實作 AWS CAF 安全功能的建議安全控制

# AWS 方案指引

# AWS 方案指引: 實作 AWS CAF 安全功能的建議安全控制

# Table of Contents

簡介 ..... 1
身分和存取控制 ..... 2
根使用者活動 ..... 2
根使用者的存取金鑰 ..... 3
針對根使用者的 MFA ..... 3
IAM 最佳實務 ..... 4
最低權限 ..... 4
工作負載層級的護欄 ..... 4
輪換 IAM 存取金鑰 ..... 5
外部共用資源 ..... 5
記錄和監控控制項 ..... 7
CloudTrail 多區域追蹤 ..... 7
服務和應用程式記錄 ..... 8
集中式記錄 ..... 8
存取 CloudTrail 日誌檔案 ..... 8
安全群組或網路 ACL 變更的提醒 ..... 9
CloudWatch 警示的警示 ..... 9
基礎設施控制 ..... 10
CloudFront 預設根物件 ..... 10
掃描應用程式程式碼 ..... 11
建立網路層 ..... 11
僅使用授權連接埠 ..... 11
公開存取 Systems Manager 文件 ..... 12
公開存取 Lambda 函數 ..... 12
更新預設安全群組 ..... 13
掃描漏洞和網路暴露 ..... 13
設定 AWS WAF ..... 14
進階的 DDoS 攻擊防護 ..... 14
控制網路流量 ..... 15
資料控制 ..... 16
在工作負載層級分類資料 ..... 16
為每個資料分類層級建立控制項 ..... 17
加密靜態資料 ..... 17
加密傳輸中的資料 ..... 18

對 Amazon EBS 快照的公開存取 ..... 18
公開存取 Amazon RDS 快照 ..... 19
公開存取 Amazon RDS、Amazon Redshift 和資源 AWS DMS ..... 19
公開存取 S3 儲存貯體 ..... 20
需要 MFA 才能刪除 S3 儲存貯體資料 ..... 20
VPCs 中的 OpenSearch Service 網域 ..... 21
KMS 金鑰刪除提醒 ..... 21
公開存取 KMS 金鑰 ..... 21
接聽程式使用安全通訊協定 ..... 22
事件回應建議 ..... 23
事件反應計畫 ..... 23
Runbook 和 手冊 ..... 23
事件驅動型自動化 ..... 24
支援 程序 ..... 24
安全事件的提醒 ..... 25
後續步驟 ..... 26
文件歷史紀錄 ..... 27
詞彙表 ..... 28
# ..... 28
A ..... 28
B ..... 31
C ..... 32
D ..... 35
E ..... 38
F ..... 40
G ..... 41
H ..... 42
I ..... 43
L ..... 45
M ..... 46
O ..... 50
P ..... 52
Q ..... 54
R ..... 54
S ..... 57
T ..... 60

U ..... 61
V ..... 62
W ..... 62
Z ..... 63
..... lxiv

# 實作 AWS CAF 安全功能的建議安全控制

Rishi Singla 和 Rovan Omar，Amazon Web Services (AWS)

2023 年 11 月 (文件歷史記錄)

安全是 的首要任務 AWS。為了協助減輕您的營運負擔，您需共同負責雲端安全與合規 AWS。 AWS 負責雲端安全，這表示 會保護執行 中所提供服務的基礎設施 AWS 雲端。您要負責雲端的安全，例如您的資料和應用程式。本指南提供安全控制，可協助您履行 中的安全責任 AWS 雲端。

AWS 雲端採用架構 (AWS CAF) 提供旨在改善雲端準備度的最佳實務。 AWS CAF 將這些最佳實務分類為六個觀點：業務、人員、治理、平台、安全和操作。本指南著重於安全角度的下列功能：

- 身分和存取管理 – 大規模管理人類和機器身分及其許可。
- 威脅偵測 – 設定記錄和監控，以偵測和調查潛在的安全設定錯誤、威脅或非預期行為。
- 保護基礎設施 – 保護系統和服務免於意外或未經授權的存取和潛在的漏洞。
- 保護資料 – 根據敏感度層級對資料進行分類。保持對資料及其在組織中的存取和使用方式的可見性和控制。
- 事件回應 – 建立機制來回應和減輕安全事件的潛在影響。

未實作這些 AWS CAF 安全功能的預防性、偵測性和回應性安全控制，可能會對您的雲端環境造成重大風險，並可能會中斷您的業務。本指南中的實作安全控制可協助您的組織保護其雲端環境。

> **Note**
>
> AWS 提供可協助您在 中安全操作的服務、工具和架構 AWS 雲端。本指南會與 AWS Well-Architected Framework、AWS Cloud Adoption Framework (AWS CAF)、AWS Security Reference Architecture (AWS SRA) 以及 發佈的其他安全建議保持一致，並加以補充 AWS。本指南中的控制項並非所有雲端安全考量的完整內容，本指南並非旨在取代這些架構。

# 管理身分和存取的安全控制建議

您可以在 中建立身分 AWS，也可以連接外部身分來源。透過 AWS Identity and Access Management (IAM) 政策，您可以授予使用者必要的許可，讓他們可以存取或管理 AWS 資源和整合的應用程式。有效的身分和存取管理有助於驗證適當的人員和機器在適當的條件下可以存取正確的資源。 AWS Well-Architected Framework 提供管理身分及其許可的最佳實務。最佳實務的範例包括依賴集中式身分提供者和使用強大的登入機制，例如多重要素驗證 (MFA)。本節中的安全控制項可協助您實作這些最佳實務。

本節中的控制項：

- 監控和設定根使用者活動的通知
- 不要為根使用者建立存取金鑰
- 為根使用者啟用 MFA
- 遵循 IAM 的安全最佳實務
- 授予最低權限許可
- 在工作負載層級定義許可護欄
- 定期輪換 IAM 存取金鑰
- 識別與外部實體共用的資源

## 監控和設定根使用者活動的通知

當您第一次建立 時 AWS 帳戶，您會從稱為根使用者的單一登入身分開始。根據預設，根使用者可完整存取 帳戶中的所有 AWS 服務 和資源。您應該嚴格控制和監控根使用者，而且只應將其用於需要根使用者憑證的任務。

如需詳細資訊，請參閱下列資源：

- 在 AWS Well-Architected Framework 中授予最低權限存取權
- 在規範指南中監控 IAM 根使用者活動 AWS

# 不要為根使用者建立存取金鑰

根使用者是 AWS 帳戶中權限最高的使用者。停用對根使用者的程式設計存取，有助於降低使用者登入資料意外暴露和後續雲端環境入侵的風險。我們建議您建立並使用 IAM 角色做為臨時登入資料，以存取您的 AWS 帳戶 和 資源。

如需詳細資訊，請參閱下列資源：

- IAM 根使用者存取金鑰不應存在於 AWS Security Hub 文件中
- 在 IAM 文件中刪除根使用者的存取金鑰
- IAM 文件中的 IAM 角色

# 為根使用者啟用 MFA

建議您為 AWS 帳戶 根使用者和 IAM 使用者啟用多個多重要素驗證 (MFA) 裝置。這會提高 中的 AWS 帳戶 安全列，並可以簡化存取管理。由於根使用者是可以執行特權動作的高度特權使用者，因此對根使用者要求 MFA 至關重要。您可以使用硬體 MFA 裝置，根據以時間為基礎的一次性密碼 (TOTP) 演算法、FIDO 硬體安全金鑰或虛擬驗證器應用程式產生數值碼。

在 2024 年，MFA 將需要存取任何 的根使用者 AWS 帳戶。如需詳細資訊，請參閱 AWS 安全部落格中的 Secure by Design： AWS 以增強 2024 年的 MFA 需求。我們強烈建議您擴展此安全實務，並要求 AWS 環境中所有使用者類型的 MFA。

如果可能，我們建議您為根使用者使用硬體 MFA 裝置。虛擬 MFA 可能無法提供與硬體 MFA 裝置相同層級的安全。您可以在等待硬體購買核准或交付時使用虛擬 MFA。

在您管理數百個帳戶的情況下 AWS Organizations，視組織的風險承受能力而定，在組織單位 (OU) 中，對每個帳戶的根使用者使用硬體型 MFA 可能無法擴展。在這種情況下，您可以選擇 OU 中充當 OU 管理帳戶的一個帳戶，然後停用該 OU 中其他帳戶的根使用者。根據預設，OU 管理帳戶無法存取其他帳戶。透過預先設定跨帳戶存取，您可以在緊急情況下從 OU 管理帳戶存取其他帳戶。若要設定跨帳戶存取，您可以在成員帳戶中建立 IAM 角色，並定義政策，以便只有 OU 管理帳戶中的根使用者才能擔任此角色。如需詳細資訊，請參閱 IAM 文件中的教學課程： AWS 帳戶 使用 IAM 角色委派跨的存取。

建議您為根使用者登入資料啟用多個 MFA 裝置。您可以註冊最多八個任何組合的 MFA 裝置。

如需詳細資訊，請參閱下列資源：

- 在 IAM 文件中啟用硬體 TOTP 字符

- 在 IAM 文件中啟用虛擬多重要素驗證 (MFA) 裝置
- 在 IAM 文件中啟用 FIDO 安全金鑰
- 使用 IAM 文件中的多重要素驗證 (MFA) 保護您的根使用者登入

## 遵循 IAM 的安全最佳實務

IAM 文件包含最佳實務清單，旨在協助您保護 AWS 帳戶 和 資源的安全。其中包括根據最低權限原則設定存取和許可的建議。IAM 安全最佳實務的範例包括設定聯合身分、要求 MFA，以及使用臨時登入資料。

如需詳細資訊，請參閱下列資源：

- IAM 文件中的 IAM 安全最佳實務
- 在 IAM 文件中使用臨時登入資料與 AWS 資源

## 授予最低權限許可

最低權限是僅授予執行任務所需許可的做法。您可以透過定義在特定條件下對特定資源可採取的動作來執行此操作。

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性定義許可，例如其標籤。您可以使用群組、身分和資源屬性來動態地大規模定義許可，而不是定義個別使用者的許可。例如，您可以使用 ABAC 來允許一組開發人員僅存取與其專案有關聯之特定標籤的資源。

如需詳細資訊，請參閱下列資源：

- 在 IAM 文件中套用最低權限許可
- IAM 文件中的 ABAC 適用於什麼 AWS

## 在工作負載層級定義許可護欄

最佳實務是使用多帳戶策略，因為它提供了在工作負載層級定義護欄的彈性。 AWS 安全參考架構提供有關如何建構帳戶的規範性指導。這些帳戶在 中以組織形式管理AWS Organizations，而帳戶會分組為組織單位 OUs)。

AWS 服務等 AWS Control Tower可協助您集中管理整個組織的控制項。我們建議您為組織內的每個帳戶或 OU 定義明確的用途，並根據該用途套用控制。 AWS Control Tower 實作預防性、偵測性和主動

控制，協助您管理資源並監控合規。預防性控制旨在防止事件發生。偵測性控制旨在於事件發生後偵測、記錄和提醒。主動控制旨在防止不合規資源的部署，方法是在佈建資源之前對其進行掃描。

如需詳細資訊，請參閱下列資源：

- 使用 Well-Architected Framework 中的帳戶來分隔工作負載 AWS
- 規範指南中的AWS 安全參考架構 (AWS SRA) AWS
- 關於 文件中的 控制項 AWS Control Tower AWS Control Tower
- AWS 在 規範指南中對 實作安全控制 AWS
- 使用 AWS 安全部落格中的服務控制政策，在 AWS 組織中的 帳戶間設定許可護欄

## 定期輪換 IAM 存取金鑰

最佳實務是針對需要長期憑證的使用案例更新存取金鑰。我們建議每 90 天或更短的時間輪換存取金鑰。輪換存取金鑰可降低使用與遭入侵或終止帳戶相關聯的存取金鑰的風險。它也會使用可能遺失、洩露或遭竊的舊金鑰來防止存取。輪換存取金鑰後，一律更新應用程式。

如需詳細資訊，請參閱下列資源：

- 針對需要 IAM 文件中長期憑證的使用案例，視需要更新存取金鑰
- 使用 AWS Prescriptive Guidance 中的 AWS Organizations 和 大規模自動輪換 IAM 使用者存取金鑰 AWS Secrets Manager
- 更新 IAM 文件中的存取金鑰

## 識別與外部實體共用的資源

外部實體是 AWS 組織外部的資源、應用程式、服務或使用者，例如另一個、根使用者 AWS 帳戶、IAM 使用者或角色、聯合身分使用者 AWS 服務、 或匿名 （或未驗證） 使用者。使用 IAM Access Analyzer 來識別組織和帳戶中與外部實體共用的資源是安全的最佳實務，例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 IAM 角色。這可協助您識別意外存取資源和資料，這是安全風險。

如需詳細資訊，請參閱下列資源：

- 在 IAM 文件中使用 IAM Access Analyzer 驗證對資源的公有和跨帳戶存取權
- 在 AWS Well-Architected Framework 中分析公有和跨帳戶存取

- 在 AWS Identity and Access Management Access Analyzer IAM 文件中使用

# 記錄和監控的安全控制建議

記錄和監控是威脅偵測的重要層面。威脅偵測是AWS 雲端採用架構 (AWS CAF) 中的安全透視功能之一。透過使用日誌資料，您的組織可以監控您的環境，以了解並識別潛在的安全錯誤組態、威脅和意外行為。了解潛在威脅可協助您的組織排定安全控制的優先順序，而有效的威脅偵測可協助您更快速地回應威脅。

本節中的控制項：

- 在 CloudTrail 中設定至少一個多區域追蹤
- 在服務和應用程式層級設定記錄
- 建立用於分析日誌和回應安全事件的集中位置
- 防止未經授權存取包含 CloudTrail 日誌檔案的 S3 儲存貯體
- 設定安全群組或網路 ACLs 變更的提醒
- 為進入 ALARM 狀態的 CloudWatch 警示設定警示

## 在 CloudTrail 中設定至少一個多區域追蹤

AWS CloudTrail 可協助您稽核 的控管、合規和營運風險 AWS 帳戶。使用者、角色或 採取的動作 AWS 服務 會在 CloudTrail 中記錄為事件。事件包括 、 AWS Command Line Interface (AWS CLI) AWS Management Console、 和 AWS SDKs和 APIs中採取的動作。此事件歷史記錄可協助您分析安全狀態、追蹤資源變更和稽核合規。

若要持續記錄 中的事件 AWS 帳戶，您必須建立追蹤。每個線索都應設定為記錄所有事件 AWS 區域。透過在所有 中記錄事件 AWS 區域，您可以確保 AWS 帳戶 記錄在您 中發生的所有事件，無論 AWS 區域 它們發生在哪個 中。多區域追蹤可確保記錄全域服務事件。

如需詳細資訊，請參閱下列資源：

- CloudTrail 文件中的 CloudTrail 偵測安全最佳實務 CloudTrail
- 轉換套用至一個區域的追蹤，以套用至 CloudTrail 文件中的所有區域 CloudTrail
- 在 CloudTrail 文件中啟用和停用全域服務事件記錄

# 在服務和應用程式層級設定記錄

AWS Well-Architected Framework 建議您保留來自 服務和應用程式的安全事件日誌。這是稽核、調查和操作使用案例安全性的基本原則。服務和應用程式日誌保留是常見的安全要求，由控管、風險和合規 (GRC) 標準、政策和程序驅動。

安全營運團隊倚賴日誌和搜尋工具來探索可能表示未經授權的活動或意外變更的潛在關注事件。您可以根據使用案例啟用不同 服務的日誌記錄。例如，您可以記錄 Amazon S3 儲存貯體存取、 AWS WAF Web ACL 流量、網路層的 Amazon API Gateway 流量或 Amazon CloudFront 分佈。

如需詳細資訊，請參閱下列資源：

- 將 Amazon CloudWatch Logs 串流到 架構部落格中的集中式帳戶以進行稽核和分析 AWS
- 在 AWS Well-Architected Framework 中設定服務和應用程式記錄

# 建立用於分析日誌和回應安全事件的集中位置

手動分析日誌和處理資訊不足以跟上與複雜架構相關聯的資訊量。分析和報告本身無法協助及時將事件指派給正確的資源。 AWS Well-Architected Framework 建議您將 AWS 安全事件和調查結果整合到通知和工作流程系統中，例如票證、錯誤或安全資訊和事件管理 (SIEM) 系統。這些系統可協助您指派、路由和管理安全事件。

如需詳細資訊，請參閱下列資源：

- 在 AWS Well-Architected Framework 中集中分析日誌、調查結果和指標
- 安全部落格中的使用 CloudTrail 和 Amazon Athena 分析安全性、合規性和操作活動 AWS
- 在 AWS 合作夥伴產品組合中提供威脅偵測和回應服務的 AWS 合作夥伴

# 防止未經授權存取包含 CloudTrail 日誌檔案的 S3 儲存貯體

根據預設，CloudTrail 日誌檔案會存放在 Amazon S3 儲存貯體中。安全最佳實務是防止未經授權存取包含 CloudTrail 日誌檔案的任何 Amazon S3 儲存貯體。這可協助您維護這些日誌的完整性、完整性和可用性，這對於鑑識和稽核目的至關重要。如果您想要為包含 CloudTrail 日誌檔案的 S3 儲存貯體記錄資料事件，您可以為此建立 CloudTrail 追蹤。

如需詳細資訊，請參閱下列資源：

- 在 Amazon S3 文件中為您的 S3 儲存貯體設定封鎖公開存取設定 Amazon S3

- CloudTrail 文件中的 CloudTrail 預防性安全最佳實務
- 在 CloudTrail 文件中建立追蹤

## 設定安全群組或網路 ACLs 變更的提醒

Amazon Virtual Private Cloud (Amazon VPC) 中的安全群組會控制允許存取的流量，並保留與其相關聯的資源。網路存取控制清單 (ACL) 允許或拒絕 VPC 子網路層級的特定傳入或傳出流量。這些資源對於管理您 AWS 環境中的存取至關重要。

建立和設定 Amazon CloudWatch 警示，在安全群組或網路 ACL 組態變更時通知您。設定此警示，在每次執行 API 呼叫以更新安全群組時 AWS 提醒您。您也可以使用 服務，例如 Amazon EventBridge 和 AWS Config，自動回應這些類型的安全事件。

如需詳細資訊，請參閱下列資源：

- AWS 安全部落格中的自動還原和接收 Amazon VPC 安全群組變更的通知
- CloudWatch 文件中的使用 Amazon CloudWatch 警示 CloudWatch
- 在 AWS Well-Architected 架構中實作可採取動作的安全事件
- 自動回應 Well-Architected Framework 中的事件 AWS

## 為進入 ALARM 狀態的 CloudWatch 警示設定警示

在 CloudWatch 中，您可以指定警示在 `OK`、 `ALARM`和 `INSUFFICIENT_DATA` 狀態之間變更狀態時所採取的動作。最常見的警示動作類型是透過傳送訊息至 Amazon Simple Notification Service (Amazon SNS) 主題來通知一或多個人員。您也可以設定警示，在 中建立 OpsItems 或事件 AWS Systems Manager。

建議您啟用警示動作，以便在受監控指標超出定義的閾值時自動發出警示。監控警示可協助您識別異常活動，並快速回應安全性和操作問題。

如需詳細資訊，請參閱下列資源：

- 在 AWS Well-Architected 架構中實作可採取動作的安全事件
- CloudWatch 文件中的警示動作

# 保護基礎設施的安全控制建議

基礎設施保護是任何安全計畫的關鍵部分。它包含控制方法，可協助您保護網路和運算資源。基礎設施保護的範例包括信任界限、defense-in-depth方法、安全強化、修補程式管理，以及作業系統身分驗證和授權。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的基礎設施保護。本節中的安全控制可協助您實作基礎設施保護的最佳實務。

本節中的控制項：

- 指定 CloudFront 分佈的預設根物件
- 掃描應用程式程式碼以識別常見的安全問題
- 使用專用 VPCs和子網路建立網路層
- 將傳入流量限制為僅授權的連接埠
- 封鎖對 Systems Manager 文件的公開存取
- 封鎖對 Lambda 函數的公開存取
- 在預設安全群組中限制傳入和傳出流量
- 掃描軟體漏洞和意外的網路暴露
- 設定 AWS WAF
- 設定進階的 DDoS 攻擊防護
- 使用defense-in-depth方法來控制網路流量

# 指定 CloudFront 分佈的預設根物件

Amazon CloudFront 透過全球資料中心網路提供 Web 內容，進而降低延遲並改善效能，進而加速 Web 內容的分佈。如果您不定義預設根物件，則分佈根的請求會通過您的原始伺服器。如果您使用的是 Amazon Simple Storage Service (Amazon S3) 原始伺服器，則請求可能會傳回 S3 儲存貯體中的內容清單，或原始伺服器私有內容清單。指定預設根物件可協助您避免公開分佈的內容。

如需詳細資訊，請參閱下列資源：

- 在 CloudFront 文件中指定預設根物件

# 掃描應用程式程式碼以識別常見的安全問題

AWS Well-Architected Framework 建議您掃描程式庫和相依性是否有問題和瑕疵。您可以使用許多原始程式碼分析工具來掃描原始程式碼。例如，Amazon CodeGuru 可以掃描 Java或 Python 應用程式中常見的安全問題，並提供修補建議。

如需詳細資訊，請參閱下列資源：

- CodeGuru 文件
- OWASP Foundation 網站上的原始程式碼分析工具
- 在 AWS Well-Architected 架構中執行漏洞管理

# 使用專用 VPCs和子網路建立網路層

AWS Well-Architected Framework 建議您將共用敏感需求的元件分組為層。這可將未經授權的存取的潛在影響範圍降至最低。例如，不需要網際網路存取的資料庫叢集應放置在其 VPC 的私有子網路中，以確保沒有往返網際網路的路由。

AWS 提供許多 服務，可協助您測試和識別公有可及性。例如， Reachability Analyzer 是一種組態分析工具，可協助您測試 VPCs中來源和目的地資源之間的連線。此外，Network Access Analyzer 可協助您識別對資源的意外網路存取。

如需詳細資訊，請參閱下列資源：

- 在 AWS Well-Architected 架構中建立網路層
- Reachability Analyzer 文件
- Network Access Analyzer 文件
- 在 Amazon Virtual Private Cloud (Amazon VPC) 文件中建立子網路

# 將傳入流量限制為僅授權的連接埠

不受限制的存取，例如來自`0.0.0.0/0`來源 IP 地址的流量，會增加惡意活動的風險，例如駭客入侵、denial-of-service(DoS) 攻擊和資料遺失。安全群組提供輸入和輸出網路流量至 AWS 資源的狀態篩選。任何安全群組都不應允許無限制的傳入存取已知的連接埠，例如 SSH 和Windows遠端桌面通訊協定 (RDP)。對於傳入流量，在您的安全群組中，僅允許授權連接埠上的 TCP 或 UDP 連線。若要

連線至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，請使用 Session Manager 或 Run Command，而非直接存取 SSH 或 RDP。

如需詳細資訊，請參閱下列資源：

- 在 Amazon EC2 文件中使用安全群組 Amazon EC2
- 使用 Amazon VPC 文件中的安全群組控制 AWS 資源的流量

## 封鎖對 Systems Manager 文件的公開存取

除非您的使用案例需要開啟公有共用， AWS Systems Manager 否則最佳實務建議您封鎖 Systems Manager 文件的公有共用。公開共用可能會提供文件的意外存取。公有 Systems Manager 文件可以公開有關您的帳戶、資源和內部程序的寶貴和敏感資訊。

如需詳細資訊，請參閱下列資源：

- Systems Manager 文件中共用 Systems Manager 文件的最佳實務
- 在 Systems Manager 文件中修改共用 Systems Manager 文件的許可

## 封鎖對 Lambda 函數的公開存取

AWS Lambda 是一項運算服務，可協助您執行程式碼，無需佈建或管理伺服器。Lambda 函數不應公開存取，因為這可能會允許對函數程式碼的意外存取。

我們建議您為 Lambda 函數設定資源型政策，以拒絕從帳戶外部存取。您可以透過移除許可或將`AWS:SourceAccount`條件新增至允許存取的 陳述式來達成此目的。您可以透過 Lambda API 或 AWS Command Line Interface () 更新 Lambda 函數的資源型政策AWS CLI。

我們也建議您啟用 【Lambda.1】 Lambda 函數政策應禁止 中的公開存取控制。 AWS Security Hub此控制項會驗證 Lambda 函數的資源型政策是否禁止公開存取。

如需詳細資訊，請參閱下列資源：

- Security Hub 文件中的AWS Lambda 控制項
- 在 Lambda 文件中使用 Lambda 的資源型政策
- Lambda 文件中 Lambda 動作的資源和條件

# 在預設安全群組中限制傳入和傳出流量

如果您在佈建 AWS 資源時未建立自訂安全群組的關聯，則資源會與 VPC 的預設安全群組相關聯。此安全群組的預設規則允許來自指派給此安全群組之所有資源的所有傳入流量，且允許所有傳出 IPv4 和 IPv6 流量。這可能會允許對資源的意外流量。

AWS 建議您不要使用預設安全群組。反之，為特定資源或資源群組建立自訂安全群組。

由於無法刪除預設安全群組，建議您變更預設安全群組規則，以限制傳入和傳出流量。設定安全群組規則時，請遵循最低權限原則。

我們也建議您啟用 【EC2.2】 VPC 預設安全群組，不應允許 Security Hub 中的傳入或傳出流量控制。此控制項會驗證 VPC 的預設安全群組是否拒絕傳入和傳出流量。

如需詳細資訊，請參閱下列資源：

- 使用 Amazon VPC 文件中的安全群組控制 AWS 資源的流量
- Amazon VPCs 文件中 VPC 的預設安全群組
- Security Hub 文件中的 Amazon EC2 控制項

# 掃描軟體漏洞和意外的網路暴露

建議您在所有帳戶中啟用 Amazon Inspector。Amazon Inspector 是一種漏洞管理服務，會持續掃描您的 Amazon EC2 執行個體、Amazon Elastic Container Registry (Amazon ECR) 容器映像，以及 Lambda 函數是否有軟體漏洞和意外的網路暴露。它也支援 Amazon EC2 執行個體的深度檢查。當 Amazon Inspector 識別漏洞或開放式網路路徑時，會產生您可以調查的問題清單。如果您的帳戶中同時設定了 Amazon Inspector 和 Security Hub，則 Amazon Inspector 會自動將安全調查結果傳送至 Security Hub 以進行集中式管理。

如需詳細資訊，請參閱下列資源：

- Amazon Inspector 文件中的使用 Amazon Inspector 掃描資源 Amazon Inspector
- Amazon Inspector 文件中的 Amazon EC2 Amazon Inspector Deep inspection
- AWS 安全部落格中的使用 Amazon Inspector 掃描 EC2 AMIs
- 在 AWS 規範指南中，在 上建置可擴展的漏洞管理計劃 AWS
- 在 AWS Well-Architected 架構中自動化網路保護
- 在 AWS Well-Architected Framework 中自動化運算保護

# 設定 AWS WAF

AWS WAF 是 Web 應用程式防火牆，可協助您監控和封鎖轉送至受保護 Web 應用程式資源的 HTTP 或 HTTPS 請求，例如 Amazon API Gateway APIs、Amazon CloudFront 分佈或 Application Load Balancer。服務會根據您指定的條件，使用請求的內容、HTTP 403 狀態碼 （禁止） 或自訂回應來回應請求。 AWS WAF 可協助保護 Web 應用程式或 APIs 免受可能影響可用性、危及安全性或耗用過多資源的常見 Web 入侵。請考慮在 AWS WAF 中設定 AWS 帳戶 ，並使用受 AWS 管規則、自訂規則和合作夥伴整合的組合，以協助保護您的應用程式免受應用程式層 （第 7 層） 攻擊。

如需詳細資訊，請參閱下列資源：

- AWS WAF 文件中的 入門 AWS WAF
- AWS 網站上的 AWS WAF 交付合作夥伴
- AWS 解決方案程式庫中的 安全自動化 AWS WAF
- 在 AWS Well-Architected 架構中實作檢查和保護

# 設定進階的 DDoS 攻擊防護

AWS Shield 針對網路和傳輸層 （第 3 層和第 4 層） 和應用程式層 （第 7 層） 上的 AWS 資源，提供防範分散式阻斷服務 (DDoS) 攻擊的保護。此服務有兩種選項： AWS Shield Standard 和 AWS Shield Advanced。Shield Standard 會自動保護支援 AWS 的資源，無需額外費用。

我們建議您訂閱 Shield Advanced，它為受保護的資源提供擴展的 DDoS 攻擊保護。您從 Shield Advanced 收到的保護會因您的架構和組態選擇而有所不同。考慮為需要下列任何一項的應用程式實作 Shield Advanced 保護：

- 保證應用程式使用者的可用性。
- 如果應用程式受到 DDoS 攻擊影響，快速存取 DDoS 緩解專家。
- AWS 知道應用程式可能受到 DDoS 攻擊的影響，以及 AWS 攻擊的通知，並呈報至您的安全或營運團隊。
- 雲端成本的可預測性，包括 DDoS 攻擊影響您使用 的時間 AWS 服務。

如需詳細資訊，請參閱下列資源：

- Shield 文件中的 AWS Shield Advanced 概觀
- Shield 文件中的AWS Shield Advanced 受保護資源

- Shield 文件中的AWS Shield Advanced 功能和選項
- 回應 Shield 文件中的 DDoS 事件
- 在 AWS Well-Architected Framework 中實作檢查和保護

## 使用defense-in-depth方法來控制網路流量

AWS Network Firewall 是一種具狀態、受管的網路防火牆和入侵偵測和預防服務，適用於 中的虛擬私有雲端 (VPCs) AWS 雲端。它可協助您在 VPC 周邊部署必要的網路保護。這包括篩選進出網際網路閘道、NAT 閘道或透過 VPN 或 的流量 AWS Direct Connect。Network Firewall 包含有助於防止常見網路威脅的功能。Network Firewall 中的具狀態防火牆可以整合流量的內容，例如連線和通訊協定，以強制執行政策。

如需詳細資訊，請參閱下列資源：

- AWS Network Firewall 文件
- 控制 Well-Architected 架構中所有層的流量 AWS

# 保護資料的安全控制建議

AWS Well-Architected Framework 將保護資料的最佳實務分為三個類別：資料分類、保護靜態資料，以及保護傳輸中的資料。本節中的安全控制可協助您實作資料保護的最佳實務。在您架構雲端中的任何工作負載之前，應該具備這些基礎最佳實務。它們可防止資料處理不當，並可協助您履行組織、法規和合規義務。使用本節中的安全控制來實作資料保護的最佳實務。

本節中的控制項：

- 在工作負載層級識別和分類資料
- 為每個資料分類層級建立控制項
- 加密靜態資料
- 加密傳輸中的資料
- 封鎖對 Amazon EBS 快照的公開存取
- 封鎖對 Amazon RDS 快照的公開存取
- 封鎖對 Amazon RDS、Amazon Redshift 和資源的公開存取 AWS DMS
- 封鎖對 Amazon S3 儲存貯體的公開存取
- 要求 MFA 刪除關鍵 Amazon S3 儲存貯體中的資料
- 在 VPC 中設定 Amazon OpenSearch Service 網域
- 設定 AWS KMS key 要刪除的提醒
- 封鎖對 的公開存取 AWS KMS keys
- 設定負載平衡器接聽程式以使用安全通訊協定

## 在工作負載層級識別和分類資料

資料分類是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。資料分類通常會降低資料重複的頻率。這可以降低儲存和備份成本，並加速搜尋。

我們建議您了解工作負載正在處理的資料類型和分類、相關聯的業務流程、資料的存放位置，以及誰擁有資料。資料分類可協助工作負載擁有者識別存放敏感資料的位置，並判斷應如何存取和共用該資料。標籤是鍵/值對，可做為中繼資料來組織 AWS 資源。標籤可協助管理、識別、組織、搜尋和篩選資源。

如需詳細資訊，請參閱下列資源：

- AWS 白皮書中的資料分類
- 在 AWS Well-Architected 架構中識別工作負載中的資料

## 為每個資料分類層級建立控制項

定義每個分類層級的資料保護控制。例如，使用建議的控制項來保護分類為公有的資料，並使用其他控制項來保護敏感資料。使用機制和工具可減少或消除直接存取或手動處理資料的需求。自動化資料識別和分類可降低分類錯誤、處理不當、修改或人為錯誤的風險。

例如，請考慮使用 Amazon Macie 掃描 Amazon Simple Storage Service (Amazon S3) 儲存貯體的敏感資料，例如個人身分識別資訊 (PII)。此外，您也可以在 Amazon Virtual Private Cloud (Amazon VPC) 中使用 VPC 流程日誌，自動偵測意外的資料存取。

如需詳細資訊，請參閱下列資源：

- 在 AWS Well-Architected 架構中定義資料保護控制
- 在 AWS Well-Architected 架構中自動化識別和分類
- 方案指引中的AWS 隱私權參考架構 (AWS PRA) AWS
- 在 Macie 文件中使用 Amazon Macie 探索敏感資料
- Amazon VPC 文件中的使用 VPC 流程日誌記錄 IP 流量
- 在 AWS for Industries 部落格中使用 偵測 PHI 和 PII 資料的常見技術 AWS 服務

## 加密靜態資料

靜態資料是網路中靜態的資料，例如儲存中的資料。實作靜態資料的加密和適當的存取控制，有助於降低未經授權的存取風險。加密是一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。您需要加密金鑰，才能將內容解密回純文字，以便使用。在 中 AWS 雲端，您可以使用 AWS Key Management Service (AWS KMS) 來建立和控制密碼編譯金鑰，以協助保護您的資料。

如 中所述為每個資料分類層級建立控制項，我們建議建立政策來指定需要加密的資料類型。包含如何判斷哪些資料應該加密，以及哪些資料應該使用另一種技術來保護的條件，例如字符化或雜湊。

如需詳細資訊，請參閱下列資源：

- 在 Amazon S3 文件中設定預設加密

- Amazon EC2 文件中的新 EBS 磁碟區和快照複本預設加密
- Amazon Aurora 文件中的加密 Amazon Aurora 資源
- 文件中的 AWS KMS 密碼編譯詳細資訊簡介 AWS KMS
- AWS 在方案指引中為靜態資料建立企業加密策略
- 在 AWS Well-Architected Framework 中強制執行靜態加密
- 如需特定 加密的詳細資訊 AWS 服務，請參閱該服務AWS 的文件

## 加密傳輸中的資料

傳輸中的資料是在您的網路中主動移動的資料，例如在網路資源之間移動。使用安全的 TLS 通訊協定和密碼套件加密傳輸中的所有資料。資源與網際網路之間的網路流量必須加密，以協助防止未經授權的資料存取。如果可能，請使用 TLS 來加密內部 AWS 環境中的網路流量。

如需詳細資訊，請參閱下列資源：

- Amazon CloudFront 文件中的檢視器與 CloudFront 之間需要 HTTPS 進行通訊 Amazon CloudFront
- AWS PrivateLink 文件
- 在 AWS Well-Architected 架構中強制執行傳輸中的加密
- 如需特定 加密的詳細資訊 AWS 服務，請參閱該服務AWS 的文件

## 封鎖對 Amazon EBS 快照的公開存取

Amazon Elastic Block Store (Amazon EBS) 提供區塊層級儲存磁碟區，可與 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體搭配使用。您可取得某個時間點的快照，藉此將 Amazon EBS 磁碟區上的資料備份至 Amazon S3。您可以公開與所有其他 共用快照 AWS 帳戶，也可以私下與您 AWS 帳戶 指定的個人共用快照。

建議您不要公開共用 Amazon EBS 快照。這可能會無意中公開敏感資料。當您共用快照時，您會讓其他人存取快照中的資料。僅與您對所有資料信任的人員共用快照。

如需詳細資訊，請參閱下列資源：

- 在 Amazon EC2 文件中共用快照
- Amazon EBS 快照不應在文件中公開還原 AWS Security Hub
- 文件中的 AWS Config ebs-snapshot-public-restorable-check

# 封鎖對 Amazon RDS 快照的公開存取

Amazon Relational Database Service (Amazon RDS) 可協助您在 中設定、操作和擴展關聯式資料庫 AWS 雲端。Amazon RDS 會在資料庫執行個體的備份時段期間建立並儲存資料庫 （資料庫） 執行個體或多可用區域資料庫叢集的自動備份。Amazon RDS 會建立資料庫執行個體的儲存體磁碟區快照，因此會備份整個資料庫執行個體，而不只是個別的資料庫。您可以共用手動快照，以複製快照或從中還原資料庫執行個體。

如果您將快照共用為公有，請確定快照中的任何資料都不是私有或敏感的。公開共用快照時，會授予存取資料的所有 AWS 帳戶 許可。這可能會導致 Amazon RDS 執行個體中的資料意外暴露。

如需詳細資訊，請參閱下列資源：

- 在 Amazon RDS 文件中共用資料庫快照
- AWS Config 文件中的 rds-snapshots-public-prohibited
- RDS 快照在 Security Hub 文件中應為私有

# 封鎖對 Amazon RDS、Amazon Redshift 和資源的公開存取 AWS DMS

您可以將 Amazon RDS 資料庫執行個體、Amazon Redshift 叢集和 AWS Database Migration Service (AWS DMS) 複寫執行個體設定為可公開存取。如果`publiclyAccessible`欄位值為 `true`，則可公開存取這些資源。允許公開存取可能會導致不必要的流量、暴露或資料外洩。建議您不要允許公開存取這些資源。

建議您啟用 AWS Config 規則或 Security Hub 控制項，以偵測 Amazon RDS 資料庫執行個體、 AWS DMS 複寫執行個體或 Amazon Redshift 叢集是否允許公開存取。

> **Note**
>
> 佈建執行個體之後，無法修改 AWS DMS 複寫執行個體的公有存取設定。若要變更公有存取設定，請刪除目前的執行個體，然後重新建立它。重新建立時，請勿選取公開存取選項。

如需詳細資訊，請參閱下列資源：

- Security Hub 文件中AWS DMS 不應公開複寫執行個體

- RDS 資料庫執行個體應該禁止 Security Hub 文件中的公開存取
- Amazon Redshift 叢集應該禁止在 Security Hub 文件中公開存取
- AWS Config 文件中的 rds-instance-public-access-check
- AWS Config 文件中的 dms-replication-not-public
- 文件中的 AWS Config redshift-cluster-public-access-check
- 在 Amazon RDS 文件中修改 Amazon RDS 資料庫執行個體
- 在 Amazon Redshift 文件中修改叢集

## 封鎖對 Amazon S3 儲存貯體的公開存取

這是 Amazon S3 安全最佳實務，可確保您的儲存貯體無法公開存取。除非您明確要求網際網路上的任何人能夠讀取或寫入您的儲存貯體，否則請確定您的儲存貯體不是公有的。這有助於保護資料的完整性和安全性。您可以使用 AWS Config 規則和 Security Hub 控制項來確認您的 Amazon S3 儲存貯體符合此最佳實務。

如需詳細資訊，請參閱下列資源：

- Amazon S3 文件中的 Amazon S3 安全最佳實務 Amazon S3
- 應在 Security Hub 文件中啟用 S3 封鎖公開存取設定
- S3 儲存貯體應該禁止 Security Hub 文件中的公有讀取存取
- S3 儲存貯體應該禁止 Security Hub 文件中的公有寫入存取
- 文件中的 AWS Config s3-bucket-public-read-prohibited 規則
- AWS Config 文件中的 s3-bucket-public-write-prohibited

## 要求 MFA 刪除關鍵 Amazon S3 儲存貯體中的資料

在 Amazon S3 儲存貯體中使用 S3 版本控制時，您可以選擇將儲存貯體設定為啟用 MFA (多重因素認證) Delete，來增加額外的安全性。當您這樣做時，儲存貯體擁有者必須在任一要求中包含兩種身分驗證形式，才能刪除版本或變更儲存貯體的版本控制狀態。建議您為包含對組織至關重要之資料的儲存貯體啟用此功能。這可以防止意外刪除儲存貯體和資料。

如需詳細資訊，請參閱下列資源：

- 在 Amazon S3 文件中設定 MFA 刪除

# 在 VPC 中設定 Amazon OpenSearch Service 網域

Amazon OpenSearch Service 是一項受管服務，可協助您在 中部署、操作和擴展OpenSearch叢集 AWS 雲端。Amazon OpenSearch Service 支援 OpenSearch和舊版Elasticsearch開放原始碼軟體 (OSS)。在 VPC 內部署的 Amazon OpenSearch Service 網域可以透過私有 AWS 網路與 VPC 資源通訊，而不需要周遊公有網際網路。此組態透過限制對傳輸中資料的存取來改善您的安全狀態。建議您不要將 Amazon OpenSearch Service 網域連接至公有子網路，並根據最佳實務設定 VPC。

如需詳細資訊，請參閱下列資源：

- 在 Amazon OpenSearch Service 文件中的 VPC 內啟動 Amazon OpenSearch Service 網域 OpenSearch
- AWS Config 文件中的 opensearch-in-vpc-only
- OpenSearch 網域應該位於 Security Hub 文件中的 VPC 中

# 設定 AWS KMS key 要刪除的提醒

AWS Key Management Service (AWS KMS) 金鑰在刪除後無法復原。如果刪除 KMS 金鑰，在該金鑰下仍然加密的資料將永久無法復原。如果您需要保留對資料的存取權，在刪除金鑰之前，您必須解密資料或使用新的 KMS 金鑰重新加密資料。只有當您確定不再需要使用 KMS 金鑰時，才應刪除 KMS 金鑰。

我們建議您設定 Amazon CloudWatch 警示，在有人啟動刪除 KMS 金鑰時通知您。由於刪除 KMS 金鑰具有破壞性且潛在危險，因此 AWS KMS 需要您設定等待期間，並在 7-30 天內刪除排程。這可讓您檢閱排定的刪除，並視需要將其取消。

如需詳細資訊，請參閱下列資源：

- 排程和取消文件中的金鑰刪除 AWS KMS
- 建立警示，以偵測文件中是否使用待刪除的 KMS 金鑰 AWS KMS
- AWS KMS keys 不應在 Security Hub 文件中意外刪除

# 封鎖對 的公開存取 AWS KMS keys

金鑰政策是控制 存取的主要方式 AWS KMS keys。每個 KMS 金鑰只有一個金鑰政策。允許匿名存取 KMS 金鑰可能會導致敏感資料洩露。我們建議您識別任何可公開存取的 KMS 金鑰並更新其存取政策，以防止對這些資源提出未簽署的請求。

如需詳細資訊，請參閱下列資源：

- AWS KMS 文件中的 安全最佳實務 AWS Key Management Service
- 變更文件中的金鑰政策 AWS KMS
- 在 文件中判斷對 的存取權 AWS KMS keys AWS KMS

## 設定負載平衡器接聽程式以使用安全通訊協定

Elastic Load Balancing 會自動將傳入的應用程式流量分散到多個目標。您可以指定一或多個接聽程式，以將負載平衡器設定為接受傳入流量。接聽程式是檢查連線請求的程序，必須使用您已設定的通訊協定與連接埠。每種類型的負載平衡器都支援不同的通訊協定和連接埠：

- Application Load Balancer 在應用程式層進行路由決策，並使用 HTTP 或 HTTPS 通訊協定。
- Network Load Balancer 在傳輸層做出路由決策，並使用 TCP、TLS、UDP 或 TCP_UDP 通訊協定。
- Classic Load Balancer 會在傳輸層 （ 使用 TCP 或 SSL 通訊協定 ） 或應用程式層 （ 使用 HTTP 或 HTTPS 通訊協定 ） 進行路由決策。

我們建議您一律使用 HTTPS 或 TLS 通訊協定。這些通訊協定可確保負載平衡器負責加密和解密用戶端與目標之間的流量。

如需詳細資訊，請參閱下列資源：

- Elastic Load Balancing 文件中的 Application Load Balancer 接聽程式
- Elastic Load Balancing 文件中的 Classic Load Balancer 接聽程式
- Elastic Load Balancing 文件中的 Network Load Balancer 接聽程式
- 確保 規範指引中的 AWS 負載平衡器使用安全接聽程式通訊協定 AWS
- AWS Config 文件中的 elb-tls-https-listeners-only
- 在 Security Hub 文件中，Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定
- Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 Security Hub 文件中的 HTTPS

# 回應事件的安全建議

當您的組織發生安全事件時，您的使用者必須準備好回應問題。所有使用者都應對組織的安全回應程序有基本的了解。規劃、訓練和經驗對於成功的事件回應計畫至關重要。理想情況下，您會在潛在安全事件發生之前準備您的組織。 AWS Well-Architected Framework 識別雲端中成功事件回應計劃所需的三個基礎：準備、操作和事件後活動。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的AWS 事件回應層面。

除了通知您事件或自動回應事件的安全控制之外，您可以為事件回應建立有限的控制。強大的事件回應狀態主要是透過您在組織中使用的計劃、程序、執行手冊、手冊和訓練計劃來建立。您可以使用本節中的控制項和建議，為您的事件回應計劃實作最佳實務。如需事件回應和實作指引之最佳實務的詳細資訊，請參閱 AWS Well-Architected Framework 中的事件回應。

本節的建議：

- 定義事件回應計劃
- 建立和維護事件回應 Runbook 和程序手冊
- 實作事件驅動型安全自動化
- 記錄營運團隊應如何與 互動 支援
- 設定安全事件的提醒

## 定義事件回應計劃

建立明確定義的事件回應計畫 (IRP)。事件回應計畫旨在成為事件回應計畫的基礎。必須自訂此計畫，以滿足每個組織的需求。

如需詳細資訊，請參閱下列資源：

- AWS 《安全事件回應指南》中的開發和測試事件回應計劃
- 在 AWS Well-Architected Framework 中制定事件管理計劃
- 識別 Well-Architected Framework 中的關鍵人員和外部資源 AWS

## 建立和維護事件回應 Runbook 和程序手冊

準備事件回應程序的關鍵部分是開發程序手冊。事件回應程序手冊提供使用者在發生安全事件時遵循的一系列建議步驟。擁有清晰的結構和步驟可簡化回應，並降低發生人為錯誤的可能性。

如需詳細資訊，請參閱下列資源：

- AWS 安全事件回應指南中的建立 手冊的內容
- 上的AWS 事件回應程序手冊範例 GitHub
- 在 AWS Well-Architected Framework 中開發和測試安全事件回應手冊

## 實作事件驅動型安全自動化

安全回應自動化是一種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 執行個體或輪換登入資料。

許多 AWS 服務 支援自動回應。例如，您可以為特定指標設定 Amazon CloudWatch 警示，而警示可以在警示變更狀態時啟動動作。透過 Amazon EventBridge，您也可以為 和 Amazon Inspector 中的調查結果設定自動回應 AWS Security Hub 和修復。

如需詳細資訊，請參閱下列資源：

- 安全部落格中的 AWS 自動修復 Amazon Inspector 安全性問題清單
- 安全部落格中的在 上開始使用安全回應自動化 AWS AWS
- AWS 解決方案程式庫中的 上的自動化安全回應 AWS
- CloudWatch 文件中的使用 Amazon CloudWatch 警示 CloudWatch
- Security Hub 文件中的自動化回應和修復
- Amazon Inspector 文件中的使用 Amazon EventBridge 建立對 Amazon Inspector 調查結果的自訂回應 Amazon Inspector

## 記錄營運團隊應如何與 互動 支援

對於您的 AWS 帳戶，您可以定義主要聯絡人和三個替代聯絡人。我們建議您為每個 AWS 帳戶 或組織提供安全聯絡人。

AWS 支援 提供各種計劃，可讓您存取工具和專業知識，以支援 AWS 解決方案的成功和營運運作狀態。此外，請考慮您的組織是否會受益於使用 AWS Managed Services 而非 支援 計劃。 AWS Managed Services (AMS) 提供持續的 AWS 基礎設施管理，包括監控、事件管理、安全指導、修補程式支援和 AWS 工作負載備份，協助您更有效率且安全地操作。AMS 支援模型可能更適合雲端營運團

隊資源有限的組織。我們建議您比較這些模型和計劃，以選擇最適合您組織的使用案例和雲端成熟度層級。

如需詳細資訊，請參閱下列資源：

- 了解 安全事件AWS 回應指南中的回應團隊和支援 AWS
- 在AWS 帳戶管理指南中更新 的替代聯絡人 AWS 帳戶
- 比較 支援 網站上的 Plans AWS
- AWS 規範指引中AWS Managed Services 用於實現目標業務成果的策略

## 設定安全事件的提醒

偵測異常與實作來控制該異常的措施一樣重要。提醒是偵測階段的主要元件。它會產生通知，根據感興趣的 AWS 帳戶 活動啟動事件回應程序。確保提醒包含團隊採取動作的相關資訊。

如需詳細資訊，請參閱下列資源：

- AWS 安全事件回應指南中的偵測
- 在 AWS Well-Architected 架構中準備鑑識功能
- 在 AWS Well-Architected 架構中實作可行的安全事件

# 後續步驟

當您繼續雲端旅程時，請務必套用這些記錄的控制、指導和修補選項。這些建議有助於改善您的雲端安全狀態，並協助您滿足 中所定義的安全責任 AWS 雲端，如 AWS 共同責任模型中所定義。

針對後續步驟，我們建議執行下列動作：

- 如需有關最佳實務和實作指引的詳細資訊，請檢閱 AWS Well-Architected Framework 的六個支柱。
- 對於 AWS 服務 您的組織使用的 ，請檢閱可用AWS Security Hub 控制項的清單，並評估您是否應該在您的環境中啟用任何這些控制項。
- 對於 AWS 服務 您的組織使用的 ，請檢閱可用的AWS Config 受管規則清單，並評估您是否應該在您的環境中啟用任何這些規則。

# 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 |
| --- | --- | --- |
| 根使用者的 MFA | 我們已更新建議，並在根使用者的 MFA 區段中提供詳細資訊。 | 2023 年 11 月 9 日 |
| 初次出版 | — | 2023 年 10 月 27 日 |

# AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。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：將您的現場部署 Oracle 資料庫遷移至 Amazon Aurora PostgreSQL 相容版本。
- 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：將您的現場部署 Oracle 資料庫遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle 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：將您的現場部署 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到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 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

請參閱原子性、一致性、隔離性、耐久性。

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-被動遷移需要更多的工作。

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

在一組資料列上運作的 SQL 函數，會計算群組的單一傳回值。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

經常用於重複性問題的解決方案，其中解決方案具有反生產力、無效或比替代解決方案更有效。

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攻擊。

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 (AIOps)

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。如需有關如何在 AWS 遷移策略中使用 AIOps 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。

原子性、一致性、隔離性、耐久性 (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》中的 ABAC for AWS。

授權資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線。

AWS 雲端採用架構 (AWS CAF)

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、安全和營運。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。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。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)

一種工具，可評估資料庫遷移工作負載、建議遷移策略，並提供工作預估值。 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。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。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 Endianness。

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。此策略可協助您快速復原，並將影響降至最低。

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。有些機器人有用或有益，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。有些其他機器人稱為惡意機器人，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受單一方控制之機器人的網路，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，讓使用者能夠快速存取他們通常無權存取 AWS 帳戶 的 。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

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

版本對最終使用者的緩慢和增量版本。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。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，為您的 AWS 工作負載帶來壓力，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。

雲端卓越中心 (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、建立營運模型)

- 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 於部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略相關的詳細資訊，請參閱遷移整備指南。

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。程式碼的每個版本都稱為分支。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

很少存取且通常是歷史資料的資料。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影像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如，Amazon SageMaker AI 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。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。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)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。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。

# 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更。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，提供分散式、分散式資料擁有權與集中式管理。

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 上建置資料周邊 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

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

資料主體

正在收集和處理其資料的個人。

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。

資料庫處理語言 (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。

深度防禦

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，defense-in-depth方法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，以管理組織的帳戶和管理該服務的許可。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)

一種程序，用於識別對軟體開發生命週期中的速度和品質造成負面影響的限制並排定優先順序。DVSM 延伸了原本專為精簡製造實務設計的價值串流映射程序。它著重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呈現，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

在星星結構描述中，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，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

防止工作負載或系統在其主要部署位置中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，例如意外設定錯誤或惡意軟體攻擊。

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 上工作負載災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

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。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，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。

偏離偵測

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偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 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。

EDI

請參閱電子資料交換。

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改善回應時間。

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

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) 委託人。這些帳戶或主體可以透過建立介面 VPC 端點私下連接至您的端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud (Amazon VPC) 文件中的建立端點服務。

企業資源規劃 (ERP)

一種系統，可自動化和管理企業的關鍵業務流程 （例如會計、MES 和專案管理）。

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 安全概念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。透過計算摘要統計並建立資料可視化來執行 EDA。

# 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：包含度量的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

一種使用頻繁和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，像是可用區域 AWS 區域、控制平面或資料平面等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。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 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。

少量擷取提示

在要求 LLM 執行類似的任務之前，提供少量示範任務和所需輸出的範例。此技術是內容內學習的應用程式，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式、推理或網域知識的任務，少量的提示非常有效。另請參閱零鏡頭提示。

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，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及以自然語言交談。如需詳細資訊，請參閱什麼是基礎模型。

# G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，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 工作流程會被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於提高裝置製造操作的速度、可擴展性和生產力。

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

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。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。它們是透過使用 AWS Config AWS Security Hub、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

# 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)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，並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

一種方法，用於現代化和升級操作技術 (OT) 系統，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠中的各種來源收集和存放資料。

保留資料

從用於訓練機器學習模型的資料集中保留的部分歷史標記資料。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的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 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。

熱資料

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，通常會在典型 DevOps 發行工作流程之外執行修補程式。

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。

## I

IaC

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，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。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、修補或修改現有的基礎設施。不可變基礎設施本質上比可變基礎設施更一致、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 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，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

2016 年 Klaus Schwab 推出的術語，透過連線能力、即時資料、自動化、分析和 AI/ML 的進展，指製造程序的現代化。

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，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC 可管理 VPCs 之間 （在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，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 的機器學習模型可解譯性 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 為 ITSM 提供了基礎。

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。如需有關將雲端操作與 ITSM 工具整合的資訊，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獲得明確指派的安全標籤值。使用者安全標籤和資料安全標籤之間的交集會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。

大型語言模型 (LLM)

預先訓練大量資料的深度學習 AI 模型。LLM 可以執行多個任務，例如回答問題、摘要文件、將文字翻譯成其他語言，以及完成句子。如需詳細資訊，請參閱什麼是 LLMs。

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 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

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、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會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)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

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。機制是在操作時強化和改善自身的循環。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。

製造執行系統

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

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。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 API，透過明確定義的介面進行通訊。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)

一種 AWS 計畫，提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於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營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 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：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、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，以及波次規劃)。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。

遷移準備程度評定 (MRA)

使用 AWS CAF 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。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱此詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

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《》中的現代化應用程式的策略 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 建議使用不可變基礎設施做為最佳實務。

# 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

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

用於工業自動化的machine-to-machine(M2M) 通訊協定。OPC-UA 提供資料加密、身分驗證和授權機制的互通性標準。

操作水準協議 (OLA)

一份協議，闡明 IT 職能群組承諾向彼此提供的內容，以支援服務水準協議 (SLA)。

操作整備審查 (ORR)

問題和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 中的操作準備度審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造業中，整合 OT 和資訊技術 (IT) 系統是工業 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 建立的線索 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的所有事件 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 CloudTrail 文件中的建立組織追蹤。

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 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

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

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，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

附接至 IAM 主體的 IAM 管理政策，可設定使用者或角色擁有的最大許可。如需詳細資訊，請參閱 IAM 文件中的許可界限。

個人身分識別資訊 (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。PII 的範例包括名稱、地址和聯絡資訊。

PII

請參閱個人身分識別資訊。

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

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

可定義許可的物件（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）。

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。

依設計的隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。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。這些控制項會在佈建資源之前對其進行掃描。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，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

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

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。

提示鏈結

使用一個 LLM 提示的輸出做為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符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。

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以提高可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。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、諮詢、告知 (RACI)。

RAG

請參閱擷取增強產生。

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、諮詢、告知 (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 個 R。

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)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

地理區域中的 AWS 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 您的帳戶可以使用哪些 。

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 個 R。

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 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

應用程式抵禦中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

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。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

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。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，如果您排除它，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 個 R。

淘汰

請參閱 7 Rs。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

**輪換**

定期更新秘密的程序，讓攻擊者更難存取登入資料。

**資料列和資料欄存取控制 (RCAC)**

使用已定義存取規則的基本、彈性 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 (IdP) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

**SCADA**

請參閱監督控制和資料擷取。

**SCP**

請參閱服務控制政策。

**秘密**

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。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 秘密中的什麼內容？。

依設計的安全性

透過整個開發程序將安全性納入考量的系統工程方法。

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、回應性和主動性。

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。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。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，並產生提醒。

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 執行個體或輪換登入資料。

伺服器端加密

由 AWS 服務 接收資料的 在其目的地加密資料。

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。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。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

的進入點 URL 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。

服務水準協議 (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。

單點故障 (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

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

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

請參閱單一故障點。

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。此結構旨在用於資料倉儲或商業智慧用途。

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。如需有關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

您 VPC 中的 IP 地址範圍。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。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

# T

標籤

做為中繼資料以組織 AWS 資源的鍵值對。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

可以用於互連 VPC 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 AWS Organizations 及其帳戶中執行任務。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 搭配使用 AWS Organizations 與其他 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

兩個比薩就能吃飽的小型 DevOps 團隊。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

也稱為繁重工作，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 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危及系統安全性的軟體或硬體瑕疵。

# 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，通常可接受中等緩慢的查詢。

視窗函數

SQL 函數，對與目前記錄在某種程度上相關的資料列群組執行計算。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，然後再遷移伺服器和應用程式。

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)

儲存模型，可一次性寫入資料，並防止資料遭到刪除或修改。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。

# Z

零時差入侵

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瑕疵或漏洞。威脅行為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。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 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。