS 和第三方服務進行通訊。透過 AWS PrivateLink 介面端點傳送的資料會保留在 AWS 網路骨幹內，不會周遊公用網際網路。
- 在工作負載中跨服務實作驗證和授權：選擇最適合用來在您工作負載中提供經驗證加密流量的 AWS 服務集。
  - 考慮用來保護服務對服務通訊的 Amazon VPC Lattice。VPC Lattice 可以使用 SigV4 驗證結合驗證政策來控制服務對服務的存取。
  - 對於使用 mTLS 的服務對服務通訊，請考慮 API Gateway 或 App Mesh。AWS Private CA 可用來建立能夠核發憑證以與 mTLS 搭配使用的私有 CA 階層。
  - 與使用 OAuth 2.0 或 OIDC 的服務進行整合時，請考慮使用 JWT 授權器的 API Gateway。
  - 對於工作負載和 IoT 裝置之間的通訊，請考慮 AWS IoT Core，它提供了幾種網路流量加密和驗證選項。
- 監控未經授權的存取：持續監控是否有意外的通訊管道、嘗試存取受保護資源的未經授權主體，以及其他不當的存取模式。
  - 如果使用 VPC Lattice 來管理服務的存取，請考慮啟用和監控 VPC Lattice 存取日誌。這些存取日誌包括請求方實體的資訊、包括來源和目的地 VPC 在內的網路資訊，以及請求中繼資料。
  - 考慮啟用 VPC Flow Logs 來擷取網路流量上的中繼資料，並定期檢閱是否有異常狀況。
  - 如需更多有關規劃、模擬和應對安全事件的指引，請參閱 AWS 安全事件應變指南和 AWS Well Architected Framework 安全支柱的事件應變章節。

資源

相關的最佳實務：

- SEC03-BP07 分析公有和跨帳戶存取權
- SEC02-BP02 使用臨時憑證
- SEC01-BP07 使用威脅模型識別威脅並優先考慮緩解措施

相關文件：

- 評估用來保護 Amazon API Gateway API 的存取控制方法
- 為 REST API 設定相互 TLS 驗證
- 如何使用 JWT 授權器保護 API Gateway HTTP 端點
- 使用 AWS IoT Core 憑證提供者來授權 AWS 服務的直接呼叫
- AWS 安全事件應變指南

相關影片：

- AWS re:invent 2022：向您介紹 VPC Lattice
- AWS re:invent 2020：針對 AWS 上 HTTP API 的無伺服器 API 驗證

相關範例：

- Amazon VPC Lattice 研討會
- 零信任第 1 集 - Phantom Service Perimeter 研討會

事故回應

即使採用了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故發生時能否有效運作，以隔離、遏制問題並進行鑑識，以及將營運恢復到已知的良好狀態。在安全事故發生前先備妥工具和存取權，然後在演練日期間定期練習事故回應，有助於確保您能夠復原，同時盡量減少業務中斷。

主題

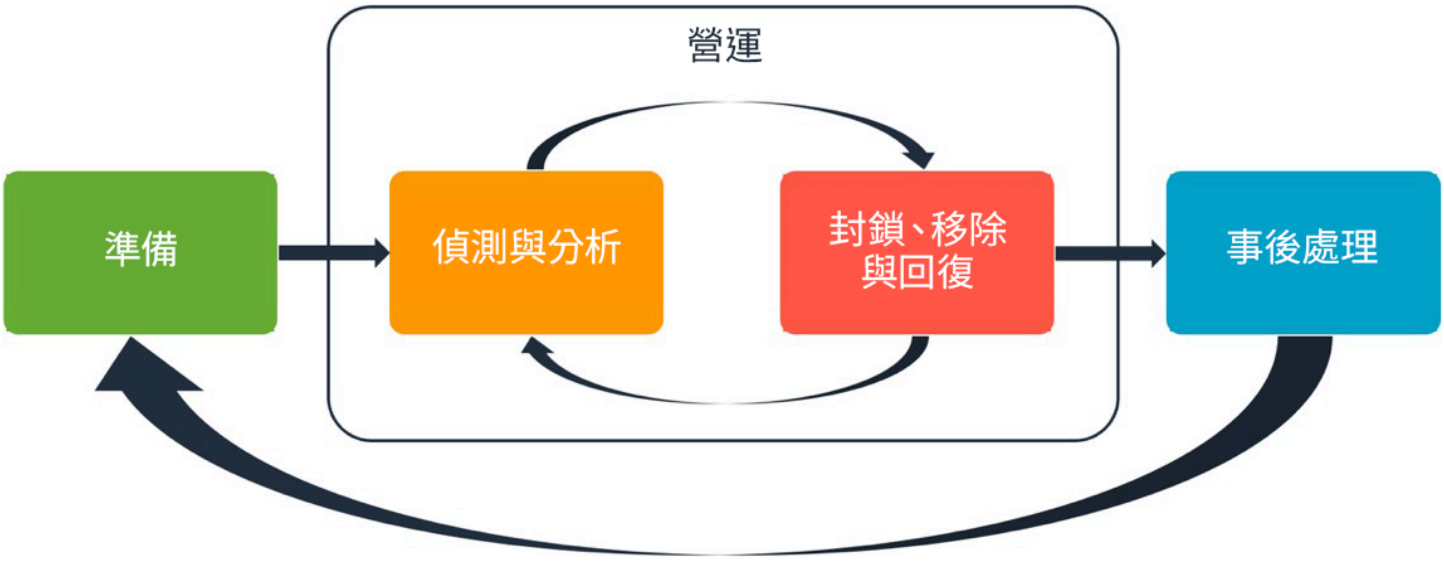
AWS 事故回應的各個層面

組織內的所有 AWS 使用者都應該對安全事故回應程序具有基本的了解，而安全人員應了解如何回應安全問題。教育、培訓和體驗是成功的雲端事故回應計畫必不可缺的一環，最好能預先實施，以因應發生安全事故的情況。雲端中成功的事故回應計畫的基礎在於 準備、 操作和 事後處理。

若要分別了解這三個層面，請參考下列說明：

- 準備：藉由啟用偵測控制並確認具備存取必要工具和雲端服務的適當權限，讓事故回應團隊做好準備，以便偵測和回應 AWS 內的事故。此外，備妥必要的程序手冊 (包括手動和自動)，以確認能夠做出可靠且一致的回應。
- 操作：依照 NIST 事故回應階段，對安全事件和可能的事故進行操作：偵測、分析、遏制、根除和復原。
- 事後處理：反覆執行安全事件和模擬的結果，以改善回應的有效性，增加從回應與調查中獲得的價值，並進一步降低風險。您必須從事故中學習，並能夠確實實施後續改進。

下圖顯示這些方面的流程，與先前提到的 NIST 事故回應生命週期一致，但涵蓋了包含遏制、根除和復原的偵測及分析操作。



AWS 事故回應的各個層面

雲端回應的設計目標

雖然事故回應的一般程序和機制，例如 NIST SP 800-61 Computer Security Incident Handling Guide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： 與利害關係人、法律顧問和組織領導階層合作，訂定回應事故的目標。共同目標包括遏制和緩解問題、復原受影響的資源、保留資料供鑑識使用、恢復已知的安全操作，以及最終從事故中學習經驗。
- 使用雲端回應： 在雲端內事件發生和資料之處實作回應模式。
- 了解您擁有什麼及需要什麼： 複製日誌、資源、快照和其他證據，並儲存在專門用於回應的集中式雲端帳戶中以便保留。運用標籤、中繼資料和機制，強制執行保留政策。您需要了解自己使用哪些服務，然後確定調查這些服務的需求。您也可以使用標籤來協助您了解自己的環境。
- 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利用適當的組態重新部署資源以移除變異，如此簡單。若發現可能是遭到入侵，則務必確認您的重新部署包含可成功緩解根本原因的措施。
- 盡可能自動化： 當問題出現或事故重複發生時，請建立機制，以程式設計方式分類並回應常見的事件。對於自動化不足以因應的獨特、複雜或敏感事故，則採取真人回應。
- 選擇可擴展的解決方案： 努力符合組織所採行雲端運算方法的可擴展性。實作能夠因應您的環境調整的偵測和回應機制，以便有效縮短偵測與回應之間的時間。
- 了解並改善程序： 主動找出流程、工具或人員當中的落差，並實施計畫來彌補落差。模擬是找出落差並改善流程的安全方法。

這些設計目標可提醒您檢閱架構實作，以確認能夠進行事故回應和威脅偵測。當您規劃雲端實作時，請考慮回應事故，最好是採用鑑識上可靠的回應方法。在某些情況下，這表示您可能會針對這些回應任務設定多個組織、帳戶和工具。這些工具和功能應透過部署管道提供給事故回應人員使用。它們不應處於靜態，否則可能造成更大的風險。

準備

為因應事故做好準備，對於須及時並有效回應的事故來說至關重要。準備工作橫跨三個領域：

- 人員：讓員工做好因應安全事故的準備，其中包括找出事故回應的相關利害關係人，並進行事故回應和雲端技術的培訓。
- 流程：備妥處理安全事故的流程，其中包括記錄架構、制定完整的事故回應計畫，以及製作程序手冊以便一致回應安全事件。
- 技術：備妥因應安全事故的技術，其中包括設定存取權、彙總和監控必要的日誌、實作有效的警示機制，以及開發回應和調查功能。

這三個領域對於有效回應事故來說同樣重要。缺少任一個領域，事故回應計畫便不完整或無法發揮效用。您需要讓人員、流程和技術三者緊密整合，才能做好因應事故的準備。

最佳實務

- SEC10-BP01 確定關鍵人員和外部資源
- SEC10-BP02 制定事件管理計畫
- SEC10-BP03 準備鑑識功能
- SEC10-BP04 開發和測試安全性事故應變程序手冊
- SEC10-BP05 預先佈建存取權
- SEC10-BP06 預先部署工具
- SEC10-BP07 執行模擬

SEC10-BP01 確定關鍵人員和外部資源

確定可以幫助您的組織回應事件的內部和外部人員、資源及法律義務。

當您在雲端定義回應事件的方法並與其他團隊 (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。

未建立此最佳實務時的曝險等級： 高

實作指引

- 確定組織中的關鍵人員 維護人員聯絡清單，將組織中參與事故回應和復原的人員納入其中。
- 確定外部合作夥伴 如有必要，可雇用外部合作夥伴，以幫助您應對事件並從中復原。

資源

相關文件：

- AWS 事件應變指南

相關影片：

- 準備和回應 AWS 環境中的安全事件

相關範例：

SEC10-BP02 制定事件管理計畫

為事件應變制定的第一份文件是事件應變計畫。事件應變計畫應是您事件應變計畫和策略的基礎。

建立此最佳實務的優勢： 開發全面且明確定義的事件應變程序，是成功且可擴展的事件應變計畫的關鍵。當安全事件發生時，明確的步驟和工作流程可協助您及時因應。您可能已具備現有的事件應變程序。無論您目前的狀態為何，都必須定期更新、重複執行和測試事件應變程序。

未建立此最佳實務時的曝險等級： 高

實作指引

事件管理計畫對於回應、減輕安全事件所造成潛在影響並從中復原而言至關重要。事件管理計畫是結構清晰的程序，可及時找出、修復和回應安全事件。

雲端有許多在內部部署環境中所見的相同營運角色和需求。建立事件管理計畫時，您必須將與業務成果和合規需求最相符的應變及復原策略納入考量。例如，如果您在 AWS 中運作的工作負載符合美國的 FedRAMP，那麼遵循 NIST SP 800-61 電腦安全處理指南便很有用。同樣地，在操作含有歐洲個人身分識別資訊 (PII) 資料的工作負載時，請考量以下情境，例如如何保護和回應與 歐盟一般資料保護規範 (GDPR) 中所要求之資料落地的相關問題。

為在 AWS 中的工作負載建立事件管理計畫時，請從 AWS 共同的責任模型 開始建置事件應變的深度防禦方法。在此模型中，AWS 會管理雲端的安全，但維護雲端的安全是您的責任。此表示您保有控制權，並對您選擇實作的安全控制項負責。此 AWS 安全事件應變指南 詳細說明在建立以雲端為中心的事件管理計畫時的重要概念和基礎指引。

有效的事件管理計畫必須經過持續的反覆測試，以與您的雲端營運目標保持同步。在您建立和制定事件管理計畫時，請考慮使用以下詳述的實作計畫。

實作步驟

定義角色和責任

處理安全事件時，需要跨組織的紀律和採取行動的傾向。在事件發生期間，您的組織結構中應該有不同的人員在事件期間負責、當責、備詢及保持通訊，例如人力資源部 (HR)、行政團隊和法務部的代表。請考量這些角色和責任，以及是否必須涉及任何第三方。請注意，許多地區都有當地法律會管理合法和不合法的事務。儘管為您的安全應變計畫建置負責、當責、備詢及通訊 (RACI) 圖表似乎很形式化，但這麼做可以促進快速直接的溝通，並清楚地概述活動不同階段的領導層。

在事件發生時，納入受影響的應用程式和資源的擁有者及開發人員是非常重要的，因為他們是主題專家 (SME)，可以提供資訊和背景資訊以協助衡量影響性。在您仰賴開發人員和應用程式擁有者的專業知識進行事件應變之前，請務必先與他們建立關係。應用程式擁有者或 SME (例如您的雲端管理員或工程師) 可能需要在環境不同於前或複雜，或是應變人員無法存取的情況下採取行動。

最後，值得信賴的合作夥伴可能會參與調查或回應，因為他們可以提供額外的專業知識和有價值的審視。若您自己的團隊沒有這些技能，您可能需要對外招聘以尋求幫助。

了解 AWS 應變團隊和支援

- AWS Support
  - AWS Support 提供一系列的計畫，可讓您存取工具和專業知識，以支援 AWS 解決方案的成功和運作狀態。如果您需要技術支援和更多資源以利規劃、部署和優化 AWS 環境，您可以選取最符合您 AWS 使用案例的支援計畫。

  - 考慮以 支援中心 (位於 AWS Management Console，需要登入) 作為中心聯絡窗口，以取得影響 AWS 資源的問題所需的支援。對 AWS Support 的存取由 AWS Identity and Access Management 所控制。如需取得 AWS Support 功能存取權的詳細資訊，請參閱 AWS Support 入門。
- AWS 客戶事件應變團隊 (CIRT)
  - AWS 客戶事件應變團隊 (CIRT) 是一個專門的全天候全球 AWS 團隊，在客戶端的有效安全事件期間為客戶提供支援 - AWS 共同的責任模型。
  - 當 AWS CIRT 支援您時，他們會為 AWS 上的有效安全事件提供分類和復原方面的協助。他們可透過使用 AWS 服務日誌協助進行根本原因分析，並為您提供復原的建議。他們也可提供安全建議和最佳實務，以協助您避免事後發生安全事件。
  - AWS 客戶可透過以下途徑洽詢 AWS CIRT： AWS Support 案例。
- DDoS 應變支援
  - AWS 提供 AWS Shield，其中包含受管的分散式拒絕服務 (DDoS) 保護服務，可為執行於 AWS 的 Web 應用程式提供保護。Shield 提供一律開啟的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，讓您無須聯絡 AWS Support 即可享有 DDoS 保護。Shield 有兩個層級：AWS Shield Standard 和 AWS Shield Advanced。若要了解這兩個層級的差異，請參閱 Shield 功能文件。
- AWS Managed Services (AMS)
  - AWS Managed Services (AMS) 可讓您持續管理 AWS 基礎設施，讓您專注在自己的應用程式上。實作最佳實務以維護您的基礎設施，AMS 有助於降低營運開銷和風險。AMS 會自動執行常見的活動，例如，變更請求、監控、修補程式管理、安全性和備份服務，而且提供佈建、執行和支援基礎設施的完整生命週期服務。
  - AMS 負責部署安全偵測控制套件，並提供全年無休的第一線提醒應變措施。提醒啟動時，AMS 會依照一組標準的自動化和手動程序手冊來驗證回應的一致性。這些程序手冊會在上線期間與 AMS 客戶共享，讓他們能夠透過 AMS 來制定和協調應變措施。

制定事件應變計畫

事件應變計畫應是您事件應變計畫和策略的基礎。事件應變計畫應納入正式文件中。事件應變計畫通常包含下列章節：

- 事件應變團隊概觀： 概述事件應變團隊的目標和職能。
- 角色和責任： 列出事件應變利害關係人，並詳細說明他們在事件發生時的角色。
- 通訊計畫： 詳細說明聯絡資訊，以及您在事件期間要如何進行通訊。

- 備份通訊方式： 最佳實務是將頻外通訊作為事件通訊的備用方法。舉例來說，AWS Wickr 就是提供安全頻外通訊通道的應用程式。
- 事件應變的階段和應採取的行動： 列舉事件應變的階段 (例如偵測、分析、消除、抑制及復原)，包括要在這些階段中採取的高階動作。
- 事件嚴重性和優先順序定義： 詳細說明如何分類事件的嚴重性、如何排定事件的優先順序，以及嚴重性定義對於呈報程序有何影響。

儘管不同規模和產業的公司都會有這些章節，但每個組織的事件應變計畫都是獨一無二的。您必須建立最適合貴組織的事件應變計畫。

資源

相關的最佳實務：

- SEC04 (您如何偵測和調查安全事件？)

相關文件：

- AWS 安全事件應變指南
- NIST：電腦安全事件處理指南

SEC10-BP03 準備鑑識功能

在安全事故發生之前，請將開發鑑識功能納入考量，以協助安全事件調查。

未建立此最佳實務時的曝險等級： 中

傳統內部部署鑑識的概念適用於 AWS。如需開始在 AWS 雲端 中建置鑑識功能的重要資訊，請參閱 AWS 雲端 中的鑑識調查環境策略。

設定鑑識的環境和 AWS 帳戶 結構後，請定義在四個階段有效執行合理鑑識方法所需的技術：

- 收集: 收集相關 AWS 日誌，例如 AWS CloudTrail、AWS Config、VPC 流程日誌和主機層級日誌。收集受影響 AWS 資源的快照、備份和記憶體傾印 (如果有的話)。
- 測驗： 檢視透過擷取和評估相關資訊所收集的資料。
- 分析： 分析收集的資料，以了解事故並從中得出結論。
- 報告： 呈現分析階段所產生的資訊。

實作步驟

準備鑑識環境

AWS Organizations 可協助您隨著 AWS 資源的成長和擴展，集中管理和控管 AWS 環境。AWS 組織會合併 AWS 帳戶，以便您可以將其當作一個單位進行管理。您可以使用組織單位 (OU) 將帳戶分組，以作為一個單位進行管理。

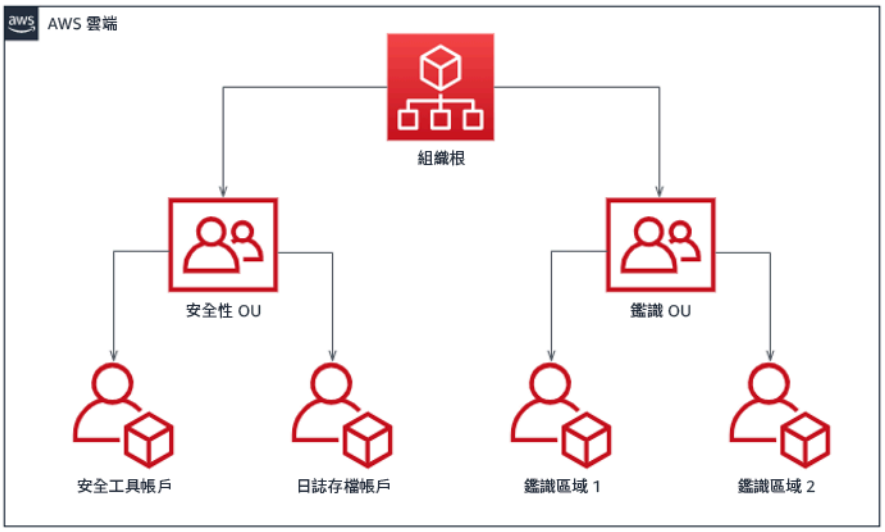
如需事故應變，建議您建立可支援事故應變功能的 AWS 帳戶 結構，其中包括 安全性 OU 和 鑑識 OU。在安全性 OU 中，您應該擁有下列項目的帳戶：

- 日誌存檔： 使用有限的許可彙總日誌存檔 AWS 帳戶 中的日誌。
- 安全性工具： 將安全性服務集中在安全工具 AWS 帳戶 中。此帳戶會以安全性服務的委派系統管理員身分運作。

在鑑識 OU 中，您可以選擇為營運所在的每個區域實作一或多個鑑識帳戶，具體視哪個區域最適合您業務和營運模式而定。如果您為每個區域建立鑑識帳戶，則可以防止該區域以外的 AWS 資源建立，並降低將資源複製到非預期區域的風險。例如，如果您只在 US East (N. Virginia) Region (#### (us-east-1) 和 US West (Oregon) 美國西部 (us-west-2)) 進行營運，則鑑識 OU 中會有兩個帳戶：一個用於 #### (us-east-1 另一個用於 us-west-2)。

您可以為多個區域建立鑑識 AWS 帳戶。您在將 AWS 資源複製到該帳戶時應小心，以確認是否符合資料主權要求。佈建新帳戶需要一些時間，因此必須在事故之前建立和檢測鑑識帳戶，以便回應人員能夠有效地使用這些帳戶進行回應。

下圖顯示範例帳戶結構，包括具有每個區域鑑識帳戶的鑑識 OU：



針對事故應變的每個區域帳戶結構

擷取備份和快照

設定重要系統和資料庫的備份，對於從安全性事故中復原和鑑識用途非常重要。備份就緒後，您可以將系統還原到先前的安全狀態。您可以在 AWS 上拍攝各種資源的快照。快照可為您提供那些資源的時間點備份。有許多 AWS 服務，可以在備份和復原方面為您提供支援。如需這些備份與復原之服務和方法的詳細資訊，請參閱 備份與復原規範指引 和 使用備份從安全性事故中復原。

尤其是當涉及勒索軟體等情況時，務必確保備份是否有充足的保護。如需保護備份的指引，請參閱 在 AWS 中保護備份的 10 大安全性最佳實務。除了確保備份的安全之外，您還應該定期測試備份和還原程序，以確認您現有的技術和程序是否如預期般運作。

自動化鑑識

在安全事件期間，事故應變團隊必須能夠快速收集和分析證據，同時維持事件周圍期間的準確性 (例如擷取與特定事件或資源相關的日誌，或收集 Amazon EC2 執行個體的記憶體傾印)。事故應變團隊手動收集相關證據既具挑戰性又耗時，尤其是範圍遍及大量執行個體和帳戶時。此外，手動收集可能容易出現人為錯誤。基於這些原因，您應盡可能開發和實作鑑識的自動化。

AWS 為鑑識提供許多自動化資源，內容列於以下的資源區段。這些資源是我們已開發和客戶已實作的鑑識模式範例。雖然這些範例在一開始可能是有用的參考架構，但請根據環境、需求、工具和鑑識程序，考慮是否加以修改或建立新的鑑識自動化模式。

資源

相關文件：

- AWS 安全事故應變指南 - 開發鑑識功能
- AWS 安全事故應變指南 - 鑑識資源
- AWS 雲端 中的鑑識調查環境策略
- 如何在 AWS 中自動化鑑識磁碟收集
- AWS 規範性指引 - 自動化事故應變和鑑識

相關影片：

- 自動化事故回應和鑑識

相關範例：

- 自動化事故應變與鑑識架構
- Amazon EC2 的自動化鑑識協調器

SEC10-BP04 開發和測試安全性事故應變程序手冊

準備事故應變流程的關鍵部分是制定程序手冊。事故應變程序手冊提供一系列規範性指引和安全性事件發生時應遵循的步驟。提供清晰的結構和步驟簡化了回應的複雜度並減少人為錯誤的可能性。

未建立此最佳實務時的曝險等級： 中

實作指引

應針對事故案例建立程序手冊，例如：

- 預期事故：應針對您預期的事故建立程序手冊。這包括拒絕服務 (DoS)、勒索軟體和憑證入侵等威脅。
- 已知的安全調查結果或提醒：應針對已知的安全性調查結果和警示 (例如 GuardDuty 調查結果) 建立程序手冊。您可能會收到 GuardDuty 調查結果並思考：「現在該怎麼辦？」 為了防止處理不當或忽略 GuardDuty 調查結果，請為每個潛在的 GuardDuty 調查結果建立程序手冊。部分修復詳細資料和指引可尋自 GuardDuty 文件。值得注意的是，在預設情況下 GuardDuty 是未啟用的狀態，並且會產生費用。如需 GuardDuty 的相關詳細資訊，請參閱 附錄 A：雲端功能定義 - 可見性與提醒。

程序手冊應包含安全分析師應完成的技術步驟，以便充分調查和應對潛在的安全事故。

實作步驟

要納入程序手冊的項目包括：

- 程序手冊概觀：這份程序手冊可處理哪些風險或事故？ 程序手冊的目標是什麼？
- 先決條件：此事故案例需要哪些日誌、偵測機制和自動化工具？ 預期的通知是什麼？
- 溝通和向上呈報資訊：誰參與其中，其聯絡資訊為何？ 每個利害關係人的責任是什麼？
- 回應步驟：在事故應變的各個階段，應採取哪些戰術步驟？ 分析師應該執行哪些查詢？ 應該執行哪些程式碼以達到預期的成果？
  - 偵測：事故的偵測方式為何？
  - 分析：判斷影響範圍的方式為何？
  - 包含：隔離事故以限制範圍的方式為何？
  - 根除：將威脅從環境中移除的方式為何？

  - 復原：受影響的系統或資源重新投入生產環境的方式為何？
- 預期成果：執行查詢和程式碼後，程序手冊的預期結果是什麼？

資源

相關 Well-Architected 的最佳實務：

- SEC10-BP02 - 制定事故管理計畫

相關文件：

- 事故應變程序手冊的架構
- 制定您自己的事故應變程序手冊
- 事故應變程序手冊範例
- 使用 Jupyter 筆記本和 CloudTrail Lake 建置 AWS 事件應變執行手冊

SEC10-BP05 預先佈建存取權

確認事件回應者具有在 AWS 中預先佈建的正確存取權限，以縮短調查直至復原所需的時間。

常見的反模式：

- 使用事件應變的根帳戶。
- 更改現有的使用者帳戶。
- 當提供即時權限提升時直接操控 IAM 許可。

若未建立此最佳實務，暴露的風險等級： 中

實作指引

AWS 建議盡可能降低或避免對長期憑證的依賴，而是採用臨時憑證和 即時 權限提升機制。長期憑證容易發生安全性風險並會增加營運負擔。對於大多數管理任務，以及事件應變任務，我們建議您實作聯合身分 以及 適用於管理存取權的臨時權限提升。在此模型中，使用者會請求提升至較高層級的權限 (例如事件應變角色)；如果使用者符合提升的資格，則會將請求傳送至核准者。如果請求獲得核准，使用者就會收到一組臨時 AWS 憑證 ，使用者可使用此憑證來完成其任務。在這些憑證過期後，使用者就必須提交新的提升權限請求。

我們建議在大多數事件應變情境中，使用臨時權限提升。正確的做法是使用 AWS Security Token Service 和 工作階段政策 來界定存取權的範圍。

當發生聯合身分不可用的情況，例如

- 與遭盜用身分提供者 (IdP) 相關的中斷。
- 設定錯誤或人為錯誤會導致聯合存取管理系統遭到破壞。
- 分散式阻斷服務 (DDoS) 事件或使系統無法使用之類的惡意活動。

在前述的案例中，應會有已設定的 緊急 存取權，可協助調查和及時修復事件。我們建議您使用 具有適當許可的 IAM 使用者， 來執行任務和存取 AWS 資源。僅將根憑證用於 需要根使用者存取權的任務。若要確認事件回應者是否具有 AWS 和其他相關系統的正確存取權，我們建議預先佈建專屬的使用者帳戶。該類使用者帳戶需要提升的存取權，且必須受到嚴格的控制和監控。必須以執行必要任務所需的最低權限來建置這些帳戶，而存取權層級應以事件管理計劃中建立的程序手冊為基礎。

使用專用和專屬的使用者及角色作為最佳實務。透過新增 IAM 政策而臨時提升權限的使用者和角色存取權，會同時使得使用者在事件發生期間的存取權不明確，又有無法將提升的權限撤銷的風險。

您必須盡可能移除相依性，來確認可在各種可能的失敗情境下獲得存取權。為了做到這一點，建立程序手冊來確認事件應變使用者的建立身分是專屬安全性帳戶中的 AWS Identity and Access Management 使用者，且不會透過任何現有的聯合或單一登入 (SSO) 解決方案來管理事件應變使用者。每個個別回應者必須具備其專屬的指定帳戶。帳戶組態必須強制執行 強式密碼政策 和多重要素驗證 (MFA)。如果事件應變程序手冊僅需要 AWS Management Console 的存取權，使用者就不應設定存取金鑰，且應明確禁止使用者建立存取金鑰。您可以使用 IAM 政策或服務控制政策 (SCP) 進行設定，如同 AWS Organizations SCP 的 AWS 安全性 最佳實務中所述。除了在其他帳戶中擔任事件應變角色的能力外，使用者不應具備任何權限。

在事件期間，必須將存取權授予其他內部或外部人員，來協助調查、修復和復原活動。在此案例中，使用先前提到的程序手冊機制，而且必須制定程序，以確認在事件完成後，立即將任何其他存取權撤回。

若要確認事件應變角色的使用是否受到適當的監控和稽核，則必須確保未在人員之間共用為此目的建立的 IAM 使用者帳戶，且除非特定任務所需，否則不得使用 AWS 帳戶 根使用者。如果需要根使用者 (例如，特定帳戶的 IAM 存取權不可用時)，請使用獨立的程序，其中有可用的程序手冊，來確認根使用者密碼和 MFA 權杖是否可用。

若要為事件應變角色設定 IAM 政策，請考慮使用 IAM Access Analyzer 來根據 AWS CloudTrail 日誌產生政策。若要這麼做，請向管理員授予在非生產帳戶上事件應變角色的存取權，並透過程序手冊加以執行。完成後，您就可以建立政策來僅允許所採取的動作。接著就可以將此政策套用至所有帳戶中的所有

事件應變角色。您可能希望為每個程序手冊建立個別 IAM 政策，來讓管理和稽核作業更輕鬆。範例程序手冊可能包含勒索軟體、資料洩漏、生產存取權遺失和其他情境的應變計劃。

使用事件應變使用者帳戶來擔任 在其他 AWS 帳戶 中專屬事件應變 IAM 角色。必須將這些角色設定為僅供安全性帳戶中的使用者擔任，而信任關係必須要求呼叫主體使用 MFA 進行驗證。這些角色必須使用嚴格控制範圍的 IAM 政策來控制存取權。確保所有對這些角色的 `AssumeRole` 請求都記錄在 CloudTrail 中並據以發出警示，而使用這些角色採取的任何動作都會記錄下來。

強烈建議必須清楚地命名 IAM 使用者帳戶和 IAM 角色，因此您可以輕鬆地在 CloudTrail 日誌中找到這些帳戶和角色。這類範例便是將 IAM 帳戶命名為 *<USER_ID>*-BREAK-GLASS 以及將 IAM 角色命名為 BREAK-GLASS-ROLE。

CloudTrail 會用來在 AWS 帳戶中記錄 API 活動，且應用來 設定對事件應變角色使用情形的警示。請參閱部落格貼文，其中會說明使用根金鑰如何設定警示。您可以修改說明，以便針對以下事件設定 Amazon CloudWatch 指標篩選條件至篩選條件： `AssumeRole` 事件，該事件與事件應變 IAM 角色相關：

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

由於事件應變角色可能具備很高的存取權限，因此必須將這些警示傳送給多個群組，並據此快速採取行動。

在事件期間，回應者可能需要存取未受 IAM 直接保護的系統。其中可能包含 Amazon Elastic Compute Cloud 執行個體、Amazon Relational Database Service 資料庫或軟體即服務 (SaaS) 平台。強烈建議使用此方法，而不是使用 SSH 或 RDP 等原生通訊協定，AWS Systems Manager Session Manager 會用於對 Amazon EC2 執行個體的所有管理存取權。您可以使用安全且受稽核的 IAM 來控制此存取權。 您也可以使用 AWS Systems Manager Run Command 文件 來自動化部分程序手冊，如此可減少使用者錯誤並縮短復原時間。如需資料庫和第三方工具的存取權，我們建議將存取憑證存放在 AWS Secrets Manager 中，並將存取權授予事件回應者角色。

最後，應將事件應變 IAM 使用者帳戶的管理作業新增至 加入者、異動者和離職者程序中， 並定期審查和測試此管理作業，以確認僅允許預期的存取。

資源

相關文件：

- 管理對 AWS 環境的臨時提升存取權

- AWS 安全事件應變指南
- AWS Elastic Disaster Recovery
- AWS Systems Manager Incident Manager
- 為 IAM 使用者設定帳戶密碼政策
- 在 AWS 中使用多重要素驗證 (MFA)
- 使用 MFA 設定跨帳戶存取權
- 使用 IAM Access Analyzer 來產生 IAM 政策
- 在多帳戶環境中 AWS Organizations 服務控制政策的最佳實務
- 如何在使用 AWS 帳戶的根存取金鑰時接收通知
- 使用 IAM 受管政策來建立精細的工作階段許可

相關影片：

- 將 AWS 中的事件應變和鑑識自動化
- 執行手冊、事件報告和事件應變的 DIY 指南
- 準備和回應 AWS 環境中的安全事件

相關範例：

- 實驗室：AWS 帳戶設定和根使用者
- 實驗室：使用 AWS 主控台和 CLI 來應變事件

SEC10-BP06 預先部署工具

確認安全人員具有預先部署的適當工具，以縮短調查直至復原的時間。

未建立此最佳實務時的曝險等級： 中

實作指引

若要自動化安全回應和操作功能，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。整合異常偵測系統 (例如 Amazon GuardDuty、AWS CloudTrail Insights 和 Amazon CloudWatch 異常檢測) 可以減輕常見閾值型提醒的負擔。

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復問題。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。

在安全調查期間，您需要能夠檢閱相關日誌以記錄和了解該事故的完整範圍和時間表。產生提醒也需要日誌，以指出特定關注的動作已發生。選擇、啟用、儲存和設定查詢與擷取機制和設定警示至關重要。此外，提供搜尋日誌資料之工具的有效方法是 Amazon Detective。

AWS 擁有 200 多種雲端服務和數千種特徵。我們建議您檢閱可支援並簡化事故應變策略的服務。

除了記錄之外，您還應該開發和實作 中繼資料，。標記可以幫助提供與 AWS 資源用途有關的上下文。標記也可用於自動化。

實作步驟

選取並設定日誌以進行分析和提醒

請參閱下列有關設定事故應變記錄的文件：

- 安全事故應變的記錄策略
- SEC04-BP01 設定服務和應用程式記錄

啟用安全服務以支援偵測和回應

AWS 提供原生偵測、預防性和回應式功能，而其他服務可用於建立自訂安全性解決方案的架構。如需安全事故應變最相關的服務清單，請參閱 雲端功能定義。

制定和實作標記策略

取得有關業務使用案例和圍繞 AWS 資源的相關內部利害關係人的上下文資訊可能很困難。執行此操作的一種方法是使用標籤的形式，此形式會將中繼資料指派給 AWS 資源，並包含使用者定義的鍵值組。您可以建立標籤，依目的、擁有者、環境、處理的資料類型以及您選擇的其他條件來分類資源。

擁有一致的標記策略可讓您快速找出和辨別與 AWS 資源有關的情境資訊，從而加快回應時間並盡可能減少用在組織情境的時間。標籤也可以作為啟動回應自動化的機制。如需要標記哪些內容的詳細資訊，請參閱 標記您的 AWS 資源。您需要先定義要在整個組織中實作的標籤。之後，您將實作並強制執行

此標記策略。如需實作和強制執行的詳細資訊，請參閱 使用 AWS 標籤政策和服務控制政策 (SCP) 實作 AWS 資源標記策略。。

資源

相關 Well-Architected 的最佳實務：

- SEC04-BP01 設定服務和應用程式記錄
- SEC04-BP02 集中分析日誌、問題清單和指標

相關文件：

- 安全事故應變的記錄策略
- 事故應變雲端功能定義

相關範例：

- 使用 Amazon GuardDuty 和 Amazon Detective 進行威脅偵測與回應
- 安全中心工作坊
- 使用 Amazon Inspector 管理漏洞

SEC10-BP07 執行模擬

在組織隨著時間成長和發展時，威脅態勢也會跟著演變，因此持續審查事件應變能力是很重要的。執行模擬 (也稱為比賽日) 是可用於執行此評估的一種方法。模擬會使用真實世界的安全事件案例，這些案例旨在模擬威脅參與者的策略、技術和程序 (TTP)，並且讓組織可藉由回應這些可能發生在現實中的模擬網路事件，來運用和評估其事件應變能力。

建立此最佳實務的好處：模擬具有多種好處：

- 驗證網路整備程度和培養事件應變人員的信心。
- 測試工具和工作流程的正確性及效率。
- 根據您的事件應變計畫，精進溝通和呈報方法。
- 提供回應罕見媒介的機會。

未建立此最佳實務時的風險暴露等級：中

實作指引

主要的模擬類型有三種：

- 桌上模擬演練：桌上模擬方法是基於討論的會議，涉及各種事故應變利害關係人的角色和責任練習，並使用已建立的溝通工具和程序手冊。模擬演練促進通常可在虛擬場地、實體場地或兩者的組合於一整天內完成。桌上模擬演練以討論為主軸，因此側重於程序、人員和協作。技術在討論中是不可或缺的一部分，但事件應變工具或腳本的實際使用通常不是桌上模擬演練的一部分。
- 紫隊模擬演練：紫隊模擬演練提高了事故應變人員 (藍隊) 和模擬威脅參與者 (紅隊) 之間的協作層級。藍隊由安全營運中心 (SOC) 的成員組成，但也可以包含在實際網路事件期間涉入的其他利害關係人。紅隊由滲透測試團隊或受過攻擊性安全培訓的主要利害關係人組成。紅隊在設計場景時會與模擬演練協調員合作，使場景精確且可行。在紫隊模擬演練期間，主要重點是偵測機制、工具和支援事件應變工作的標準操作程序 (SOP)。
- 紅隊模擬演練：在紅隊模擬演練期間，攻方 (紅隊) 會進行模擬，以在預定範圍內達到某個目標或一組目標。守方 (藍隊) 不一定知道模擬演練的範圍和持續時間，這對他們應對實際事件的能力可呈現出更真實的評估。由於紅隊模擬演練可能是侵入性測試，請謹慎行事並施加控制，以確認該模擬演練不會對您的環境造成實際傷害。

考慮定期推行網路模擬。每種模擬演練類型都可以為參與者和整個組織提供特有的好處，因此您可以選擇從較不複雜的模擬類型 (例如桌上模擬演練) 開始著手，然後再進入更複雜的模擬類型 (紅隊模擬演練)。您應根據自身的安全成熟度、資源和所需的結果來選擇模擬類型。由於複雜性和成本較高，有些客戶可能不會選擇執行紅隊模擬演練。

實作步驟

無論您選擇的模擬類型為何，模擬通常會執行下列實作步驟：

1. 定義核心演練元素：定義模擬案例和模擬的目標。這兩者都應獲得領導階層的允許。
2. 找出關鍵利害關係人：模擬演練至少需要模擬演練協調員和參與者。根據情境，可能會涉及法律、通訊或主管領導階層等其他利害關係人。
3. 建立和測試情境：如果特定元素不可行，則可能需要在情境建置期間加以重新定義。預計最終的情境會成為此階段的輸出。
4. 促進模擬：模擬的類型將決定使用的促進形式 (編撰的場景對比於高度技術性的模擬場景)。協調員應使其促進策略與模擬演練目標相對應，他們應盡可能吸引所有模擬演練參與者，以提供最大的效益。
5. 撰寫事後報告 (AAR)：找出進展順利的領域、可以改進的領域，以及潛在的差距。AAR 應衡量模擬的有效性以及團隊對於模擬事件的應變能力，以便在未來的模擬追蹤進展幅度。

資源

相關文件：

- AWS 事故應變指南

相關影片：

- AWS GameDay - Security Edition

操作

操作是進行事故回應的核心。這也是採取行動回應和補救安全事故的所在。操作包括以下五個階段：偵測、分析、 遏制、根除和 復原。下表中可找到這些階段和目標的說明。

階段	目標
偵測	識別潛在的安全事件。
分析	判斷安全事件是否為事故，並評估事故的範圍。
遏制	盡量縮小並限制安全事件的範圍。
根除	移除與安全事件相關的未經授權資源或成品。實作造成安全事故的緩和措施。
復原	將系統還原至已知的安全狀態，並監控這些系統以確認威脅未再發生。

這些階段應做為您回應和操作安全事故時的指引，以便採取有效且可靠的方式來回應。您採取的實際行動會因事故而有所不同。舉例來說，對於涉及勒索軟體的事故與涉及公有 Amazon S3 儲存貯體的事故將採取不同的回應步驟。此外，這些階段不一定會依序發生。在遏制和根除之後，您可能需要返回分析，以了解採取的行動是否有效。

涵蓋人員、流程和技術的完整準備，是讓操作發揮效用的關鍵。因此，請依照 準備 一節的最佳實務，以便有效回應作用中安全事件。

若要深入了解，請參閱《 AWS安全事件應變指南》中的 操作 一節。

事後處理

威脅態勢不斷變化，因此組織有效保護環境的能力也務必同樣保持動態。持續改進的關鍵在於反覆執行事故和模擬的結果，以便改善有效偵測、回應和調查可能發生的安全事件的能力、減少可能的漏洞、縮短回應時間，並且恢復安全操作。下列機制可協助您驗證組織是否具備最新功能和知識，以便在任何情況下有效回應。

最佳實務

- SEC10-BP08 建立從事故中學習的架構

SEC10-BP08 建立從事故中學習的架構

實作 經驗教訓 的架構和根本原因分析能力，不僅有助改善事故應變能力，還有助防止事故重複發生。透過學習每個事故，您可以協助避免重複相同的錯誤、披露或錯誤設定，不僅能夠改善安全狀態，還可以盡可能縮短因可預防情況而損失的時間。

未建立此最佳實務時的曝險等級： 中

實作指引

實作 經驗教訓 是非常重要的，其可在高層級實現以下幾點：

- 什麼時候開設經驗教訓課程？
- 經驗教訓課程中包含哪些內容？
- 經驗教訓課程的進行方式？
- 這個課程的參與者以及參與方式？
- 如何找出待改善之處？
- 您將如何確保有效地追蹤和實作待改善之處？

此架構不應該針對或責怪個人，而應該專注於改善工具和流程。

實作步驟

除了前述所列的高層級結果之外，確保您提出正確問題以從流程中獲得最大價值 (即協助您找到可行改善之處的資訊) 非常重要。考慮這些問題，有助您發起經驗教訓的討論：

- 事故是什麼？

- 第一次識別事故的時間？
- 事故的識別方式？
- 哪些系統對活動發出提醒？
- 涉及哪些系統、服務和資料？
- 具體發生的事故？
- 哪些方面做得很好？
- 哪些方面做得不好？
- 哪個流程或程序失敗或未能擴展以回應事故？
- 在以下幾個領域有哪些可以改善之處：
  - 人員
    - 需要聯絡的對象實際上是否有空，並且聯絡人清單是最新的嗎？
    - 人們是否缺少有效回應和調查事故所需的培訓或能力？
    - 適當的資源是否已準備就緒且可供使用？
  - 流程
    - 是否遵循流程和程序？
    - 是否已記錄並提供這類事故的流程和程序？
    - 是否缺少必要的流程和程序？
    - 回應人員是否能夠即時存取所需的資訊以回應問題？
  - 技術
    - 現有的提醒系統是否能有效地識別活動，並據以發出提醒？
    - 我們如何將偵測時間縮短 50%？
    - 是否需要改善現有提醒，或是需要針對此類事故建立新的提醒？
    - 現有的工具是否允許對事故進行有效的調查 (搜尋/分析)？
    - 可以做什麼來協助加快這類事故的識別速度？
    - 可以做什麼來協助避免這類事故再次發生？
    - 負責改善計畫的人是誰，您將如何測試是否已實作此計畫？
    - 實作和測試其他監控或預防性控制措施和流程的時間表為何？

這份清單並不詳盡，但可作為起點，幫助您識別組織和企業的需求，以及如何分析這些需求，以便最有效地從事故中學習並持續改善安全狀態。最重要的是透過將經驗教訓納入事故應變流程，文件和利害關係人期望的標準部分。

資源

相關文件：

- AWS 安全事故應變指南 - 建立從事故中學習的架構
- NCSC CAF 指南 - 經驗教訓

應用程式安全

應用程式安全 (AppSec) 介紹如何為開發工作負載的安全屬性進行設計、建置與測試的整體過程。您應該安排組織成員接受適當訓練，了解您的建置與發佈基礎結構的安全屬性，以及應用自動化來識別出安全問題。

採用應用程式安全測試做為軟體開發生命週期 (SDLC) 與發佈後程序中的常規部分，有助於確保您可建立一套結構化機制，專門識別、修正應用程式安全問題，以及防止這些問題進入您的生產環境。

您的應用程式開發方法應該在設計、建置與操作工作負載期間納入安全控制。過程當中，可以調整程序，達到持續減少缺陷和最低技術負債。例如，在設計階段中應用威脅建模有助於提早發現設計瑕疵，修正更加簡單，成本節省更多，而不需要等到日後才能進行緩解。

解決瑕疵的成本與複雜性通常比過去在 SDLC 中來得低。最簡單的解決問題方法就是別讓問題發生，因此從使用威脅模型開始，有助於您專注在設計階段的正確成果。隨著 AppSec 計劃逐漸成熟，您可以自動化方式提高測試量，改善意見回饋對建置人員的準確性 (保真度)，同時縮短安全檢閱所需要的時間。這些動作全都可以改善所建置軟體的品質，並且加快功能進入生產階段。

這些實作指導方針著重在四大區域：組織和文化、管道的安全性、管道中的安全性，以及相依性管理。每個區域都會提供一組可實作原則，並針對設計、建置與操作工作負載的做法提供端對端檢視。

在 AWS 中，您可以使用許多方法來解決應用程式安全計劃問題。當中有一些方法依賴技術，而其他方法則著重在應用程式安全計劃的人員和組織層面。

最佳實務

- SEC11-BP01 應用程式安全訓練
- SEC11-BP02 自動化在整個開發和發佈生命週期的測試
- SEC11-BP03 定期進行滲透測試
- SEC11-BP04 手動程式碼檢閱
- SEC11-BP05 集中化套件和相依性的服務
- SEC11-BP06 以程式設計方式部署軟體
- SEC11-BP07 定期評估管道的安全屬性
- SEC11-BP08 打造在工作負載團隊中納入安全所有權的計劃

SEC11-BP01 應用程式安全訓練

提供可讓組織內建置人員接受安全開發和操作應用程式等常見實務的訓練。採用著重安全的開發方法，有助於減少只能在安全審查階段偵測到問題的可能性。

預期成果： 軟體的設計與建置應考慮安全層面。組織中的建置人員如果接受過從威脅模型開始的安全開發方法訓練，其所生產軟體的整體品質與安全都能獲得改善。這種方法能縮短遞送軟體或功能所花費的時間，因為其必須在安全審查階段之後重新作業的機率較低。

就這項最佳實務的目的而言，安全開發與所編寫的軟體，以及支援軟體開發生命週期 (SDLC) 的工具或系統相關。

常見的反模式：

- 一直等到安全審查階段，才開始考慮系統的安全屬性。
- 將所有的安全性決定工作全部留給安全團隊。
- 未在 SDLC 溝通如何做出與整體安全期待或組織政策相關的決定。
- 太晚參與安全審查程序。

建立此最佳實務的優勢：

- 可在開發生命週期初期更清楚了解組織對於安全的要求。
- 可以更快識別、修復安全問題，進而加快功能交付速度。
- 改善軟體和系統的品質。

未建立此最佳實務時的風險暴露等級：中

實作指引

提供組織內建置人員的訓練。一開始上威脅模型相關課程，有助於奠定安全訓練的良好基礎。理想狀況下，建置人員應該能夠自助存取與其各自工作負載相關的資訊。這種存取能協助人員做出有關建置中系統安全屬性的明智決策，而不需要詢問其他團隊。參與安全團隊進行審查的程序應該清楚定義，並能輕鬆實施。在審查程序中的步驟則應納入安全訓練當中。如果有已知的實作模式或範本，則其應可輕鬆找出，且連結至整體安全需求。考慮使用 AWS CloudFormation、 AWS Cloud Development Kit (AWS CDK) 建構模組、Service Catalog，或者其他的範本工具，以便降低自訂組態的需求。

實作步驟

- 一開始安排建置人員上威脅模型相關課程，奠定良好基礎，並有助於進行考量安全層面的訓練。
- 提供存取 AWS 培訓 和認證、產業，或 AWS 合作夥伴訓練的權限。
- 提供有關組織安全審查程序的培訓，明確劃分安全團隊、工作負載團隊和其他相關人員之間的責任分配。
- 發布關於如何達到您的安全要求的自助式指南，包含程式碼片段和範本（如有提供）。
- 定期取得建置人員團隊安全審查程序與訓練體驗方面的意見回饋，並使用該意見回饋進行改善。
- 使用演練日或錯誤修復日活動，協助減少問題數量，並提升建置人員的技能水平。

資源

相關的最佳實務：

- SEC11-BP08 打造在工作負載團隊中納入安全所有權的計劃

相關文件：

- AWS 培訓 和認證
- 如何思考雲端安全管控
- 如何建立威脅模型
- 加速訓練 – AWS 技能培養

相關影片：

- 預防性安全：考量與方法

相關範例：

- 威脅模型相關的研討會
- 開發人員的產業認知

相關服務：

- AWS CloudFormation

- AWS Cloud Development Kit (AWS CDK) (AWS CDK) 建構模組
- Service Catalog
- AWS 錯誤大集合

SEC11-BP02 自動化在整個開發和發佈生命週期的測試

自動化在整個開發和發佈生命週期的安全署性測試。自動化可以讓軟體在發佈之前更容易一致且重複地找出潛在問題，因此能降低將供應軟體的安全問題風險。

預期成果： 自動化測試的目標是提供以程式設計方式，及早偵測潛在問題，而且常常是遍及整個開發生命週期。啟用自動化迴歸測試時，您可以對變更之後的軟體重新執行功能性與非功能性的測試，確認先前測試過的軟體運作仍如預期。如果定義安全單元測試來檢查常見的錯誤組態，例如損壞或缺失的驗證，您就能夠在開發過程中及早發現和修正這些問題。

測試自動化會使用專用測試個案來進行應用程式驗證，測試期間以應用程式需求和所需功能為基礎。自動化測試會將產生的測試輸出與其個別預期輸出進行比較，得到最後結果，進而加快整體的測試生命週期。包括像是迴歸測試與單位測試套組的測試方法最適合自動化應用。自動化安全屬性測試，建置人員就能接收自動化意見回饋，而不需要等待舉行安全檢閱。採用靜態或靜態程式碼分析的自動化測試，可以提高程式碼品質，並協助及早在開發生命週期中偵測出潛在的軟體問題。

常見的反模式：

- 未傳達測試個案與自動化測試的測試結果。
- 僅在即將發佈前執行自動化測試。
- 自動化有經常改變需求的測試個案。
- 無法提供如何解決安全測試結果的指引。

建立此最佳實務的優勢：

- 降低人員評估系統安全署性的依賴性。
- 可在跨多個工作串流之間找到一致結果，進而提高一致性。
- 降低造成安全問題被導入產品線上軟體的可能性。
- 因提早捕捉到軟體問題，而縮短偵測與矯正之間的範圍時段。
- 提高跨多個工作串流之系統或重複行為的能見度，其可用來促進整體組織改進。

未建立此最佳實務時的風險暴露等級：中

實作指引

隨著軟體逐漸建置，採用各種不同機制來測試軟體，確保您正根據應用程式的業務邏輯為主的功能性需求，以及著重應用程式可靠性、效能和安全性的非功能性需求，進行應用程式的測試作業。

靜態應用程式安全測試 (SAST) 分析原始程式碼是否有異常的安全模式，並提供可能存在缺陷程式碼的提示。SAST 依賴靜態輸入來測試某個範圍的已知安全問題，這些輸入包括文件 (需求規格、設計文件，以及設計規格4) 和應用程式原始程式碼。靜態程式碼分析器可協助加快大量程式碼的分析作業。NIST 品質群組則提供原始程式碼安全分析器的比較，其中包括能用於位元組程式碼掃描器和二進位程式碼掃描器的開放原始碼工具。

應用動態分析安全測試 (DAST) 方法以補充您的靜態測試，這個方法會在應用程式執行期間進行測試，找出潛在的意外行為。動態測試可用來偵測出靜態分析無法偵測出的潛在問題。在程式碼儲存、建置和管道等階段進行測試，您就可以檢查進入程式碼當中的各種不同潛在問題類型。Amazon CodeWhisperer 提供程式碼建議，包括在建置人員的 IDE 中執行安全掃描。Amazon CodeGuru Reviewer 可以找出關鍵問題、安全問題，以及在應用程式開發期間難以發現的錯誤，並提供改善程式碼品質的建議。

開發人員安全研討會使用 AWS 開發人員工具，像是 AWS CodeBuild、AWS CodeCommit 和 AWS CodePipeline，執行包括 SAST 和 DAST 測試方法的發佈管道自動化。

隨著 SDLC 繼續進行，建立包括安全團隊定期進行應用程式檢閱的反覆程序。收集自這些安全檢閱的意見回饋應加以解決，並在發佈準備度檢閱時加以驗證。這些檢閱作業會建立堅實強大的應用程式安全狀態，並提供建置人員可解決潛在問題的可行動意見回饋。

實作步驟

- 實作一致的 IDE、程式碼檢閱，以及包括安全測試的 CI/CD 工具。
- 考慮 SDLC 中的哪個位置適合封鎖管道，而不只是通知建置人員出現需要矯正的問題。
- 開發人員安全研討會提供在發佈管道中整合靜態與動態測試的範例。
- 使用自動化工具執行測試或程式碼分析，這些工具包括像是已與開發人員 IDE 完成整合的 Amazon CodeWhisperer，以及可在遞交認可時掃描程式碼的 Amazon CodeGuru Reviewer，協助建置人員在正確時間得到意見回饋。
- 使用 AWS Lambda 進行建置時，您可以使用 Amazon Inspector 來掃描多個功能的應用程式程式碼。
- AWS CI/CD 研討會提供在 AWS 上建置 CI/CD 管道的起點。

- 如果將自動化測試納入 CI/CD 管道，您應該使用票證系統來追蹤通知，以及軟體問題的矯正。
- 如果是可能會產生發現結果的安全測試，連結矯正的指引將有助於建置人員改善程式碼品質。
- 定期分析自動化工具所找到的發現結果，以便找出下次自動化、建置人員訓練或認知行銷活動的優先順序。

資源

相關文件：

- 持續交付與持續部署

- AWS DevOps 能力合作夥伴
- AWS 安全能力合作夥伴 (應用程式安全)
- 選擇 Well-Architected CI/CD 方法
- 使用 Amazon EventBridge 和 Amazon CloudWatch Events 監控 CodeCommit 事件
- Amazon CodeGuru 檢閱中的機密偵測
- 配合有效管控，加速在 AWS 的部署
- AWS 如何達到自動化安全、無人為介入的部署

相關影片：

- 無人為介入：Amazon 的自動化持續交付管道
- 自動化跨帳戶 CI/CD 管道

相關範例：

- 開發人員的產業認知
- AWS CodePipeline 管控 (GitHub)
- 開發人員安全研討會
- AWS CI/CD 研討會

SEC11-BP03 定期進行滲透測試

定期對您的軟體進行滲透測試。這項機制有助於找出無法在自動化測試或手動程式碼審查時偵測到的潛在軟體問題。同時也有助於您了解偵測控制措施的效用。滲透測試應嘗試判斷軟體是否會透過非預期的方式執行，例如暴露原本應受保護的資料，或是授與超乎預期的較廣泛權限。

預期成果： 滲透測試可用來為您的應用程式安全屬性進行偵測、修復和驗證。軟體開發生命週期 (SDLC) 期間應該進行定期與排程型滲透測試。從滲透測試找到的發現結果應事先解決，才能安排軟體發行。您應該分析從滲透測試得到的發現結果，並找出是否有任何問題可使用自動化找出。實施包括主動意見回饋機制的定期和可重複滲透測試程序，可協助建置人員得知指引，並改善軟體品質。

常見的反模式：

- 只對已知或普遍存在的安全問題進行滲透測試。
- 滲透測試應用程式 (不含相依第三方工具和程式庫)。
- 只對套件安全問題進行滲透測試，且不評估已實作的商業邏輯。

建立此最佳實務的優勢：

- 提高軟體在發行前的安全屬性信心。
- 可找出偏好應用程式模式，並藉以提高軟體品質的機會。
- 在開發生命週期初期進行的意見回饋循環流程，當中的自動化或額外訓練可以改善軟體的安全屬性。

未建立此最佳實務時的風險暴露等級：高

實作指引

滲透測試是一種結構化的安全測試練習，過程當中，您會執行計劃的安全性缺口情境，對安全控制進行偵測、修復與驗證。滲透測試從偵察活動開始，過程中會根據目前的應用程式設計與其相依性收集資料。已經建置並執行精選的安全特定測試情境清單。這些測試的主要目的在於找出您的應用程式中的安全問題，這些問題可能會被利用來非預期地存取環境，或未經授權存取資料。當您推出新功能，或是每當應用程式遭遇重大的功能變更或進行技術實作，您就應該進行滲透測試。

您應該識別開發生命週期中最適合進行滲透測試的階段。這項測試的執行時間應該盡量延到系統功能接近預定發行階段之時，而且要保留足夠修復任何問題的時間。

實作步驟

- 建立處理滲透測試範圍限制方式的結構化程序，前提是這個關於威脅模型的程序是維持內容的好方法。
- 識別開發週期中最適合進行滲透測試的時機。進行測試時應該是預期應用程式進行最少變更，而且有足夠時間進行修復。
- 訓練建置人員學會從滲透測試發現結果預期哪些內容，以及如何取得關於修復的資訊。
- 使用工具，透過自動化共通或可重複測試，加速滲透測試程序。
- 分析滲透測試發現結果來找出系統性安全問題，並使用這份資料，得知其他的自動化測試與持續進行的建置人員教育。

資源

相關的最佳實務：

- SEC11-BP01 應用程式安全訓練
- SEC11-BP02 自動化在整個開發和發佈生命週期的測試

相關文件：

- AWS 滲透測試會提供在 AWS 上進行滲透測試的詳細指引
- 配合有效管控，加速在 AWS 的部署
- AWS 安全能力合作夥伴
- 現代化您在 AWS Fargate 上的滲透測試架構
- AWS Fault injection Simulator

相關範例：

- 自動化配合 AWS CodePipeline 的 API 測試 (GitHub)
- 自動化安全協助程式 (GitHub)

SEC11-BP04 手動程式碼檢閱

對您製作的軟體進行手動程式碼檢閱。此程序有助於確認編寫程式碼的人員並非檢查程式碼品質的唯一人員。

預期成果： 在開發期間納入手動程式碼檢閱步驟可提高所編寫軟體的品質，因此有助於提升技能較差團隊成員的程度，而且有機會找出適合實施自動化的位置。手動程式碼檢閱可獲自動化工具和測試支援。

常見的反模式：

- 未在部署前先執行程式碼檢閱。
- 編寫程式碼和檢閱程式碼是相同人員。
- 未使用自動化來協助或協調程式碼檢閱。
- 建置人員在開始檢閱程式碼之前未先經過應用程式安全的訓練。

建立此最佳實務的優勢：

- 程式碼品質更高。
- 經由重複使用常用方法而使程式碼開發更具一致性。
- 減少在滲透測試與後期階段找出問題的數量。
- 團隊內部的知識轉移效能更高。

未建立此最佳實務時的風險暴露等級：中

實作指引

檢閱步驟應該是在整體程式碼管理流程中的實作部分。具體步驟依據分支、提取請求與合併所使用的不同方法而定。您可能使用 AWS CodeCommit 或第三方解決方案，例如，GitHub、GitLab 或 Bitbucket。無論使用哪種方法，您都一定要確認這些程序必須經過檢閱程式碼，才能部署至生產環境。使用 Amazon CodeGuru Reviewer 等工具可以讓協調程式碼檢閱過程變得更簡單。

實作步驟

- 在程式碼管理流程中實作手動檢閱步驟，並先執行這項檢閱之後，再繼續執行。
- 考慮 Amazon CodeGuru Reviewer 用於程式碼檢閱的管理與協助。
- 實作的核准流程必須先完成程式碼檢閱，程式碼才能進入下一個階段。

- 確認已經安排程序，可以識別將在手動程式碼檢閱期間找到，並可自動偵測出的問題。
- 採用符合您的程式碼開發實務之方法，整合手動程式碼檢閱步驟。

資源

相關的最佳實務：

- SEC11-BP02 自動化在整個開發和發佈生命週期的測試

相關文件：

- 使用 AWS CodeCommit 儲存庫中的提取請求
- 使用 AWS CodeCommit 中的核准規則範本
- 關於使用 GitHub 中的提取請求
- 使用 Amazon CodeGuru Reviewer 自動進行程式碼檢閱
- 使用 Amazon CodeGuru Reviewer CLI，自動化偵測 CI/CD 管道中的安全性漏洞與錯誤

相關影片：

- 使用 Amazon CodeGuru 持續改善程式碼品質

相關範例：

- 開發人員安全研討會

SEC11-BP05 集中化套件和相依性的服務

提供可讓建置人員團隊取得軟體套件和其他相依性的集中化服務。這樣套件就能先接受驗證，再納入編寫的軟體，並提供在您的組織中被使用的軟體分析的資料來源。

預期成果： 軟體由一組其他軟體套件，加上原先所寫程式碼共同組成。因此取用重複使用的實作功能變得很簡單，例如 JSON 剖析器或加密程式庫。依照邏輯方式集中這些套件與相依性的來源，可以為安全團隊提供先驗證過套件再提供使用的機制。這個方法也能減少由於現有套件變更或直接由建置人員團隊從網際網路納入任意套件，而引發未預期的風險問題。使用這個方法再加上手動與自動測試流程，就能提高對於開發中軟體品質的信心。

常見的反模式：

- 從網際網路的任意儲存庫中取出套件。
- 新套件未經測試就提供給建置人員。

建立此最佳實務的優勢：

- 更清楚了解哪些套件將用於建置中的軟體。
- 可以在了解過實際使用情況而需要更新套件時通知工作負載團隊。
- 降低在軟體中納入有問題套件的風險。

未建立此最佳實務時的風險暴露等級：中

實作指引

提供可讓建置人員輕鬆取得的套件和其他相依性集中化服務。集中化服務可依照邏輯方式進行集中，而非實作成單一龐大的系統。這個方法可讓您用符合建置人員需求的方式提供服務。您應該實作一種能在發生更新或新需求萌生時，快速在儲存庫新增套件的方法。AWS 服務，例如 AWS CodeArtifact 或類似的 AWS 合作夥伴解決方案就能提供發揮這種能力的方法。

實作步驟：

- 實作依照邏輯方式集中，而且各種軟體開發所在環境均可使用的儲存庫服務。
- 將儲存庫的存取作業納入 AWS 帳戶 銷售程序。
- 建置自動化測試流程，在將套件發行至儲存庫之前先進行測試。
- 維護最常使用的套件、語言，以及變更程度最高團隊的規格表。
- 提供可讓建置人員團隊自動要求新套件與提供意見回饋的機制。
- 定期掃描儲存庫中的套件，識別最近所找到問題的潛在影響。

資源

相關的最佳實務：

- SEC11-BP02 自動化在整個開發和發佈生命週期的測試

相關文件：

- 配合有效管控，加速在 AWS 的部署
- 使用 CodeArtifact 套件來源控制工具組加強您的套件安全
- 偵測使用 Amazon CodeGuru Reviewer 記錄日誌中的安全問題
- 軟體成品的供應鏈層級 (SLSA)

相關影片：

- 預防性安全：考量與方法
- 安全的 AWS 原則 (re:Invent 2017)
- 當安全性、安全和緊迫性都很重要時：Handling Log4Shell

相關範例：

- 多重區域套件發行管道 (GitHub)
- 使用 AWS CodePipeline 在 AWS CodeArtifact 上發行 Node.js 模組 (GitHub)
- AWS CDK Java CodeArtifact 管道範例 (GitHub)
- 使用 AWS CodeArtifact 分發私有.NET NuGet 套件 (GitHub)

SEC11-BP06 以程式設計方式部署軟體

盡可能以程式設計方式進行軟體部署。此方法可減少部署失敗或因人為疏失而發生非預期問題的機率。

預期成果：讓人員遠離資料是在 AWS 雲端 中安全建置的重要原則。這項原則包括軟體的部署方式。

不仰賴人員的軟體部署具備更高的可信度，因為測試結果就是部署結果，而且每次部署都會一致。軟體應該不需要變更就能在不同環境中運作。使用十二因素應用程式開發的原則時，特別是指組態外部化，可以將相同的程式碼部署到多個環境，而不需要任何變更。密碼編譯型簽署的軟體套件是用來確認環境之間未發生任何變更的好方法。這個方法的最終成果是降低變更程序中的風險，並且改善軟體發佈一致性。

常見的反模式：

- 手動部署軟體至生產環境。
- 手動執行因應不同環境需求的軟體變更。

建立此最佳實務的優勢：

- 提高軟體發佈程序的可信度。
- 降低變更失敗影響到業務功能的風險。
- 因變更風險降低而增加發佈規律。
- 部署其間意外事件的自動回復能力。
- 可以密碼編譯方式證明所測試的軟體就是實際部署的軟體。

未建立此最佳實務時的風險暴露等級：高

實作指引

建置 AWS 帳戶 結構，以便排除環境的持續人員存取，並使用 CI/CD 工具來執行部署。建立應用程式的架構，使其能從外部來源取得環境特定組態資料，例如 AWS Systems Manager 參數存放區。簽署通過測試的套件，並在部署期間驗證這些簽章。設定 CI/CD 管道，以便推送應用程式程式碼，並可使用Canary 來確認部署成功。使用像是 AWS CloudFormation 或 AWS CDK 等工具來定義基礎架構，接著使用 AWS CodeBuild 和 AWS CodePipeline 來執行 CI/CD 操作。

實作步驟

- 建置定義明確的 CI/CD 管道，以便簡化部署程序。
- 使用 AWS CodeBuild 和 AWS 程式碼管道提供 CI/CD 功能時，可以讓您輕鬆地將安全測試整合至管道中。
- 遵循使用多個帳戶整理您的 AWS 環境白皮書中的環境區隔相關指引。
- 確認已在執行生產工作負載的環境中無持續人員存取。
- 建立應用程式的架構，使其支援組態資料的外部化。
- 考慮使用藍/綠部署模型進行部署。
- 實作 Canary 來驗證軟體部署成功。
- 使用像是 AWS Signer 或 AWS Key Management Service (AWS KMS) 等密碼編譯工具來簽署與驗證將要部署的軟體套件。

資源

相關的最佳實務：

- SEC11-BP02 自動化在整個開發和發佈生命週期的測試

相關文件：

- AWS CI/CD 研討會
- 配合有效管控，加速在 AWS 的部署
- 自動化安全、無人為介入的部署
- 使用 AWS Certificate Manager Private CA 和 AWS Key Management Service 非對稱金鑰的程式碼簽署
- 程式碼簽署，AWS Lambda 的信任和完整性控制

相關影片：

- 無人為介入：自動化在 Amazon 的持續交付管道

相關範例：

- 使用 AWS Fargate 的藍/綠部署

SEC11-BP07 定期評估管道的安全屬性

採用 Well-Architected 安全原則保護您的流程，特別注意權限的區隔。定期評估管道基礎設施的安全屬性。有效管理管道的安全，就能讓您的軟體通過管道中重重的安全性考驗。

預期成果：用於建置與部署軟體的管道應該遵循針對環境中任何其他工作負載所建議的相同實務。管道中所實作的測試不應由使用測試的建置人員進行編輯。這些管道應該只具備其預計部署所需要的權限，並且應實作保護措施，防止部署至錯誤的環境。管道不應只依賴長期憑證資訊，並且應設定成能夠發出狀態資訊，以驗證建置環境的完整性。

常見的反模式：

- 安全測試可能遭建置人員避開。
- 部署管道的權限過於廣泛。
- 管道未設定進行輸入驗證。
- 未定期檢閱與 CI/CD 基礎設施相關的權限。
- 使用長期有效或硬式編碼的登入資料。

建立此最佳實務的優勢：

- 經由此類管道完成建置與部署的軟體完整性具備更高的可信度。
- 可在發現可疑活動時停止部署作業。

未建立此最佳實務時的風險暴露等級：高

實作指引

從支援 IAM 角色的受管 CI/CD 服務開始，可以減少登入資料外洩情況。套用這些安全支柱原則至您的 CI/CD 管道基礎設施，有助於您判斷哪些地方可以改善安全性。遵循 AWS 部署管道參考架構是建置 CI/CD 環境的好起點。定期檢閱管道實作及分析意外行為日誌，有助於了解用於部署軟體之管道的用量模式。

實作步驟

- 從 AWS 部署管道參考架構開始行動。
- 考慮使用 AWS IAM Access Analyzer，以程式設計方式產生管道的最低權限 IAM原則。
- 整合您的管道與監控與警示，以便您可在 AWS 受管服務 Amazon EventBridge 發生意外或異常活動時收到通知，這樣您就可以將資料路由至像是 AWS Lambda 或 Amazon Simple Notification Service (Amazon SNS) 等目的地。

資源

相關文件：

- AWS 部署管道參考架構
- 監控 AWS CodePipeline
- AWS CodePipeline 安全最佳實務

相關範例：

- DevOps 監控儀表板 (GitHub)

SEC11-BP08 打造在工作負載團隊中納入安全所有權的計劃

打造一項計劃或一種機制，賦予建置人員團隊能對其本身所建軟體做出安全決策的能力。您的安全團隊仍需在審查過程中確認這些決策，但是在建置人員團隊中納入安全所有權的做法，可以建置更快且更安全的工作負載。這項機制也能推動所有權文化，積極影響您所建置系統的運作。

預期成果：若要賦予建置人員團隊安全所有權和決策能力，您可以訓練建置人員對於安全的觀念，或者配合在建置人員團隊中納入或連結安全部門人員，增強人員的訓練。每種方法都有效用，而且可讓團隊在開發週期前期階段就做出品質更好的安全決策。這個所有權模式是以訓練應用程式安全為基礎。從處理特定工作負載的威脅模型開始，有助於讓設計專注在適當環境內容。成立著重建置人員的安全社群，或是指派與建置人員團隊合作的安全部門工程師的另一項好處，在於您可以更深入了解軟體的編寫方式。這項了解有助於判斷出下一個可以用自動化達到改善的區域。

常見的反模式：

- 將所有的安全決策全部留給安全團隊。
- 未及早在開發程序初期解決安全需求。
- 未諮詢建置人員與安全部門人員在計劃運作方面的意見回饋。

建立此最佳實務的優勢：

- 縮短完成安全檢閱的時間。
- 減少必須在安全檢閱階段中偵測出的安全問題。
- 改善所編寫軟體的整體品質。
- 有機會找出並了解具備高度改善價值的系統性問題或區域。
- 減少因安全檢閱發現結果而必須進行的重新作業量。.
- 改善對於安全功能的感覺。

未建立此最佳實務時的風險暴露等級：低

實作指引

從 SEC11-BP01 應用程式安全訓練 的指引開始。接著找出您認為最適合組織的計劃操作模式。其中兩種主要模式分別是訓練建置人員，以及在建置人員團隊當中納入安全部門人員。在您決定初步方法之後，您應該透過單一或小組型工作負載團隊進行先行試驗，證明該模式適合您的組織。建置人員與組織的安全部門所提供的領導支援，有助於計劃達成與成功實施。隨著這項計劃不斷建置，您一定要選擇可

以用來顯示計劃價值的矩陣。了解 AWS 如何解決這個問題可以學到相當多知識。這項最佳實務非常強調組織層面變更與文化。您所使用的工具應該能支援建置人員與安全社群之間的協作。

實作步驟

- 從訓練建置人員處理應用程式安全開始。
- 建立專為教育建置人員的社群和上線計劃。
- 挑選計劃名稱。守門人、擁護者或倡導者是常見手法。
- 找出要應用的模式：訓練建置人員、納入安全部門工程師，或是安排親和性安全角色。
- 從安全部門、建置人員和可能的其他相關小組當中，找出專案贊助者。
- 計劃當中所涉多人的追蹤矩陣，檢閱所花時間，以及建置人員與安全團隊人員的意見回饋。使用這些矩陣來達成改善。

資源

相關的最佳實務：

- SEC11-BP01 應用程式安全訓練
- SEC11-BP02 自動化在整個開發和發佈生命週期的測試

相關文件：

- 如何達成威脅建模
- 如何思考雲端安全管控

相關影片：

- 預防性安全：考慮與方法

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設施，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：

- Sarita Dharankar，Amazon Web Services Well-Architected 安全支柱主管
- Adam Cerini，Amazon Web Services 資深解決方案架構師
- 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
- Charlie Hammell，Amazon Web Services 首席企業架構師
- 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
- John Formento，Amazon Web Services 資深解決方案架構師
- Paul Hawkins，Amazon Web Services CISO 辦公室主任
- Sam Elmalak：Amazon Web Services 資深技術主管
- Pat Gaw，Amazon Web Services 首席安全顧問
- Daniel Begimher，Amazon Web Services 資深安全顧問
- Danny Cortegaca，Amazon Web Services 資深安全解決方案架構師
- Ana Malhotra，Amazon Web Services 安全解決方案架構師
- Debashis Das，Amazon Web Services CISO 辦公室主任
- Reef Dsouza，Amazon Web Services 首席解決方案架構師
- Brad Burnett，Amazon Web Services 身分安全解決方案架構師
- Anna McAbee，Amazon Web Services 威脅偵測與事故回應資深安全解決方案架構師
- Jason Garman，Amazon Web Services 首席安全解決方案架構師

深入閱讀

如需其他協助，請參考以下資源：

- AWS Well-Architected Framework 白皮書
- AWS 架構中心

文件修訂

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
已更新最佳實務指引	最佳實務已更新，納入了以下方面的新指引：安全操作工作負載和保護傳輸中的資料。	December 6, 2023
已更新最佳實務指引	對事故回應的指引和最佳實務進行了重大更新。 準備中更新了多個最佳實務。事故回應方面新增了兩個新領域：操作和事後處理。已新增新的最佳實務 SEC10-BP08 建立從事故中學習的架構。	October 3, 2023
已更新最佳實務指引	最佳實務已更新，納入了以下方面的新指引：準備和模擬。	July 13, 2023
新框架的更新。	最佳實務已更新，納入了規範性指引，並增加了新的最佳實務。已新增應用程式安全 (AppSec) 的新最佳實務領域。	April 10, 2023
白皮書已更新	最佳實務更新了新的實作指引。	December 15, 2022
白皮書已更新	已擴充最佳實務並新增了改善計劃。	October 20, 2022
小幅度更新	已更新 IAM 資訊以反映目前的最佳實務。	June 28, 2022

小幅度更新	已新增額外的 AWS PrivateLink 資訊，並更正了中斷的連結。	May 19, 2022
小幅度更新	已新增 AWS PrivateLink。	May 6, 2022
小幅度更新	已移除非包容性語言。	April 22, 2022
小幅度更新	已新增 VPC Network Access Analyzer 的相關資訊。	February 2, 2022
小幅度更新	已將永續性支柱新增至簡介。	December 2, 2021
小幅度更新	修正了中斷的連結。	May 27, 2021
小幅度更新	整體的編輯變更。	May 17, 2021
主要更新	已新增有關管控的章節、已將詳細資訊新增至不同的章簡，已在整體中加入新的功能和服務。	May 7, 2021
小幅度更新	更新了連結。	March 10, 2021
小幅度更新	修正了中斷的連結。	July 15, 2020
新框架的更新	更新帳戶、身份和許可管理的指導方針。	July 8, 2020
新框架的更新	更新以擴展每個領域的建議、新的最佳實務、服務和功能。	April 30, 2020
白皮書已更新	更新以反映新的 AWS 服務和功能以及更新的參考。	July 1, 2018
白皮書已更新	已更新「系統安全組態和維護」一節，以反映新的 AWS 服務和功能。	May 1, 2017

初版	安全支柱 – AWS Well Architected Framework 已發佈。	November 1, 2016

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。