在 上實作安全控制 AWS

AWS 方案指引

AWS 方案指引: 在 上實作安全控制 AWS

Table of Contents

在 上實作安全控制 AWS

Iqbal Umair、Gurpreet Kaur Cheema、Wasim Hossain、Joseph Nguyen、San Brar 和 Lucia Vanta，Amazon Web Services (AWS)

2023 年 12 月 (文件歷史記錄)

安全對每家公司都至關重要，而且是 AWS Well-Architected Framework 中的關鍵支柱。但是，許多人不知道如何遵循安全考量事項進行操作並為雲端環境建立全面的自動化安全測試和修復策略。透過使用 AWS 服務 和 工具 AWS Config，例如 Amazon GuardDuty AWS CloudFormation，您可以建立安全測試策略並將其建置到您的 AWS 雲端 環境。

為了協助符合公司的安全政策和標準，安全控制是技術或管理防護機制，有助於防止、偵測或降低威脅執行者利用安全漏洞的能力。其旨在保護資源和資料的機密性、完整性和可用性。以下是安全控制的範例：

- 為需要登入應用程式的使用者實作多重要素驗證
- 記錄、監控和查詢動作，以便對帳戶活動執行即時稽核
- 確保敏感資料已加密
- 確保根據公司的保留政策儲存日誌

安全控制有四種類型：預防性、主動性、偵測性以及回應式。本指南更詳細地描述了每種類型，並重點介紹如何在 AWS 雲端中實作和自動化這些控制。本指南可協助您實作持續且主動的安全控制。

目標對象

本指南面向負責在 AWS 雲端中實作安全控制的架構師和安全工程師。如果您的公司尚未定義安全政策、控制目標或標準 (如 控管架構中的安全控制 所述)，我們建議您在繼續本指南之前完成這些控管任務。

目標業務成果

公司使用安全控制來減輕 IT 系統風險或作為針對此風險的對策。控制定義了滿足 IT 程式及其安全策略的主要安全目標的要求基準。適當的控制可透過保護資料和 IT 資產的機密性、完整性和可用性，來改善公司的安全狀態。如果沒有控制，就很難知道需要在哪裡關注和投資來建立安全基準。

安全控制可用於解決各種情況。範例包括滿足源自於風險評定的要求、達到產業標準或遵守法規。滿足安全控制表明您已衡量系統的風險，確定了所需的保護層級，並主動實作了解決方案。其他因素 (例如業務、產業和地理位置) 都可以決定您所需的安全控制。

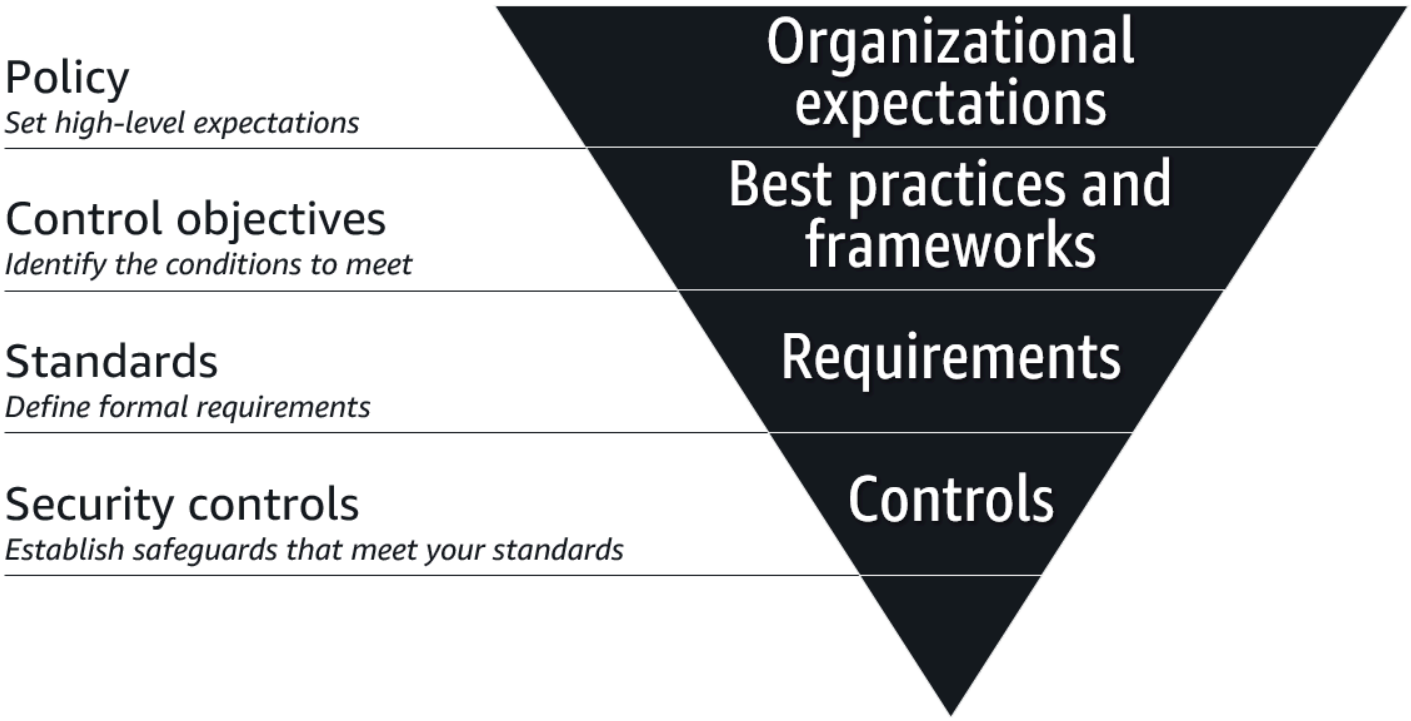
以下是實作安全控制的常見使用案例：

- 應用程式的安全評定已根據正在處理的資料敏感性識別存取控制的需求。
- 您必須遵守安全標準，例如支付卡產業資料安全標準 (PCI DSS)、HIPAA (美國健康保險流通與責任法案) 或國家標準技術研究所 (NIST)。
- 您需要保護商業交易的敏感資訊。
- 您的公司已擴展到需要安全控制的地理區域，例如需要遵守一般資料保護規範 (GDPR) 的區域。

閱讀本指南後，您應熟悉四種類型的安全控制，了解其如何成為安全控管架構的一部分，並準備好開始在 AWS 雲端中實作和自動化安全控制。

控管架構中的安全控制

從基礎層面進行規劃非常重要。如何開始？ 下圖顯示如何根據政策、控制目標、標準和安全控制建置安全控管策略。



以下是安全控管策略的階層元件：

- 政策 – 政策是任何網路安全控管策略的基礎。它是一份說明公司預期 (例如必須履行的法定、法規或合約義務) 的文件。政策可能因產業和區域而異。
- 控制目標 – 控制目標是可協助您符合政策意圖的目標，例如業界認可的最佳實務。對於雲端運算，許多公司採用雲端控制矩陣 (CCM) (雲端安全聯盟網站)，這是網路安全控制目標的架構。
- 標準 – 標準是滿足控制目標的正式制定的要求。標準可能包括程序、動作或組態，並且可量化，以便您可以根據標準衡量效能。
- 安全控制 – 安全控制是您為實作標準所採取的技術或管理機制。所有安全控制都映射至標準，但並非所有標準都映射至安全控制。安全控制測試旨在監控和衡量您是否有效地滿足定義的標準。

本指南重點介紹如何在 AWS 雲端中設計和實作常見類型的安全控制。

安全控制的類型

安全控制有以下四種主要類型：

- 預防性控制 – 這些控制旨在防止事件發生。
- 主動性控制 – 這些控制旨在防止建立不合規的資源。
- 偵測性控制 – 這些控制旨在事件發生後偵測、記錄和提醒。
- 回應性控制 – 這些控制旨在驅動不良事件或偏離安全基準的補救措施。

有效的安全策略包括所有四種類型的安全控制。雖然預防性控制是協助防止未經授權的存取或對網路進行不必要變更的第一道防線，但請務必確保建立偵測性和回應性控制，以便您知道事件何時發生，且可以立即採取適當的措施進行修復。使用主動性控制可增加另一層安全性，因為它補充了預防性控制，而預防性控制通常在本質上更嚴格。

以下章節更詳細地描述了每種類型的控制。討論了每種控制類型的目標、實作程序、使用案例、技術考量事項和目標結果。

預防性控制

預防性控制旨在防止事件發生的安全控制。這些防護機制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。預防性控制的範例是具有唯讀存取權的 AWS Identity and Access Management (IAM) 角色，因為它有助於防止未經授權的使用者執行意外的寫入動作。

檢閱下列有關此類型控制的資訊：

- 目標
- 流程
- 使用案例
- 技術
- 業務成果

目標

預防性控制的主要目的是最大限度地減少或避免威脅事件發生的可能性。此控制應有助於防止未經授權存取系統，並有助於防止意外的變更影響系統。以下是預防性控制的目標：

- 職責分離 – 預防性控制可以建立限制權限的邏輯界限，允許許可僅在指定帳戶或環境中執行特定任務。範例包括：
  - 將工作負載分段至特定服務的不同帳戶
  - 分隔並考慮獨立的生產、開發和測試環境
  - 將存取權和責任委派給多個實體以執行特定功能，例如使用 IAM 角色或擔任的角色以僅允許特定的工作職能執行某些動作
- 存取控制 – 預防性控制可以一致地授予或拒絕對環境中資源和資料的存取。範例包括：
  - 防止使用者超出預期許可，稱為權限提升
  - 僅限授權使用者和服務存取應用程式和資料
  - 保持管理員群組較小
  - 避免使用根使用者憑證
- 強制執行 – 預防性控制可以協助您的公司遵守其政策、指引和標準。範例包括：
  - 作為最低安全基準的鎖定組態
  - 實作其他安全措施，例如多重要素驗證
  - 避免由未經核准的角色執行的非標準任務和動作

流程

預防性控制映射是將控制映射至需求並使用政策透過限制、停用或封鎖來實作這些控制的程序。在映射控制時，考慮控制對環境、資源和使用者的主動影響。以下是映射控制的最佳實務：

- 禁止某項活動的嚴格控制應該映射至該動作需要審核、核准和變更程序的生產環境。
- 開發或封閉環境可能需要較少的預防性控制才能提供建置和測試的敏捷性。
- 資料的分類、資產的風險層級和風險管理政策決定了預防性控制。
- 映射至現有架構作為遵守標準和法規的證據。
- 依地理位置、環境、帳戶、網路、使用者、角色或資源實作預防性控制。

使用案例

標籤處理

建立可以存取帳戶中的所有資料的角色。如果存在敏感的加密資料，過度寬鬆的權限可能會帶來風險，這取決於可以擔任該角色的使用者或群組。透過在 AWS Key Management Service (AWS KMS) 中使用金鑰政策，您可以控制誰可以存取金鑰並解密資料。

權限提升

如果管理和寫入許可指派得太寬泛，則使用者可以規避其預期許可的限制並授予自己其他權限。建立和管理角色的使用者可以指派許可界限，該界限定義了角色允許的最大權限。

工作負載鎖定

如果您的企業沒有使用特定服務的可預見需求，請啟用服務控制政策，以限制哪些服務可以在組織的成員帳戶中操作，或根據 限制服務 AWS 區域。如果威脅行為者設法洩露和存取您組織中的帳戶，此預防性控制可以減少影響範圍。如需詳細資訊，請參閱本指南中的 服務控制政策。

對其他應用程式的影響

預防性控制可以強制使用 IAM、加密和日誌記錄等服務和功能，以符合應用程式的安全要求。您也可以使用這些控制來限制威脅行為者因意外錯誤或組態錯誤而可能利用的操作，從而協助防範漏洞。

技術

服務控制政策

在 中 AWS Organizations，服務控制政策 SCPs) 會定義組織中成員帳戶的最大可用許可。這些政策可協助帳戶遵守組織的存取控制指導方針。為您的組織設計 SCP 時，請注意下列事項：

- SCPs是預防性的控制，因為它們定義和強制執行組織成員帳戶中 IAM 角色和使用者的允許許可上限。
- SCPs只會影響組織成員帳戶中的 IAM 角色和使用者。它不會影響組織管理帳戶中的使用者和角色。

您可以透過定義每個 AWS 區域的許可上限來使 SCP 更加精細。

IAM 許可界限

在 AWS Identity and Access Management (IAM) 中，許可界限用於設定身分型政策可授予 IAM 實體（使用者或角色）的最大許可。實體的許可界限可讓其僅執行由身分型政策和許可界限同時允許的動作。使用許可界限時，請注意下列事項：

- 您可以使用 AWS 受管政策或客戶受管政策來設定 IAM 實體的界限。
- 許可界限不會自行授予許可。許可界限政策會限制授予 IAM 實體的許可。

業務成果

節省時間

- 透過在設定預防性控制後新增自動化，您可以減少手動介入需求並降低錯誤頻率。
- 使用許可界限作為預防性控制有助於安全和 IAM 團隊專注於關鍵任務，例如控管和支援。

法規合規

- 公司可能需要遵守內部或產業法規。這些可以是區域限制、使用者和角色限制或服務限制。SCP 可以協助您保持合規並避免違規處罰。

降低風險

- 隨著成長，建立和管理新角色和政策的請求數量也會增加。了解為每個應用程式手動建立許可所需的內容變得更具挑戰性。建立預防性控制作為基準，有助於防止使用者執行意外動作，即使他們意外取得存取權亦如此。
- 將預防性控制套用至存取政策提供了額外層來協助保護資料和資產。

主動性控制

主動控制是旨在防止建立不合規資源的安全控制。這些控制可以減少回應式和偵測性控制處理的安全事件數量。這些控制可確保已部署的資源在部署之前符合要求；因此，不存在需要回應或修復的偵測事件。

例如，您可能具有一個偵測性控制，當 Amazon Simple Storage Service (Amazon S3) 儲存貯體變成可公開存取時通知您。您也可能具有可修復此問題的回應式控制。雖然您已具有這兩個控制，但是可以新增主動性控制來多加一道保護。透過 AWS CloudFormation，主動控制可以防止建立任何已啟用公有存取的 S3 儲存貯體。威脅執行者仍然可以繞過此控制，並在 CloudFormation 之外部署或修改資源。在這種情況下，偵測性和回應式控制將修復安全事件。

檢閱下列有關此類型控制的資訊：

- 目標
- 流程
- 使用案例
- 技術

- 業務成果

目標

- 主動性控制可協助您改進安全操作和品質程序。
- 主動性控制可以協助您遵守安全政策、標準，以及法規或合規義務。
- 主動性控制可以防止建立不合規資源。
- 主動性控制可以減少安全調查結果的數量。
- 主動性控制提供了另一層保護，防止威脅執行者繞過預防性控制並嘗試部署不合規資源。
- 主動性控制與預防性、偵測性和回應式控制相結合，可以協助您解決潛在的安全事件。

流程

主動性控制可補充預防性控制。主動性控制可降低組織的安全風險，並強制部署合規資源。這些控制會在建立或更新資源之前評估資源合規性。主動性控制通常透過使用 CloudFormation 勾點來實作。如果資源未通過主動性控制驗證，您可以選擇使資源部署失敗或顯示警告訊息。以下是建置主動性控制的一些秘訣和最佳實務：

- 確保主動性控制已映射至組織的合規要求。
- 確保主動性控制遵循關聯服務的安全最佳實務。
- 使用 CloudFormation StackSets 或其他解決方案，在多個 AWS 區域 或 帳戶中部署主動控制。
- 確保與主動性控制關聯的警告或失敗訊息明確且清晰。這可協助開發人員了解資源未通過評估的原因。
- 建置新的主動式控制項時，在觀察模式下啟動。這表示您傳送警告訊息，而非使資源部署失敗。這可協助您了解主動性控制的影響。
- 在 Amazon CloudWatch Logs 中啟用日誌記錄以進行主動性控制。
- 如果您需要監控特定主動性控制的調用，請使用 Amazon EventBridge 規則並訂閱 CloudFormation 勾點的調用事件。

使用案例

- 防止部署不合規資源
- 符合合規要求

- 透過在部署之前強制修復安全問題來提高程式碼品質
- 減少部署之後與修復安全問題關聯的營運停機時間

技術

CloudFormation 勾點

AWS CloudFormation 可協助您設定 AWS 資源、快速且一致地佈建資源，以及在整個 AWS 帳戶 和區域的生命週期中管理資源。CloudFormation 勾點會在部署資源之前，主動評估 CloudFormation 資源的組態。如果找到不合規資源，則會傳回失敗狀態。根據勾點失敗模式，CloudFormation 可能會使操作失敗或顯示警告，以允許使用者繼續部署。您可以使用可用的勾點，也可以開發自己的勾點。

AWS Control Tower

AWS Control Tower 可協助您設定和管理 AWS 多帳戶環境，遵循規範最佳實務。 AWS Control Tower 提供預先設定的主動控制，您可以在登陸區域中啟用這些控制。如果您的登陸區域是使用 設定 AWS Control Tower，您可以使用這些選用的主動控制做為組織的起點。您可以視需要在 CloudFormation 中建置額外的自訂主動性控制。

業務成果

減少人工和錯誤

主動性控制可降低導致部署不合規資源的人為錯誤風險。這些控制還可減少開發週期後期的人工，因為它們使開發人員在部署之前考慮資源安全性。這將左移實務套用於建置安全資源，因為它強制在開發生命週期的早期實現合規性。

降低了成本

在部署之後修正安全問題通常成本較高。在開發週期的早期識別並修正問題可降低開發成本。

節省時間

由於主動性控制可防止部署不合規資源，因此可以減少您用於分類和修正安全問題的時長。它們還包括安全調查結果的數量，偵測性控制將在開發週期後期識別這些安全調查結果。

法規合規

如果您的組織需要遵守內部或產業法規，主動性控制可以協助您保持合規並避免違規處罰。

降低風險

主動性控制可協助開發人員部署合規並更安全地建置資源，因此主動性控制可降低組織的安全風險。

偵測性控制

偵測性控制是安全控制，旨在事件發生後偵測、記錄和提醒。偵測性控制是控管架構的基礎部分。這些防護機制是第二道防線，通知您繞過預防性控制的安全問題。

例如，您可以套用偵測性控制來偵測 Amazon Simple Storage Service (Amazon S3) 儲存貯體是否可公開存取並通知您。雖然您可能已採取預防性控制，在帳戶層級停用對 S3 儲存貯體的公開存取，然後停用透過 SCP 的存取，但威脅行為者可以透過以管理使用者身分登入來規避這些預防性控制。在這些情況下，偵測性控制可以提醒您組態錯誤和潛在威脅。

檢閱下列有關此類型控制的資訊：

- 目標
- 流程
- 使用案例
- 技術
- 業務成果

目標

- 偵測性控制可協助您改進安全操作程序和品質程序。
- 偵測性控制可協助您履行法規、法律或合規義務。
- 偵測性控制為安全營運團隊提供了回應安全問題的可見性，包括繞過預防性控制的進階威脅。
- 偵測性控制可以協助您識別對安全問題和潛在威脅的適當回應。

流程

您可以分兩個階段實作偵測性控制。首先，您將系統設定為將事件和資源狀態記錄至集中位置，例如 Amazon CloudWatch Logs。集中式日誌記錄到位後，您可以分析這些日誌以偵測可能表示威脅的異常狀況。每個分析都是一個映射回您的原始需求和政策的控制。例如，您可以建立偵測性控制，以在日誌中搜尋特定模式，並在符合時產生提醒。安全團隊使用偵測性控制來提高對系統可能面臨的威脅和風險的整體可見性。

使用案例

偵測可疑行為

偵測性控制有助於識別任何異常活動，例如洩露特權使用者憑證或者存取或外洩敏感資料。這些控制是重要的反應因素，可以協助您的公司識別和了解異常活動的範圍。

偵測詐欺

這些控制有助於偵測和識別公司內部的威脅，例如規避政策和執行未經授權的交易的使用者。

合規

偵測性控制可協助您符合合規要求，例如支付卡產業資料安全標準 (PCI DSS)，並有助於防止身分盜用。這些控制可以協助您探索和保護受法規合規約束的敏感資訊，例如個人身分識別資訊。

自動化分析

偵測性控制可以自動分析日誌以偵測異常狀況和未經授權活動的其他指標。

您可以自動分析來自不同來源的日誌 (例如 AWS CloudTrail 日誌、VPC 流程日誌和網域名稱系統 (DNS) 日誌)，以發現潛在惡意活動的跡象。為了協助處理組織，請將多個 的安全提醒或問題清單彙總 AWS 服務 到集中位置。

技術

常見的偵測性控制是實作一或多個監控服務，這些服務可以分析資料來源 (例如日誌) 以識別安全威脅。在 中 AWS 雲端，您可以分析 AWS CloudTrail 日誌、Amazon S3 存取日誌和 Amazon Virtual Private Cloud 流量日誌等來源，以協助偵測異常活動。 AWS Amazon GuardDuty、Amazon Detective AWS Security Hub CSPM和 Amazon Macie 等安全服務具有內建的監控功能。

GuardDuty 和 Security Hub

Amazon GuardDuty 使用威脅情報、機器學習和異常偵測技術來持續監控您的日誌來源是否有惡意或未經授權的活動。儀表板可讓您深入了解 AWS 帳戶 和 工作負載的即時運作狀態。您可以將 GuardDuty 與 AWS Security Hub CSPM 整合，後者是一種雲端安全狀態管理服務，可檢查是否遵守最佳實務、彙總提醒並啟用自動修復。GuardDuty 會將調查結果傳送至 Security Hub，作為集中資訊的一種方式。您可以進一步將 Security Hub 與安全資訊和事件管理 (SIEM) 解決方案整合，以擴展組織的監控和提醒功能。

Macie

Amazon Macie 是一種全受管資料安全和資料隱私權服務，該服務使用機器學習和模式比對來協助探索和保護 AWS中的敏感資料。以下是 Macie 中提供的一些偵測性控制和功能：

- Macie 會檢查儲存貯體庫存和儲存在 Amazon S3 中的所有物件。此資訊可以在單一儀表板檢視中呈現，提供可見性並協助您評估儲存貯體安全性。
- 為了探索敏感資料，Macie 使用內建的受管資料識別符，並且還支援自訂資料識別符。
- Macie 原生整合了其他 AWS 服務 和 工具。例如，Macie 將調查結果作為 Amazon EventBridge 事件發佈，這些事件會自動傳送至 Security Hub。

以下是在 Macie 中設定偵測性控制的最佳實務：

- 在所有帳戶上啟用 Macie。透過使用委派的管理功能，使用 AWS Organizations在多個帳戶上啟用 Macie。
- 使用 Macie 評估您帳戶中 S3 儲存貯體的安全狀態。這有助於透過提供資料位置和存取的可見性來防止資料遺失。如需詳細資訊，請參閱分析您的 Amazon S3 安全狀態 (Macie 文件)。
- 透過執行和排程自動處理和資料探索作業，自動探索 S3 儲存貯體中的敏感資料。這會定期檢查 S3 儲存貯體中是否有敏感資料。

AWS Config

AWS Config 稽核並記錄 AWS 資源的合規性。 AWS Config 會探索現有 AWS 資源並產生完整的庫存，以及每個資源的組態詳細資訊。如果存在任何組態變更，則會記錄這些變更並提供通知。這可以協助您偵測並復原未經授權的基礎設施變更。您可以使用 AWS 受管規則，也可以建立自訂規則。

以下是在 AWS Config中設定偵測性控制的最佳實務：

- AWS Config 為組織中的每個成員帳戶和包含您要保護之資源 AWS 區域 的每個帳戶啟用 。
- 針對任何組態變更，設定 Amazon Simple Notification Service (Amazon SNS) 提醒。
- 將組態資料儲存在 S3 儲存貯體中，並使用 Amazon Athena 進行分析。
- 使用自動化 (AWS Systems Manager的一項功能) 來自動修復不合規資源。
- 使用 EventBridge 或 Amazon SNS 設定有關不合規 AWS 資源的通知。

Trusted Advisor

AWS Trusted Advisor 可以用作偵測性控制的服務。透過一組檢查， Trusted Advisor 識別您可以最佳化基礎設施、改善效能和安全性或降低成本的領域。 Trusted Advisor 會根據您可以遵循的 AWS 最佳實務提供建議，以改善您的服務和資源。商業和企業支援計劃可讓您存取 AWS Well-Architected Framework 支柱的所有可用檢查。

以下是在 Trusted Advisor中設定偵測性控制的最佳實務：

- 檢閱檢查層級摘要
- 針對警告和錯誤狀態實作資源特定的建議。
- Trusted Advisor 經常檢查以主動檢閱和實作其建議。

Amazon Inspector

Amazon Inspector 是一項自動化漏洞管理服務，在啟用之後，可持續掃描您的工作負載，以尋找任何意外的網路暴露或軟體漏洞。它將調查結果融入風險分數中，可以協助您確定後續步驟，例如修復或確認合規狀態。

以下是在 Amazon Inspector 中設定偵測性控制的最佳實務：

- 在所有帳戶上啟用 Amazon Inspector 並將其整合到 EventBridge 和 Security Hub 中，以設定安全漏洞的報告和通知。
- 根據 Amazon Inspector 風險分數，排定修復和其他動作的優先順序。

業務成果

減少人工和錯誤

您可以使用基礎設施即程式碼 (IaC) 來實現自動化。自動化部署、監控組態及修復服務和工具可降低手動錯誤的風險，並減少擴展這些偵測性控制所需的時間和精力。自動化有助於制定安全執行手冊，並減少安全分析師的手動操作。定期審核有助於調整自動化工具並持續反覆運算並改進偵測性控制。

針對潛在威脅採取適當動作

從日誌和指標中擷取和分析事件對於取得可見性至關重要。這有助於分析師針對安全事件和潛在威脅採取行動，以協助保護您的工作負載。可以快速識別存在的漏洞，有助於分析師採取適當的動作來解決和修復這些漏洞。

更好的事件回應和調查處理

自動化偵測性控制工具可以提高偵測、調查和復原的速度。基於定義條件的自動提醒和通知可讓安全分析師適當地調查和回應。這些回應因素可以協助您識別和了解異常活動的範圍。

回應性控制

回應性控制是安全控制，旨在驅動不良事件或偏離安全基準的補救措施。技術回應性控制的範例包括修補系統、隔離病毒、關閉程序或重新啟動系統。

檢閱下列有關此類型控制的資訊：

- 目標
- 流程
- 使用案例
- 技術
- 業務成果

目標

- 回應性控制可以協助您為常見類型的攻擊 (例如網路釣魚或暴力破解) 建立執行手冊。
- 回應性控制可以實作對潛在安全問題的自動回應。
- 回應式控制可以自動修復 AWS 資源上的意外或未經核准的動作，例如刪除未加密的 S3 儲存貯體。
- 回應性控制可以與預防性和偵測性控制進行協調，以建立一種全面、主動的方法來解決潛在的安全事件。

流程

偵測性控制是建立回應性控制的先決條件。您必須能夠偵測安全問題，然後才能進行修復。然後，您可以建立針對安全問題的政策或回應。例如，如果發生暴力攻擊，將實作修復程序。修復程序存在後，可以使用程式設計語言 (例如 Shell 指令碼) 將其自動化並作為腳本執行。

考慮回應性控制是否可能破壞現有的生產工作負載。例如，如果偵測性安全控制是 S3 儲存貯體不得公開存取和修復是關閉 Amazon S3 的公開存取，這可能會對您的公司及其客戶產生重大影響。如果 S3 儲存貯體為公有網站提供服務，則關閉公有存取可能會導致中斷。資料庫是一個類似的範例。如果資料庫不得透過網際網路公開存取，則關閉公開存取可能會影響應用程式的連線。

使用案例

- 自動回應偵測到的安全事件
- 自動修復偵測到的安全漏洞
- 自動復原控制可減少營運停機時間

技術

安全中樞

AWS Security Hub CSPM 會自動將所有新調查結果和現有調查結果的所有更新作為事件傳送至 EventBridge。您也可以建立自訂動作，將選定的調查結果和洞察結果傳送至 EventBridge。您可以設定 EventBridge 來回應每種類型的事件。事件可以啟動執行修復動作的 AWS Lambda 函數。

AWS Config

AWS Config 使用 規則來評估您的 AWS 資源，並協助您修復不合規的資源。 使用AWS Systems Manager 自動化 AWS Config 套用修復。在自動化文件中，您可以定義要在 AWS Config 判定為不合規的資源上執行的動作。建立自動化文件之後，您可以透過 AWS 管理主控台 或使用 APIs，在 Systems Manager 中使用它們。您可以選擇手動或自動修復不符合標準的資源。

業務成果

最大限度地減少資料損失

在網路安全事件發生後，使用回應性安全控制可以協助最大限度地減少資料損失以及對系統或網路的損壞。回應性控制還可以協助盡快還原關鍵業務系統和程序，從而增強工作負載的恢復能力。

降低成本

自動化降低了與人力資源關聯的成本，因為團隊成員不必手動回應事件或根據具體案例進行管理。

後續步驟

閱讀本指南後，您應熟悉四種類型的安全控制，了解其如何成為安全控管架構的一部分，並準備好開始在 AWS 雲端中實作和自動化安全控制。如需詳細資訊，我們建議您檢閱包含在 資源 部分中的參考。

我們也建議您採取下列後續步驟來評估雲端基礎設施的安全性並開始實作安全控制：

1. 啟用和設定 AWS Security Hub CSPM。作為最佳實務，我們建議啟用可用的標準控制。如需詳細資訊，請參閱安全標準和控制 (Security Hub 文件)。
2. 啟用和設定 AWS Config。如需詳細資訊，請參閱入門 (AWS Config 文件）。
3. 使用 Security Hub AWS Config AWS Trusted Advisor、Amazon Macie 和 Amazon Inspector AWS 服務 等功能，評估您的組織和帳戶基礎設施、識別需要改進的領域，以及檢閱這些服務中的 和建議。使用 Security Hub 中的安全檢查功能來產生安全標準的安全分數。如需詳細資訊，請參閱確定安全分數 (Security Hub 文件)。
4. 根據已確定的改進實作預防性、主動性、偵測性和回應性安全控制。
5. 進行後續安全評定，以評估所實作安全控制的有效性。在 Security Hub 中，確定安全分數是否已提升。反覆運算以改進或新增安全控制。
6. 建立執行安全評定的定期頻率，例如每年。

常見問答集

如果我的時間和資源有限且無法實作所有這些控制類型，我應關注什麼？

建議您實作 AWS Security Hub CSPM。Security Hub 具有一組自動化安全控制，稱為 AWS 基礎安全最佳實務標準 (Security Hub 文件)。這是一組由安全專家管理的高度策劃 AWS 的安全最佳實務。您可以在關聯資源發生變更時連續執行這些標準控制，也可以定期執行。每個控制都有特定的嚴重性評分，可協助您排定修正作業的優先順序。如需詳細資訊，請參閱執行安全檢查 (Security Hub 文件)。如果您正在使用 AWS Control Tower，也可以檢閱並選擇啟用其預防性、偵測和主動性控制。

資源

AWS 文件

- AWS 安全參考架構 (AWS SRA)
- AWS CAF 安全觀點
- 安全、身分和合規的最佳實務
- AWS (AWS 解決方案) 上的自動化安全回應
  - 解決方案登陸頁面
  - 實作指南

AWS 部落格文章

- 身分指南 – 使用 AWS 身分的預防性控制 – SCPs
- 如何為 AWS Organizations中的帳戶實作唯讀服務控制政策 (SCP)
- 多帳戶環境中 AWS Organizations 服務控制政策的最佳實務
- 使用服務控制政策維護合規並確保永遠將其套用
- 何時何地使用 IAM 許可界限
- 主動確保資源安全並符合 AWS CloudFormation 勾點要求

其他資源

- 雲端控制矩陣 (CCM) (雲端安全聯盟)
- 許可界限範例 (GitHub)

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
主動性控制	我們在本指南中新增了有關主動性控制的資訊，包括主動性控制部分。	2023 年 12 月 4 日
初次出版	—	2022 年 12 月 12 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：將內部部署 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，但需要比主動-被動遷移更多的工作。

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，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。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

永久刪除資料集中個人資訊的程序。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)

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，例如在網際網路上編製資訊索引的 Web 爬蟲程式。某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

部落格文章中的 Stephen Orban 定義了這些階段： AWS 雲端 企業策略部落格上的邁向雲端優先之旅和採用階段。如需有關它們如何與 AWS 遷移策略關聯的資訊，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)

AI 欄位???，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。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

在整個資料生命週期中追蹤資料的來源和歷史記錄的程序，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。

deployment

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 擴展了最初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 上工作負載的災難復原 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

將人類可讀取的純文字資料轉換為加密文字的運算程序。

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) 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界限會限制故障的影響，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。少量的提示對於需要特定格式、推理或網域知識的任務來說非常有效。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 CSPM、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，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

請參閱基礎設施即程式碼。

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的部署最佳實務。

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。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。

設計隱私權

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

請參閱擷取增強生成。

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

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 個 R。

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 管理主控台 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)

服務效能層面的測量，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。

單一故障點 (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，這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

危害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，通常可接受中等速度的查詢。

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，並防止刪除或修改資料。授權使用者可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。