AWS 技術指南

AWS 安全事件回應指南

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

AWS 安全事件回應指南: AWS 技術指南

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

Amazon 的商標或商業外觀不得用於 Amazon 產品或服務之外的任何產品或服務，不得以可能在客戶中造成混淆的任何方式使用，不得以可能貶低或損毀 Amazon 名譽的任何方式使用。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

摘要 1
簡介 2
開始之前 2
AWS CAF 安全觀點 2
事件回應的基礎 3
教育 4
共同的責任 4
雲端中的事故回應 6
Cloud Response 的設計目標 6
雲端安全事件 7
事件網域 7
雲端安全事件指標 8
了解雲端運算 9
資料隱私權 10
AWS 對濫用和洩漏的因應 10
準備 – 人員 12
定義角色和責任 12
提供培訓 13
定義回應機制 13
塑造接納和調適的安全文化 13
預測回應 14
合作夥伴和回應窗 14
未知風險 15
準備 – 技術 18
準備存取 AWS 帳戶 18
間接存取 19
直接存取 19
替代存取 19
自動化存取 19
受管服務存取 20
準備流程 20
決策樹 21
使用備用帳戶 21
查看或複製資料 21

共用 Amazon EBS 快照 22
共用 Amazon CloudWatch Logs 22
使用不可變儲存 22
啟動事件附近的資源 23
隔離資源 24
啟動鑑識工作站 24
雲端提供者支援 25
AWS Managed Services 25
AWS 支援 25
DDoS 回應支援 26
模擬 27
安全事件回應模擬 27
模擬步驟 27
模擬範例 28
反覆 29
執行手冊 29
建立執行手冊 29
開始使用 30
自動化 30
自動化事件回應 30
事件驅動回應 35
事件回應範例 37
服務網域事件 37
身分 37
資源 37
基礎設施網域事件 38
調查決策 39
擷取暫時性資料 40
使用 AWS Systems Manager 40
自動執行擷取 40
結論 41
其他資源 42
媒體 42
第三方工具 43
行業參考 43
文件修訂 44

附錄 A：雲端功能定義 45
日誌記錄和事件 45
可見性和提醒 46
自動化 48
安全的儲存 48
自訂 49
附錄 B：範本程式碼 50
範例 AWS CloudTrail 事件 50
AWS CloudWatch Events 範例 51
基礎設施網域 CLI 活動範例 51
附錄 C：範例執行手冊 53
事件回應執行手冊 – 根用途 53
目標 53
前提 53
危害指標 53
修復步驟 – 建立控制 54
進一步動作項目 – 判斷影響 54
聲明 55

AWS 安全事件回應指南

發佈日期：2020 年 11 月 23 日 (文件修訂)

本指南概述在客戶的 AWS 雲端環境中，回應安全事件的基礎原理。它重點概述了雲端安全和事件回應概念，並辨別可供回應安全問題之客戶使用的雲端功能、服務和機制。

本白皮書適用於擔任技術角色的人員，並假設您已熟悉資訊安全的一般原則、對目前內部部署環境中的事件回應具有基本了解，並且熟悉雲端服務。

簡介

安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足對安全最為敏感的組織需求。AWS 雲端具有共同責任模式。AWS 負責管理雲端本身的安全。雲端內部的安全由您負責。這表示您保有對您選擇實施之安全措施的掌控權。您可以使用數百種工具和服務，來協助實現安全目標。這些功能可協助您建立安全基準，以滿足在雲端中執行應用程式的目標。

如果出現偏離基準的情況 (例如由於組態設定不當)，您可能需要做出回應並進行調查。想要成功執行此操作，您必須了解 AWS 環境中的安全事件回應基本概念，以及在出現安全問題之前準備、教育和培訓雲端團隊所需考慮的問題。請務必了解您可以使用哪些控制和功能、查看解決潛在問題的主題範例，並識別可運用自動化和提高回應速度的修復方法。

由於安全事件回應是很複雜的主題，因此我們鼓勵您從小型事件開始，開發執行手冊、利用基本功能，並建立初始的事件回應機制庫，以便迭代和改進。這項初步工作應納入法律部門以及非安全團隊，如此才能更加了解事件回應 (IR) 以及您所做的選擇，對公司目標所造成的影響。

主題

- 開始之前
- AWS CAF 安全觀點
- 事件回應的基礎

開始之前

除了本文件之外，我們也鼓勵您檢閱 安全、身分與合規性最佳實務和AWS 雲端採用架構 (CAF) 的安全觀點白皮書。AWS CAF 提供指南，支援在組織遷移到雲端時，居中協調不同的組織部分。CAF 指南分為幾個與實施以雲端為基礎 IT 系統相關的重點領域，我們稱為觀點。安全觀點描述如何跨多個工作流實施安全計劃，其中一個著重於事件回應。本文詳述我們在協助客戶於該工作流中評估和實施成功機制方面的一些經驗。

AWS CAF 安全觀點

安全觀點包含四個元件：

- 指令控制建立管控、風險與合規模型，以供整個環境在其中操作。
- 預防控制保護工作負載，並減緩威脅和漏洞。
- 偵測控制為企業在 AWS 中的部署操作提供完整的可見度與透明度。

- 回應控制為偏離安全基準的可能變動提供補救。

雖然 IR 通常在回應控制元件下查看，但它們依賴於其他元件並受其影響。例如，指令和預防安全控制有助於建立基準，讓您可以監控和調查任何偏離此基準的情況。這種方法不僅可消除雜訊，並有助於防禦性的安全設計。

事件回應的基礎

組織內的所有 AWS 使用者都應該對安全事件回應流程有基本的了解，而安全人員必須深入了解如何因應安全問題。在處理安全事件之前，經驗和教育對於雲端事件回應計劃至關重要。雲端中成功的事件回應計劃的基礎是教育、準備、模擬和反覆查看。

如想了解每一個層面，請參閱以下說明：

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

教育

主題

- 共同的責任
- 雲端中的事故回應
- 雲端安全事件
- 了解雲端運算

共同的責任

安全和合規的責任由 AWS 和您共同承擔。這種共同模式有助減輕您的營運負擔，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。

您需負責管理訪客作業系統 (包括更新和安全修補程式) 和應用程式軟體，以及設定 AWS 提供的安全控制，如安全群組、網路存取控制清單和以及身分和存取管理。您應該仔細考慮所使用的服務，因為您的責任取決於所選擇的服務、這些服務與 IT 環境的整合，以及適用的法律和法規。圖 2 顯示套用至基礎設施服務 (如 Amazon Elastic Compute Cloud (Amazon EC2)) 的共同責任模式的典型表示。它將大部分責任分為兩類：雲端本身的安全 (由 AWS 管理) 和雲端中的安全 (由客戶管理)。責任歸屬可能會產生變化，具體取決於您使用的服務。若是 Amazon S3 和 Amazon DynamoDB 等抽象服務，AWS 運作基礎設施層、作業系統和平台，客戶則存取端點以存放及擷取資料。客戶負責管理其資料 (包括加密選項)，對其資產進行分類，以及使用 IAM 工具來套用適當的許可。

但是，共同責任模式會隨著容器和其他服務的增加而產生變化，這些變化會將操作模式移往服務提供者。當我們移往操作模式的左側，從 IaaS 和資料中心轉向 PaaS，服務提供者的責任就會增加。當遷移到圖表左側時，客戶在雲端中的責任更少，操作時間更輕鬆。請注意下圖以及在雲端中操作或運作能力的差異。隨著您在雲端中的共同責任發生變化，您的事件回應或鑑識選項也會發生變化。身為客戶，在規劃事件回應時，您還需要確保根據操作模型中的能力進行規劃，並在所選模型中發生互動之前，先規劃好可能的互動。規劃和理解這些權衡並符合您的管控需求，是事件回應的關鍵步驟。

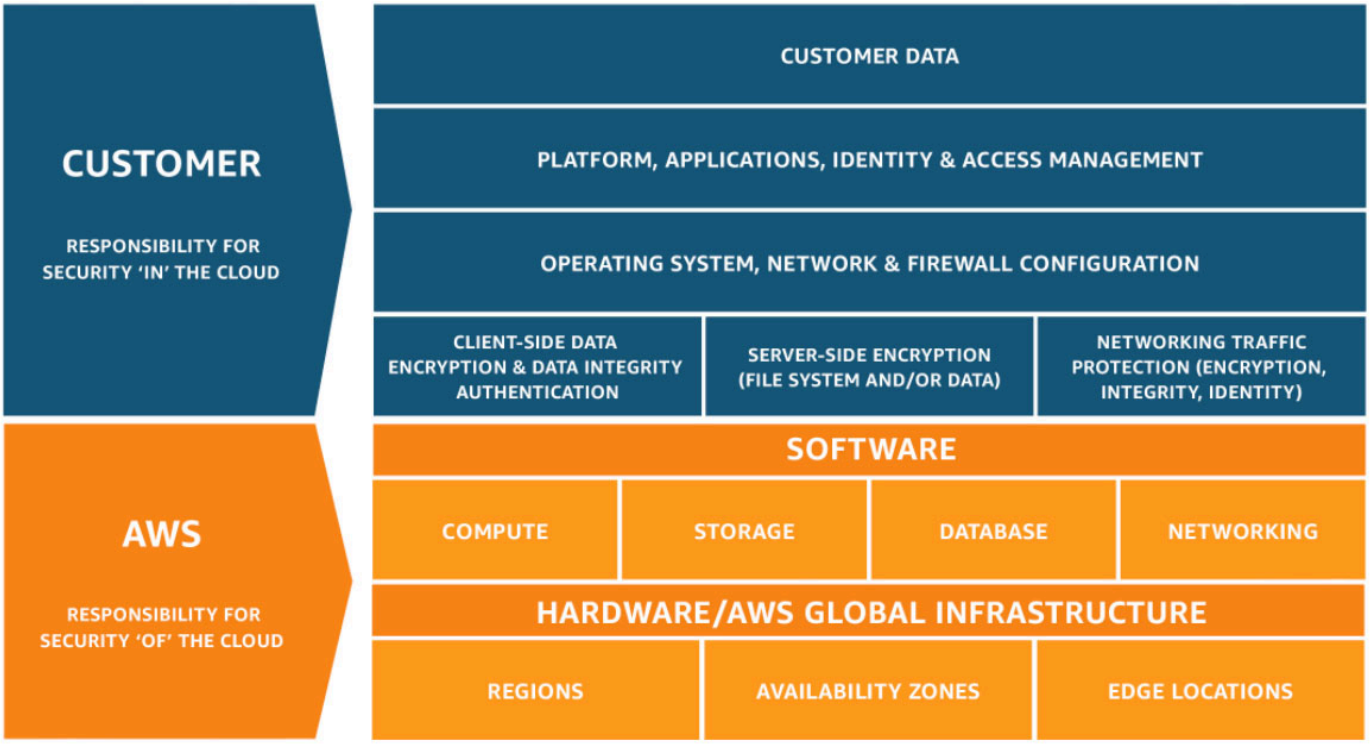
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

圖 1：共同責任模式

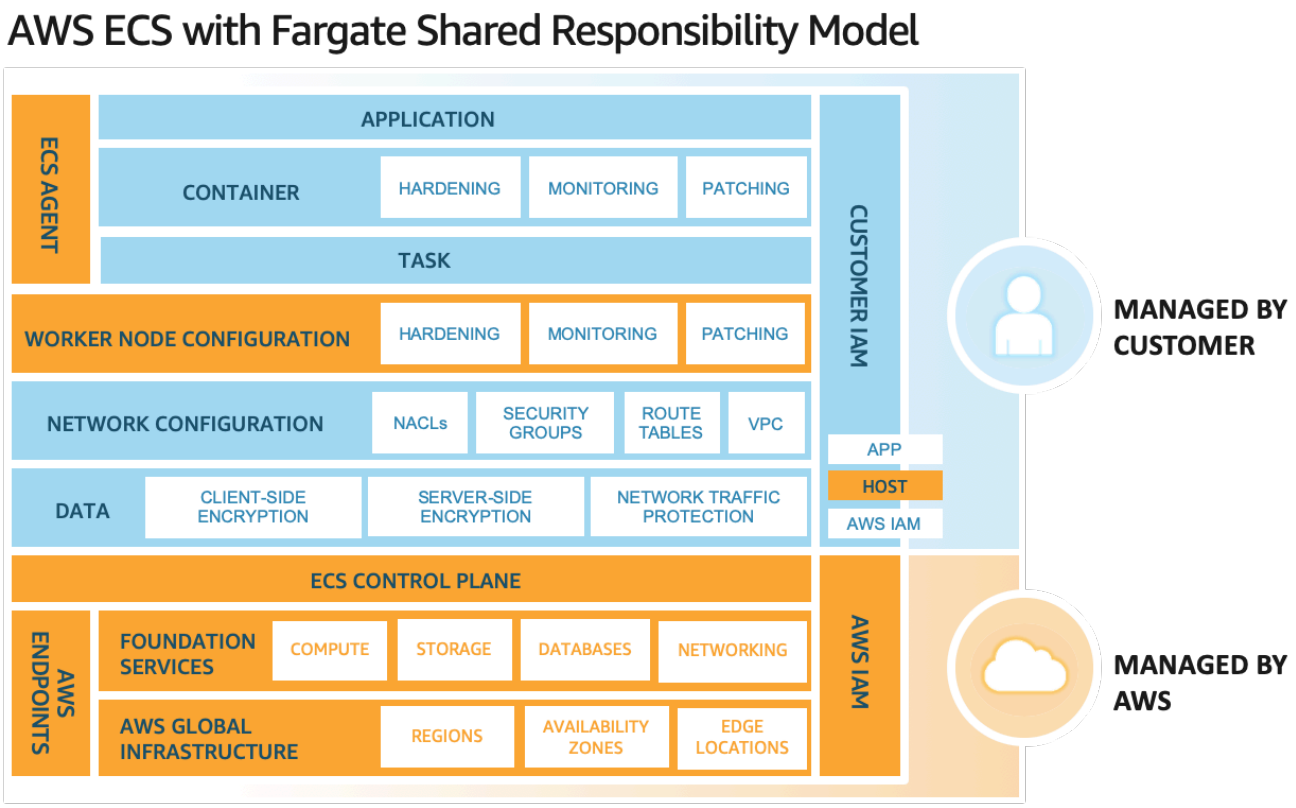

圖 2：具有 AWS Fargate 類型共同責任模式的 Amazon Elastic Container Service (Amazon ECS)

除了您與 AWS 的直接關係之外，可能還有其他實體在您的特定責任模型中負有責任。例如，可能有內部組織單位對操作的某些方面負責。可能還有合作夥伴或其他第三方負責開發、管理或操作您的某些雲端技術。

建立符合您操作模型的適當事件回應與鑑識執行手冊，這一點極為重要。您的成功取決於針對所選取的操作模型，您對需建立的工具類型或需購買工具的理解程度。您的組織越了解可用的工具，您就越能做好妥善的準備，以符合企業管控風險和合規 (GRC) 模式的需求。

雲端中的事故回應

Cloud Response 的設計目標

雖然事件回應的一般程序和機制，例如 NIST SP 800-61 Computer Security Incident Handling 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 - 與您的利害關係人、法律顧問和組織領導階層合作，訂定回應事件的目標。一些常見目標包括遏制和減輕問題、復原受影響的資源、保留鑑識資料，以及歸因。
- 使用雲端回應 - 在事件發生和資料之處實作回應模式。
- 了解您擁有和需求的是哪些 - 將日誌、快照和其他證據複製到集中的安全雲端帳戶加以保留。運用標籤、中繼資料和機制，強制執行保留政策。例如，您可以選擇使用 Linux dd 命令或相當的 Windows 命令，製作完整的資料複本，以用於調查。
- 使用重新部署機制 - 如果安全異常可能歸因於組態設定不當，修復的方法可能就是透過使用適當的組態，重新部署資源以移除變異那麼簡單。請盡可能讓您的回應機制安全地在不明狀態中執行多次。
- 盡可能自動化 - 當您發現問題或事件重複時，請建置機制，以程式設計方式分類並回應常見的情況。對於獨一無二、新和敏感的事件，請以人力回應。
- 選擇可擴展的解決方案 - 努力符合組織雲端運算方法的可擴展性，並縮短偵測和回應之間的時間。
- 了解並改善程序 – 當您找出程序、工具或人員中的缺口時，請實作計劃來修正這些缺口。模擬是找出缺口和改善流程的安全方法。

NIST 的設計目標是提醒您檢閱架構，以便能夠同時執行事件回應和威脅偵測。在規劃雲端實施時，請考慮回應事件或鑑識事件。在某些情況下，這表示您可能為這些回應任務專門設定了多個組織、帳戶和工具。這些工具和功能應透過部署管道來提供給事件回應人員，它們不應是靜態的，因為這會導致更大的風險。

雲端安全事件

主題

- 事件網域
- 雲端安全事件指標

事件網域

在客戶的責任範圍內，安全事件可能發生在三個網域：服務、基礎設施和應用程式。網域之間的差異與您在回應時使用的工具有關。請考慮這些網域：

- 服務網域 – 服務網域中的事件會影響客戶的 AWS 帳戶、IAM 許可、資源中繼資料、帳單等方面。服務網域事件是專門使用 AWS API 機制回應的事件，或者其根本原因與組態或資源使用權限相關聯的事件，並且可能具有相關的服務導向記錄。

- 基礎設施網域 – 基礎設施網域中的事件包括與資料或網路相關的活動，例如前往 VPC 內 Amazon EC2 執行個體的流量、Amazon EC2 執行個體上的流程和資料，及容器或其他未來服務等方面。對基礎設施網域事件的回應通常涉及擷取、恢復或取得事件相關資料以進行鑑識。這可能包括與執行個體作業系統的互動，在某些情況下，還可能涉及 AWS API 機制。
- 應用程式網域 – 應用程式網域中的事件發生在應用程式程式碼或部署到服務或基礎設施的軟體中。此網域應包含在您的雲端威脅偵測和回應執行手冊中，並且可能包含與基礎設施網域中的回應類似的回應。藉助適當且考慮周全的應用程式架構，您可以使用雲端工具透過自動鑑識、恢復和部署來管理該網域。

在這些網域中，您必須考慮可能對帳戶、資源或資料採取行動的行為者。無論是內部還是外部，都可以使用風險架構來確定組織面臨的具體風險，並據以做好準備。

在服務網域中，可以專門利用 AWS API 實現目標。例如，處理 Amazon S3 儲存貯體的資料洩露事件涉及 API 呼叫以擷取儲存貯體的政策、分析 S3 存取日誌以及在需要時查看 AWS CloudTrail 日誌。在此範例中，調查不太可能涉及資料鑑識工具或網路流量分析工具。

在基礎設施網域，您可以在工作站的作業系統中組合使用 AWS API 和熟悉的數位鑑識/事件應變 (DFIR) 軟體，例如為 IR 工作準備的 Amazon EC2 執行個體。基礎設施網域事件可能涉及分析網路封包擷取、Amazon Elastic Block Store (Amazon EBS) 磁碟區上的磁碟區塊或從執行個體取得的揮發性記憶體。

雲端安全事件指標

有許多安全事件可能無法歸類為事件，但最好還是調查這些事件。若要偵測 AWS 雲端環境中的安全相關事件，您可以使用這些機制。這並非詳盡清單，但請考慮下列一些潛在指標範例：

- 日誌和監控功能 – 查看 AWS 日誌 (如 Amazon CloudTrail、Amazon S3 存取日誌和 VPC 流程日誌) 以及安全監控服務 (如 Amazon GuardDuty、Amazon Detective 和 AWS Security Hub 以及 Amazon Macie)。此外，還可以使用 Amazon Route 53 運作狀態檢查和 Amazon CloudWatch 警示等監控功能。同樣地，使用 Windows 事件、Linux 系統日誌及其他可在應用程式中產生的應用程式專屬日誌，並使用 CloudWatch Agent 登入到 Amazon CloudWatch。
- 帳單活動 – 帳單活動突然產生變化，可能代表發生安全事件。
- 威脅情報 – 如果您訂閱了第三方威脅情報摘要，可以將該資訊與其他日誌記錄和監控工具相關聯，以確定潛在的事件指標。
- 合作夥伴工具 – AWS 合作夥伴網路 (APN) 中的合作夥伴，提供了數百種領先業界的產品，可協助您實現安全目標。如需詳細資訊，請參閱安全合作夥伴解決方案和AWS Marketplace 中的安全解決方案。

- AWS Outreach – 如果我們發現濫用或惡意活動，AWS 支援 可能會聯絡您。如需詳細資訊，請參閱 AWS 對濫用和洩漏的回應一節。
- 單次聯絡 – 由於注意到不尋常事情的可能是您的客戶、開發人員或組織中的其他員工，因此請務必準備一個眾所皆知、廣為宣傳的安全團隊聯絡方法。熱門選擇包括票證系統、聯絡人電子郵件地址和 Web 表單。如果您的組織與一般公眾合作，您可能還需要一個面向公眾的安全聯絡機制。

AWS 提供的其中一個自動化和偵測工具是 AWS Security Hub。Security Hub 可讓您在一個位置全方面檢視 AWS 帳戶中的高優先順序安全警示和合規狀態，以便更加了解這些指標。AWS Security Hub 不是安全資訊與事件管理 (SIEM) 軟體，也不會存放日誌資料，而是彙總、組織來自多個 AWS 服務的安全警示或問題清單，並加以排定優先順序。Security Hub 還可讓您建立從多個來源產生的自訂洞察。這為安全營運團隊提供了選項，並在事件發生時深入了解更多資訊。Security Hub 會根據 AWS 最佳實務和貴組織遵循的產業標準，使用自動合規檢查持續監控您的環境。

另外，您還可以透過調查 Amazon Detective 或 Amazon Athena 中的安全問題清單，或使用 Amazon CloudWatch Events 或事件匯流排規則，將問題清單傳送至支援票證、聊天、SIEM、安全協同運作自動化與回應 (SOAR) 及事件管理工具，或是傳到自訂修復手冊，針對安全與合規問題清單採取應變措施。事件型自動化可讓您自動回應發生的事件。與內部部署環境相比，這個方法改變了安全性以及您在雲端中處理事件的方式。

了解雲端運算

AWS 提供一系列安全功能，您可以使用這些功能來調查跨網域的安全事件。例如，AWS 提供許多日誌記錄機制，如 AWS CloudTrail 日誌、Amazon CloudWatch Logs、Amazon S3 存取日誌等。您應該考慮使用中的服務，務必啟用這些服務的相關日誌。AWS 還提供集中式記錄解決方案，可協助您了解如何集中和存放常見類型的雲端日誌。啟用這些日誌記錄來源後，您必須決定如何分析它們，例如使用 Amazon Athena 查詢 Amazon S3 儲存貯體中保存的日誌。

此外，還有許多 APN 合作夥伴產品可以簡化分析日誌的過程，例如 APN 安全能力計劃中所述的產品。還有幾項 AWS 服務可協助您獲得有關此資料的寶貴洞察，例如 Amazon GuardDuty (威脅偵測服務) 和 AWS Security Hub，它們可以提供所有 AWS 帳戶之高優先順序安全警示和合規性狀態的全方位檢視。此外，Amazon Detective 會從您的 AWS 資源中收集日誌資料，並使用機器學習、統計分析和圖論，來協助您識別潛在安全問題或可疑活動的根本原因。如需您可在調查期間利用的其他雲端功能的詳細資訊，請參閱附錄 A：雲端功能定義。

主題

- 資料隱私權
- AWS 對濫用和洩漏的因應

資料隱私權

我們知道客戶非常關心隱私和資料安全，因此也實作可信賴和複雜的技術與實體控制措施，旨在防止未經授權的存取或揭露客戶內容。維持客戶信任是持續不斷的承諾。您可以到我們的資料隱私權常見問答集頁面，進一步了解 AWS 資料隱私權承諾。

這些刻意自我施加的控制措施，限制了 AWS 在客戶環境中協助回應的能力。正因為如此，專注於理解和建構共同責任模式中的能力，是在 AWS 雲端取得成功的關鍵。事件發生之前就在 AWS 帳戶中啟用日誌記錄和監控功能非常重要，但事件回應還有其他方面，對於成功的計劃也是至關重要。

加州消費者資料隱私權

2018 年《加州消費者隱私保護法》(CCPA) 賦予受 CCPA 約束的「消費者對於企業所持有之消費者相關個人資訊的各種權利」。如需受 CCPA 約束之 AWS 與客戶相關的隱私權和資料安全政策的資訊，請參閱為加州消費者隱私保護法做好準備白皮書的指引。

一般資料保護規範

《一般資料保護規範》(GDPR) 是歐盟隱私權法 (歐洲議會與理事會於 2016 年 4 月 27 日所頒布的 2016/679 規定)，於 2018 年 5 月 25 日生效。GDPR 取代歐盟資料保護行政命令 (也稱為 95/46/EC 行政命令)，它旨在協調整個歐盟 (EU) 的資料保護法，透過實施單一資料保護法來約束每個成員國。如需 GDPR 相關的 AWS 合規資訊，請參閱在 AWS 上瀏覽 GDPR 指南白皮書。

AWS 對濫用和洩漏的因應

濫用活動是指 AWS 客戶的執行個體或其他資源，被觀察到的惡意、冒犯性、非法，或可能損害其他網際網路網站的行為。AWS 與您合作，來共同偵測並解決 AWS 資源中的可疑和惡意活動。如果有來自您的資源的意外或可疑行為，可能表明您的 AWS 資源遭到入侵，表示您的業務面臨潛在風險。請記住，您的 AWS 帳戶中有其他聯絡方式。新增聯絡人時，請務必根據安全和計費的最佳實務。雖然您的根帳戶電子郵件是 AWS 通訊的主要目標，但 AWS 也會將安全問題和帳單問題傳遞給次要電子郵件地址。新增僅傳送給一個人的電子郵件地址，代表您在 AWS 帳戶中增加了單一故障點。請務必新增至少一個通訊群組清單到您的聯絡人。

AWS 使用以下機制來偵測資源中的濫用活動：

- AWS 內部事件監控。
- 針對 AWS 網路地址空間的外部安全情報。
- 針對 AWS 資源的網際網路濫用投訴。

儘管 AWS 濫用回應團隊積極監控和關閉在 AWS 上執行的未經授權活動，但大多數濫用投訴都是針對在 AWS 上擁有合法業務的客戶。非故意濫用活動的一些常見原因包括：

- 資源受損 – 未修補的 Amazon EC2 執行個體可能受到感染並成為僵屍網路代理。
- 非故意濫用 – 過於激進的 Web 編目程式可能會被某些網際網路網站歸類為阻斷服務攻擊。
- 二次濫用 – AWS 客戶所提供服務的最終使用者，可能會在公有 Amazon S3 儲存貯體上發佈惡意軟體檔案。
- 虛假投訴 – 網際網路使用者有時會錯誤地將合法活動報告為濫用行為。

AWS 致力於與 AWS 客戶合作，以防止、偵測和減少濫用，並防止未來再次發生。我們鼓勵您檢閱 AWS 可接受的使用政策，該政策描述了禁止使用 Amazon Web Services 及其關係企業所提供 Web 服務的情況。若想及時回應來自 AWS 的濫用通知，請確保您的 AWS 帳戶聯絡資訊準確無誤。當您收到 AWS 濫用警告時，您的安全和操作人員應立即調查此事。延遲回應可能會延長對自己和他人的聲譽影響以及法律影響。更重要的是，遭牽連的濫用資源可能會受到惡意使用者的破壞，而忽略這種破壞，可能會放大對您的業務的損害。

準備 – 人員

自動化程序可讓組織將更多時間投注於提高雲端環境和應用程式安全的措施。自動化事件回應也讓人力能夠用於建置事件關聯性、演練模擬、設計新的回應程序、執行研究、開發新的技能，以及測試或建置新的工具。雖然自動化程度提高，但安全組織內的分析人員和回應人員仍需要持續接受教育。同質性過高的團隊會造成盲點，因此必須成立多元化團隊，在複雜多變的情況下提供不同的思想體系、文化觀點以及工作和生活經驗。規劃活動時的最有力做法之一，是確保在團隊和回應計劃中融入多元化。由不同觀點組成的團隊可以找出從未被察覺的盲點，並找出從沒被想過的解決方案。

主題

- 定義角色和責任
- 定義回應機制
- 塑造接納和調適的安全文化
- 預測回應

定義角色和責任

在處理新的或大規模事件時，事件回應的技能和機制是最重要的。這些事件取決於您團隊制定的書面標準，以及您團隊的實踐。由於我們無法預測或編纂事件將採取的所有潛在方向，所以我們依靠自動化來執行簡單的重複性任務，例如收集執行個體記憶體或診斷日誌，然後讓人類做出艱難的決策。對於處理不明確的安全事件，需要跨組織紀律、採取果斷行動以及實現目標的能力。在您的組織結構中，在發生事件時應該有許多人是負責者、當責者、事先諮詢者或事後被告知者，例如來自人力資源 (HR)、管理團隊和法律部門的代表。請考量這些角色和責任，以及是否涉及其他第三方。請注意，在許多地區，有當地法律規定可以做和不能做的事情。為事件建置負責者、當責者、事先諮詢者或事後被告知者 (RACI) 圖表看似官僚，但這樣做可以達成快速、直接的溝通，並清楚概述不同事件階段的領導地位。

受信賴的合作夥伴可能參與調查或回應，他們可提供額外的專業知識和寶貴的審查意見。當您自己的團隊沒有這些技能時，您可能需要聘請外部人員提供協助。如果您僱用外部單位，請務必讓此單位訓練您的團隊成員。當這些外部單位與您的內部開發人員和操作人員合作時，他們可以擴充團隊成員的技能，而且這些新的專業知識對於未來的 IR 計劃非常有價值。

發生事件時，納入受影響應用程式和資源的擁有者和開發人員很重要，因為他們是可以提供資訊和脈絡的領域專家 (SME)。在依賴開發人員和應用程式擁有者的專業知識回應事件之前，請務必先和他們進行練習並建立關係。應用程式擁有者或 SME 可能需要在不熟悉環境、複雜程度出乎意料，或回應人員無權存取的情況下採取行動。應用程式 SME 應該與 IR 團隊一起練習並適應團隊合作。

提供培訓

若想減少依賴關係並縮短回應時間，請務必讓安全團隊和回應人員接受雲端服務的相關教育訓練，並有機會在組織使用的特定雲端平台上實際操作。其中一些培訓出自流程開始時的團隊建設和執行手冊建置。在建構執行手冊的初始步驟中盡量納入越多人員，可以更加了解內部團隊。當團隊在桌上模擬演練中開始遵循執行手冊，訓練就會變得更加真實。

AWS 和其他第三方也提供線上安全講座 (AWS 安全講座)，供您下載和演練。您的組織可透過為員工提供額外的培訓來學習程式設計技能、開發程序 (包括版本控制系統和部署實務) 以及基礎設施自動化，而獲益良多。

AWS 透過數位培訓、課堂培訓、APN 合作夥伴和認證，提供多種培訓選項和學習途徑。如需進一步了解，請參閱 AWS 培訓與認證。

定義回應機制

您的回應機制取決於您的管控、風險和合規 (GRC) 模式。理想情況下，GRC 模式應在規劃事件回應之前就先建構好。如果您尚未開始建置 GRC，對於建置良好的事件回應機制，這是必須完成的第一步。當您與其他團隊 (例如法律顧問、領導階層、業務利害關係人和其他團隊) 一起考慮在雲端中應對事件的方法時，您必須了解自己擁有什麼、需要什麼。確定利害關係人和相關聯絡人，並確保您有適當的存取權限來執行必要的回應。

雲端可以透過服務 API 為您提供更高的可視性和功能，而 GRC 模式可展示如何在回應中使用這些服務。找出團隊的 AWS 帳戶號碼、Virtual Private Cloud (VPC) 的 IP 範圍、對應的網路圖、日誌、資料位置和資料分類。以上許多技術程序在 準備 – 技術一節中都有討論。然後，開始記錄事件回應程序 (通常稱為程序或執行手冊)，這些程序定義了調查和補救事件的步驟。

塑造接納和調適的安全文化

在 AWS，我們了解到當安全團隊成為業務和開發人員的合作推動者時，客戶和我們自己的內部團隊是最成功的，這些團隊培養出一種文化，能確保所有利害關係人合作並提升為保持敏捷、高度回應的安全狀態。改進組織的安全文化並非本文的主題，但如果您的安全團隊保持開放心胸，您也能從非安全部門人員獲得相關情報。當安全團隊保持開放、易親近，並有領導階層的支持，他們就更能獲得安全事件的額外及時通知、合作和回應。

在某些組織中，員工可能會害怕因回報安全問題而遭到報復；有時則是根本不知道該如何回報問題。而在其他情況下，員工可能不想浪費時間，或是不好意思將某事回報為安全事件，怕之後被發現這並不是

問題。從領導團隊以下，重要的是促進接納文化，並邀請每個人都成為組織安全的一分子。提供一個明確的管道，讓任何人在認為出現潛在風險或威脅時，能開啟高嚴重性票證。以熱切和開放的心態歡迎這些通知，但更重要的是，向非安全工作人員明確表示您歡迎這些通知。強調您寧願收到潛在問題的過度通知，而非完全收不到任何通知。最好是開發人員能提出自己的失誤，然後讓研究人員在公開文章中指出問題。

這些通知提供了寶貴的機會，能在壓力下進行回應性調查。制定回應程序時，它們可以作為重要的回饋迴圈。

預測回應

因為不可能預測所有潛在的事件，所以必須繼續依靠人工分析。花時間仔細培訓員工並為組織做好準備，可協助您預測意外情況；但是，您的組織不用單打獨鬥。與受信賴的安全合作夥伴合作找出未預期的安全事件，可讓組織獲得額外的可見性和洞察力。

合作夥伴和回應窗

雲端之旅對於每個組織來說都是獨一無二的。但是，其他組織已經遇到的模式和做法，受信賴的安全合作夥伴會提醒您注意。我們鼓勵您找到外部 AWS 安全 APN 合作夥伴，以提供外部專業知識和不同觀點，並為您增強回應能力。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。

1955 年，Joseph Luft 和 Harrington Ingham 創造了周哈里窗 (Johari window)，這是一個將特徵映射到不同類別的做法。周哈里窗是四個象限組成的網格，類似於下圖。

	Known to You	Not Known to You
Known to Others	**Obvious**	**Blind Spot**
Not Known to Others	**Internally Known**	**Unknown**

圖 3：根據事件回應而修改的周哈里窗

周哈里窗原本並非用於資訊安全，但我們可以調整這個概念，將其當作簡單的心理模型，來考慮評估組織威脅時遇到的困難。在我們修改後的概念中，四個象限分別為：

- 顯而易見 – 您的團隊和 APN 合作夥伴都知道的風險。
- 內部已知 – 您的團隊熟悉但 APN 合作夥伴並不熟悉的風險。這表示您擁有內部專業知識或內行人知識。
- 盲點 – 您的 APN 合作夥伴熟悉的風險，但您的團隊並不熟悉。
- 未知 – 您或您的 APN 合作夥伴都不熟悉的風險。

這個圖很簡單，卻代表了受信賴 APN 合作夥伴可以實現的價值。最關鍵的是，可能有您不知道的盲點項目，但具有適當專業知識的 APN 合作夥伴會提醒您。雖然雙方都熟悉顯而易見象限中的風險，但 APN 合作夥伴可能會推薦您不熟悉的控制和解決方案。此外，當您將內部已知象限的風險告知 APN 合作夥伴，APN 合作夥伴可能能找出降低風險的最佳控制措施。當您自我衡量改進措施時，請聯絡 APN 合作夥伴以提供專家建議。

未知風險

如果您一直專注於客製化警示、透過自動化改進事件回應程序以及改善安全防禦，那麼您可能想知道下一步要改進什麼。您可能對未知風險感到好奇，如圖 3 的未知類別所示。您可以透過以下方法降低未知風險：

- 定義安全性聲明 – 您可以聲明哪些真理？ 您的環境中絕對真實的安全基本值是什麼？ 清楚地定義這些可讓您逆向搜尋。比起稍後才對安全性聲明進行逆向工程，這在雲端之旅的初期更容易完成。
- 教育、溝通和研究 – 為員工成立雲端安全專家，或者納入專家合作夥伴，以協助審查您的環境。挑戰您的假設，提防機巧的推理。在流程中建立回饋迴圈，為工程團隊提供與安全團隊溝通的機制。您還可以擴展監控相關安全郵件清單和資訊安全披露的方法。
- 減少攻擊面 – 提高防禦能力，以避免風險，並給自己更多的時間抵禦未知攻擊。阻止並減慢攻擊者的速度，並強迫他們暴露蹤跡。
- 威脅情報 – 訂閱來自世界各地的最新和相關威脅、風險及指標的持續摘要。
- 警示 – 產生通知，提醒您注意異常、惡意或昂貴的活動。例如，您可以針對在不使用的區域或服務中發生的活動建立通知。
- 機器學習 – 使用機器學習來識別特定組織或個人角色的複雜異常狀況。為了協助識別異常行為，您還可以分析網路、使用者和系統的正常特徵。

在考慮盲點和未知項目時，威脅情報是主要主題。周哈里窗顯示的是如何對您知道和不知道的內容進行分類，而威脅情報則顯示如何解釋您還不知道的內容。威脅情報是一門學科，可協助公司了解威脅模型的各個角落，找出貴公司可能尚未知道的威脅。

通常，威脅情報包括：

1. 找到新的威脅。
2. 定義新模式。
3. 定義新的自動化取得技術。
4. 重複以上過程。

雖然這個做法會有幫助，但維護威脅情報團隊對許多企業 (甚至大型企業) 可能是個負擔。最後，問題就變成須符合您的威脅模型、規模和風險逆境。請考慮下列問題：

- 您的威脅模型是否與企業所處的標準垂直領域有很大不同？
- 您的風險承受能力是否過低，因此需要這樣的團隊？
- 為企業經營一個團隊，在財務上是否合理？
- 您的風險概況是否足以吸引合理的人才參與您的事業？

如果任何一個問題的回答為否，則您應尋求威脅情報合作夥伴。許多大型知名公司都提供具有競爭力的服務。

AWS 提供讓您自行管理這些問題的工具和服務。使用機器學習辨別惡意模式是經過充分研究的領域，其模式由客戶、AWS 專業服務、APN 合作夥伴以及透過 Amazon GuardDuty 和 Amazon Macie 等 AWS 服務來實施。其中一些模式已在 AWS re:Invent 會議議程上討論過。如需詳細資訊，請參閱本白皮書的媒體一節。

客戶也在擴展其傳統上以業務為中心的資料湖，以便在開發安全資料湖時，能利用類似的架構模式。安全營運團隊也將傳統日誌記錄和監控工具 (如 Amazon OpenSearch Service 和 OpenSearch Dashboards) 的使用擴展到大數據架構中。

這些客戶正在從 AWS CloudTrail 事件日誌、VPC 流程日誌、Amazon CloudFront 存取日誌、資料庫日誌和應用程式日誌中收集內部資料，然後將這些資料與公有資料和威脅情報相結合。藉助這些寶貴的資料，客戶已經擴展到在其安全營運團隊中包含資料科學和資料工程技能，以利用諸如 Amazon EMR、Amazon Kinesis Data Analytics、Amazon Redshift、Amazon QuickSight、AWS Glue、Amazon SageMaker 和 AWS 上的 Apache MxNet 等工具來建構自訂解決方案，用於識別和預測其業務獨特的異常情況。

最後，請參閱來自 APN 合作夥伴之數百種業界領先產品的安全合作夥伴解決方案，這些產品與您內部部署環境中的現有控制在功能上相當、相同或可以相互整合。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中部署全方位的安全架構，以及擁有更流暢的體驗。

準備 – 技術

主題

- 準備存取 AWS 帳戶
- 準備流程
- 雲端提供者支援

準備存取 AWS 帳戶

在事件發生期間，您的事件回應團隊必須能夠存取事件涉及的環境和資源。在事件發生之前，請確定您的團隊擁有適當的存取權，以執行其職責。若要這樣做，您必須知道團隊成員需要何種存取權層級 (例如，他們可能採取哪種動作)，而且您必須提前佈建存取權。此存取權限來自貴公司的管控、風險管理和合規 (GRC) 政策。團隊成員的身分驗證和授權應在事件發生之前就進行記錄和測試，以確保成員能夠及時執行回應，而不致出現延誤。為了正確回應事件，準備工作的一部分應該是審查 AWS 帳戶的配置方式，以及如何允許和組織跨帳戶角色。

在此階段，您必須與開發人員、架構師、合作夥伴、管控團隊和合規團隊密切合作，以了解回應人員所需的存取層級。與組織的雲端架構師一起確定並討論 AWS 帳戶策略和雲端身分策略，了解設定了哪些身分驗證和授權方法，例如：

- 聯合 – 使用者從身分識別提供者處擔任 AWS 帳戶中的 IAM 角色。
- 跨帳戶存取 – 使用者在多個 AWS 帳戶之間擔任 IAM 角色。
- 身分驗證 – 使用者以在單個 AWS 帳戶中建立的 AWS IAM 使用者驗證。

這些選項定義了對 AWS 進行身分驗證的技術選項，以及如何在回應期間獲得存取權限，但某些組織可能需依賴其他團隊或合作夥伴來協助回應。專為回應安全事件所建立的使用者帳戶通常具有特殊權限，以提供足夠的存取權。因此，這類使用者帳戶應限制使用、不宜用於日常活動。

在建立新的存取機制之前，請與雲端團隊合作，了解 AWS 帳戶的組織和管控方式。許多客戶使用 AWS Organizations 協助集中管理帳單、跨 AWS 帳戶共用資源，以及控制存取、合規和安全。組織的一個核心功能是可以利用它將服務控制政策套用於帳戶群組，讓您可以進行大規模的政策管理。如需大規模實施管控機制的更多資訊，請參閱 AWS 大規模管控。了解您的組織如何組織和管控 AWS 帳戶之後，請考慮以下一般回應模式，以協助確定哪些方法適合您的組織。

主題

- 間接存取
- 直接存取
- 替代存取
- 自動化存取
- 受管服務存取

間接存取

如果您使用間接存取，則在安全專家組成的事件回應團隊所提供的戰術指導下，帳戶擁有者或應用程式團隊需在其 AWS 帳戶中執行經過授權的補救措施。此方法在執行任務時的速度較慢且較複雜，但是適合用於回應人員不熟悉帳戶或雲端環境的情況。

直接存取

若要向事件回應人員提供直接存取權限，請將 AWS IAM 角色部署到 AWS 帳戶中，讓安全工程師或事件回應人員在發生安全事件期間擔任這些角色。如果事件影響到您的正常身分驗證程序，事件回應程序可以透過正常的聯合流程，或透過特殊的緊急流程來進行驗證。您授予給事件回應 IAM 角色的許可，取決於您預期回應人員要執行的動作。

替代存取

如果您認為某個安全事件正在影響您的安全、身分或通訊系統，則可能需要尋求替代機制和存取權限來調查和補救影響。使用專門建構的新 AWS 帳戶，回應人員可以透過備用的安全基礎設施來協作和工作。

例如，回應人員可以利用雲端中啟動的新基礎設施，例如使用 Amazon WorkSpaces 的遠端工作站，以及 Amazon WorkMail 提供的電子郵件服務。您必須準備適當的存取控制 (使用 IAM 政策) 來委派存取許可，以便您的安全備用 AWS 帳戶可以承擔受影響 AWS 帳戶的許可。

委派適當存取權限後，您可以使用受影響帳戶中的 AWS API 來共用相關資料 (如日誌和磁碟區快照)，以便在隔離的環境中執行調查工作。如需此跨帳戶存取的詳細資訊，請參閱教學：使用 IAM 角色將存取權委派至 AWS 帳戶。

自動化存取

當您遷移到使用自動化回應安全事件時，您必須建立專門供自動化資源 (如 Amazon EC2 執行個體或 AWS Lambda 函數) 使用的 IAM 角色。然後，這些資源可以擔任 IAM 角色並繼承指派給該角色的許

可。您不必建立和分發 AWS 憑證，而是改為將許可委派給 AWS Lambda 函數或 Amazon EC2 執行個體。AWS 資源會自動接收一組臨時憑證，並使用它們簽署 API 請求。

您還可以為自動化或工具考慮使用安全的方法，以便在 Amazon EC2 執行個體的作業系統內進行驗證和執行。雖然有許多工具可以執行此自動化，但請考慮使用 AWS Systems Manager Run Command，此命令可讓您使用安裝在 Amazon EC2 執行個體作業系統上的代理程式，從遠端安全地管理執行個體。

AWSSystems Manager Agent (SSM Agent) 預設安裝在某些 Amazon EC2 Amazon Machine Images (AMI) 上，例如用於 Microsoft Windows Server 和 Amazon Linux。但是，您可能需要在其他版本的 Linux 和混合執行個體上手動安裝代理程式。無論是使用 Run Command 還是其他工具，在收到要調查的第一個安全相關警示之前，都請先完成先決條件設定和組態。

受管服務存取

您的組織可能已與資訊技術提供者建立合作關係，可代表您管理服務和解決方案。這些合作夥伴在支援組織安全方面負有共同責任，請務必在異常發生之前先釐清這層關係。無論您是否已與 AWS Managed Services 供應商 (MSP) 合作夥伴、AWS Managed Services 或是受管安全服務合作夥伴合作過，您都必須確定每個合作夥伴與您的雲端環境相關的責任、供應商對您的雲端服務已經擁有哪些存取權限、他們還需要哪些存取權限，以及需要他們協助時的聯絡點或呈報路徑。最後，您應該與您的合作夥伴一起練習，確保您的回應計劃是可預測和成功的。

準備流程

設定和測試了適當的存取權限後，您的事件回應團隊必須定義和準備調查及補救措施所需的相關流程。此階段需投注大量精力，因為您必須充分規劃對於雲端環境中安全事件的適當回應。

請與您的內部雲端服務團隊和合作夥伴密切合作，找出確保程序可行所需的任務。合作或互相指派回應活動任務，並確保必要的帳戶設定已就緒。我們建議您提前準備流程和先決條件設定，以便為您的組織提供以下回應功能。

主題

- 決策樹
- 使用備用帳戶
- 查看或複製資料
- 共用 Amazon EBS 快照
- 共用 Amazon CloudWatch Logs
- 使用不可變儲存

- 啟動事件附近的資源
- 隔離資源
- 啟動鑑識工作站

決策樹

有時候，不同的條件會需要不同的動作或步驟。例如，您可能會根據 AWS 帳戶的類型 (開發與生產)、資源的標籤、這些資源的 AWS Config 規則合規狀態或其他輸入，而採取不同的動作。

為了支援您建立和記錄這些決策，我們建議您與其他團隊和利害關係人一起草擬決策樹。決策樹與流程圖類似，這是一種可用於支援決策的工具，協助您根據潛在條件和輸入 (包括機率) 決定最佳的動作和結果。

使用備用帳戶

受影響帳戶中發生的事件可能需要加以回應的同時，最好也一併調查受影響帳戶外部的資料。有些客戶備有流程，會使用預先設定好必須佈建之資源的範本，建立獨立的隔離 AWS 帳戶環境。這些範本是透過 AWS CloudFormation 或 Terraform 等服務進行部署，該服務提供建立相關 AWS 資源集合的簡單方法，並以有序且可預測的方式進行佈建。

使用範本機制預先設定這些帳戶，在事件的初始階段就不需進行人為互動，並確保以可重複和可預測的方式來準備環境和資源，如此也可通過稽核驗證。此外，此機制還提高了在鑑識環境中維護資料安全和控制資料的能力。

此方法需要您與雲端服務和架構師團隊合作，以決定可用於調查的適當 AWS 帳戶流程。例如，您的雲端服務團隊可以使用 AWS Organizations 來產生新帳戶，並使用範本或指令碼方法預先設定這些帳戶。

當您需要讓大型組織遠離潛在威脅時，這種區隔方法最適合。這種區隔方法使用一個全新、基本上未連線的 AWS 帳戶，表示組織的使用者 (在多帳戶文件中標記為安全的組織單位 (OU)) 能夠移動至此帳戶、執行所需的鑑識活動，並可視需要，將整個帳戶移交給法律實體。這種鑑識和歸因方法需要大量的審查和規劃，並應符合企業的 GRC 政策。雖然這項工作並不容易，但在累積出龐大的帳戶基礎之前就先完成，會事倍功半。

查看或複製資料

回應人員需要存取日誌或其他證據才能進行分析，因此須確保他們能夠查看或複製資料。回應人員的 IAM 許可政策至少應該要提供唯讀存取許可，讓他們能夠進行調查。若要啟用適當的存取權限，您可以考慮一些預先建置的 AWS 受管政策，例如 SecurityAudit 或 ViewOnlyAccess。

例如，回應人員可能希望將資料 (如 AWS CloudTrail 日誌) 從一個帳戶中的 Amazon S3 儲存貯體，複製到另一個帳戶中的 Amazon S3 儲存貯體以製作時間點複本。例如，ReadOnlyAccess 受管政策提供的許可，讓回應人員能夠執行這些動作。若要了解如何使用 AWS Command Line Interface (CLI) 執行此操作，請參閱如何將所有物件從一個 Amazon S3 儲存貯體複製到另一個儲存貯體？。

共用 Amazon EBS 快照

許多客戶在調查涉及其 Amazon EC2 執行個體的安全事件時，會使用 Amazon Elastic Block Store (Amazon EBS) 快照。Amazon EBS 磁碟區的快照是增量備份。如需 Amazon EBS 增量快照的詳細資訊，請參閱 Amazon EBS 快照。

若要在獨立帳戶中對 Amazon EBS 磁碟區進行調查，您必須修改快照的許可，以便與其他指定的 AWS 帳戶共用快照。您授權的使用者可使用您共用的快照，做為建立他們自己之 EBS 磁碟區的基礎，而原始快照仍然不受影響。如需詳細資訊，請參閱共用 Amazon EBS 快照。

如果快照已加密，則還必須共用用於加密快照的自訂 AWS Key Management Service (AWS KMS) 客戶受管金鑰 (CMK)。您可以在建立自訂 CMK 時為其套用跨帳戶許可，也可以之後再套用。快照受限於其建立的區域，但您可以透過將快照複製到其他區域，來與該區域共用快照。如需詳細資訊，請參閱複製 Amazon EBS 快照。

共用 Amazon CloudWatch Logs

Amazon CloudWatch Logs 中記錄的日誌 (如 Amazon VPC 流程日誌) 可以透過 CloudWatch Logs 訂閱與另一個帳戶 (例如集中式安全帳戶) 共用。例如，日誌事件資料可從集中 Amazon Kinesis 串流讀取以執行自訂處理和分析。當您從多個帳戶收集日誌記錄資料時，自訂處理特別有用。最好在安全相關的事件發生之前，就先在雲端之旅及早建立此設定。如需詳細資訊，請參閱與訂閱共用的跨帳戶日誌資料。

使用不可變儲存

將日誌和其他證據複製到備用帳戶後，務必好好保護複製的資料。除了保護輔助證據之外，您也必須保護來源資料的完整性。這些機制稱為不可變儲存，透過防止資料被篡改或刪除，來保護資料的完整性。

您可以使用 Amazon S3 的原生功能，設定 Amazon S3 儲存貯體以保護資料的完整性。例如，使用 S3 物件鎖定功能，可以在固定時間內或永遠避免刪除或覆寫物件。使用 S3 儲存貯體政策來管理存取許可、設定 S3 版本控制以及啟用 MFA Delete，是限制資料寫入或讀取的其他方法。這種設定類型對於儲存調查日誌和證據非常有用，通常稱為單寫多讀 (WORM)。您還可以使用 AWS Key Management Service (AWS KMS) 的伺服器端加密來保護資料，並驗證只有適當的 IAM 主體有權解密資料。

此外，如果您希望在調查完成後將資料安全地保存在長期儲存空間，請考慮使用物件生命週期政策，將資料從 Amazon S3 移動到 Amazon S3 Glacier。Amazon S3 Glacier 是成本極低的雲端儲存服務，為資料封存和長期備份提供安全且耐用的儲存。它旨在提供 99.999999999% 的耐用性，並提供全面的安全和合規功能。

此外，您還可以使用 Amazon S3 Glacier 文件庫鎖定來保護 Amazon S3 Glacier 中的資料，此功能可讓您使用文件庫鎖定政策，輕鬆部署和強制執行個別 Amazon S3 Glacier 文件庫的合規控制。您可以在文件庫鎖定政策中指定安全控制功能，例如 WORM，並鎖定該政策以防未來進行編輯。鎖定之後，就無法變更政策。Amazon S3 Glacier 會強制執行文件庫鎖定政策中設定的控制，以協助您實現合規目標，例如資料保留。您可以使用 AWS Identity and Access Management (IAM) 政策語言，在文件庫鎖定政策中部署各種合規控制。

啟動事件附近的資源

對於剛接觸雲端的回應人員來說，可能會想在現有工具所在的場所進行雲端調查。根據經驗，使用雲端技術回應事件的 AWS 客戶可以獲得更好的結果 — 可以自動化隔離、更輕鬆地製作副本、更快準備好證據以供分析，也可以更快完成分析。

最佳實務是在資料所在的雲端中執行調查和鑑識，而不是先將資料傳輸到資料中心，然後才進行調查。您幾乎可以隨時隨地，使用雲端的安全運算和儲存功能來執行安全的回應操作。許多客戶選擇預先建構一個單獨的 AWS 帳戶，準備好用於執行調查，但有可能發生在同一個 AWS 帳戶中進行分析的情況。如果出於合規和法律原因，您的組織預計會保留記錄，那麼最好為長期儲存和法律活動保留一個單獨的帳戶。

此外，最佳實務是在事件發生的同一個 AWS 區域中執行調查，而不是將資料複製到另一個區域。我們建議採用這種做法，主要是因為在區域之間傳輸資料需要再多花一點時間。對於您營運的每個 AWS 區域，務必確保事件回應流程和回應人員都遵守相關的資料隱私法。如果您需要在區域之間移動資料，請務必考慮在司法管轄區之間移動資料造成的法律影響。一般來說，最佳實務是將資料保存在同一個國家管轄範圍內。

如果您認為某個安全事件正在影響您的安全、身分或通訊系統，則可能需要尋求替代機制和存取權限來調查和補救影響。AWS 提供快速啟動新基礎設施，以供用於安全、備用工作環境的能力。例如，在調查情況的可能嚴重性時，您可能會想建立一個新的 AWS 帳戶，其中包含法律顧問、公共關係和安全團隊所需的安全工具，用以進行溝通和繼續工作。AWS WorkSpaces (用於虛擬桌面)、AWS WorkMail (用於電子郵件) 和 Amazon Chime (用於通訊) 等服務可為應變團隊、領導階層和其他參與者提供溝通、調查和修復問題所需的功能和連線能力。

隔離資源

在調查過程中，您可能需要隔離資源，來因應安全異常情況。隔離資源的目的是限制潛在影響、防止受影響資源進一步傳播、限制意外暴露資料，以及防止進一步未經授權的存取。

與任何回應一樣，這裡也適用業務、監管、法律或其他考慮因素。請務必根據預期和未預期的後果，權衡您打算採取的行動。如果雲端團隊有使用資源標籤，則這些標籤可協助您識別資源的重要性或需聯絡的擁有者。

啟動鑑識工作站

部分事件回應活動可能包括分析磁碟映像、檔案系統、RAM 傾印或事件涉及的其他成品。許多客戶建置了自訂的鑑識工作站，供其用來掛載任何受影響資料磁碟區的副本 (稱為 EBS 快照)。若要這麼做，請遵循下列基本步驟：

1. 選擇可用作鑑識工作站的基本 Amazon Machine Image (AMI) (例如 Linux 或 Microsoft Windows)。
2. 從該基本 AMI 啟動 Amazon EC2 執行個體。
3. 加強作業系統、移除不必要的軟體套件，並設定相關的稽核和記錄機制。
4. 安裝您偏好的開放原始碼或私有工具組，以及您需要的任何供應商軟體和套件。
5. 停止 Amazon EC2 執行個體，並從已停止的執行個體建立新 AMI。
6. 建立每週或每月的流程，使用最新的軟體修補程式來更新和重建 AMI。

使用 AMI 佈建鑑識系統後，您的事件回應團隊可以使用此範本建立新的 AMI，以便為每次調查啟動新的鑑識工作站。您可以預先設定將 AMI 作為 Amazon EC2 執行個體啟動的程序，來簡化部署過程。例如，您可以在文字檔案中建立所需鑑識基礎設施資源的範本，然後使用 AWS CloudFormation 將其部署到您的 AWS 帳戶中。

當資源可以透過範本快速部署時，訓練有素的鑑識專家就能在每次調查中使用新的鑑識工作站，而不是重複使用基礎設施。運用此程序，可以確保其他鑑識檢查不會交叉污染。

執行個體類型和位置

Amazon EC2 提供各式各樣的最佳化執行個體類型，以滿足不同的使用案例。執行個體類型由不同的 CPU、記憶體、儲存和聯網容量組合而成，讓您有靈活性可應用程式選擇適當的資源組合。許多執行個體類型都包括多種執行個體大小，讓您能夠根據目標工作負載的需求來擴展資源。對於事件回應執行個體，請遵循貴公司的 GRC 政策，從執行生產執行個體的網路中進行定位和區隔。

AWS 增強型聯網使用單一根目錄 I/O 虛擬化 (SR-IOV) 在支援的執行個體類型上提供高效能聯網功能。SR-IOV 是一種相較於傳統虛擬網路界面可提高 I/O 效能及降低 CPU 使用率的裝置虛擬化方式。增強聯網提供更高的頻寬、更高的每秒封包數 (PPS) 效能，以及一致較低的執行個體間延遲。使用增強型聯網無需額外收費。如需哪些執行個體類型支援 10 或 25 Gbps 網路速度以及其他進階功能的相關資訊，請參閱 Amazon EC2 執行個體類型。

雲端提供者支援

主題

- AWS Managed Services
- AWS 支援
- DDoS 回應支援

AWS Managed Services

AWS Managed Services (AMS) 為您的 AWS 基礎設施提供持續的管理，讓您能夠專注於應用程式。透過實作維護基礎設施的最佳實務，AMS 有助於降低營運開銷及風險。AMS 可自動化常見的活動，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。

身為基礎設施營運商，AMS 負責部署一套安全偵測控制措施，並使用「跟隨太陽」模式，對警示提供全天候的第一線回應。觸發警示時，AMS 會遵循一組標準的自動和手動執行手冊，以確保回應一致。這些執行手冊會在布設期間分享給 AMS 客戶，因此他們可以使用 AMS 開發和協調回應。AMS 鼓勵與客戶聯合執行安全回應模擬，以便在真實事故發生之前備妥營運力量。

AWS 支援

AWS 支援 提供各種方案，可讓您運用各種工具與專業知識，協助您的 AWS 解決方案取得成功並正常運作。所有支援方案均提供全日 24 小時全年無休的客戶服務、AWS 文件、白皮書以及支援論壇。如果您需要技術支援及其他資源來協助規劃、部署或最佳化您的 AWS 環境，您可以選擇最適合您 AWS 使用案例的支援方案。

您應將AWS Management Console中的支援中心視為聯絡中心，用以取得會影響 AWS 資源之問題的相關支援。對 AWS 支援 的存取由 IAM 控制。如需取得 AWS 支援功能存取權限的詳細資訊，請參閱存取支援。

此外，如果您需要報告 Amazon EC2 的濫用情況，請聯絡 AWS 濫用團隊。

DDoS 回應支援

阻斷服務 (DoS) 攻擊會使最終使用者無法使用您的網站或應用程式。攻擊者會使用各種消耗網路頻寬或其他資源的技術，中斷合法最終使用者的存取。DoS 攻擊的最簡單形式是，由單個來源的獨立攻擊者針對目標執行攻擊。

而在分散式阻斷服務 (DDoS) 攻擊中，攻擊者會使用多個來源 (可能被一組協作者入侵或控制) 來協調針對目標的攻擊。在 DDoS 攻擊中，每個協作者或遭盜用主機都參與攻擊，因此產生大量的封包或請求，讓預期目標不堪負荷。

AWS 提供 AWS Shield 給客戶，此功能提供受管的 DDoS 保護服務，可保護在 AWS 上執行的 Web 應用程式。AWS Shield 不只提供永遠開啟的偵測服務，還提供自動的內嵌風險降低功能，可將應用程式停機與延遲時間縮到最短，因此無須聯絡 AWS 支援 也能輕鬆享受 DDoS 保護。AWS Shield 有兩種方案：標準與進階。

所有 AWS 客戶都受 AWS Shield Standard 的自動保護，且不額外收取費用。AWS Shield Standard 可防止最常見、發生的網路和傳輸層 DDoS 攻擊，以您的網站或應用程式做為目標。當您將 AWS Shield Standard 與 Amazon CloudFront 和 Amazon Route 53 搭配使用時，可獲得所有已知基礎設施 (第 3 層和第 4 層) 攻擊的全面可用性保護。

如果需要針對在 Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (ELB)、Amazon CloudFront 和 Amazon Route 53 資源上執行的 Web 應用程式提供更高一層的攻擊防護，可訂閱 AWS Shield Advanced。此外，AWS Shield Advanced 還可讓您全天候聯絡 AWS DDoS 應變團隊 (DRT)。如需關於 AWS Shield Standard 和 AWS Shield Advanced 的詳細資訊，請參閱AWS Shield。

模擬

主題

- 安全事件回應模擬
- 模擬步驟
- 模擬範例

安全事件回應模擬

安全事件回應模擬 (SIRS) 是內部事件，它提供了一個結構化機會，可在實際場景中練習事件回應計劃和程序。SIRS 事件基本上就是用來準備和反覆改善您的回應能力。對於進行 SIRS 活動，客戶可能會發現有價值的原因包括：

- 驗證整備程度。
- 培養信心，從模擬和培訓員工學到經驗。
- 遵守合規或合約義務。
- 產生用於認證的成品
- 保持敏捷性，專注於增量改進。
- 改進速度和工具。
- 精簡溝通和上報。
- 培養安然面對罕見和意外情形的能力。

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

模擬步驟

無論您是自行設計 SIRS，還是由值得信賴的合作夥伴奠定基礎，模擬通常都遵循以下步驟：

1. 尋找重要問題 – 定義應導致回應的觸發器。
2. 找出技術熟練的安全工程師 – 模擬需要建置者和測試者。

3. 建置真實的模型系統 – 模擬必須是真實且適當的。如果不夠真實，參與者可能不重視演練。如果太簡化，演練可能被認為太瑣碎。先從簡單的演練開始，再朝向完整的事件發展。
4. 建置和測試場景元素 – 可能需要建置相關的模擬材料，例如記錄成品、電子郵件通知和提醒，以及潛在的執行手冊。
5. 邀請其他安全人員和跨組織參與者 – 邀請需要培訓和參與的所有人。如果一般法律顧問、行政主管和公關部門屬於模擬的一部分，您也應該邀請他們參與。
6. 執行模擬 – 選擇要不要事先通知員工將有 SIRS 事件模擬。
7. 表揚、衡量、改進和重複 – 模擬有壓力因素，因此鼓勵和表揚參與者的努力非常重要。鼓勵之後，就需要衡量成果、改進和反覆迭代下一次模擬。AWS 鼓勵您養成這些活動的習慣。

> **Important**
>
> 如果要計劃安全事件回應模擬 (SIRS)，請參閱滲透測試並檢閱其他模擬事件章節，了解有關如何繼續進行的最新資訊。

模擬範例

安全模擬必須切合實際，才能提供預期的價值。當您或您的合作夥伴努力建立自己的模擬時，請一定要將過去的真實事件視為潛在模擬演練的寶貴來源。以下是 AWS 客戶發現可用於初始模擬的幾個範例：

- 對網路組態或資源進行未經授權的變更。
- 由於開發人員組態設定不當，而被錯誤公開的憑證。
- 由於開發人員組態設定不當，而被錯誤地公開存取的敏感內容。
- 隔離與可疑惡意 IP 地址進行通訊的 Web 伺服器。

除了寶貴的體驗式學習之外，執行 SIRS 活動也會產生輸出 (例如獲得的經驗)，您可以將其用作計劃下一個過程的輸入：這就是迭代。

反覆

上一節界定了 SIRS 活動的一些優點。這些優點之一是透過增量改進而獲得敏捷性。模擬應可產生寶貴的結果，供您運用來改進安全回應。它們為組織提供關於何者可運作、何者無法運作的回饋迴圈。藉助這些知識，您可以增量建立新程序或更新現有程序，以改善回應。

主題

- 執行手冊
- 自動化

執行手冊

偵測到安全異常情況時，隔離事件及返回正常狀態是回應計劃重要的元素。例如，如果由於安全組態設定不當而發生異常，修復的方法可能就是透過使用適當的組態，重新部署資源以移除變異那麼簡單。若要這樣做，您需要提前規劃並定義自己的安全回應程序，這些步驟通常稱為執行手冊。

執行手冊是組織執行一或多個任務之程序的文件記錄形式。此文件通常存放在內部數位系統或紙本形式。您目前可能已有事件回應執行手冊，否則就需要建立一份，以便符合安全保證架構。但是，當您手動遵循書面執行手冊，您會增加犯錯的可能性。因此，我們建議自動執行所有可重複的任務。自動化可讓您的回應團隊擺脫常見任務，將精力投注於更重要的任務，例如關聯事件、模擬練習、設計新的回應程序、進行研究、開發新技能以及測試或建置新工具。但是，在將任務分解為可程式化的邏輯並反覆迭代到正確的自動化之前，您必須先編寫執行手冊。

建立執行手冊

若想為雲端建立執行手冊，我們建議您先專注於目前產生的警示。如果產生警示，請務必調查該警示。從定義所執行手動程序的描述開始。在此之後，請測試程序並反覆查看執行手冊的模式，以改善您所作回應的核心邏輯。應判斷例外狀況，以及這些情境的其他解決方案有哪些。例如，在開發環境中，不妨終止組態錯誤的 Amazon EC2 執行個體。但是，如果生產環境中發生相同的事件，與其終止執行個體，您可以停止執行個體，向利害關係人確認重要資料不會遺失，並且可接受終止。

確定最佳解決方案後，就可以將邏輯解構成為以程式碼為基礎的解決方案，許多回應人員可將其做為工具使用，以做到自動回應，並免除回應人員面對的變通或猜測。這可加快回應的生命週期。下一個目標是透過提醒或事件本身叫用 (而不是由回應人員執行)，讓此程式碼能夠完全自動化。

入門

如果您不確定從何處開始，請考慮從 AWS Trusted Advisor、AWS Security Hub 的基本安全最佳實務以及 AWS Config 規則 (包括 AWS Config 規則 Gitthub 儲存庫) 產生的警示開始。然後，專注於由服務產生的事件，這些事件將描述您所關心的系統。

Amazon GuardDuty 和存取分析器可描述應用程式在 AWS 中使用的許多網域，這就是通常建議使用它們的原因；然而，Amazon Inspector 和 Amazon Macie 對於具有資料和終點問題的網域，則具有特定用途。如需 Amazon GuardDuty 問題清單的資訊，請參閱《Amazon GuardDuty 使用者指南》。存取分析器問題清單可在《Amazon Access Analyzer 使用者指南》中找到。Macie 問題清單可在《Amazon Macie 使用者指南》中找到。Amazon Inspector 問題清單可在《Amazon Inspector 使用者指南》中找到。Security Hub 讓您能夠將這些問題清單統一放到一個位置，並迅速對其作出一致回應，因此我們建議將其作為修補的中心位置。

當問題清單或警示發生任何變化時，上述所有服務都會透過 Amazon CloudWatch Events 傳送通知，包括新產生的警示和現有警示的更新。您可以設定 Amazon CloudWatch Events 規則，來觸發 AWS Lambda 函數執行事件驅動的回應。不過，建構自訂洞察並從應用程式網域新增您自己的問題清單的能力，可增加使用 Security Hub 的重要理由。如需詳細資訊，請參閱事件驅動回應一節。

自動化

自動化是一種力量倍增器，這表示它可以擴展回應人員的工作量，以符合組織的速度。從手動程序轉向自動化程序，可讓您將更多時間花在提高 AWS 雲端環境的安全性。

主題

- 自動化事件回應
- 事件驅動回應

自動化事件回應

若要將安全工程和操作功能自動化，您可以使用 AWS 提供的完整 API 和工具集。您可以完全自動執行身分管理、網路安全、資料保護和監控功能。建置安全自動化後，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狀態並手動回應事件。

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

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

但是，您的目標應該是進一步縮短偵測機制和回應機制之間的時間差距。在過去，這個時間差距可能高達數小時、數天甚至數個月。SANS 在 2016 年進行的事件回應調查發現，21% 的受訪者表示其偵測時間需要兩到七天，而只有 29% 的受訪者能夠在同一時間範圍內修復事件。而在雲端，您可以建置事件驅動的回應功能，將回應時間差距縮短到數秒鐘。

主題

- 自動回應的選項
- 掃描方法中的成本比較

自動回應的選項

請務必在企業實施和組織結構之間取得平衡。圖 4 使用雷達圖來說明 AWS 實施中，每個自動回應選項的技術屬性差異。在圖表中，技術屬性離圖表中心越遠，相應的自動化回應技術屬性的強度就越大。例如，AWS Lambda 提供的速度較快，需要較少的技術技能。AWS Fargate 提供較高的靈活性，需要較少的維護和技術技能。表 1 概述這些自動化選項，並摘要顯示每個選項的技術屬性。

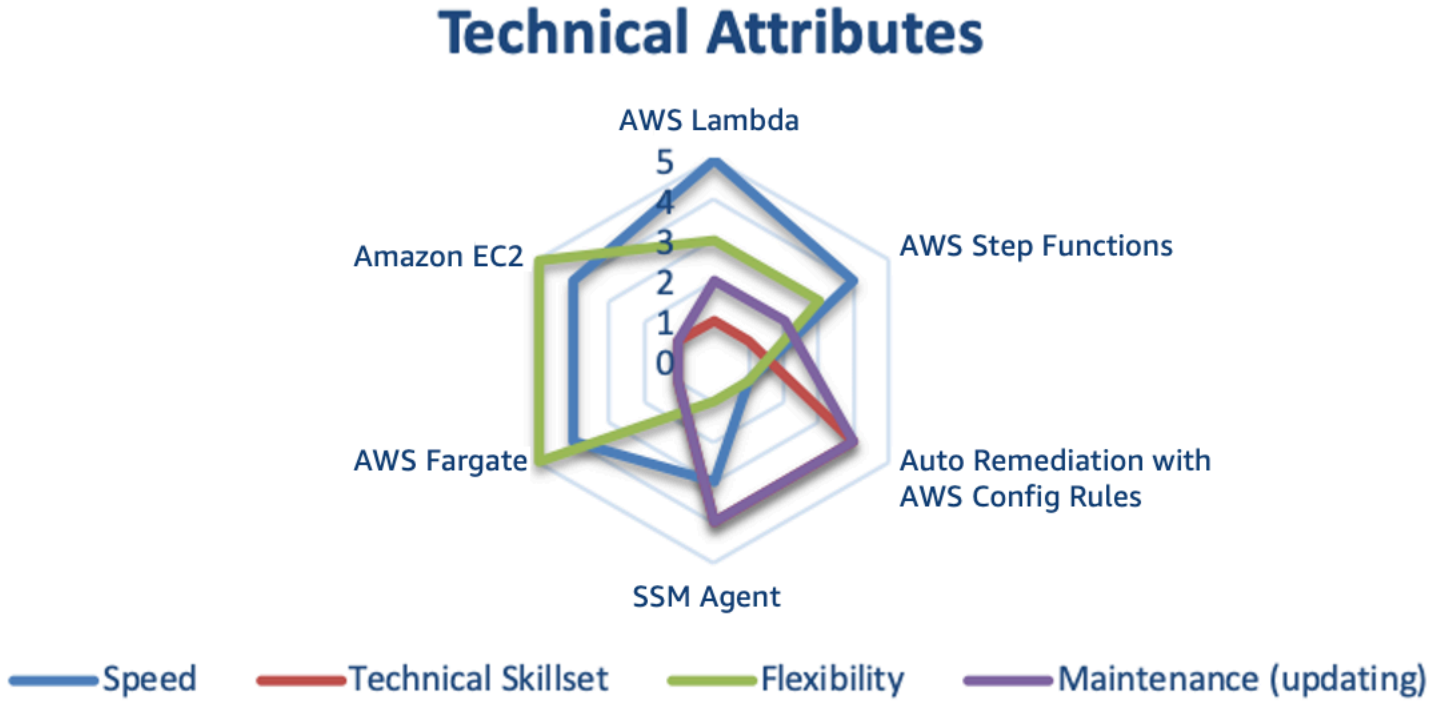

圖 4：各自動回應方法的技術屬性差異

表 1：自動回應的選項

AWS 服務或功能	描述	屬性摘要*
AWS Lambda	系統僅使用 AWS Lambda、使用您的組織企業語言。	速度 靈活性 維護 技能
AWS Step Functions	使用 AWS Step Functions 、Lambda 和 SSM Agent 的系統。	速度 靈活性 維護 技能
使用 AWS Config 規則 自動修補	一組 AWS Config 規則 規則和自動修補，用於評估環境並將其推回到核准規格。	維護和技能 速度和靈活性
SSM Agent	一套自動化規則和文件，用於許多環境和內部系統並進行更正。	維護和技能 速度 靈活性
AWS Fargate	AWS Fargate 系統使用開放原始碼 Step Functions 程式碼以及來自 Amazon CloudWatch 和其他系統的事件，來進行偵測和修復。	靈活性 速度 維護和技能
Amazon EC2	在完整執行個體上執行的系統，類似於 AWS Fargate 選項。	靈活性 速度 維護

AWS 服務或功能	描述	屬性摘要*
		技能

* 每個服務或功能的屬性依遞減順序列出。例如，AWS Lambda 提供的速度較快，需要較少的技術技能。AWS Fargate 提供較高的靈活性，需要較少的維護和技術技能。

在 AWS 環境中考慮這些自動化選項時，您還需要考慮集中化和掃描週期 (每秒事件數 [EPS])。

集中化是指一個中心帳戶，用於驅動組織的所有偵測和修復。這個方法看起來是立即可用的最佳選擇，也是目前的最佳實務。但在某些情況下，您需要偏離這種方法，理解時機取決於您如何處理下屬帳戶。我們鼓勵您從運用 AWS Organizations 中的多帳戶架構或 AWS Control Tower中的安全工具帳戶開始。

表 2：集中化的優點和缺點

	集中化	去集中化
優點	組態管理簡單 無法取消或修改回應	架構簡單 初始設定較快
缺點	增加架構的複雜性 須將帳戶和資源上線/離線	需要管理更多的資源 難以維護軟體基準

實施這些做法的成本比較，也可能推動決定最佳選項的企業決策。每秒事件數 (EPS) 是用於估算成本的最佳指標。更簡單和更便宜的方法，最終可能是集中式也可能是非集中式方法，但我們不可能審查您在您的帳戶中如何具體評估成本。在將這些事件傳送到中央帳戶以進行回應時，請務必考慮 EPS。EPS 越高，將這些事件傳送到集中帳戶的成本就越高。

掃描方法中的成本比較

偵測異常的掃描方法和驗證之間的時間範圍，將進一步決定成本。對於掃描方法，您可以選擇事件型或定期掃描審查。表 3 顯示這兩種方法的優缺點。

表 3：不同掃描方法的優缺點

	事件型	定期掃描
優點	從事件到回應的時間較短 較不需要查詢其他 API 呼叫	可完整查看特定的時間點
缺點	資源周圍的狀態脈絡有限 觸發的事件可能是針對不可用的資源	針對大型帳戶的服務配額 API 呼叫量大時，可能會遇到調節

在許多情況下，在完全成熟的組織中，結合使用兩種掃描方法可能是最好的選擇。AWS Security Hub 和 AWS 基礎安全最佳實務標準提供兩種掃描方法的組合。

圖 5 使用雷達圖來說明每個自動化方法的每秒事件數 (EPS) 成本比較。例如，Amazon EC2 和 AWS Fargate 執行 0-10 EPS 的成本最高，而 AWS Lambda 和 AWS Step Functions 執行 76+ EPS 的成本最高。

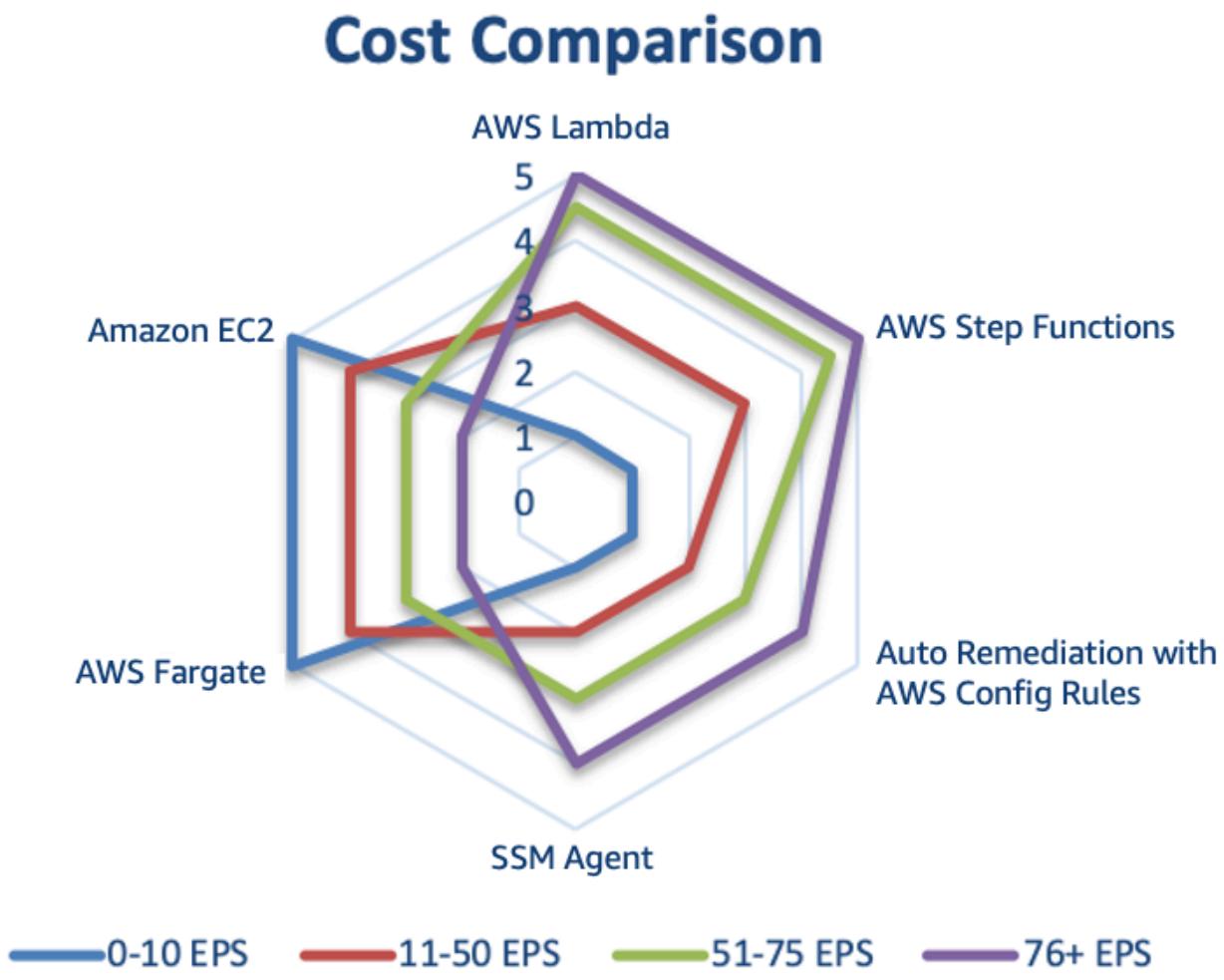

圖 5：自動化選項掃描方法的成本比較 (每秒事件數 [EPS])

事件驅動回應

使用事件驅動的回應系統，偵測機制會觸發回應機制，以自動修復事件。您可以使用事件驅動的回應功能，減少偵測機制與回應機制之間體現價值的時間。若要建立此事件驅動架構，您可以使用 AWS Lambda；這是一種無伺服器運算服務，可執行程式碼以回應事件，並自動為您管理基礎運算資源。

例如，假設您有一個已啟用 AWS CloudTrail 服務的 AWS 帳戶。如果已停用 AWS CloudTrail (透過 `cloudtrail:StopLogging` API)，回應程序是再次啟用服務並調查停用 AWS CloudTrail 日誌記錄的使用者。您可以透過程式設計方式再次啟用日誌記錄 (透過 `cloudtrail:StartLogging` API)，而不是在AWS Management Console中手動執行這些步驟。如果您使用程式碼實作此功能，則回應目標是盡快執行此任務，並通知回應人員已執行回應。

您可以將邏輯分解為在 AWS Lambda 函數中執行的簡單程式碼，以便執行這些任務。然後，您可以使用 Amazon CloudWatch Events 監控特定 `cloudtrail:StopLogging` 事件，並在發生事件時呼叫函數。當 Amazon CloudWatch Event 叫用此 AWS Lambda 回應函數時，您可以將特定事件的詳細資訊傳遞給它，包括停用 AWS CloudTrail 的主體資訊、停用時間、受影響的特定資源以及其他相關資訊。您可以使用此資訊來豐富日誌中的問題清單，然後產生僅包含回應分析師所需特定值的通知或警示。

理想情況下，事件驅動回應的目標是讓 Lambda 回應函數執行回應任務，然後通知回應人員已使用任何相關資訊成功解決異常。然後由人類回應人員決定如何判斷其發生的原因，以及如何防止今後再次發生。此回饋迴圈可進一步改善雲端環境的安全。若想實現此目標，您必須培養一種文化，讓安全團隊能夠與開發和營運團隊更緊密地合作。

事件回應範例

主題

- 服務網域事件
- 基礎設施網域事件

服務網域事件

服務網域事件通常僅透過 AWS API 處理。

身分

AWS 為雲端服務提供 API，數百萬客戶使用這些 API 來建置新的應用程式並推動業務成果。這些 API 可以透過許多方法呼叫，如軟體開發套件 (SDK)、AWS CLI 和 AWS Management Console。若想透過這些方法與 AWS 互動，IAM 服務可協助您安全地控制對 AWS 資源的存取。您可以使用 IAM，在帳戶層級控制誰經過驗證 (已登入) 和獲得授權 (具備許可) 可使用資源。如需可與 IAM 搭配使用的 AWS 服務清單，請參閱可搭配 IAM 運作的 AWS 服務。

當您首次建立 AWS 帳戶，您會先有單一的登入身分 (SSO)，可以完整存取帳戶中所有 AWS 服務與資源。此身分稱為 AWS 帳戶根使用者，是藉由您用來建立帳戶的電子郵件地址和密碼以登入並存取。強烈建議您不要將根使用者用於日常任務，尤其是不要用於管理任務。反之，我們建議您遵循最佳實務：僅將根使用者用於建立第一個 IAM 使用者、安全地存放根使用者憑證，並僅執行少量帳戶和服務管理任務。如需詳細資訊，請參閱建立個別 IAM 使用者。

雖然這些 API 為數百萬客戶提供了寶貴價值，但如果不對的人存取了您的 IAM 帳戶或根憑證，某些 API 可能會遭到濫用。例如，您可以使用 API 在帳戶內啟用日誌記錄，例如 AWS CloudTrail。但是，如果攻擊者取得您的憑證，他們也可以使用 API 停用這些日誌。您可以設定遵循最低權限模式的適當 IAM 許可，並正確保護您的 IAM 憑證，來防止此類濫用。如需詳細資訊，請參閱 AWS Identity and Access Management 使用者指南中的 IAM 最佳實務。如果確實發生此類事件，則會有多個偵測控制來識別您的 AWS CloudTrail 日誌記錄已被停用，包括 AWS CloudTrail、AWS Config、AWS Trusted Advisor、Amazon GuardDuty 和 AWS CloudWatch Events。

資源

其他可能被濫用或設定錯誤的功能因組織而異，具體取決於每個客戶在雲端的執行方式。例如，某些組織將某些資料或應用程式設為公開存取，而某些組織將其應用程式和資料保密。並非所有安全事件都是

惡意事件；某些事件可能是由於無意或不正確的設定引起的。請考慮哪些 API 或功能對您的組織有重大影響，以及您對於它們是經常使用還是不常使用。

您可以使用工具和服務來找出許多設定不當的安全組態。例如，AWS Trusted Advisor 提供一系列最佳實務檢查。APN 合作夥伴也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。其中許多產品和解決方案已透過 AWS 合作夥伴能力計劃預先符合資格。我們鼓勵您造訪「APN 安全能力計劃」的組態與漏洞分析區段，瀏覽這些解決方案並判斷它們是否能夠滿足您的要求。

基礎設施網域事件

基礎設施網域通常包括應用程式的資料或網路相關活動，例如到達 VPC 中 Amazon EC2 執行個體的流量，以及 Amazon EC2 執行個體作業系統中執行的處理程序。

例如，假設您的監控解決方案通知您，Amazon EC2 執行個體上存在潛在的安全異常情況。以下動作是解決此問題的常見步驟：

1. 在對環境進行任何變更之前，請先從 Amazon EC2 執行個體擷取中繼資料。
2. 為執行個體啟用終止保護，來保護 Amazon EC2 執行個體免遭意外終止。
3. 切換 VPC 安全群組，來隔離 Amazon EC2 執行個體。但是，請注意 VPC 連接追蹤和其他阻隔技術。
4. 將 Amazon EC2 執行個體與任何 AWS Auto Scaling 群組分開。
5. 從任何相關的 Elastic Load Balancing 服務中取消註冊 Amazon EC2 執行個體。
6. 快照 連接到 EC2 執行個體的 Amazon EBS 資料磁碟區，以便保留和跟進調查。
7. 將 Amazon EC2 執行個體標記為隔離以便進行調查，並新增任何相關中繼資料，例如與調查相關的故障票證。

您可以使用 AWS API、AWS 開發套件、AWS CLI 和 AWS Management Console，執行上述所有步驟。若想透過這些方法與 AWS 互動，IAM 服務可協助您安全地控制對 AWS 資源的存取。您可以使用 IAM，在帳戶層級控制誰經過驗證，以及獲得授權可使用資源。IAM 服務為您提供身分驗證和授權，讓您可以執行這些動作並與服務網域互動。

Amazon EBS 磁碟區的快照是 EBS 資料磁碟區的時間點區塊層級副本，以非同步方式進行複製，可能需要一些時間才能完成，但它是該資料的未來增量。您可以從這些副本建立新的 EBS 磁碟區，並將其掛載到鑑識 EC2 執行個體，以便由鑑識調查人員進行離線深入分析。下圖顯示結果的簡化版本，並未描述所有網路元件 (如子網路、路由表和網路存取控制清單)。

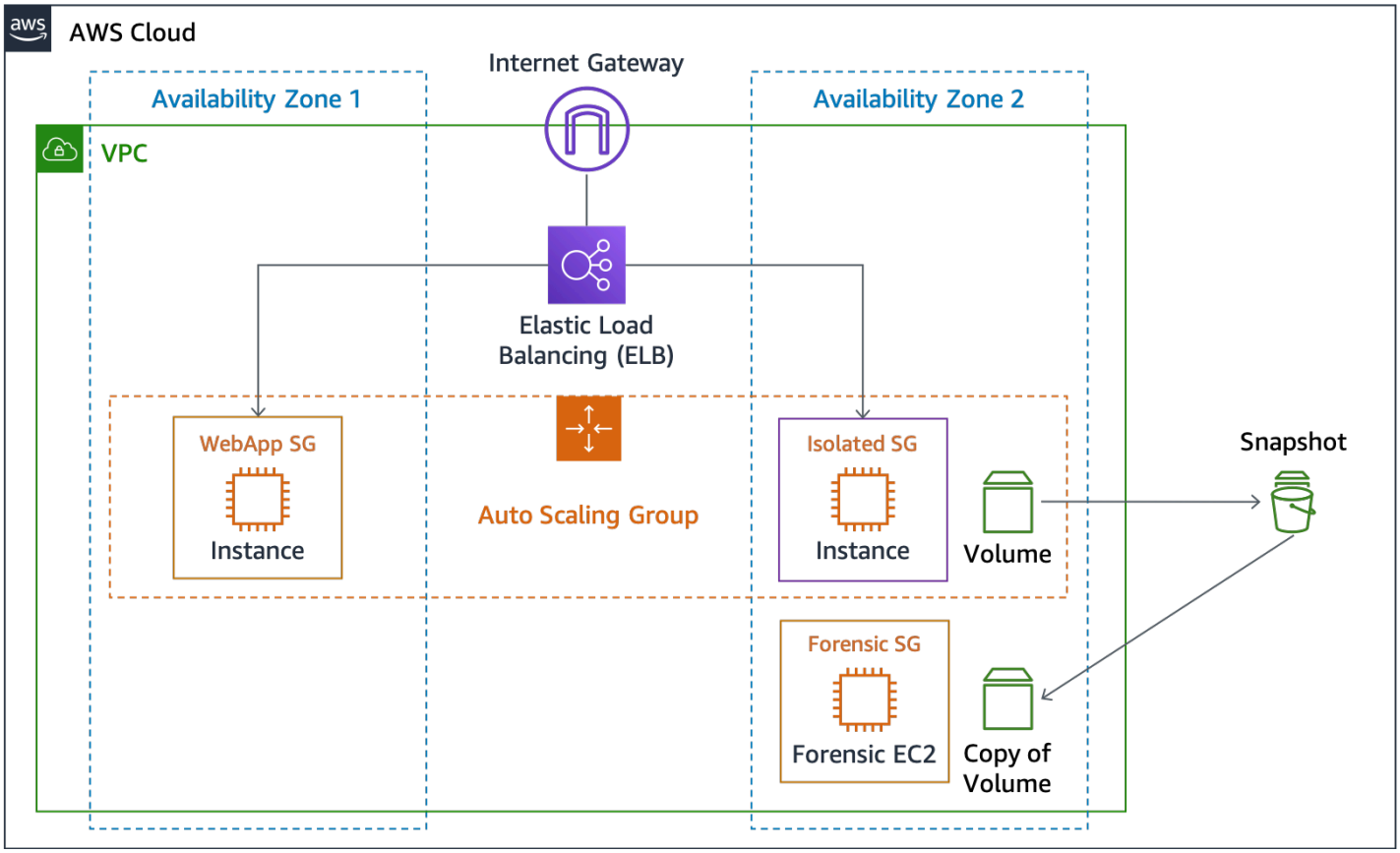

圖 6：EC2 執行個體隔離和快照

主題

- 調查決策
- 擷取暫時性資料
- 使用 AWS Systems Manager
- 自動執行擷取

調查決策

此時，您可以選擇離線調查 (立即關閉執行個體) 或線上調查 (讓執行個體保持執行中)。離線調查的一個優點是，執行個體關閉後，它不再影響現有環境。此外，您可以從 EBS 快照建立受影響執行個體的副本，並在隔離的 AWS 帳戶中查看該副本 (此帳戶具有專門為調查而設計的隔離環境)。但是，如果線上調查可讓您從主機作業系統擷取暫時性證據 (如記憶體或網路流量)，則可選擇不立即關閉執行個體。

擷取暫時性資料

即使您不選擇執行線上調查，但也需了解從執行個體中擷取暫時性資料的必要機制。線上調查需要與 Amazon EC2 執行個體上執行的作業系統進行互動。在這種情況下，您需要的不僅僅是 AWS IAM 服務，以便在 Amazon EC2 執行個體上執行任務。雖然您可以使用標準方法 (例如 Linux Secure Shell (SSH) 或 Microsoft Windows 遠端桌面 (RDP)) 直接向電腦進行驗證，但與作業系統進行手動互動並不是最佳實務。我們建議您以程式設計方式使用自動化工具，在主機上執行任務。

使用 AWS Systems Manager

AWS Systems Manager Run Command 可協助您從遠端在目標執行個體上安全地執行 Linux Shell 指令碼和 Windows PowerShell 命令的隨需變更。儘管您可以透過 AWS IAM 服務中的許可呼叫 Run Command，但您必須先將 Amazon EC2 執行個體啟用為受管執行個體、在電腦上安裝 SSM Agent (如果預設情況下未安裝)，然後設定 AWS IAM 許可。如果您有興趣使用 Run Command 進行自動化或回應活動，在執行調查之前，請務必先完成先決條件活動。

AWS Systems Manager (包括 Run Command) 與 AWS CloudTrail 服務整合，該服務可擷取由 Systems Manager 或代表 Systems Manager 進行的 API 呼叫，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。使用 AWS CloudTrail 所收集的資訊，您可以判定提出了什麼樣的請求、提出請求的來源 IP 地址、提出請求的人員、提出請求的時間等。CloudTrail 會建立所有 Systems Manager API 動作的日誌，包括 API 請求，以便使用 Run Command 來執行命令或建立 Systems Manager 文件。

您可以使用 AWS Systems Manager Run Command 服務來叫用執行 Linux Shell 指令碼和 Windows PowerShell 命令的 SSM Agent。這些指令碼可以載入和執行特定的工具以從主機擷取其他資料，例如 Linux Memory Extractor (LiME) 核心模組。然後，您可以將記憶體擷取傳輸到 VPC 網路中的鑑識 Amazon EC2 執行個體，或傳輸到 Amazon S3 儲存貯體以便耐久儲存。

自動執行擷取

呼叫 SSM Agent 的一個方法是，當執行個體被標記為特定標籤時，透過 Amazon CloudWatch Events 定位 Run Command。例如，如果您將 `Response=Isolate+MemoryCapture` 標籤套用至受影響的執行個體，則可以設定 Amazon CloudWatch Events 來觸發兩個動作：

- 執行隔離活動的 Lambda 函數
- Run Command，用於執行 Shell 命令以透過 SSM Agent 匯出 Linux 記憶體

這個由標籤驅動的回應，是另一個事件驅動回應方法。

結論

隨著您繼續進行雲端之旅，請務必考慮上述針對 AWS 環境的基本安全事件回應概念。您可以組合使用可用控制、雲端功能和修復選項，來協助您提高雲端環境的安全性。您還可以從小型開始，隨著採用可提高回應速度的自動化功能而反覆進行迭代，以便在發生安全事件時做好更充分的準備。

其他資源

如需其他資訊，請參閱：

- AWS Well-Architected
- AWS 雲端採用架構頁面
- AWS 集中式記錄解決方案
- 使用 AWS Glue 和 Amazon QuickSight 將 AWS CloudTrail日誌視覺化
- 如何監控 Amazon EC2 執行個體上，以主機為基礎的入侵偵測系統警示
- 使用 Amazon CloudWatch 存放及監控作業系統和應用程式日誌檔案
- Amazon S3 中的 Identity and Access Management
- 使用版本控制 (Amazon S3)
- 使用 MFA Delete
- 使用 AWS KMS 受管金鑰伺服器端加密 (SSE-KMS) 來保護資料
- 使用 AWS 主控台和 CLI 處理事件回應
- 為加州消費者隱私保護法做好準備

媒體

- AWS re:Invent 2014 (SEC402)：雲端中的入侵偵測
- AWS re:Invent 2014 (SEC404)：雲端中的事件回應
- AWS re:Invent 2015 (SEC308)：在雲端中處理安全事件
- AWS re:Invent 2015 (SEC316)：利用安全事件回應模擬來強化您的架構
- AWS re:Invent 2016 (SEC313)：從概念到程式碼再到執行，自動化安全事件回應
- AWS re:Invent 2017 (SID302)：透過自動化和 Alexa 強制增強您的安全團隊
- AWS re:Invent 2016 (SAC316)：安全自動化：花更少的時間保護您的應用程式
- AWS re:Invent 2016 (SAC304)：預測性安全：使用大數據加強防禦
- AWS re:Invent 2017 (SID325)：Amazon Macie：對於安全和合規工作負載，由機器學習提供支援的資料可視性
- AWS London Summit 2018：在 AWS 中自動化事件回應和鑑識

第三方工具

以下指向第三方工具的連結是外部連結，未經 AWS 認可。AWS 不提供關於這些工具或頁面的任何保證或陳述。

- AWS_IR – 用於緩解主機和金鑰洩漏的 Python 可安裝命令列公用程式。
- MargaritaShotgun – 遠端記憶體擷取工具。
- ThreatPrep – 用於評估關於事件處理整備程度之 AWS 帳戶最佳實務的 Python 模組。
- ThreatResponse Web – 與 AWS_IR 命令列工具搭配使用的 Web 型分析平台。
- GRR Rapid Response – 用於事件回應的遠端即時鑑識。
- Linux Write Blocker – 用於啟用 Linux 軟體寫入封鎖的核心修補程式和使用者空間工具。

行業參考

- NIST SP 800-61R2：電腦安全事故處理指南

文件修訂

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
次要更新	錯誤修正和許多次要變更。	2021 年 6 月 2 日
小幅度更新	更正中斷的連結。	2021 年 3 月 5 日
白皮書已更新	更正了中斷的連結和大量文字變更，以提高可讀性。	2020 年 11 月 23 日
小幅度更新	修正「使用 AWS 主控台和 CLI 處理事件回應」的連結。	2020 年 6 月 30 日
白皮書已更新	針對新的安全服務、威脅情報、容器的共同責任、自動化和 CCPA 進行了更新。新增具有範例決策樹和執行手冊的附錄。	2020 年 6 月 11 日
初始出版	白皮書初始出版	2019 年 6 月 1 日

附錄 A：雲端功能定義

AWS 提供 150 多種雲端服務和數千項功能。其中多項提供原生偵測、預防性和回應功能，其他則可用於建構自訂的安全解決方案。本節包含與雲端中的事件回應最相關的部分服務。

主題

- 日誌記錄和事件
- 可見性和提醒
- 自動化
- 安全的儲存
- 自訂

日誌記錄和事件

AWS CloudTrail – AWS CloudTrail 是一種支援您 AWS 帳戶的管控、合規、作業稽核和風險稽核的服務。使用 CloudTrail 可以記錄、持續監控和保留 AWS 基礎設施中所有與動作相關的帳戶活動。CloudTrail 可提供 AWS 帳戶活動的事件歷史記錄，包括透過 AWS Management Console、AWS 開發套件、命令列工具及其他 AWS 服務所採取的動作。這個事件歷史記錄簡化了安全分析、資源變更追蹤和故障排除的程序。

驗證過的日誌檔案對於安全和鑑識調查十分重要。若要判斷日誌檔案在 CloudTrail 傳遞後是否已被修改、刪除或保持不變，您可使用 CloudTrail 日誌檔案完整性驗證。此功能以產業標準演算法而內建：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得 CloudTrail 日誌檔案無法透過運算方式來修改、刪除或偽造，而不被偵測出來。

預設情況下，由 CloudTrail 傳送到您的儲存貯體的日誌檔案，會透過 Amazon 伺服器端加密進行加密。您可以選擇將 AWS Key Management Service (AWS KMS) 受管金鑰 (SSE-KMS) 用於 CloudTrail 日誌檔案。

Amazon CloudWatch Events – Amazon CloudWatch Events 提供近乎即時的系統事件串流，說明 AWS 資源的變動情形，或是何時 AWS CloudTrail 發佈 API 呼叫。使用您可以快速設定的簡單規則，您可以比對事件並將它們路由到一或多個目標函數或串流。CloudWatch Events 在營運變更時會查覺到。CloudWatch Events 會回應這些操作變更並視需要進行修正動作，透過傳送訊息以回應環境、啟用功能、執行變更和擷取狀態資訊。某些安全服務 (如 Amazon GuardDuty) 會以 CloudWatch Events 的形式產生輸出。

AWS Config – AWS Config 是一種可讓您評估、稽核和評判 AWS 資源的組態的服務。Config 會持續不斷地監控和記錄您的 AWS 資源組態，並可依據所需的組態自動評估記錄的組態。使用 Config，您可以手動或自動檢視組態變更以及 AWS 資源之間的關係。您可以查看詳細的資源組態歷史記錄，也可依據內部準則指定的組態來判斷整體合規情況。這可讓您簡化合規稽核、安全分析、變更管理和操作故障診斷的程序。

Amazon S3 存取日誌 – 如果您將敏感資訊存放在 Amazon S3 儲存貯體中，則可以啟用 S3 存取日誌來記錄這些資料的每次上傳、下載和修改。此日誌獨立於記錄儲存貯體本身變更 (例如變更存取政策和生命週期政策) 的 CloudTrail 日誌，且是後者的補充。

Amazon CloudWatch Logs – 您可以使用 Amazon CloudWatch Logs，從您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中使用 CloudWatch Logs 代理程式監控、存放和存取日誌檔案 (如作業系統、應用程式和自訂日誌檔案)。此外，Amazon CloudWatch Logs 還可以擷取來自 AWS CloudTrail、Amazon Route 53 DNS 查詢、VPC 流程日誌、Lambda 函數及其他來源的日誌。然後，您可以從 CloudWatch Logs 擷取關聯的日誌資料。

Amazon VPC Flow Logs – 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。建立流量日誌之後，您可以在 Amazon CloudWatch Logs 中檢視及擷取其資料。VPC 流程日誌可協助您處理多項任務。例如，您可以使用流程日誌來為特定流量沒有觸達執行個體的原因進行故障診斷，有助您診斷限制性過高的安全群組規則。您也可以使用流程日誌做為安全工具，來監控執行個體的流量。

AWS WAF 日誌 – AWS WAF 現在支援對服務檢查的所有 Web 請求進行完整記錄。您可將這些記錄存放在 Amazon S3 供合規與稽核所需之用，並將其用於偵錯和其他鑑識用途。這些記錄有助於讓您了解特定規則觸發的原因，以及特定 Web 請求封鎖的原因。您還可以把日誌與 SIEM 和日誌分析工具整合。

其他 AWS 日誌 – 隨著創新的步伐，我們幾乎每天都會為客戶部署新功能，這表示有數十個 AWS 服務提供日誌記錄和監控功能。如需每個 AWS 服務所提供功能的相關資訊，請參閱該服務的 AWS 文件。

可見性和提醒

AWS Security Hub – AWS Security Hub 讓您可以全面了解各 AWS 帳戶的優先安全提醒和合規狀態。Security Hub 將多項 AWS 服務 (例如 Amazon GuardDuty、Amazon Inspector 及 Amazon Macie) 和 AWS 合作夥伴解決方案的安全提醒或問題彙整於一處，妥善整理並依優先順序排序。系統會透過整合式儀表板提供圖表和表格，以視覺化方式概述偵測結果，以便您擬定實際措施。您也可以使用自動化的合規檢查，根據貴組織遵循的 AWS 最佳實務和產業標準，持續監控您的運作環境。

Amazon GuardDuty – Amazon GuardDuty 是受管威脅偵測服務，可持續監控惡意或未經授權的行為，協助您保護 AWS 帳戶和工作負載。該服務可監控各種暗示帳戶可能遭到入侵的活動，例如不尋常的

API 呼叫或可能的未經授權部署。GuardDuty 也能偵測可能受到危害的執行個體或攻擊者進行的偵察活動。

GuardDuty 會透過整合的威脅情報饋送識別可疑的攻擊者，並使用機器學習偵測帳戶和工作負載活動中的異常狀況。如果偵測到潛在的威脅，服務會將詳細的安全提醒傳送到 GuardDuty 主控台和 AWS CloudWatch Events。這樣就能對提醒採取動作，而且很容易將提醒整合到現有的事件管理系統和工作流程系統。

Amazon Macie – Amazon Macie 是 AI 支援的安全服務，可自動探索、分類和保護存放在 AWS 中的敏感資料，以協助您避免資料遺失。Amazon Macie 透過機器學習辨識個人身分識別資訊 (PII) 或智慧財產等敏感資料、指派商業價值，並提供此資料存放位置的可見性，以及該資料在組織的使用方式。Amazon Macie 會持續監控異常的資料存取活動，並在偵測到未經授權存取或資料意外洩漏的風險時傳送提醒。

AWS Config 規則 – AWS Config 規則代表資源的偏好組態，它會比對相關資源的組態變更 (在 AWS Config 中記錄) 進行評估。您可在儀表板上查看比對資源組態和規則的評估結果。使用 Config 規則，您可以從組態的角度評估整體合規性及風險狀態、檢視一段時間內的合規趨勢，以及找出哪個組態變更導致資源不符合規則。

AWS Trusted Advisor – AWS Trusted Advisor 是線上資源，可藉由最佳化您的 AWS 環境，協助您降低成本、提高效能，以及提升安全性。Trusted Advisor 提供即時的指導，協助您依循 AWS 最佳實務佈建您的資源。商業和企業支援計劃客戶可獲得完整的 Trusted Advisor 檢查，包含 CloudWatch Events 整合。

Amazon CloudWatch – Amazon CloudWatch 是一項針對 AWS 雲端資源和在 AWS 上執行的應用程式進行監控的服務。您可以使用 Amazon CloudWatch 收集和追蹤指標、收集和監控日誌檔、設定警示，以及自動對 AWS 資源的變更做出反應。Amazon CloudWatch 可以監控各種 AWS 資源，例如 Amazon EC2 執行個體、Amazon DynamoDB 表、Amazon RDS 資料庫執行個體，也可以監控應用程式和服務產生的自訂指標以及應用程式產生的所有日誌檔。您可以使用 Amazon CloudWatch 來全面了解系統的資源使用率、應用程式效能和運作狀態。您可以使用這些洞察據以做出反應，保持應用程式順暢運作。

AWS Inspector – Amazon Inspector 是一項自動化的安全性評估服務，可協助改善在 AWS 上部署之應用程式的安全及合規。Amazon Inspector 會自動評定應用程式的漏洞或偏離最佳實務的程度。在執行評估之後，Amazon Inspector 會產生一份詳細的安全問題清單，而內容是根據嚴重性依序排列。您可以直接檢視這些問題清單，或透過 Amazon Inspector 主控台或 API 在詳細的評估報告中檢視。

Amazon Detective – Amazon Detective 可自動從您的 AWS 資源中收集日誌資料，並使用機器學習、統計分析和圖論來建置關聯的資料集，讓您能夠輕鬆地進行更快、更有效的安全調查。Amazon

Detective 可分析來自多個資料來源 (例如 Virtual Private Cloud (VPC) Flow Logs、AWS CloudTrail 和 Amazon GuardDuty) 的數萬億個事件，並自動建立資源、使用者，以及他們在一段時間進行互動的統一互動式檢視。透過這種統一的檢視，您可在一處視覺化呈現所有詳細資訊和內容，以識別問題清單的根本原因，向下鑽研相關的歷史活動，並快速確定根本原因。

自動化

AWS Lambda – AWS Lambda 是一種無伺服器運算服務，可執行程式碼以回應事件，並自動為您管理基礎運算資源。您可以搭配自訂邏輯，使用 Lambda 延伸其他 AWS 服務，或建立自己的後端服務，在 AWS 規模、效能及安全性中運作。Lambda 在高可用性的運算基礎設施上執行您的程式碼，並為您執行運算資源的所有管理工作。這包括伺服器和作業系統維護、容量佈建和自動擴展、程式碼和安全修補程式部署，以及程式碼監控和日誌記錄。您需要做的就是提供程式碼。

AWS Step Functions – AWS Step Functions 可讓您使用視覺化工作流程，來協調分散式應用程式和微服務的元件。Step Functions 提供圖形化的主控台，可排列應用程式的元件，並將這些元件以視覺化的方式呈現為一連串的步驟，這讓建置和執行多步驟應用程式的工作變得簡單。Step Functions 會自動觸發和追蹤每個步驟，並在發生錯誤時重試，讓您的應用程式能如預期依序執行。

Step Functions 會記錄每個步驟的狀態，一旦有哪個環節出了差錯，您就能迅速診斷並偵錯問題。不需編寫程式碼即可變更和新增步驟，因此您可以輕鬆改進應用程式並且更快創新。AWS Step Functions 是 AWS 無伺服器平台的一部分，可以輕鬆為無伺服器應用程式協調 AWS Lambda 函數。您還可以將 Step Functions 用於使用運算資源 (如 Amazon EC2 和 Amazon ECS) 的微型服務協同運作。

AWS Systems Manager – AWS Systems Manager 能讓您查看及控制 AWS 的基礎設施。Systems Manager 提供統一的使用者界面，讓您可以檢視來自多項 AWS 服務的操作資料，並可讓您自動化跨 AWS 資源的操作任務。藉助 Systems Manager，您可以按應用程式對資源進行分組，檢視營運資料以進行監控和疑難排解，並對資源群組採取動作。Systems Manager 可以將執行個體保持在其定義的狀態，執行隨需執行個體變更，例如更新應用程式或執行 shell 指令碼，以及執行其他自動化和修補任務。

安全的儲存

Amazon S3 – Amazon S3 是專為從任何位置存放和擷取任何資料量所建置的物件儲存。它的設計是為了提供 99.999999999% 的耐久性，並可為每個產業市場領導者所用的數百萬個應用程式存放資料。Amazon S3 提供全面的安全性，旨在滿足您的法規要求。它提供客戶靈活性，使其可針對成本最佳化、存取控制和合規管理資料。Amazon S3 提供就地查詢功能，允許您直接在 Amazon S3 的靜態資料上執行強大的分析功能。Amazon S3 是目前最受支援的雲端儲存服務，可與最大的第三方解決方案社群、系統整合商合作夥伴和其他 AWS 服務整合在一起。

Amazon S3 Glacier – Amazon S3 Glacier 是成本極低的雲端儲存服務，為資料封存和長期備份提供安全且耐用的儲存。它的設計可提供 99.999999999% 的耐用性，提供全面的安全性，旨在滿足您的法規要求。Amazon S3 Glacier 提供就地查詢功能，允許您直接在靜態封存資料上執行強大的分析功能。為了保持低成本兼適用於各種擷取需求，Amazon S3 Glacier 提供三個存取封存的選項，擷取時間從數分鐘到數小時。

自訂

以上並未詳列所有服務和功能，AWS 仍在持續增加新功能。如需詳細資訊，建議您查看 AWS 的最新消息和 AWS 雲端安全頁面。除了 AWS 提供作為原生雲端服務的安全服務之外，您可能也有興趣在 AWS 服務之上自行建置功能。

我們建議在帳戶中啟用一組基本的安全服務，例如 AWS CloudTrail、Amazon GuardDuty 和 Amazon Macie，不過最終您可能會想擴充這些功能，好從日誌資產中獲取更多價值。有許多可用的合作夥伴工具，例如 APN 安全能力計劃中列出的項目。您也可以自行編寫查詢來搜尋日誌。憑藉 AWS 提供的大量受管服務，這一點再簡單不過了。還有許多額外的 AWS 服務可協助您進行本白皮書範圍之外的調查，例如 Amazon Athena、Amazon OpenSearch Service、Amazon QuickSight、Amazon Machine Learning 和 Amazon EMR。

附錄 B：範本程式碼

範例 AWS CloudTrail 事件

以下範例顯示名為 `Alice` 的 IAM 使用者，使用 AWS CLI 透過 `ec2-stop-instances` 呼叫 Amazon EC2 `StopInstancesaction`。

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

AWS CloudWatch Events 範例

以下 Amazon CloudWatch Events 範例顯示名為 `jane-roe-test` 的 AWS IAM 使用者，被發現在 `www.github.com` 上公開曝光，並且可能被未經授權的使用者濫用。

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

基礎設施網域 CLI 活動範例

以下 AWS CLI 命令展示了回應基礎設施域內事件的範例。本範例使用 AWS API 來執行本文中介紹的許多初始事件回應活動。

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
```

```
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

附錄 C：範例執行手冊

以下範例執行手冊代表大型執行手冊的單一項目。本執行手冊不是官方的，僅供範例參考。 製作執行手冊時，每個場景都有可能演變成更大的項目，這些項目具有不同的起點和危害指標，但都有相似的結果或需要採取的動作。意識到這種變化還可能開啟其他情況，進而做出更好或更有洞察力的反應。

事件回應執行手冊 – 根用途

目標

本執行手冊的目標是提供如何管理根 AWS 帳戶使用情況的具體指導。本執行手冊不能替代深入的事件回應策略。本執行手冊重點介紹 IR 生命週期：

- 建立控制。
- 判斷影響。
- 根據需要加以復原。
- 調查根本原因。
- 改善。

下面列出危害指標 (IOC)、初始步驟 (停止危害) 以及執行這些步驟所需的詳細 CLI 命令。

前提

- 已設定並安裝 CLI。
- 報告程序已就緒。
- Trusted Advisor 處於作用中狀態。
- Security Hub 處於作用中狀態。

危害指標

- 帳戶有異常活動。
  - 建立 IAM 使用者。
  - CloudTrail 關閉。
  - Cloudwatch 關閉。

  - SNS 暫停。
  - Step Functions 暫停。
- 啟動新的 AMI 或意外的 AMI。
- 變更帳戶上的聯絡人。

修復步驟 – 建立控制

針對可能遭到入侵帳戶的 AWS 文件列出以下的特定任務。可能遭到入侵帳戶的相關文件可以在以下網址找到：如果我發現自己的 AWS 帳戶中有未經授權的活動，我該怎麼辦？

1. 盡快聯絡 AWS 支援 和 TAM。
2. 變更和輪換根密碼，並新增與根關聯的 MFA 裝置。
3. 輪換密碼、存取/私有金鑰以及修復步驟相關的 CLI 命令。
4. 檢閱根使用者採取的動作。
5. 開啟這些動作的執行手冊。
6. 關閉事件。
7. 檢閱事件並了解發生了什麼事。
8. 修正根本問題、實施改進，並根據需要更新執行手冊。

進一步動作項目 – 判斷影響

檢閱建立的項目和變動呼叫。可能有些項目已經建立，以允許未來存取。需要查看的一些項目為：

- IAM 跨帳戶角色。
- IAM 使用者。
- S3 儲存貯體。
- EC2 執行個體。
- [由您的應用程式和基礎設施推動此清單。]

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。

© 2020 Amazon Web Services, Inc. 或其關係企業。保留所有權利。