



在上建置可擴展的漏洞管理計劃 AWS

AWS 規範指南



AWS 規範指南: 在上建置可擴展的漏洞管理計劃 AWS

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

簡介	1
目標對象	2
目標	2
準備	3
定義計劃	3
分配所有權	4
制定披露計劃	5
準備您的環境	5
AWS 帳戶 結構	6
標籤	6
監控佈告欄	7
設定安全服務	7
Amazon Inspector	7
AWS Security Hub	8
準備指派發現項目	10
使用現有工具	11
使用 Security Hub	12
分類及補救	13
指派發現項	13
評估結果並排定優先	14
補救搜尋結果	15
範例	16
安全團隊範例	16
雲端團隊範例	17
應用團隊示例	18
報告和改善	20
安全性作業會議	20
Security Hub 洞察	20
結論和後續步驟	21
資源	23
AWS 服務文件	23
其他 AWS 資源	23
文件歷史紀錄	24
詞彙表	25

#	25
A	25
B	28
C	29
D	32
E	35
F	37
G	38
H	38
I	39
L	41
M	42
O	46
P	48
Q	50
R	50
S	53
T	55
U	57
V	57
W	57
Z	58
.....	lix

建置可擴充的弱點管理程式 AWS

安娜 McAbee 和梅根·奧尼爾，Amazon Web Services () AWS

2023 年十月 ([文件歷史記錄](#))

根據您使用的基礎技術，各種工具和掃描可以在雲端環境中產生安全性發現結果。如果沒有處理這些發現的流程，它們就可以開始累積，通常會在短時間內導致數千到數萬個發現結果。不過，透過結構化的弱點管理方案，以及適當的工具運作，您的組織可以處理並分類來自不同來源的大量發現項目。

弱點管理著重於探索、排定優先順序、評估、補救和報告弱點。另一方面，修補程式管理著重於修補或更新軟體，以移除或修復安全性弱點。修補程式管理只是弱點管理的其中一個層面。一般而言，我們建議同時建立一個patch-in-place 程序 (也稱為mitigate-in-place程序) 來解決重要的、立即修補的案例，以及定期執行的標準程序，以便發行修補的 Amazon Machine Image (AMI)、容器或軟體套件。這些程序可協助您的組織做好快速回應零時差弱點的準備。對於生產環境中的關鍵系統而言，使用 patch-in-place 流程可以比在整個叢集中推出新的 AMI 更快、更可靠。對於定期排程的修補程式，例如作業系統 (OS) 和軟體修補程式，我們建議您使用標準開發程序進行建置和測試，就像進行任何軟體層級變更一樣。這為標準操作模式提供了更好的穩定性。您可以使用[修補程式管理員](#)、功能或其他協力廠商產品做為 patch-in-place 解決方案。AWS Systems Manager如需使用修補程式[管理員的詳細資訊](#)，請參閱[AWS 雲端採用架構：作業觀點中的修補程式管理](#) 此外，您可以使用 [EC2 Image Builder](#) 自動化自訂和 up-to-date 伺服器映像的建立、管理和部署。

建置可擴充的弱點管理程式，除了雲端設定風險外，還 AWS 包括管理傳統軟體和網路弱點。雲端組態風險 (例如未加密的 [Amazon Simple Storage Service \(Amazon S3\)](#) 儲存貯體，應遵循與軟體弱點類似的分類和修復程序。在這兩種情況下，應用程序團隊必須擁有其應用程序的安全性，包括基礎結構，並負責。這種擁有權分配是有效且可擴充的弱點管理計畫的關鍵。

本指南討論如何簡化弱點的識別和修復，以降低整體風險。您可以使用下列各節來建置弱點管理程式並反覆運算：

1. [準備](#) — 準備好您的人員、流程和技術，以識別、評估和修復環境中的弱點。
2. [分類和補救](#) — 將安全發現結果傳遞給相關利益相關者，識別適當的補救措施，然後採取補救措施。
3. [報告並改善](#) — 使用報告機制找出改進的機會，然後重複執行弱點管理程式。

建立雲端弱點管理程式通常需要反覆運算。排定本指南中的建議優先順序，並定期重新審視您的待處理項目，以隨時掌握技術變更和您的業務需求。

目標對象

本指南適用於擁有三個主要團隊負責安全性相關調查結果的大型企業：安全團隊、Cloud Center of Excellence (CCoE) 或雲端團隊，以及應用程式 (或開發人員) 團隊。本指南使用最常見的企業營運模式，並以這些作業模式為基礎，以便更有效率地回應安全發現結果並改善安全性結果。使用的 Organizations 可 AWS 能具有不同的結構和不同的操作模式；但是，您可以修改本指南中的許多概念，以適應不同的營運模式和較小的組織。

目標

本指南可以幫助您和您的組織：

- 制定政策以簡化弱點管理並確保責任
- 建立機制，將安全責任分配給應用團隊
- AWS 服務 根據可擴充弱點管理的最佳實務進行相關設定
- 分配安全發現項目的擁有
- 建立機制以報告和重複執行您的弱點管理程式
- 改善安全性尋找可見度並改善整體安全狀態

準備您的可擴充弱點管理方案

準備建置可擴充的弱點管理計畫，包括教育人員、開發程序，以及根據最佳實務實作適當的技術。對於有效的弱點管理程式而言，人員、程序和技术同樣重要，您必須將它們緊密整合，以大規模管理弱點。

本指南的這一部分將檢閱您可以採取的基本動作，以準備可擴充的弱點管理方案。AWS

主題

- [定義弱點管理計劃](#)
- [分配安全所有權](#)
- [制定漏洞披露計劃](#)
- [準備您的 AWS 環境](#)
- [監控 AWS 安全性佈告欄](#)
- [設定 AWS 安全服務](#)
- [準備指派安全發現項目](#)

定義弱點管理計劃

準備雲端弱點管理程式的第一步是定義弱點管理計劃。此計劃包括貴組織遵循的政策與流程。所有利益相關者都應記錄並訪問該計劃。弱點管理方案是一份高階文件，通常包含下列各節：

- 目標與範圍 — 概述弱點管理的目標、功能和範圍。
- 角色和職責 — 列出弱點管理利害關係人，並詳細說明他們的責任。
- 弱點嚴重性和優先順序定義 — 決定如何將弱點的嚴重性分類，以及如何排定優先順序。
- 修正的服務等級協定 (SLA) — 針對每個嚴重性層級，定義補救擁有者必須解決安全性發現的最長時間。由於 SLA 合規性是擁有有效且可擴充的弱點管理計畫不可或缺的一部分，因此請考慮如何追蹤您是否符合這些 SLA。
- 例外處理 — 詳細說明提交、核准及更新例外的處理。此過程應確保異常是合法的，有時間限制和跟蹤的。
- 弱點資訊的來源 — 列出產生安全發現項目的來源或工具。如需可能 AWS 服務 是安全性發現項目來源的詳細資訊，請參閱本指南[設定 AWS 安全服務](#)中的。

雖然這些章節在不同規模和產業的公司中都很常見，但每個組織的弱點管理計畫都是獨一無二的。您必須建立最適合您組織的弱點管理計畫。期望隨著時間的推移迭代您的計畫，以納入學到的經驗教訓和不斷發展

分配安全所有權

[AWS 共同的責任模型](#)定義了如何 AWS 及其客戶分擔雲端安全性和合規性的責任。在此模型中，AWS 保護執行中提供之所有服務的基礎結構 AWS 雲端，而且 AWS 客戶必須負責保護其資料和應用程式的安全。

您可以在組織內鏡像此模型，並在雲端和應用程式團隊之間分配責任。這可協助您更有效地擴充雲端安全性方案，因為應用程式團隊會取得其應用程式特定安全層面的所有權。共用責任模型最簡單的解釋是，如果您有權限設定資源，則您必須負責該資源的安全性。

將安全性責任分配給應用程式團隊的關鍵部分是建置自助式安全工具，以協助您的應用程式團隊自動化最初，這可以是共同努力。安全團隊可以將安全性需求轉換為程式碼掃描工具，然後應用程式團隊可以使用這些工具來建置解決方案，並與其內部開發人員社群共用解決方案。這有助於提高其他需要滿足類似安全性需求的團隊的效率。

下表概述將擁有權分配給應用程式團隊的步驟，並提供範例。

步驟	動作	範例
1	定義您的安全性需求 — 您想要達成什麼目的？這可能來自安全標準或合規性要求。	安全性需求範例為應用程式識別的最低權限存取權。
2	列舉安全性需求的控制項 — 從控制角度來看，這項要求實際上意味著什麼？我需要做些什麼來實現這一目標？	若要達到應用程式身分識別的最低權限，下列是兩個範例控制項： <ul style="list-style-type: none">• 使用 AWS Identity and Access Management (IAM) 角色• 請勿在 IAM 政策中使用萬用字元
3	控制項的文件指引 — 透過這些控制項，您可以提供哪些指引	一開始，您可以先記錄簡單的範例政策，包括安全和不安全

步驟	動作	範例
	給開發人員，以協助他們遵守控制項？	的 IAM 政策和 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策。接下來，您可以在持續整合和持續交付 (CI/CD) 管道中內嵌政策掃描解決方案，例如使用 AWS Config 規則 進行主動評估。
4	開發可重複使用的成品 — 借助指導，您能否使其更加容易並為開發人員開發可重複使用的成品？	您可以建立基礎結構即程式碼 (IaC)，以部署遵循最低權限原則的 IAM 政策。您可以將這些可重複使用的成品儲存在程式碼儲存庫

自助服務可能不適用於所有安全性需求，但它可以用於標準案例。透過遵循這些步驟，組織可讓其應用程式團隊以可擴充的方式處理更多自己的安全責任。整體而言，分散式責任模型可在許多組織中實現更多協同合作的安全性實務

制定漏洞披露計劃

如需弱點管理 [defense-in-depth](#) 方法，請建立弱點洩漏程式，讓組織內部或外部的人員報告安全性弱點或風險。

對於組織內部的人員，請建立提交風險或弱點的程式。這可以通過售票系統或電子郵件來完成。無論您選擇哪種流程，您的員工都必須了解流程，並且可以輕鬆提交他們遇到的任何漏洞或風險。

對於組織外部人員，請建立外部網頁以提交潛在安全漏洞。舉例來說，請參閱 [AWS 弱點報告](#) 網頁。本網頁還應包含披露指南，以幫助保護您組織的數據和資產。漏洞洩露計劃不應鼓勵潛在的有害活動，因此您必須制定明確的政策和指導方針。建立一個成熟、負責任的揭露計畫是一個目標，在您的計畫成熟時努力。大多數人不是從外部披露程序開始，並且需要時間才能正確使用。

準備您的 AWS 環境

在實作任何弱點管理工具之前，請確定您的 AWS 環境已架構為支援可擴充的弱點管理程式。您 AWS 帳戶與組織的標記政策結構可以簡化建置可擴充弱點管理計畫的程序。

開發結 AWS 帳戶 構

[AWS Organizations](#) 協助您集中管理和控管 AWS 環境，隨著您的業務成長並擴充其 AWS 資源。中的組織會 AWS 帳戶 將您 AWS Organizations 合併為邏輯群組或組織單位，以便您可以將它們作為單一單位進行管理。您可以透過稱為管 AWS Organizations 理帳戶的專屬帳戶進行管理。如需詳細資訊，請參閱 [AWS Organizations 術語與概念](#)。

建議您在 AWS Organizations 中管理 AWS 多帳戶環境。這有助於建立公司帳戶和資源的完整清查。這項完整的資產清查是弱點管理的重要環節。應用程式團隊不應使用組織外部的帳戶。

[AWS Control Tower](#) 協助您設定和管理 AWS 多帳戶環境，遵循規範的最佳做法。如果您尚未建立多帳戶環境，AWS Control Tower 這是一個很好的起點。

我們建議您使用 [AWS 安全參考架構 \(AWS SRA\)](#) 中所述的 [專屬帳戶結構](#) 和最佳作法。[安全工具帳戶](#) 應該擔任您安全性服務的委派管理員。本指南稍後將提供有關在此帳戶中設定弱點管理工具的詳細資訊。在 [工作負載組織單位 \(OU\)](#) 的專用帳戶中託管應用程式。這會為每個應用程式建立強大的工作負載層級隔離和明確的安全性界限 如需有關使用多帳戶方法的設計原則和優點的資訊，請參閱 [使用多個帳戶組織 AWS 環境](#) (AWS 白皮書)。

具備蓄意的帳戶結構，並從專屬帳戶集中管理安全服務，是可擴充的弱點管理計畫的關鍵層面。

定義、實作及強制執行標籤

標籤是索引鍵值配對，可做為組織 AWS 資源的中繼資料。如需詳細資訊，請參閱 [標記您的 AWS 資源](#)。您可以使用標籤來提供業務內容，例如業務單位、應用程式擁有者、環境和成本中心。下表顯示了一組範例標籤。

金鑰	值
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
環境	生產

標籤可協助您排定發現項目的優先 例如，它可以幫助您：

- 識別負責修補弱點的資源擁有者

- 追蹤哪些應用程式或業務單位有大量發現項目
- 提升特定資料分類的發現項目嚴重性，例如個人識別資訊 (PII) 或支付卡產業 (PCI) 資料
- 識別環境中的資料類型，例如較低層級開發環境中的測試資料或生產資料

若要協助您達成有效的大規模標記，請遵循[標記 AWS 資源的最佳做法 \(AWS 白皮書\)](#) 中建立標記策略中的指示。

監控 AWS 安全性佈告欄

我們強烈建議您定期且頻繁地監控[AWS 安全性佈告欄](#)。安全性佈告欄可以通知您任何新的安全性相關弱點、受影響的服務和適用的更新。您也可以訂閱安全性公告的 [RSS 摘要](#)，並建立程序以擷取和處理這些公告，做為弱點管理計畫的一部分。

設定 AWS 安全服務

AWS 提供各種安全服務，旨在協助保護您的 AWS 環境。針對弱點管理方案，建議您 AWS 服務在每個帳戶中啟用下列項目：

- [Amazon GuardDuty](#) 可協助您偵測環境中的主動威脅。發 GuardDuty 現項目可協助您識別在您的環境中遭到惡意利用的未知弱點。它還可以幫助您了解未修補漏洞的影響。
- [AWS Health](#) 讓您持續掌握資源效能以及您 AWS 服務和帳戶的可用性。
- [AWS Identity and Access Management Access Analyzer](#) 分析 AWS 環境中以資源為基礎的政策，以識別與外部實體共用的資源。這可協助您識別與非預期存取資源和資料相關的弱點。針對帳戶外部共用資源的每一個執行個體，IAM Access Analyzer 都會產生一份問題清單。
- [Amazon Inspector](#) 是一種弱點管理服務，可持續掃描您的 AWS 工作負載，找出軟體弱點和意外的網路暴露。
- [AWS Security Hub](#) 協助您根據安全性產業標準檢查 AWS 環境，並識別雲端組態風險。它也彙總來自其他安全性服務和協力廠商 AWS 安全性工具的發現項目，以提供 AWS 安全狀態的全面檢視。

本節討論如何啟用和設定 Amazon Inspector 和 Security Hub，以協助您建立可擴展的弱點管理計畫。

在漏洞管理計劃中使用 Amazon Inspector

[Amazon Inspector](#) 是一項弱點管理服務，可持續掃描您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、亞馬遜彈性容器登錄 (Amazon ECR) 容器映像，以及軟體弱點和意外網路暴露的

AWS Lambda 功能。您可以使用 Amazon Inspector 來獲得整個 AWS 環境中軟體弱點的能見度並排定優先順序。

Amazon Inspector 會在資源的整個生命週期中持續評估您的環境。它會自動重新掃描資源，以回應可能引入新弱點的變更。例如，當您在 EC2 執行個體上安裝新套件、安裝修補程式，或發佈影響資源的新常見弱點和曝光 (CVE) 時，它會重新掃描。當 Amazon Inspector 識別出漏洞或開放網路路徑時，就會產生可供您調查的發現。此發現項目提供有關此弱點的完整資訊，包括下列項目：

- [Amazon Inspector 風險評分](#)
- [常見漏洞評分系統 \(CVSS\) 評分](#)
- 受影響資源
- 來自 Amazon 的 CVE 漏洞情報數據 [Recorded Future](#)，以及 [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
- 補救建議

[有關設置 Amazon Inspector 查器的說明](#)，請參閱 [Amazon Inspector 查器入門](#)。本教學中的啟用 Amazon Inspector 步驟提供兩個組態選項：獨立帳戶環境和多帳戶環境。如果您想要監視中 AWS Organizations 某個 AWS 帳戶 組織成員的多個帳戶，建議您使用多帳戶環境選項。

當您為多帳戶環境設定 Amazon Inspector 時，您可以將組織中的帳戶指定為 Amazon Inspector 委派的管理員。委派的管理員可以管理組織成員的發現項目和某些設定。例如，委派管理員可以檢視所有成員帳戶的彙總發現項目詳細資料、啟用或停用成員帳號的掃描，以及檢閱掃描的資源。AWS SRA 建議您建立 [安全工具帳戶](#)，並將其用作 Amazon Inspector 委派的管理員。

AWS Security Hub 在弱點管理程式中使用

建置可擴充的弱點管理程式，除了雲端設定風險外，還 AWS 包括管理傳統軟體和網路弱點。[AWS Security Hub](#) 協助您根據安全性產業標準檢查 AWS 環境，並識別雲端組態風險。Security Hub 也會彙總來自其他安全性服務和協力廠商安全性工具的安全性發現項目，以提供您 AWS 安全狀態的全面檢視。AWS

在下列各節中，我們提供設定 Security Hub 以支援弱點管理程式的最佳做法和建議：

- [設定 Security Hub](#)
- [啟用 Security Hub 標準](#)
- [管理 Security Hub 發現項](#)
- [彙總其他安全服務和工具的發現項目](#)

設定 Security Hub

如需設定指示，請參閱[設定 AWS Security Hub](#)。若要使用 Security Hub，您必須啟用[AWS Config](#)。如需詳細資訊，請參閱安全中心說明文件 AWS Config 中的[啟用和設定](#)。

如果您已與 AWS Organizations 組織管理帳戶整合，您可以將帳戶指定為 Security Hub 委派的系統管理員。如需指示，請參閱[指定 Security Hub 委派的系統管理員](#)。AWS SRA 建議您建立[資訊安全工具帳戶](#)，並將其用作 Security Hub 委派的系統管理員。

委派的系統管理員會自動擁有為組織中所有成員帳戶設定 Security Hub 的存取權，以及檢視與這些帳戶相關聯的發現項目。我們建議您啟用 AWS Config 安全中心在所有 AWS 區域 和所有 AWS 帳戶。您可以將 Security Hub 設定為自動將新的組織帳戶視為 Security Hub 成員帳戶。如需指示，請參閱[管理屬於組織的成員帳戶](#)。

啟用 Security Hub 標準

Security Hub 會針對安全性控制執行自動且持續的安全性檢查，產生發現項目 控制項與一或多個安全性標準相關聯。這些控制項可協助您判斷是否符合標準中的需求。

當您在安全中心啟用標準時，Security Hub 會自動啟用適用於標準的控制項。Security Hub 使用 AWS Config [規則](#)來執行控制項的大部分安全性檢查。您可以隨時啟用或停用 Security Hub 標準。如需詳細資訊，請參閱[中的安全性控制項和標準 AWS Security Hub](#)。如需完整的標準清單，請參閱 [Security Hub 標準參考資料](#)。

如果您的組織還沒有偏好的安全性標準，建議您使用[AWS 基礎安全性最佳作法 \(FSBP\)](#) 標準。此標準旨在偵測何時 AWS 帳戶 及資源偏離安全性最佳實務。AWS 策劃此標準並定期更新，以涵蓋新功能和服務。對 FSBP 發現項目進行分類後，請考慮啟用其他標準。

管理 Security Hub 發現項

Security Hub 提供數項功能，可協助您解決整個組織的大量發現項目，並瞭解 AWS 環境的安全性狀態。為了協助您管理發現項目，我們建議您啟用下列兩個 Security Hub 功能：

- 使用[跨區域彙總來彙總](#)發現項目、尋找更新、見解、控制合規狀態，以及從多個彙總區域 AWS 區域到單一彙總區域的安全分數。
- 使用[整合的控制項發現項目](#)，藉由移除重複的發現項目來減少 在帳戶中開啟合併控制項發現項目時，Security Hub 會針對控制項的每個安全性檢查產生單一新的發現項目或尋找更新，即使控制項套用至多個已啟用的標準也是如此。

彙總其他安全服務和工具的發現項目

除了產生安全性發現項目之外，您還可以使用 Security Hub 彙總來自多個 AWS 服務 支援協力廠商 安全性解決方案的尋找資料。本節著重於將安全性發現項目傳送至 Security Hub。下一節討論如何將 Security Hub 與可從 Security Hub 接收發現項目的產品整合。[準備指派安全發現項目](#)

您可以將許多 AWS 服務協力廠商產品和開放原始碼解決方案與 Security Hub 整合。如果您剛開始使用，我們建議您執行以下操作：

1. 啟用 AWS 服務 整合 AWS 服務 — 在您同時啟用 Security Hub 和整合式服務之後，大多數將發現項目傳送至 Security Hub 的整合都會自動啟動。對於弱點管理計劃，我們建議您在每個帳戶中啟用 Amazon Inspector GuardDuty AWS Health、Amazon 和 IAM 存取分析器。這些服務會自動將其發現項目傳送至 Security Hub。如需支援 AWS 服務 整合的完整清單，請參閱將[AWS 服務 發現項目 傳送至 Security Hub](#)。

Note

AWS Health 如果符合下列其中一個條件，就會將發現項目傳送至安全性中樞：

- 發現項目與 AWS 安全服務相關聯
- 尋找項目類型碼包含文字 securityabuse、或 certificate
- 尋找 AWS Health 服務是 risk 或 abuse

2. 設定第三方整合 — 如需目前支援的整合清單，請參閱[可用的第三方合作夥伴產品整合](#)。選取任何可傳送發現項目至 Security Hub 或從 Security Hub 接收發現項目的其他工具。您可能已經擁有其中一些第三方工具。依照產品指示設定與 Security Hub 的整合。

準備指派安全發現項目

在本節中，您會設定團隊用來管理和指派安全性發現項目的工具。本節包括下列選項：

- [管理現有工具和工作流程中的發現](#)— 此選項 AWS Security Hub 與團隊用於管理日常任務的現有系統集成，例如產品積壓。對於已建立工具來管理其工作流程的團隊，建議使用此選項。
- [管理安全中心的發現項目](#)— 此選項會設定 Security Hub 事件的通知，以便適當的小組接收警示，並可處理 Security Hub 中的發現項目。

決定哪個工作流程最適合您的團隊，並確保安全發現項目能夠迅速向其各自的所有者提供。

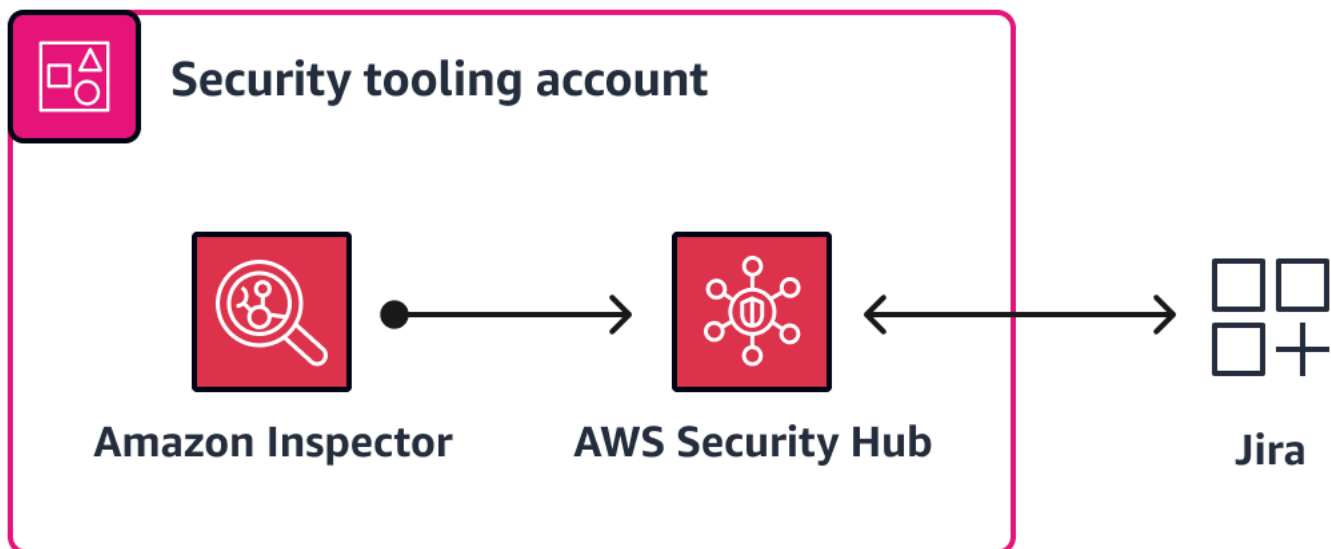
管理現有工具和工作流程中的發現

我們建議您為企業組織提供額外的 Security Hub 整合，這些組織已建立團隊用來管理或執行日常工作的工具。您可以將 Security Hub 尋找資料匯入數個技術平台。範例包括：

- [安全性資訊與事件管理 \(SIEM\) 系統](#) 可協助保安團隊分類營運安全事件。SIEM 系統提供應用程式和網路硬體產生的安全警示的即時分析。
- [治理、風險與法規遵循 \(GRC\) 系統](#) 可協助法規遵循與治理團隊監控與報告風險管理資料。GRC 工具是企業可用來管理政策、評估風險、控制使用者存取權限，以及簡化法規遵循的軟體應用程式。您可以使用 GRC 工具來整合業務流程、降低成本並提高效率。
- 產品積壓和票務系統可協助應用程式和雲端團隊管理功能並排定開發工作的優先順序 [Atlassian Jira](#) 並且 [Microsoft Azure DevOps](#) 是這些系統的例子。

將 Security Hub 發現項目直接與這些現有的企業系統整合，可以改善平均復原時間 (MTTR) 和安全性結果，因為日常作業工作流程不需要變更。團隊無需使用不同的工作流程和工具，因此可以更快地回應和從安全發現項目中學習。整合使得尋址安全發現項目成為正常標準工作流程的一部分。

Security Hub 與多個第三方合作夥伴產品整合。如需完整清單和指示，請參閱 Security Hub 文件中的 [可用協力廠商合作夥伴產品整合](#)。常見的整合包括 [Atlassian - Jira Service Management](#) [AWS Security Hub 與 Jira 軟體雙向整合](#)，以及 [ServiceNow - ITSM](#) 下圖顯示如何將 Amazon Inspector 設定為將發現項目傳送到 Security Hub，然後設定 Security Hub 以將所有發現項目傳送至 Jira。



管理安全中心的發現項目

您可以使用 [Amazon EventBridge 規則](#) 和 [Amazon 簡單通知服務 \(Amazon SNS\) 主題](#)，為 Security Hub 發現項目建立雲端通知系統。此系統會在建立發現項目時通知適當的專案團隊。對於這種方法，中 [開發結 AWS 帳戶 構](#) 描述的多帳戶策略至關重要，因為應用程式被分成專用帳戶。這可協助您針對每個發現項目通知正確的團隊。

安全或雲端團隊可能會選擇接收來自所有人的事件 AWS 帳戶。在此情況下，請在 Security Hub 委派管理員帳戶內建立 EventBridge 規則，然後訂閱通知這些團隊的 Amazon SNS 主題。對於應用程式團隊，請在各自的應用程式帳戶中設定 EventBridge 規則和 SNS 主題。當應用程式帳戶內發生 Security Hub 發現項目時，負責的小組就會收到有關發現項目的通知。

Security Hub 已自動將所有新發現項目和所有更新傳送至現有發現項目，以 EventBridge 做為 Security Hub 發現項目-匯入的事件。每個 Security Hub 發現項目-匯入的事件都包含一個發現項目 您可以對 EventBridge 規則套用篩選器，讓尋找項目僅在發現項目符合篩選器時啟動規則。如需指示，請參閱 [設定自動傳送發現項目的 EventBridge 規則](#)。如需有關建立和訂閱 Amazon SNS 主題的詳細資訊，請參閱 [設定 Amazon SNS](#)。

使用此方法時，請考慮下列事項：

- 對於應用程式團隊，請在每個 AWS 帳戶 應用程式託管位 AWS 區域 置建立 EventBridge 規則。
- 對於安全性和雲端團隊，請在 Security Hub 委派的系統管理員帳戶中建立 EventBridge 規則。這會通知團隊有關成員帳戶中的所有發現。
- 如果安全發現的狀態為，Amazon SNS 會每天傳送通知NEW。如果您要關閉每日通知，可以建立自訂 AWS Lambda 函數，在 Amazon SNS 訂閱者收到通知NOTIFIED後，將搜尋結果的狀態從NEW變更為。

分類與修正您環境中的安全性發現項目 AWS

將安全性發現項目分類涉及將發現項目路由至適當的利益相關者，評估並排定發現項目的優先順序，然後對其進行修正。本節詳細檢閱上述每個步驟，並提供可擴充性和效率的建議。其中也包含可協助說明分類和補救程序的範例。

主題

- [定義安全發現項目的擁有](#)
- [評估安全發現項目並排定](#)
- [補救安全性發現項目](#)
- [分類與修正安全性發現項目的範例](#)

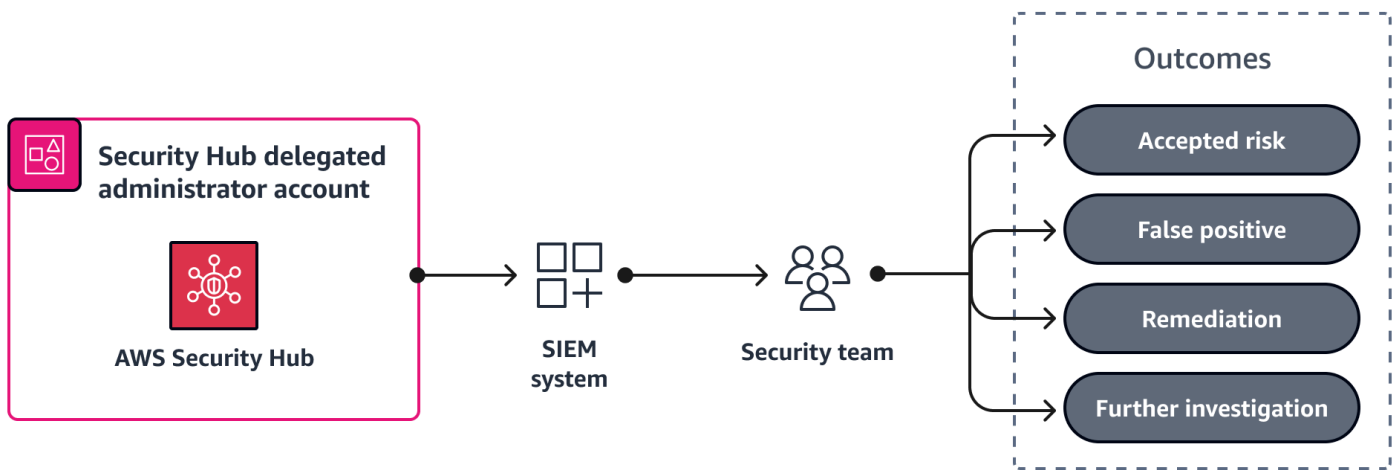
定義安全發現項目的擁有

定義擁有權模型以分類安全發現項目可能具有挑戰性，但並不一定如此。安全格局不斷變化，從業人員必須靈活適應這些變化。採用靈活的方法來開發您的擁有權模型以進行安全性發現。您的初始模型應該使您的團隊能夠立即採取行動。我們建議從基本擁有權邏輯開始，並隨著時間的推移改進該邏輯。如果您延遲定義完美的所有權標準，安全發現的數量將繼續增加。

為了協助將發現項目指派給適當的團隊和資源，我們建議您整合 AWS Security Hub 合團隊用來管理其日常工作的任何現有系統。例如，您可以將 Security Hub 與安全性資訊和事件管理 (SIEM) 系統或產品待處理和票務系統整合。如需詳細資訊，請參閱本指南中的 [準備指派安全發現項目](#)。

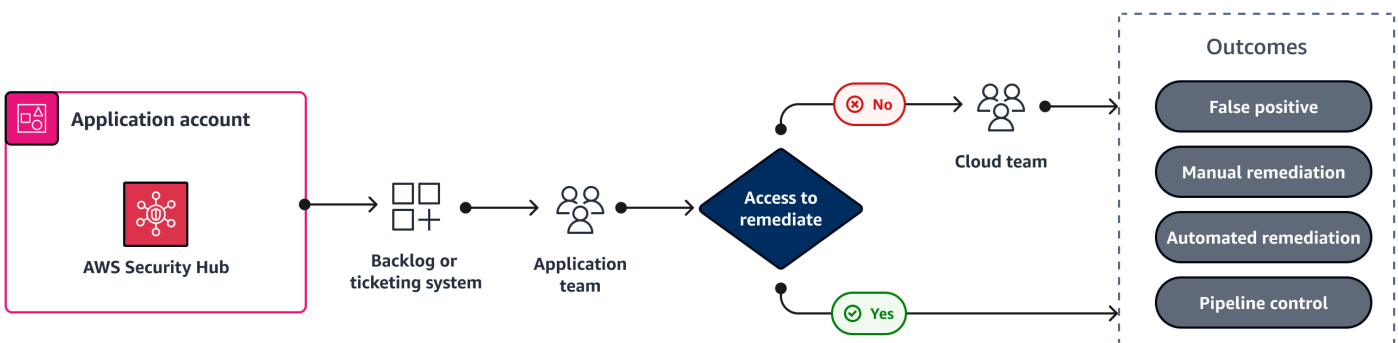
以下是您可以用作起點的股權模型範例：

- 安全性團隊會檢閱潛在的作用中威脅，並協助評估安全發現項目並排定。安全團隊擁有適當評估上下文的專業知識和工具。他們瞭解其他安全性相關資料，協助他們評估弱點並排定優先順序，並調查威脅偵測事件。如果需要尋找嚴重性或其他調整，請參閱本指南中的 [評估安全發現項目並排定](#) 章節。如需範例，請參閱本指南 [安全團隊範例](#) 中的 〈〉。



- 在雲端和應用程式團隊之間散佈安全性發現項目 — 如[分配安全所有權](#)本節所述，有權設定資源的團隊負責其安全配置。應用程式團隊負責與其建置和設定的資源相關的安全性發現項目，而雲端小組則負責處理與廣泛組態相關的安全性發現項目。[在大多數情況下，應用程式團隊無法存取變更廣泛的組態 AWS 服務，例如中的服務控制政策 \(SCP\) AWS Control Tower、與網路相關的 VPC 組態 AWS Organizations，以及 IAM 身分中心。AWS](#)

對於將應用程式分隔到專用帳戶的多帳戶環境中，您通常可以將帳戶的安全性相關發現項目整合到應用程式的待處理或票務系統中。從該系統中，雲端團隊或應用程式團隊可以解決發現問題。如需範例，請參閱本指南[應用團隊示例](#)中的[雲端團隊範例](#)或。



- 將剩餘、未解決的發現項目指派給雲端團隊 — 剩餘發現項目可能與雲端團隊可以解決的預設設定或廣泛的組態有關。該團隊可能擁有最具歷史意義的知識和解決問題的機會。總體而言，這通常是發現項目總數的一個明顯較小的子集。

評估安全發現項目並排定

有效的弱點管理計畫的重要元件之一，就是能夠評估安全性發現項目並排定優先順序。這就是拉入上下文，組織歷史和調整檢測系統的地方。安全性發現的優先順序有助於建立適當的回應等級速度。

對於 Amazon Inspector 和 Amazon AWS Security Hub GuardDuty，發現結果包含嚴重性標籤或分數。我們建議您優先調查 Security Hub 中的所有關鍵和高嚴重性發現項目，包括與基礎安全最佳實務 (FSBP) 標準、Amazon Inspector 和 GuardDuty 尋找嚴重性標籤的分數決定如下：

- [Amazon Inspector 分數](#)是每個發現項目的高度情境化分數。計算方式是將通用弱點評分系統 (CVSS) 基本分數資訊與網路連接性結果和可利用性資料建立關聯。使用此分數，您可以將發現項目的優先順序集中在最重要的發現項目和易受攻擊的資源上。除了分數之外，Amazon Inspector 還提供有關[常見弱點和入侵程式 \(CVE\)](#) 的增強型弱點情報。這是 Amazon CVE 的可用情報摘要，以及業界標準的安全情報來源，例如「記錄的未來」和「網路安全與基礎設施安全機構」(CISA)。例如，Amazon Inspector 可以提供用於惡意利用弱點的已知惡意軟體套件名稱。如需詳細資訊，請參閱[弱點情報](#)。
- 每個 GuardDuty 發現項目都有[指派的嚴重性層級和值](#)，以反映發現項目對您環境的潛在風險。此等級和值由 AWS 安全工程師決定。例如，High 嚴重性等級表示資源已遭到入侵，並且正在主動用於未經授權的目的。我們建議您將 High 嚴重性 GuardDuty 發現視為優先順序，並立即進行補救，以防止進一步未經授權的使用。
- [Security Hub 控制項發現的嚴重性](#)取決於遭到惡意利用的難度和入侵的可能性。難度取決於使用弱點執行威脅案例所需的複雜程度或複雜性。入侵的可能性表示威脅案例會導致您的或資源中斷或破壞的 AWS 服務可能性。

為了調整發現項目，您可以直接在相應的服務主控台中或使用服務的 API 來隱藏或封存特定發現項目。此外，您可以使用[自動化規則](#)對 Security Hub 中的發現項目進行變更。GuardDuty 和 Amazon Inspector 的發現會自動發送到 Security Hub。您可以使用自動化規則，根據您定義的條件，以近乎即時的方式自動更新 (例如變更嚴重性) 或隱藏發現項目。建立自動化規則時，我們建議您將前後關聯新增至規則描述，例如建立或修改日期、建立者，以及需要規則的原因。此資訊通常有助於 future 參考。

補救安全性發現項目

評估發現項目並排定優先順序之後，下一個動作就是修正發現項目。您可以採取許多不同的動作來修正發現項目。對於軟件漏洞，您可以更新操作系統或應用修補程序。對於雲配置的發現，您可以更新資源配置。一般而言，您為修正所採取的動作可分為下列其中一個結果：

- 手動修復 — 您可以手動提供弱點的修正程式，例如修改 AWS 資源的內容以啟用加密。如果發現項目來自 Security Hub 中受管理的檢查，則發現項目會包含手動修正發現項目之指示的連結。
- 可重複使用的成品 — 您更新基礎結構作為代碼 (IaC) 以修復該漏洞，並知道其他人可以從類似的解決方案中受益。考慮將更新的 IaC 和解決方案的簡短摘要上傳到內部共享代碼存儲庫。
- 自動修復 — 會透過您建立的機制自動修復弱點。

- **管道控制** — 您可以在持續整合和持續交付 (CI/CD) 管道中套用控制項，以防止在弱點存在時進行部署。
- **已接受的風險** — 您不採取任何行動或實作補償控制項，且您接受弱點所帶來的風險。在專屬位置追蹤已接受的風險，例如風險登錄。
- **誤報** — 您不採取任何動作，因為您已判斷發現項目未正確識別弱點。

您可以採取的各種動作以及可用來修復弱點的工具的完整清單已超出本指南的範圍。不過，有些服務和工具可協助您大規模修復弱點值得注意，包括：

- **修補程式管理員** 是一項功能 AWS Systems Manager，可以使用安全性相關更新和其他類型的更新來自動修補受管理節點的程序。您可以使用修補程式管理員以套用適用於作業系統和應用程式的修補程式。
- **AWS Firewall Manager** 協助您集中設定及管理所有帳戶和應用程式的防火牆規則 AWS Organizations。建立新的應用程式時，Firewall Manager 可透過強制執行一組通用的安全規則，讓新的應用程式和資源更容易符合規範。
- 「**自動化安全回應**」AWS 是一種 AWS 解決方案，可與 Security Hub 搭配使用，並根據業界合規標準和安全威脅的最佳做法，提供預先定義的回應和補救動作。

分類與修正安全性發現項目的範例

本節提供安全性、雲端和應用程式團隊的分類程序範例。它討論了每個團隊通常解決的發現項目類型，並提供如何回應的範例。此外，還包括高階修復指引。

本節包含下列範例：

- **安全性團隊範例：建立 Security Hub 自動化規則**
- **雲端團隊範例：變更 VPC 組態**
- **應用程式小組範例：建立 AWS Config 規則**

安全性團隊範例：建立 Security Hub 自動化規則

安全團隊會收到與威脅偵測相關的調查結果，包括 Amazon GuardDuty 發現項目。如需依 AWS 資源類型分類之 GuardDuty 尋找類型的完整清單，請參閱 GuardDuty 文件中的 [尋找類型](#)。安全團隊必須熟悉所有這些尋找類型。

在此範例中，安全性團隊接受安全性發現項目的相關風險等級，AWS 帳戶 該發現項目嚴格用於學習目的，且不包含重要或敏感資料。此帳戶的名稱是 sandbox，帳戶 ID 為 123456789012。安全性團隊可以建立 AWS Security Hub 自動化規則，以隱藏此帳戶中的所有 GuardDuty 發現項目。他們可以從涵蓋許多常見使用案例的範本建立規則，也可以建立自訂規則。在 Security Hub 中，我們建議預覽條件的結果，以確認規則傳回預期的發現項目。

Note

此範例會強調顯示自動化規則的功能。我們不建議隱藏帳戶的所有 GuardDuty 發現項目。內容很重要，而且每個組織都必須根據資料類型、分類和緩解控制項，選擇要隱藏的發現項目。

以下是用來建立此自動化規則的參數：

- 規則：
 - 規則名稱為 Suppress findings from Sandbox account
 - 規則描述為 Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account
- 標準：
 - `AwsAccountId = 123456789012`
 - `ProductName = GuardDuty`
 - `WorkflowStatus = NEW`
 - `RecordState = ACTIVE`
- 自動化動作：
 - `Workflow.status` 是 SUPPRESSED

如需詳細資訊，請參閱 Security Hub 文件中的 [自動化規則](#)。安全性團隊有許多選項，可用來調查和補救偵測到的威脅的發現項目。如需詳盡的指引，請參閱 [AWS 保安事故應變指南](#)。我們建議您查看本指南，以確認您已經建立了強大的事件響應流程。

雲端團隊範例：變更 VPC 組態

雲端團隊負責對具有常見趨勢的安全性發現項目進行分類和修復，例如變更可能不適合您的使用案例的 AWS 預設設定。這些發現項目往往會影響許多 AWS 帳戶 或資源，例如 VPC 組態，或包含應在整個環境中設置的限制。在大多數情況下，雲團隊會進行手動的一次性更改，例如添加或更新策略。

在您的組織使用 AWS 環境一段時間之後，您可能發現一組反模式正在開發。反模式是一個經常使用的解決方案，其中解決方案是適得其反的，效果不佳，或不是替代方案有效的重複性問題。作為這些反模式的替代方案，您的組織可以使用更有效的環境限制，例如 AWS Organizations 服務控制政策 (SCP) 或 IAM 身分中心許可集。SCP 和許可集可為資源類型提供其他限制，例如防止使用者設定公用 Amazon Simple Storage Service (Amazon S3) 儲存貯體。雖然限制每個可能的安全性組態可能很誘人，但是 SCP 和權限集有原則大小限制。我們建議採用平衡的預防和偵探控制方法。

以下是雲端團隊可能負責的 AWS Security Hub [基礎安全性最佳做法 \(FSBP\)](#) 標準中的一些控制項：

- [\[EC2.2\] VPC 預設安全性群組不應允許輸入和輸出流量](#)
- [\[EC2.6\] 應在所有 VPC 中啟用虛擬私人雲端流程記錄](#)
- [\[EC2.23\] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求](#)
- [\[CloudTrail.1\] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)
- [\[Config 1\] AWS Config 應該被啟用](#)

在此範例中，雲端團隊正在處理 FSBP 控制 EC2.2 的發現。此控制項的[文件](#)建議不要使用預設安全性群組，因為它允許透過預設的輸入和輸出規則進行廣泛存取。由於無法刪除預設安全性群組，因此建議您變更規則設定以限制輸入和輸出流量。為了有效解決此問題，雲端團隊應該使用已建立的機制來修改所有 VPC 的安全性群組規則，因為每個 VPC 都有此預設安全性群組。在大多數情況下，雲端團隊會使用[AWS Control Tower](#)自訂或基礎結構即程式碼 (IaC) 工具 (例如[HashiCorp Terraform](#)或) 來管理 VPC 組態。[AWS CloudFormation](#)

應用程式小組範例：建立 AWS Config 規則

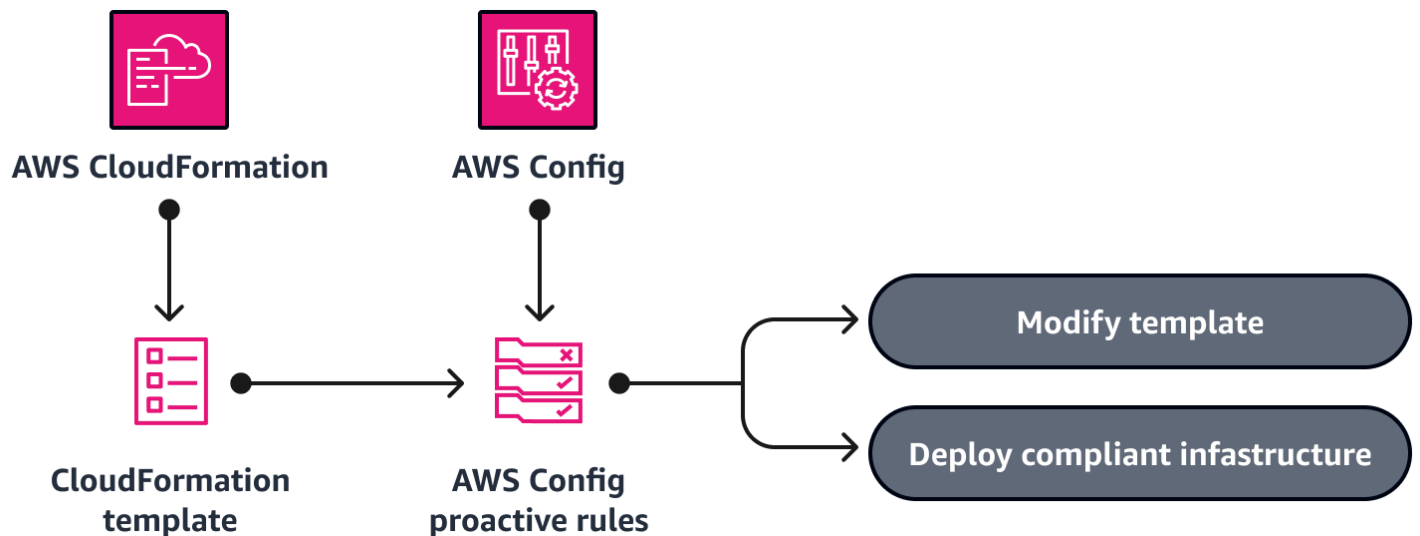
以下是應用程式或開發團隊可能負責的 [Security Hub 基礎安全性最佳作法 \(FSBP\)](#) 安全性標準中的一些控制項：

- [\[CloudFront.1\] CloudFront 發行版應該配置一個默認的根對象](#)
- [\[EC2.19\] 安全性群組不應允許不受限制地存取高風險連接埠](#)
- [\[CodeBuild.1\] CodeBuild GitHub 或比特桶源存儲庫網址應該使用 OAuth](#)
- [\[ECS.4\] ECS 容器應以非特權的方式執行](#)
- [\[ELB.1\] 應將 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS](#)

在此範例中，應用程式小組正在處理 FSBP 控制 EC2.19 的發現項目。此控制項會檢查安全性群組的不受限制傳入流量是否可供風險最高的指定通訊埠存取。如果安全性群組中的任何規則允許來自這些連

接埠的輸入流量，0.0.0.0/0則::/0此控制項會失敗。此控制項的[說明文件](#)建議刪除允許此流量的規則。

除了處理個別安全性群組規則之外，這是應該產生新 AWS Config [規則](#)的發現項目的絕佳範例。透過使用[主動評估模式](#)，您可以協助防止 future 部署有風險的安全性群組規則。主動模式會在部署資源之前評估資源，以避免資源設定錯誤及其相關的安全性發現。實作新服務或新功能時，應用程式團隊可以在主動模式下執行規則，做為其持續整合和持續交付 (CI/CD) 管線的一部分，以識別不符合規範的資源。下圖顯示如何使用主動式 AWS Config 規則來確認 AWS CloudFormation 範本中定義的基礎結構是否符合標準。



在這個例子中可以獲得另一個重要的效率。當應用程式小組建立主動 AWS Config 規則時，他們可以在通用程式碼儲存庫中共用它，以便其他應用程式團隊可以使用它。

與 Security Hub 控制項相關聯的每個發現項目都包含有關發現項目的詳細資料，以及修正問題之指示的連結。雖然雲端團隊可能會遇到需要手動一次性補救的發現項目，但我們建議您在適當情況下建立主動式檢查，以便儘早識別開發程序中的問題。

報告並改善您的弱點管理方案

有效的弱點管理報告包括檢閱資料、監控趨勢，以及分享知識。這可提供可見性，並協助團隊改善其組織中的安全狀態 AWS 雲端。

每月舉行安全性作業會議

每月安全性作業會議是促進跨團隊持續持續擁有權、責任和一致性的有效機制。在會議中，安全性、雲端和應用程式團隊的利益相關者會檢閱資料，以取得未完成的安全性發現結果、服務層級協定 (SLA) 以外的發現結果，以及發現最多的團隊。

這些會議可協助您的團隊識別反模式，例如增加更多限制的機會。也可以發現並共享預防性控制和自動化機會。這些會議還有助於識別弱點管理方案中有效的方法，而且在弱點管理方案中運作不佳，以便您可以進行改進。

透過檢閱資料、識別反模式和問題，以及共用控制項和自動化的相關資訊，團隊可以獲得寶貴的見解，並持續進行改進，以強化其安全狀態並減少與安全性相關的 SLA。

使用 Security Hub 深入解析來識別反模式

[AWS Security Hub 深入解析](#)也可協助您識別反模式，並追蹤修正發現項目的進度。Security Hub 洞察是相關發現項目的集合。該洞見會識別需要注意和介入的安全區域。Security Hub 深入解析可協助您識別特定需求並開發報告。資訊 Security Hub 提供數個內建的[受管理見解](#)。若要追蹤您的 AWS 環境和使用情況特有的安全性問題，您可以建立[自訂深入解析](#)。

結論和後續步驟

總而言之，有效的弱點管理計畫需要徹底的準備工作，並要求您啟用正確的工具和整合、微調這些工具、有效率地分類問題，以及持續報告和改進。透過遵循本指南中的最佳做法，組織可以在其上建置可擴充的弱點管理程式，AWS 以協助保護其雲端環境的安全。

您可以擴充此程式，以納入其他安全性相關弱點和發現項目，例如應用程式安全性弱點。AWS Security Hub 支援[自訂產品整合](#)。請考慮使用 Security Hub 做為其他安全性工具和產品的整合點。這項整合可讓您充分利用您在弱點管理程式中建立的程序和工作流程，例如直接整合產品待處理項目，以及每月的安全性檢閱會議。

下表概述了本指南中描述的階段和行動項目。

Phase (階段)	動作項目
準備	<ul style="list-style-type: none"> • 定義弱點管理計畫。 • 分配發現的所有權。 • 制定漏洞洩露計畫。 • 開發一個 AWS 帳戶 結構。 • 定義、實施和強制執行標籤。 • 監控 AWS 安全性佈告欄。 • 透過委派的管理員啟用 Amazon Inspector。 • 透過委派的系統管理員啟用 Security Hub。 • 啟用 Security Hub 標準。 • 設定 Security Hub 跨區域彙總。 • 啟用安全中心中的合併控制項發現項目 • 設定和管理 Security Hub 整合，包括與 SIEM、GRC 或產品積壓或票務系統的適用下游整合
分類及補救	<ul style="list-style-type: none"> • 根據多帳戶策略路由搜尋結果。 • 將發現項目路由到安全性、雲端和應用程式或開發人員團隊。 • 調整安全性發現項目，以確保它們可針對您的特定環境採取行動。

Phase (階段)	動作項目
	<ul style="list-style-type: none">盡可能開發自動補救機制。盡可能實作 CI/CD 管線控制或其他護欄，以協助防止發現安全性。使用 Security Hub 自動化規則來提升或隱藏發現項目。
報告和改善	<ul style="list-style-type: none">每月舉行安全性作業會議。使用 Security Hub 深入解析來識別反模式。

資源

AWS 服務文件

- [產品整合](#) (AWS Security Hub)
- [整合 AWS Security Hub 於 Jira Service Management Cloud](#) (AWS Security Hub)
- [自動化規則](#) (AWS Security Hub)
- [主動評估規則](#) (AWS Config)
- [修補程式管理員](#) (AWS Systems Manager)

其他 AWS 資源

- [標記 AWS 資源的最佳做法](#) (AWS 白皮書)
- [自動化安全回應 AWS](#) (AWS 解決方案資料庫)
- [AWS 保安事故應變指南](#) (AWS 技術指南)
- [AWS 安全性公告](#)

文件歷史紀錄

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

變更	描述	日期
初次出版	—	2023 年 10 月 12 日

AWS 規範指南詞彙表

以下是 AWS Prescriptive Guidance 所提供策略、指南和模式的常用術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的內部部署 Oracle 資料庫遷移至 Amazon Aurora Postgre SQL-Compatible Edition。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將您的內部部署 Oracle 資料庫遷移至 中的 Oracle 的 Amazon Relational Database Service (Amazon RDS) AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將內部部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移至相同平台的雲端服務。範例：遷移 Microsoft Hyper-V 應用程式至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱 [屬性型存取控制](#)。

抽象服務

請參閱 [受管服務](#)。

ACID

請參閱 [原子、一致性、隔離、持久性](#)。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但比 [主動被動遷移](#) 需要更多工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。目標資料庫在遷移期間不接受任何交易。

彙總函數

在一組資料列上操作並計算該群組單一傳回值的 SQL 函數。彙總函數的範例包括 SUM 和 MAX。

AI

請參閱 [人工智慧](#)。

AIOps

請參閱 [人工智慧操作](#)。

匿名化

在資料集中永久刪除個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常性問題的常用解決方案，其解決方案具有反效益、無效或效果不如替代方案。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體侵害。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是 [產品組合探索和分析程序](#) 的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱[什麼是人工智慧？](#)

人工智慧操作 (AI Ops)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需遷移策略 AI Ops 中 AWS 如何使用的詳細資訊，請參閱[操作整合指南](#)。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子度、一致性、隔離、持久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱 AWS Identity and Access Management (IAM) 文件[ABAC AWS](#)中的。

權威性資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將來自權威資料來源的資料複製到其他位置，以處理或修改資料，例如匿名、編輯或假名化資料。

可用區域

與其他可用區域中的故障 AWS 區域 隔離的不同位置，並對相同區域中的其他可用區域提供低成本、低延遲的網路連線。

AWS 雲端採用架構 (AWS CAF)

來自的指導方針和最佳實務架構 AWS，可協助組織制定高效且有效的計劃，以成功地遷移至雲端。AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、平台、安全和操作。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。為此，AWS CAF 提供人員開發、訓練和通訊的指引，協助組織成功採用雲端。如需詳細資訊，請參閱[AWS CAF 網站](#)和[AWS CAF 白皮書](#)。

AWS 工作負載資格架構 (AWS WQF)

評估資料庫遷移工作負載、建議遷移策略並提供工作估算的工具。AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的[機器人](#)。

BCP

請參閱[業務持續性規劃](#)。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以搭配 Amazon Detective 使用行為圖表來檢查失敗的登入嘗試、可疑API的呼叫和類似的動作。如需詳細資訊，請參閱偵測文件中的[行為圖中的資料](#)。

大端序系統

首先儲存最高有效位元組的系統。另請參閱[端點](#)。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 (藍色) 中執行目前的應用程式版本，並在另一個環境 (綠色) 中執行新的應用程式版本。此策略可協助您在影響最小的情況下快速復原。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。某些機器人很有用或有益，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。某些其他稱為壞機器人的機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到[惡意軟體](#)感染且由單一方控制的[機器人](#)網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱[關於分支](#)（GitHub 文件）。

碎片存取

在特殊情況下，以及透過核准的程序，使用者取得其通常無權存取 AWS 帳戶之存取權的快速方法。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS [實作碎片程序](#) 指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和[綠地](#)策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 [AWS 上執行容器化微服務](#) 白皮書的[圍繞業務能力進行組織](#) 部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱[AWS 雲端採用架構](#)。

Canary 部署

版本向最終使用者緩慢且增量的版本。當您有信心時，您可以部署新版本並完全取代目前的版本。

CCoE

請參閱 [Cloud Center of Excellence](#)。

CDC

請參閱 [變更資料擷取](#)。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以使用 CDC 進行各種用途，例如稽核或複寫目標系統中的變更，以維持同步。

混亂工程

故意引入故障或破壞性事件，以測試系統的復原能力。您可以使用 [AWS Fault Injection Service \(AWS FIS \)](#) 執行實驗，以強調 AWS 工作負載並評估其回應。

CI/CD

請參閱 [持續整合和持續交付](#)。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務接收資料之前，在本機加密資料。

Cloud Center of Excellence (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端企業策略部落格上的 [CCoE 文章](#)。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲端運算通常連接到 [邊緣運算](#) 技術。

雲端操作模型

在 IT 組織中，用於建置、成熟和最佳化一或多個雲端環境的操作模型。如需詳細資訊，請參閱 [建置您的雲端操作模型](#)。

採用雲端階段

組織在遷移至時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎：進行基礎投資以擴展雲端採用（例如，建立登陸區域、定義 CCoE、建立操作模型）
- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段由 Stephen Orban 在企業 AWS 雲端 策略部落格的 [The Journey Toward Cloud-First 和採用階段](#) 部落格中定義。如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱 [遷移準備指南](#)。

CMDB

請參閱 [組態管理資料庫](#)。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub 或 Bitbucket Cloud。每個版本的程式碼都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常為歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

使用機器學習從數位映像和影片等視覺化格式分析和擷取資訊的 [AI](#) 欄位。例如，AWS Panorama 提供將 CV 新增至內部部署攝影機網路的裝置，而 Amazon 則 SageMaker 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載變得不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常會在遷移 CMDB 的產品組合探索和分析階段使用來自的資料。

一致性套件

您可以組合的 AWS Config 規則和修復動作集合，以自訂合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶和區域中或整個組織中的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的[一致性套件](#)。

持續整合和持續交付 (CI/CD)

自動化軟體發程序的來源、建置、測試、暫存和生產階段的程序。CI/CD is commonly described as a pipeline. CI/CD 可協助您自動化程序、提高生產力、改善程式碼品質，以及更快交付。如需詳細資訊，請參閱[持續交付的優點](#)。CD 也可表示持續部署。如需詳細資訊，請參閱[持續交付與持續部署](#)。

CV

請參閱[電腦視覺效果](#)。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱[資料分類](#)。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變化。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構架構，提供分散式、分散式資料擁有權，並具有集中式管理和治理。

資料最小化

僅收集和處理嚴格必要資料的原則。在中實作資料最小化 AWS 雲端可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性防護機制，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱[在上建立資料周邊 AWS](#)。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個資料生命週期中追蹤資料的原始伺服器 and 歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫操作語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱[資料庫定義語言](#)。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

defense-in-depth

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS

Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，方法 defense-in-depth 可能會結合多重要素驗證、網路分割和加密。

委派的管理員

在中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶，以管理組織的帳戶並管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的 [可搭配 AWS Organizations 運作的服務](#)。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 [環境](#)。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS 上實作安全控制中的 [偵測性控制](#)。

開發值串流映射 (DVSM)

用於識別和排序限制的程式，這些限制會對軟體開發生命週期中的速度和品質產生不利影響。DVSM 延伸了最初專為精實生產實務設計的價值串流映射程序。它專注於透過軟體開發程序建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬表示法，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在 [星狀結構描述](#) 中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為與文字類似。這些屬性通常用於查詢限制、篩選和結果集標籤。

災難

阻止工作負載或系統在其主要部署位置實現其業務目標的事件。這些事件可能是自然災難、技術故障或人為動作的結果，例如意外錯誤組態或惡意軟體攻擊。

災難復原 (DR)

您用來將 [災難造成的停機時間和資料遺失降至最低的策略和程序](#)。如需詳細資訊，請參閱 AWS Well-Architected Framework [中的雲端中的工作負載災難復原 AWS：復原](#)。

DML

請參閱[資料庫操作語言](#)。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何搭配 strangler fig 模式使用網域驅動設計的資訊，請參閱[使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET \(ASMX \) Web 服務](#)。

DR

請參閱[災難復原](#)。

漂移偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源 中的漂移，或者您可以使用 AWS Control Tower 來[偵測您的登陸區域中可能會影響對治理要求合規性的變更](#)。
<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html>

DVSM

請參閱[開發值串流映射](#)。

E

EDA

請參閱[探索性資料分析](#)。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與[雲端運算](#) 相比，邊緣運算可以減少通訊延遲並縮短回應時間。

加密

將純文字資料轉換為可人工讀取的運算程序。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱[服務端點](#)。

端點服務

您可以在虛擬私有雲端（VPC）中託管以與其他使用者共用的服務。您可以使用 建立端點服務，AWS PrivateLink 並將許可授予其他 AWS 帳戶 或 AWS Identity and Access Management（IAM）主體。這些帳戶或主體可以透過建立介面端點，私下連線至您的VPC端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud（AmazonVPC）文件中的[建立端點服務](#)。

企業資源規劃（ERP）

可自動化和**管理企業關鍵業務流程**（例如會計[MES](#)、和專案管理）的系統。

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service（AWS KMS）文件中的[信封加密](#)。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如，AWS CAF安全特徵包括身分和存取管理、偵測控制、基礎設施安全、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱[計畫實作指南](#)。

ERP

請參閱[企業資源規劃](#)。

探索性資料分析 (EDA)

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。EDA 透過計算摘要統計資料和建立資料視覺化來執行。

F

事實資料表

[星狀結構描述](#) 中的中央資料表。它存放有關業務操作的量化資料。一般而言，事實資料表包含兩種類型的資料欄：包含量值的資料，以及包含維度資料表外部索引鍵的資料。

快速失敗

使用頻繁且增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在中 AWS 雲端，邊界，例如可用區域 AWS 區域、控制平面或資料平面，這些邊界會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱[AWS 故障隔離界限](#)。

功能分支

請參閱[分支](#)。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為數值分數，可透過各種技術計算，例如 Shapley 累加解釋 (SHAP) 和整合式漸層。如需詳細資訊，請參閱[使用的機器學習模型可解譯性：AWS](#)。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

FGAC

請參閱[精細存取控制](#)。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過[變更資料擷取](#)使用連續資料複寫，以盡可能在最短時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

G

地理封鎖

請參閱[地理限制](#)。

地理限制 (地理封鎖)

在 Amazon 中 CloudFront，此選項可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的[限制內容的地理分佈](#)。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程被視為舊版，而以[中繼線為基礎的工作流程](#)是現代的首選方法。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為[棕地](#)。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

高階規則，可協助管理跨組織單位 () 的資源、政策和合規性OUs。預防性防護機制會強制執行政策，以確保符合合規標準。它們是透過使用服務控制政策和IAM許可界限來實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。其實作方式是使用 AWS Config、AWS Security Hub、Amazon GuardDuty、AWS Trusted Advisor、Amazon Inspector 和自訂 AWS Lambda 檢查。

H

HA

請參閱[高可用性](#)。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如, Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分, 而轉換結構描述可能是一項複雜任務。[AWS 提供有助於結構描述轉換的 AWS SCT](#)。

高可用性 (HA)

工作負載在遇到挑戰或災難時持續運作的能力, 無需介入。HA 系統設計為自動容錯移轉、持續提供高品質效能, 以及處理不同的負載和故障, 並將效能影響降至最低。

歷史現代化

一種用於現代化和升級操作技術 (OT) 系統的方法, 以更好地滿足製造業的需求。歷史記錄器是一種資料庫類型, 用於從工廠的不同來源收集和存放資料。

異質資料庫遷移

將來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如 Microsoft SQL Server 遷移至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

常用資料

經常存取的資料, 例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別, 才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性, 修正程式通常在典型 DevOps 的發行工作流程之外建立。

超級護理期間

在切換後, 遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常, 此期間的長度為 1-4 天。在超級護理期間結束時, 遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

laC

將[基礎設施視為程式碼](#)。

身分型政策

連接至一或多個 IAM 主體的政策, 其定義其在 AWS 雲端環境中的許可。

閒置應用程式

在 90 天內，平均 CPU 和記憶體用量介於 5% 到 20% 的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱 [工業物聯網](#)。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有基礎設施。與可變基礎設施相比，不可避免的 [基礎設施](#) 本質上更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 [使用不可變基礎設施部署](#) 最佳實務。

傳入（傳入）VPC

在 AWS 多帳戶架構中，VPC 接受、檢查和路由來自應用程式外部的網路連線。[AWS Security Reference Architecture](#) 建議設定具有傳入、傳出和檢查的網路帳戶 VPCs，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

由 [Klaus Schwab](#) 於 2016 年推出的術語，指透過連線能力、即時資料、自動化、分析和 AI/ML 的進步來現代化製造程序。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱 [建置工業物聯網 \(IIoT\) 數位轉型策略](#)。

檢查 VPC

在 AWS 多帳戶架構中，集中 VPC 管理 VPCs（在相同或不同的 AWS 區域）、網際網路和內部部署網路之間的網路流量檢查。[AWS Security Reference Architecture](#) 建議設定具有傳入、傳出和檢查的網路帳戶 VPCs，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱[什麼是 IoT？](#)

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱[使用的機器學習模型可解釋性 AWS](#)。

IoT

請參閱[物聯網](#)。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 提供的基礎 ITSM。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需整合雲端操作與 ITSM 工具的相關資訊，請參閱[操作整合指南](#)。

ITIL

請參閱[IT 資訊庫](#)。

ITSM

請參閱[IT 服務管理](#)。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會被明確指派安全標籤值。使用者安全標籤與資料安全標籤之間的交集決定使用者可以看到哪些資料列和資料欄。

登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱[設定安全且可擴展的多帳戶 AWS 環境](#)。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱[標籤型存取控制](#)。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的[套用最低權限許可](#)。

隨即轉移

請參閱 [7 Rs](#)。

小端序系統

首先儲存最低有效位元組的系統。另請參閱[永久性](#)。

較低的環境

請參閱[環境](#)。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱[機器學習](#)。

主要分支

請參閱[分支](#)。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬程式、間諜軟體和鍵盤側錄程式。

受管服務

AWS 服務可 AWS 操作基礎設施層、作業系統和平台，而且您可以存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

用於追蹤、監控、記錄和控制生產程序的軟體系統，可將原物料轉換為工廠的成品。

MAP

請參閱[遷移加速程式](#)。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在運作時強化和改善本身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的[建置機制](#)。

成員帳戶

除了屬於中組織一部分的管理帳戶 AWS 帳戶之外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

MES

請參閱[製造執行系統](#)。

訊息佇列遙測傳輸 (MQTT)

根據[發佈/訂閱](#)模式的輕量型 machine-to-machine (M2M) 通訊協定，適用於資源受限的 [IoT](#) 裝置。

微服務

小型、獨立的服務，透過定義明確的方式進行通訊，APIs通常由小型、獨立的團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱[使用無 AWS 伺服器服務整合微服務](#)。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型，透過定義明確的介面進行通訊APIs。此架構中的每個微服務都可以進行更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱[在上實作微服務 AWS](#)。

Migration Acceleration Program (MAP)

提供諮詢支援、訓練和服務，以協助組織建立強大的操作基礎以遷移至雲端，並協助抵銷遷移初始成本的 AWS 計畫。MAP 包含以系統化方式執行舊版遷移的遷移方法，以及一組可自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 [AWS 遷移策略](#) 的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括操作、業務分析師和擁有者、遷移工程師、開發人員和在衝刺中工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的 [遷移工廠的討論](#) 和 [雲端遷移工廠指南](#)。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：EC2 使用 AWS Application Migration Service 重新託管遷移至 Amazon。

遷移產品組合評估 (MPA)

線上工具，提供驗證商業案例以遷移至的資訊 AWS 雲端。MPA 提供詳細的產品組合評估（伺服器大小調整、定價、TCO 比較、遷移成本分析）以及遷移規劃（應用程式資料分析和資料收集、應用程式分組、遷移優先順序和波規劃）。此 [MPA 工具](#)（需要登入）可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移就緒狀態評估 (MRA)

使用取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序 AWS CAF。如需詳細資訊，請參閱 [遷移準備程度指南](#)。MRA 是 [AWS 遷移策略](#) 的第一個階段。

遷移策略

用於將工作負載遷移至的方法 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 [7 個 Rs](#) 項目，並請參閱將 [組織動員以加速大規模遷移](#)。

機器學習 (ML)

請參閱[機器學習](#)。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱[中的應用程式現代化策略 AWS 雲端](#)。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱[中的評估應用程式的現代化準備 AWS 雲端](#)程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱[將單一體系分解為微服務](#)。

MPA

請參閱[遷移產品組合評估](#)。

MQTT

請參閱[訊息佇列遙測傳輸](#)。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性，AWS Well-Architected Framework 建議使用[不可變的基礎設施](#)作為最佳實務。

O

OAC

請參閱[原始存取控制](#)。

OAI

請參閱[原始存取身分](#)。

OCM

請參閱[組織變更管理](#)。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱[操作整合](#)。

OLA

請參閱[操作層級協議](#)。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱[開啟程序通訊 - Unified Architecture](#)。

開放程序通訊 - Unified Architecture (OPC-UA)

工業自動化的 machine-to-machine (M2M) 通訊協定。OPC-UA 提供與資料加密、身分驗證和授權方案的互通性標準。

操作層級協議 (OLA)

闡明哪些功能性 IT 群組承諾相互交付的協議，以支援服務層級協議 (SLA)。

操作預備檢閱 (ORR)

問題及相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的[操作就緒檢閱 \(ORR \)](#)。

操作技術 (OT)

與實體環境搭配使用的硬體和軟體系統，以控制工業操作、設備和基礎設施。在製造中，整合 OT 和資訊技術 (IT) 系統是 [Industry 4.0](#) 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱[操作整合指南](#)。

組織追蹤

由建立的追蹤 AWS CloudTrail 會記錄 AWS 帳戶中組織中所有的事件 AWS Organizations。在屬於組織的每個 AWS 帳戶中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱文件中的 CloudTrail[為組織建立追蹤](#)。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變革採用、解決轉型問題，以及推動文化和組織變革，協助組織準備和轉換新系統和策略。在 AWS 遷移策略中，由於雲端採用專案所需的變更速度，此架構稱為人員加速。如需詳細資訊，請參閱[OCM指南](#)。

原始存取控制 (OAC)

在中 CloudFront，用於限制存取以保護您的 Amazon Simple Storage Service (Amazon S3) 內容的增強型選項。OAC 支援所有中的所有 S3 儲存貯體 AWS 區域，伺服器端加密使用 AWS KMS (SSE-KMS)，以及對 S3 儲存貯體的動態PUT和DELETE請求。

原始存取身分 (OAI)

在中 CloudFront，此選項用於限制存取，以保護您的 Amazon S3 內容。當您使用時OAI，會 CloudFront 建立 Amazon S3 可以驗證的主體。已驗證的主體只能透過特定 CloudFront 分發存取 S3 儲存貯體中的內容。另請參閱[OAC](#)，它提供更精細和增強的存取控制。

ORR

請參閱[操作預備檢閱](#)。

OT

請參閱[操作技術](#)。

傳出（輸出）VPC

在 AWS 多帳戶架構中，VPC處理從應用程式內啟動之網路連線的。[AWS Security Reference Architecture](#) 建議設定具有傳入、傳出和檢查的網路帳戶VPCs，以保護應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

連接至IAM主體的IAM管理政策，以設定使用者或角色可擁有的最大許可。如需詳細資訊，請參閱IAM 文件中的[許可界限](#)。

個人身分資訊（PII）

直接檢視或與其他相關資料配對時，可用來合理推斷個人身分的資訊。的範例PII包括名稱、地址和聯絡資訊。

PII

請參閱[個人識別資訊](#)。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱[可程式邏輯控制器](#)。

PLM

請參閱[產品生命週期管理](#)。

政策

可以定義許可（請參閱[身分型政策](#)）、指定存取條件（請參閱[資源型政策](#)）或定義組織中所有帳戶的最大許可 AWS Organizations（請參閱[服務控制政策](#)）的物件。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則

可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱[在微服務中啟用資料持久性](#)。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱[評估遷移準備程度](#)。

述詞

傳回 true 或的查詢條件 false，通常位於 WHERE 子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS 上實作安全控制中的[預防性控制](#)。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中[角色術語和概念](#)中的主體。

設計隱私

一種系統工程方法，在整個工程過程中將隱私權納入考量。

私有託管區域

容器，其中包含您希望 Amazon Route 53 如何回應一個或多個內網域及其子網域的 DNS 查詢的資訊 VPCs。如需詳細資訊，請參閱 Route 53 文件中的[使用私有託管區域](#)。

主動控制

旨在防止部署不合規資源的[安全控制](#)。這些控制項會先掃描資源，然後再佈建。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的[控制項參考指南](#)，並請參閱在上實作安全[控制項中的主動](#)控制項。 AWS

產品生命週期管理 (PLM)

從設計、開發和啟動，到成長和成熟，再到拒絕和移除，產品整個生命週期的資料和程序管理。

生產環境

請參閱[環境](#)。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

擬匿名化

將資料集中的個人識別碼取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

publish/subscribe (pub/sub)

一種模式，可在微服務之間啟用非同步通訊，以提高可擴展性和回應能力。例如，在微服務型中[MES](#)，微服務可以將事件訊息發佈到其他微服務可以訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取SQL關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱[負責、負責、已諮詢、知情 \(RACI \)](#)。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱[負責、負責、已諮詢、知情 \(RACI \)](#)。

RCAC

請參閱[資料列和資料欄存取控制](#)。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 [7 Rs](#)。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷和服務還原之間的可接受延遲上限。

重構

請參閱 [7 Rs](#)。

區域

地理區域 AWS 的資源集合。每個 AWS 區域 都獨立於其他，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱 [指定 AWS 區域 哪些帳戶可以使用](#)。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 [7 Rs](#)。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 [7 Rs](#)。

轉譯形式

請參閱 [7 Rs](#)。

回購

請參閱 [7 Rs](#)。

彈性

應用程式抵抗中斷或從中斷中復原的能力。[在中規劃復原能力時，高可用性和災難復原](#)是常見的考量因素 AWS 雲端。如需詳細資訊，請參閱[AWS 雲端 復原能力](#)。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責任、負責、已諮詢、知情（RACI）矩陣

定義所有涉及遷移活動和雲端操作之各方的角色和責任的矩陣。矩陣名稱衍生自矩陣中定義的責任類型：負責人（R）、責任（A）、已諮詢（C）和知情（I）。支援（S）類型為選用。如果您包含支援，則矩陣稱為RASCI矩陣，如果您排除該矩陣，則稱為RACI矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS 上實作安全控制中的[回應性控制](#)。

保留

請參閱 [7 Rs](#)。

淘汰

請參閱 [7 Rs](#)。

輪換

定期更新[秘密](#)的程序，讓攻擊者更難存取憑證。

資料列和資料欄存取控制（RCAC）

使用已定義存取規則的基本靈活SQL表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱[復原點目標](#)。

RTO

請參閱[復原時間目標](#)。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者（IdPs）使用的開放標準。此功能會啟用聯合單一登入（SSO），因此使用者可以登入 AWS Management Console 或呼叫操作，AWS API 而不必 IAM 為您組織中的每個人建立使用者。如需 SAML 2.0 型聯合的詳細資訊，請參閱 IAM 文件中的[關於 SAML 2.0 型聯合](#)。

SCADA

請參閱 [監控控制和資料擷取](#)。

SCP

請參閱 [服務控制政策](#)。

秘密

在 AWS Secrets Manager 中，以加密形式存放的機密或限制資訊，例如密碼或使用者憑證。它由秘密值及其中繼資料組成。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 [Secrets Manager 文件中的 Secrets Manager 秘密中的內容？](#)。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：[預防性](#)、[偵測性](#)、[回應性](#) 和 [主動](#)。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊和事件管理（SIEM）系統

結合安全資訊管理（SIM）和安全事件管理（SEM）系統的工具和服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生警示。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為[偵測](#)或[回應](#)式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換憑證。

伺服器端加密

由接收資料的 AWS 服務 加密其目的地的資料。

服務控制政策 (SCP)

為 AWS Organizations 中的組織的所有帳戶提供集中控制許可的政策。SCPs 定義管理員可委派給使用者或角色之動作的防護機制或設定限制。您可以使用 SCPs 做為允許清單或拒絕清單，以指定允許或禁止的服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中[的服務控制政策](#)。

服務端點

URL 的進入點 AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考中的[AWS 服務端點](#)。

服務層級協議 (SLA)

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務層級指標 (SLI)

服務效能方面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由[服務層級指標](#)測量。

共同責任模式

描述您與共同 AWS 承擔雲端安全與合規責任的模型。AWS 負責雲端的安全，而負責雲端的安全。如需詳細資訊，請參閱[共同責任模式](#)。

SIEM

請參閱[安全資訊和事件管理系統](#)。

單一失敗點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱[服務層級協議](#)。

SLI

請參閱[服務層級指示器](#)。

SLO

請參閱[服務層級目標](#)。

split-and-seed 模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱[中的階段式應用程式現代化方法 AWS 雲端](#)。

SPOF

請參閱[單一失敗點](#)。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構專為[資料倉儲](#)或商業智慧用途而設計。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 [Martin Fowler 引入](#)，作為重寫單一系統時管理風險的方式。如需如何套用此模式的範例，請參閱[使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET \(ASMX \) Web 服務](#)。

子網

中 IP 地址的範圍 VPC。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 [Amazon CloudWatch Synthetics](#) 來建立這些測試。

T

標籤

作為中繼資料的鍵值對，用於組織您的 AWS 資源。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱[標記您的 AWS 資源](#)。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱[環境](#)。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可用來互連 VPCs 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的[什麼是傳輸閘道](#)。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中執行任務 AWS Organizations，並在其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱文件中的 AWS Organizations [AWS Organizations 搭配使用其他 AWS 服務](#)。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

一個小型 DevOps 團隊，您可以使用兩個披薩來饋送。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱[量化深度學習系統的不確定性](#)指南。

未區分的任務

也稱為繁重型，是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱[環境](#)。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等

兩個之間的連線VPCs，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱[Amazon 文件中的VPC互連內容](#)。VPC

漏洞

損害系統安全性的軟體或硬體缺陷。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等慢的查詢。

視窗函數

對以某種方式與目前記錄相關聯之資料列群組執行計算的SQL函數。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器 and 應用程式。

WORM

請參閱[寫入一次，讀取許多](#)。

WQF

請參閱[AWS工作負載資格架構](#)。

寫入一次，讀取許多 (WORM)

一次性寫入資料的儲存模型，可防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為[不可變的](#)。

Z

零時差漏洞

利用[零時差漏洞](#)的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的缺陷或漏洞。威脅發動者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

殭屍應用程式

平均CPU和記憶體用量低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。