VMware Cloud on AWS 概觀和操作模型

AWS 規定指引

AWS 規定指引: VMware Cloud on AWS 概觀和操作模型

Table of Contents

簡介 1
概觀 2
遷移挑戰 2
遷移考量事項 3
目標業務成果 3
最佳實務 5
資料庫遷移選項 6
操作模型 7
內部部署操作模型 7
佈建和組態團隊 7
操作運作狀態團隊 7
生命週期管理團隊 8
容量管理團隊 8
可用性和持續性團隊 8
安全團隊 9
BAU 核心 IT 流程團隊 9
BAU 資源管理團隊 9
VMware on AWS 操作模型 10
從您的組織到 VMware 的高層級任務轉換 11
典型的內部部署操作模型 11
VMware on AWS 操作模型 11
VMware Cloud on AWS 操作模型中的高層級責任 12
後續步驟和資源 13
資源 13
文件歷史紀錄 14
詞彙表 15
..... 15
A 15
B 18
C 19
D 21
E 24
F 26
G 27

H 28
I 29
L 31
M 31
O 34
P 36
Q 38
R 38
S 41
T 43
U 45
V 45
W 45
Z 46
..... xlvii

VMware 雲端 AWS 概觀與營運模式

Deepak Kumar 和 Punit Solanki，Amazon Web Services (AWS)

2024 年三月 (文件歷史記錄)

此策略說明遷移至 VMware Cloud on Amazon Web Services (AWS) 的原因 、貴組織為確保轉換順利且有效而採取的步驟、以及支援新雲端環境的操作模型中所需的變更。您的組織可能會在遷移期間遇到數個挑戰。規劃和遵循正確的策略可以協助您實現最佳業務成果。

AWS 為想要在雲端中將程序和系統現代化的組織提供可擴充、可靠、靈活且符合成本效益的雲端環境。VMware Cloud on AWS 支援您在中使用 VMware 虛擬伺服器的工作負載 AWS 雲端，並提供輕鬆存取 AWS 服務，協助您將應用程式現代化。它可讓您的公司在短時間內採用雲端，將風險降至最低，並管理複雜性。VMware Cloud on AWS 環境熟悉、易於使用並可透過最新的技術創新進行現代化。VMware Cloud on 還 AWS 可以解鎖各種附加服務，例如 Amazon Relational Database Service 服務 (Amazon RDS) 和 Amazon 路線 53，這些服務可協助您的應用程式現代化並改善其效能。

此策略適用於想要瞭解如何使用 VMware Cloud 及其整合以改善業務成果和決策程序的資深管理人員、執行長和營運經理。 AWS

概觀

VMware 提供基礎設施管理和虛擬化工具，傳統上以資料中心為目標。VMware Cloud on 為組織 AWS 提供與 AWS 服務整合的進階 VMware 功能，以及提供服務支援與整合的單一連絡窗口。

VMware Cloud on 可 AWS 讓您存取 VMware 基礎架構，該基礎架構可提供基礎架構虛擬化工具，並提供運算、儲存、網路、安全性和雲端管理功能，以便在混合雲環境中執行企業工作負載。

VMware 雲端 AWS 包含三個 VMware 基礎架構元件：vSphere、NSX 和 vSAN。vSphere 提供運算虛擬化、NSX 提供網路虛擬化，以及 vSAN 提供儲存虛擬化功能。此外，VMware vCenter Server 可讓您從中央位置管理 vSphere 基礎設施，包括驗證和授權。啟用 VMware 雲端後 AWS，您可以在隔離的單租用戶虛擬私有雲 (VPC) 中在 Amazon Elastic Compute Cloud (Amazon EC2) M7i (英特爾至強藍寶石急流)、i4i (英特爾至強冰湖) 和 i3en (英特爾至強級串聯湖) 執行個體上運行基於 VMware 的工作負載。

Amazon EC2 m7i.metal-24xl 實例由定制的第四代英特爾至強可擴展處理器（藍寶石急流）提供支持，具有高達 3.8 GHz 的全核心渦輪頻率。這些處理器配備 Intel 加速器引擎，專為加速成長最快工作負載的效能而設計。此主機類型只能用於提供外部儲存裝置的軟體定義資料中心 (SDDC)。

Amazon EC2 I4i 是一種通用主機類型，可提供比 I3 更高層級的運算、記憶體和儲存體，並且更適合大規模的企業應用程式。在大多數情況下 AWS 都提供 VMware 雲端服務 AWS 區域；如需完整清單，請參閱 VMware 說明文件。

VMware 上的主要使用案例 AWS 為：

- 資料中心延伸 – AWS 雲端 的可擴展性和全球影響力讓您能夠快速、順暢且符合成本效益地滿足資料中心容量和區域覆蓋區域延伸需求。
- AWS 整合式應用程式 — 使用 AWS 服務可協助您將應用程式現代化，或實作設計混合式應用程式的策略。
- 災難復原方案 — 您可以透過 AWS 雲端式災難復原即服務 (DRaaS) 功能強化現有 VMware 型災難復原方法，藉此簡化、加速及現代化災難復原解決方案。
- 雲端移轉機會 — 透過 AWS 雲端 在內部部署資料中心共用常見的 VMware Cloud Foundation 雲端基礎架構 AWS 雲端，您可以簡化並加速將關鍵任務生產工作負載大規模移轉至大規模，而無需轉換或重新架構工作負載。

遷移挑戰

VMware 至 VMware 雲端的 AWS 移轉程序所面臨的主要挑戰包括：

- 工作負載評定 – 您的組織應準備好管理遷移評定所需的額外工作，而且您的網路系統應該能夠處理增加的工作負載。
- 技能 – 建議您聘請具有正確技能和經驗的專業人士來規劃和執行遷移。這些個人負責：
  - 建立計畫，以確保可以長期有效地管理您的工作負載。
  - 建立遷移時間表。
  - 長遠估計遷移的成本和潛在的節省。
- 網路設計和安全性通訊協定 — 您的組織必須瞭解並評估 VMware Cloud on 的網路設計需求 AWS 和安全性因素，以確保資料隱私權和機密性。建議您遵循內部安全通訊協定，並培訓將參與遷移專案的員工。

遷移考量事項

- 遷移工作的關鍵部分是規劃在 AWS上執行工作負載的容量。組織應該準備好了解合規要求和工作負載未來所需的容量，並執行規劃和成本預算。
- 您也應該對現有資料中心的退出策略進行評估。根據應用程式的大小和複雜性，有些應用程式可能會更快速且更容易遷移，而其他應用程式則可能需要較長時間。可以使用自動化來簡化和加速遷移。
- 取得正確的授權是至關重要的。移至 AWS 涉及對主機伺服器的變更，這可能需要變更授權。
- 建議您規劃情境評定、分析可能的成本、了解潛在的安全性問題以及收集組織資源需求的相關資訊。
- 遷移會分三個不同的階段進行：規劃、建置和遷移。每個階段都有自己的一系列挑戰和考量事項，如 VMware 網站上的遷移指南中所述。

目標業務成果

在上成功移轉至 VMware 雲端可 AWS 協助您達成下列目標：

- 簡化操作 – 您的組織可以透過在內部部署資料中心環境和 AWS 雲端中使用相同的 VMware Cloud Foundation 技術，包括 vSphere、vSAN、NSX 和 vCenter Server，以簡化其混合式 IT 操作。您可以保留目前使用的相同 VMware 佈建、儲存和生命週期政策。這表示可以輕鬆地在內部部署環境與 AWS 之間移動應用程式，無需購買新硬體、重寫應用程式或變更操作。
- 提升可用性 — VMware 雲端可 AWS 協助加速將 VMware 工 vSphere 負載移轉至 AWS 雲端. 適用於 VMware Cloud 的 Amazon `i3en.metal` EC2 執行個體可 AWS 提供高聯網輸送量和更低的延遲，因此您可以將資料中心遷移到雲端，以便快速撤離資料中心、災難復原和應用程式現代化。這使您能夠充分利用 AWS 雲端的可擴展性、可用性、安全性和全球覆蓋範圍。

- 應用程式現代化 — 您可以使用 AWS 服務來豐富您在 AWS 工作負載上的 VMware Cloud 架構。例如，您可以將 VMware 應用程式連線到 Amazon Relational Database Service (Amazon RDS) 或者 Amazon EMR 管理的資料庫。
- 降低成本 — VMware Cloud on AWS 可讓組織將一致且透明的混合式 IT 環境營運成本最佳化。您不需要在內部部署環境中部署自訂硬體，也不需要修改應用程式即可遷移至混合雲端模型。您可以使用 VMware 內部部署和 VMware Cloud 提供的原則和管理工具，以 AWS 獲得一致的體驗和一致的效能。這種利用現有投資的能力有助於節省資金。
- 敏捷擴充功能 — VMware Cloud on 的設計可 AWS 在不受內部部署環境限制的情況下進行擴充。您的組織可以利用的大規模可擴充性和全球影響力，以快速、無縫且符合成本效益的方式滿足其容量和區域覆蓋區域擴充需求。 AWS 雲端
- 私有雲 — VMware Cloud on AWS 透過整合運算、儲存、網路虛擬化和生命週期自動化，為私有雲和公有雲提供統一的雲端基礎架構。作為完全統一的軟體堆疊，它為組織提供通往私有雲端的最快路徑以及跨 VMware 型公有雲端的一致基礎設施。
- 輕鬆採用 – 如果您是雲端的新手，並且擁有 VMware 的經驗，可以輕鬆地將內部部署技能套用至 VMware Cloud on AWS。傳統 vCenter 管理介面在雲端和內部部署中的外觀和運作方式都相同。您現有的 VMware 管理員可以將他們現有的技能套用至 AWS. 這樣可以降低人員配置和人事成本，因為其無需僱用新員工或重新培訓工程師和管理員。與全新平台相比，您的組織可以 AWS 更快地提升並使用 VMware Cloud。
- 獲得合作夥伴的專業知識 — 您可以從全球合作 AWS 夥伴社群的專業知識中獲益，他們可以幫助您解決遷移挑戰並在雲端中進行創新。如需詳細資訊，請參閱 AWS 合作夥伴網路。
- 雲端服務產品組合 — 您可以使用 VMware 的雲端服務，或利用一系列廣泛的 AWS 服務，將您的應用程式現代化，並在整個雲端環境中提升彈性、能見度和成本最佳化。
- 轉換為可變成本模式 — VMware Cloud on 可 AWS 協助您從固定成本模式轉變為可變成本模式，並讓您擺脫冗長且昂貴的資料中心合約和災難復原位置。您可以在硬體、維護和升級方面節省成本，投資於其他有利於組織的專案。

最佳實務

請遵循本節中的建議，以取得 VMware Cloud on AWS 的最佳結果。

- 基礎設施彈性 – VMware Cloud on AWS 在 AWS 全球基礎設施頂部執行，並由 VMware 管理。VMware 和 AWS 負責軟體定義的資料中心 (SDDC) 組態、軟體更新和硬體維護。為了保護您的工作負載免受區域和資料中心故障的影響，建議您使用 SDDC 的內建功能。如需詳細資訊，請參閱 VMware 基礎設施服務水準協議。
- 虛擬機器和資料靈活性 – 在每個 SDDC 叢集中，VMware Cloud on AWS 提供兩個 vSAN 資料庫：工作負載資料儲存 (儲存客戶虛擬機) 和 vSAN 資料儲存 (儲存管理虛擬機)。您的雲端管理員會管理工作負載資料儲存，VMware 會管理 vSAN 資料儲存。基礎設施備份會每天完成，但基礎設施組態無法立即還原。請記住，您的變更直到第二天才會備份。
- 連線靈活性 – 應用程式工作負載可用性的關鍵是高度穩固且容錯的網路連線。為了確保一個網路連線故障不會影響其他連線，應該提供足夠的網路容量以滿足您的需求。對於基本連線，IPsec 虛擬私有網路 (VPN) 是最經濟的選擇，因為 VPN 使用網際網路連線。如果想要避免單點故障，建議使用多個網際網路服務供應商 (ISP)，並追蹤 IPsec VPN 的連線參數。

  每當您需要一致的效能，或者預期內部部署環境與 SDDC 中的工作負載之間有更持續的流量時，建議您使用 AWS Direct Connect。也可以選擇使用 IPSec VPN 作為備份，且 AWS Direct Connect 作為主要連線選項。
- 災難復原 – 硬體故障、人為錯誤和自然災害都可能導致災難事件。為了在此類事件發生時確保輕鬆的業務連續性，應該制定可靠的資料保護策略。在 VMware Cloud for AWS 中，可以使用 VMware Site Recovery 來避免在操作功能完整的災難復原站點時產生成本和工作量。如需詳細資訊，請參閱部落格文章使用 VMware Cloud on AWS 進行災難復原的設計考量事項。
- 標準和延伸叢集復原能力 – 在標準 (未延伸) SDDC 中，在單一 AWS 可用區域中佈建所有主機。VMware vSphere 高可用性會保護標準叢集不受基本主機故障影響。具有多個節點的 SDDC 透過設定廉價磁碟備援陣列 (RAID) 和可以忍受的故障數 (FTT) 設定來提供資料備援。這些組態會定義虛擬機器可以容忍的主機和裝置故障次數。

  如果基礎設施可用性很重要，建議您為工作負載設定延伸叢集。這提供了一種多可用區域安排，其中資料會同步複寫到不同可用區域中的主機。此選項為 SDDC 提供額外的穩定性層級。如需詳細資訊，請參閱部落格文章 VMware Cloud on AWS 的恢復能力設計考量事項和最佳實務。

資料庫遷移選項

在您的企業組合中，可能有幾種類型的資料庫。當您遷移至 AWS 時，可以選擇隨即轉移資料庫 (主機轉換) 或切換至由 AWS 管理的資料庫服務 (平台轉換)。

如果決定對資料庫進行主機轉換，AWS 會提供許多服務和工具，協助您安全地移動、儲存和分析資料。如果選擇切換至由 AWS 管理的資料庫服務，可以從多種選項中進行選擇 (例如 Amazon RDS)，因此不必在功能、效能或規模上妥協。

最佳的資料庫遷移策略可讓您充分利用 AWS 雲端，包括遷移應用程式以使用專門設計的雲端原生資料庫。請考慮升級您的應用程式，並選擇最適合應用程式之工作流程需求的資料庫。

有七種常見策略可以將資料庫和應用程式遷移至雲端：

- 主機轉換 – 將應用程式或資料庫移至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體 (虛擬機器)
- 平台轉換 – 透過切換到 AWS 受管資料庫服務來現代化應用程式，例如 Amazon Relational Database Service (Amazon RDS) for Oracle 或 Amazon RDS for SQL Server
- 重新購買 – 遷移至其他產品或授權
- 重構 – 透過使用專用資料庫 (例如 Amazon Aurora 或者 Amazon DynamoDB)，重新架構或重新構想您的應用程式來充分利用雲端原生技術
- 淘汰 – 停用或移除不再需要的舊版資料庫
- 保留 – 將資料庫保留在內部部署環境中，因為沒有業務理由遷移資料庫
- 重新放置 – 虛擬機器監視器等級隨即轉移至 VMware Cloud on AWS

如果規劃將關聯式資料庫移至 AWS，建議您閱讀關聯式資料庫遷移策略。

操作模型

每個組織都有一個涉及各種團隊的內部部署基礎設施操作模型，包括合作夥伴。如果您的組織將其工作負載移至 VMware Cloud on AWS，其目前的操作模型將會改變。例如，支援內部部署環境的團隊包括容量管理團隊、操作團隊和災難復原團隊。但是，當您移至 VMware Cloud on AWS 時，這些任務會由您的組織、VMware 和 AWS 共用。

現有的團隊可能還必須學習新的工具和程序來管理 VMware Cloud on AWS 環境。

本節描述當您從內部部署遷移至 VMware Cloud on AWS 時的操作模型變更與共同的責任。

主題

- 內部部署操作模型
- VMware on AWS 操作模型
- 從您的組織到 VMware 的高層級任務轉換

內部部署操作模型

VMware 內部部署操作通常由八個團隊處理：佈建與組態、操作運作狀態、生命週期管理、容量管理、可用性與持續性、安全性、照常營業 (BAU) 核心 IT 以及 BAU 資源管理團隊。下列各節會加以說明。

佈建和組態團隊

此團隊著重於為客機和主機安裝作業系統、根據準則建立組態以及修補基礎設施元件。具體而言：

- 作業系統組態與安裝 – 客機作業系統的組態，在有可用的更新時安裝與更新作業系統
- 設定管理和運輸叢集的網路和安全性
- 儲存佈建與組態 – 在符合特定閾值時佈建新的邏輯單元號碼 (LUN) 和儲存體
- 硬體佈建 – 硬體的堆放
- 修補基礎設施堆疊 – 修補網路元件、儲存元件和 Hypervisor
- 組態管理 – 管理持續整合與持續交付 (CI/CD) 管道與工具

操作運作狀態團隊

此團隊會設定虛擬機器 (VM) 和 Hypervisor 的監控和日誌。他們也會為 VM 設定所有與安全相關的組態。操作運作狀態團隊負責：

- 監控和記錄客機作業系統 – 在客機作業系統上安裝監控和記錄代理程式，它可用來監控系統的運作狀態
- 基礎設施監控與記錄 – 在所有基礎設施元件上設定監控和記錄，包括 Hypervisor、實體網路裝置和儲存裝置
- 防毒 – 在客機作業系統上安裝代理程式以保護系統和應用程式
- 硬體故障監控 – 設定硬體的閾值，以監控故障並在故障時更換硬體
- 虛擬機加密

生命週期管理團隊

此團隊專注於作業系統和應用程式修補以整合更新，包括重大安全性更新、錯誤修正以及供應商針對下列項目所發行的修補程式：

- 作業系統修補
- 應用程式軟體和元件
- 聯網 (VMware NSX)
- 儲存 (VMware vSAN)
- 運算虛擬化 (VMware vSphere)

容量管理團隊

此團隊專注於資源預測，其中包括了解目前基礎設施的增長率，以及使用工具來預測未來需求。此團隊會根據需求訂購硬體以便未來可託管更多虛擬機器，這是一個有時限的活動。容量管理團隊負責：

- 資源容量納入 – 決定資料中心中應永遠可用的資源
- 資源預測 – 使用工具和過去的使用率指標；預測要購買的資源以滿足未來需求

可用性和持續性團隊

此團隊負責設定、測試和維護高可用性和災難復原，包括虛擬機器和 Hypervisor 故障。具體而言：

- 作業系統與應用程式備份 – 設定備份與還原功能，並確保備份不會失敗
- 復原 – 安裝和設定復原工具
- 高可用性

- 災難復原 – 設定工具，例如 VMware Site Recovery Manager
- 業務持續性

安全團隊

安全團隊透過在 vCenter 上設定許可並設定基礎設施安全性，包括 Secure Shell (SSH) 存取和 vCenter 的連線，專注於維護基礎設施的安全性狀態。該團隊負責：

- 角色和許可 – 管理使用者的驗證和授權
- 基礎設施安全性 – 設定資料中心的基礎設施安全性
- 傳輸中與靜態資料保護
- 防火牆和 VPN 設定
- 事件回應 – 決定安全事件發生時應遵循的步驟
- 管理作業系統和應用程式的漏洞

BAU 核心 IT 流程團隊

該團隊負責：

- 變更管理
- 變更工作流自動化
- 事件管理
- 問題管理

BAU 資源管理團隊

此團隊管理：

- 軟體授權 – 管理作業系統和應用程式的授權
- 軟體庫存清單
- 管理組態管理資料庫 (CMDB)
- VMware 授權 – 授權核心基礎設施元件，例如 VMware ESXi、vSAN、vCenter 和 NSX

VMware on AWS 操作模型

當您將工作負載從內部部署資料中心移至 VMware Cloud on AWS 時，角色和責任有很大的轉變。您的組織、VMware 和 AWS 現在可共用操作任務。

vSphere 管理員在內部部署中執行的活動 (例如設定虛擬網路以及管理虛擬機器、應用程式和安全性) 仍必須在 VMware on AWS 環境中處理。不過，其他任務 (例如修補和升級 Hypervisor、vSAN 和 NSX、監控實體硬體以及在故障期間新增和移除主機) 以及基礎設施安全性由 VMware 和 AWS 在幕後進行處理。

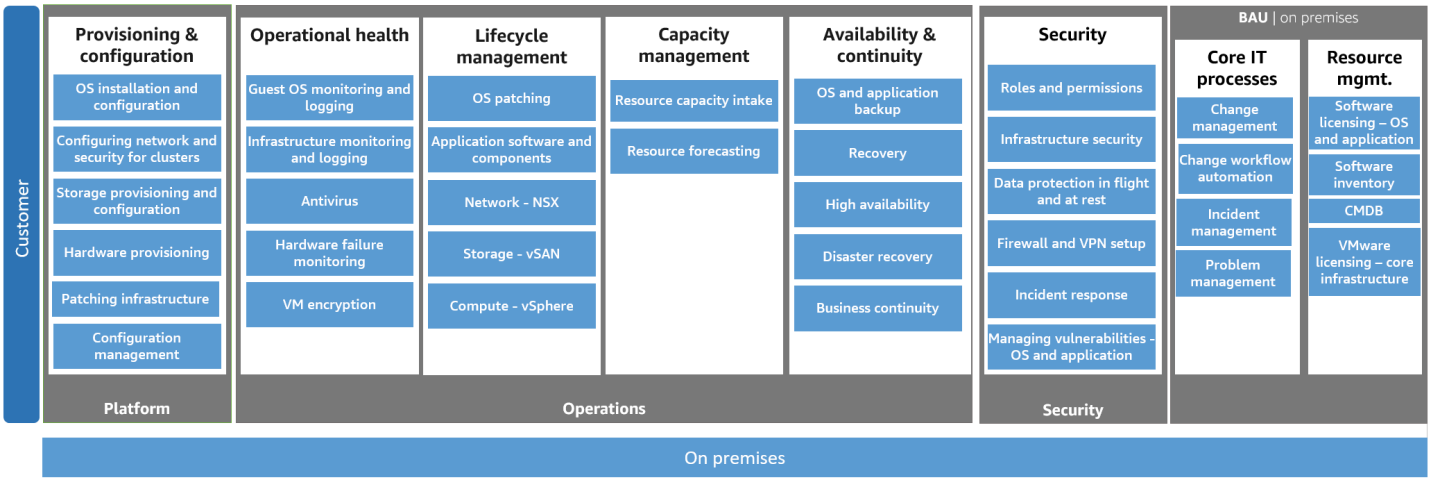
VMware 和 AWS 所管理的活動包括：

- 佈建基礎設施堆疊 (vSphere、NSX 和 vSAN) – 當您的組織使用 VMware Cloud on AWS 時，VMware 會佈建並管理虛擬化管理程序元件，包括 vSphere (運算虛擬化)、NSX (網路虛擬化) 和 vSAN (儲存虛擬化)。如果您要新增容量，VMware 會將主機新增至現有叢集，並設定網路、安全性和儲存體。
- 基礎設施監控與記錄 – VMware 與 AWS 會監控基礎設施並管理記錄。如果發生故障，則其會在幕後更換硬體和其他元件。
- NSX、vSAN 和 vSphere 的生命週期管理 – VMware Cloud on AWS 定期對 SDDC 執行更新。這些更新可確保持續提供新功能和錯誤修正，並在 SDDC 機群中維持一致的軟體版本。
- 基礎設施安全 – AWS 全球基礎設施包括 AWS 區域，這些是包含叢集化資料中心的世界各地的實體位置。將每個邏輯資料中心群組稱為可用區域。每個可用區域都有獨立的電源、冷卻、網路和實體安全。AWS 區域 符合最高等級的安全性、合規性和資料保護。
- 業務連續性 – 藉助叢集上的高可用性 (HA) 功能，當基礎硬體發生故障時，虛擬機器會自動重新啟動。如果您使用延伸的 vSAN 叢集，當作用中可用區域當機時，虛擬機器會在不同的可用區域中自動重新啟動。
- 儲存體加密 – vSAN 會在 VMware Cloud on AWS 中加密所有使用者靜態資料。根據預設，SDDC 中部署的每個叢集都會啟用加密，且無法關閉加密。
- 核心基礎設施元件的 VMware 授權 – VMware 提供 VMware Cloud on AWS 核心基礎設施元件的授權，例如 ESXi、vSAN、NSX 和 vCenter。

從您的組織到 VMware 的高層級任務轉換

典型的內部部署操作模型

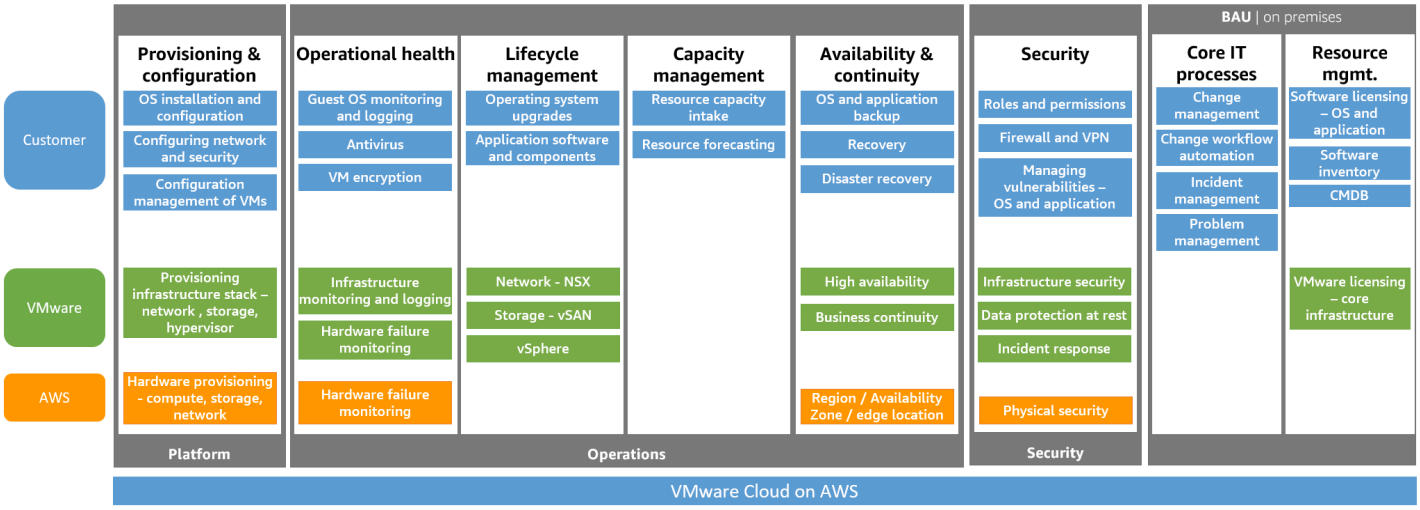
VMware 內部部署任務和活動由不同的操作團隊管理，如前一節 內部部署操作模型 中所述，並在下圖中說明。您也可以與合作夥伴分擔這些責任，他們可協助您管理諸如生命週期管理、操作運作狀態和新硬體組態等活動。操作團隊負責資料中心操作的繁重工作，例如修補和升級 Hypervisor；管理諸如 vSphere、vSAN 和 NSX 等 VMware 軟體元件；在硬體發生故障時與廠商聯絡；收集日誌；將其保留以分析根本原因；以及等待零件更換。



VMware on AWS 操作模型

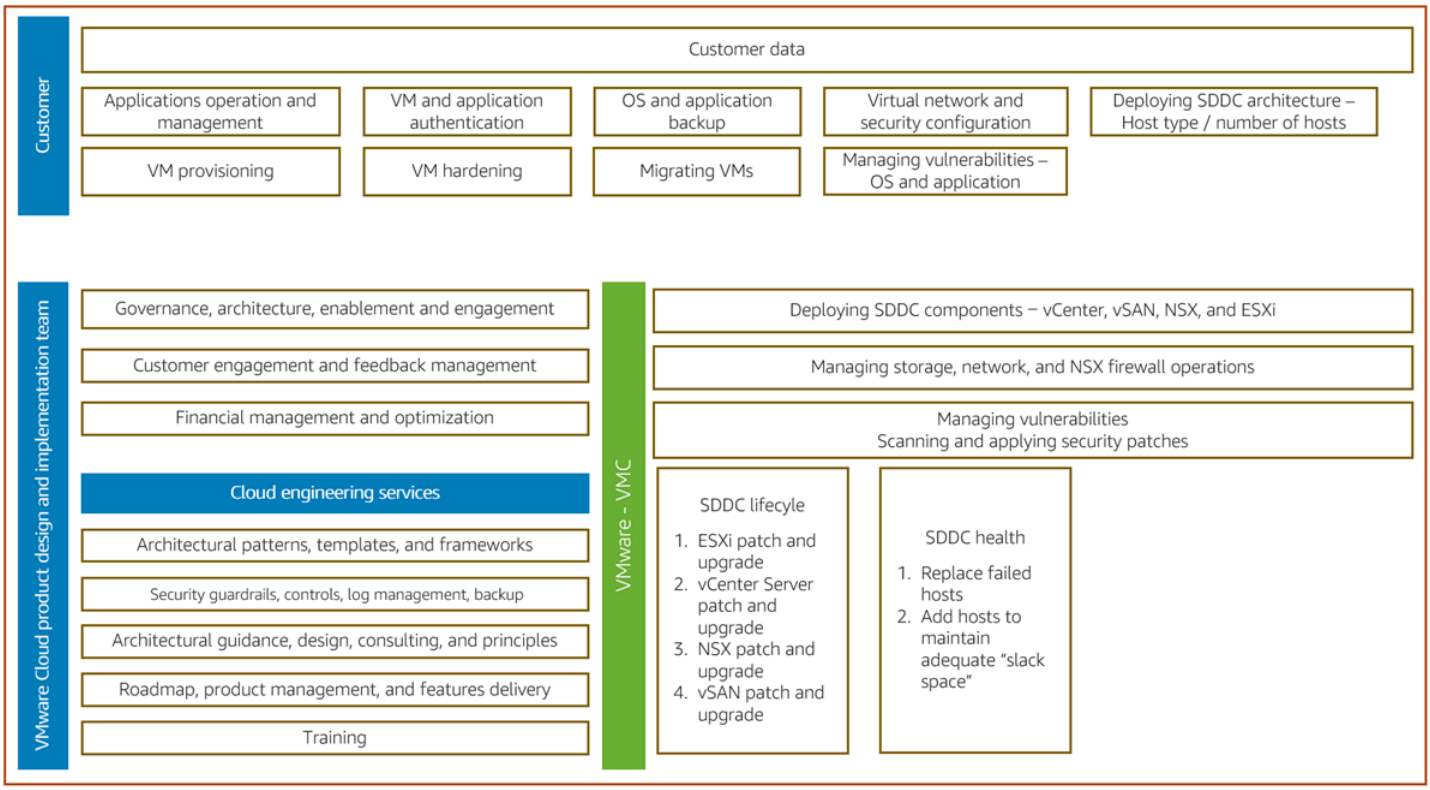
VMware Cloud on AWS 將 VMware 的旗艦運算、儲存和網路虛擬化產品 (vSphere、vSAN 和 NSX) 與 vCenter 管理整合在一起，並將這些服務優化，以便在具有彈性的裸機 AWS 基礎設施上執行。在內部部署和雲端中具有相同架構和操作經驗的團隊可以充分利用 AWS 和 VMware 混合雲端體驗的優點。

當您將工作負載移至 VMware Cloud on AWS 時，您可以與其他兩個利益相關者共用該操作模型。如下圖所示，組織的操作責任較少。VMware 和 AWS 會分擔繁重的工作和大部分耗時的任務，例如修補、升級、硬體監控和佈建新硬體。當硬體發生故障時，組織的操作團隊不再需要等待更換，出現故障的硬體會在幾分鐘內移除並新增



VMware Cloud on AWS 操作模型中的高層級責任

下圖會說明您的組織與 VMware 的高層級責任。這些已在前面的章節 內部部署操作模型 和 VMware on AWS 操作模型 中詳細討論。



後續步驟和資源

如需有關如何從 VMware Cloud on AWS 中受益的詳細資訊，請聯絡 AWS 帳戶代表。

可以透過 AWS 解決方案提供商計畫 (SPP) 直接購買 VMware Cloud on AWS。該計畫使您可以透過 AWS 或 VMware，或透過 AWS 解決方案提供商或您選擇的 VMware VPN 解決方案提供商，購買 VMware Cloud on AWS。

資源

參考

- VMware Cloud on AWS 在支援關鍵業務應用程式方面的商業價值 (IDC 白皮書)
- 了解 VMware Cloud on AWS (VMware 指南)
- 透過 VMware Cloud on AWS 實現混合雲端環境的優勢 (解決方案簡介和網路研討會)
- VMware Cloud on AWS 的雲端遷移 (VMware 技術資源)

工具

- 用於管理 VMware Cloud on AWS 的 PowerShell 模組 (PowerShell Gallery)
- 定價與 TCO 計算器 (VMware 網站)

合作夥伴

- 加入 AWS Partner Network (APN 網站)
- VMware Cloud on AWS 合作夥伴倡議 (APN 網站)

模式

- 使用 VMware HCX 將 VMware SDDC 遷移到 VMware Cloud on AWS (AWS 方案指引)

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
已更新支援的執行個體類型清單	使用 M7i 執行個體類型的相關資訊更新概觀。	2024年3月19 日
已更新支援的執行個體類型清單	已更新概觀及有關 I4i 執行個體類型的資訊。	2023 年 1 月 27 日
初次出版	—	2022 年 4 月 28 日

《AWS 方案指引》詞彙表

以下是由《AWS 方案指引》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：將您的內部部署 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：將您的內部部署 Oracle 資料庫遷移至 AWS 雲端中的 Amazon Relational Database Service (Amazon RDS) for Oracle。
- 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：將您的內部部署 Oracle 資料庫遷移至 AWS 雲端中 EC2 執行個體上的 Oracle。
- 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。此遷移案例特定於 VMware Cloud on AWS，它支援內部部署環境與 AWS 之間的虛擬機器 (VM) 相容性和工作負載可移植性。在將基礎設施遷移至 VMware Cloud on AWS 時，您可以使用內部部署資料中心的 VMware Cloud Foundation 技術。範例：將託管 Oracle 資料庫的虛擬機器監視器重新放置到 VMware Cloud on 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

請參閱以屬性為基礎的存取控制。

抽象的服務

請參閱受管理服務。

酸

請參閱原子性、一致性、隔離性、耐用性。

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。它比主動-被動遷移更具彈性，但需要更多的工作。

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。

聚合函數

在一組資料列上運作，並計算群組的單一傳回值的 SQL 函數。彙總函式的範例包括SUM和MAX。

AI

請參閱人工智慧。

艾奧運

請參閱人工智慧作業。

匿名化

永久刪除資料集中個人資訊的程序。匿名化可以幫助保護個人隱私。匿名資料不再被視為個人資料。

反模式

一種經常使用的解決方案，用於解決方案的生產力適得其反，效果不佳或效果低於替代方案。

應用控制

一種安全性方法，只允許使用核准的應用程式，以協助保護系統免受惡意軟體的攻擊。

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) 文件中的適用於 AWS 的 ABAC。

授權資料來源

儲存資料主要版本的位置，被認為是最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以便處理或修改資料，例如匿名化、編輯或將其虛擬化。

可用區域

AWS 區域 內一個有所區別的位置，隔離了其他可用區域的故障，並對同區域內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)

AWS 的指導方針和最佳實務架構，可協助組織制定高效且有效的計畫以成功移至雲端。AWSCAF 將指引分為六個焦點區域 (稱為層面)：業務、人員、控管、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。對於此層面，AWS CAF 為人員發展、培訓和通訊提供指引，以協助組織為成功採用雲端做好準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS Workload Qualification Framework (AWS WQF)

一種評估資料庫遷移工作負載、建議遷移策略並提供工作預估的工具。AWSWQF 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

BCP

請參閱業務連續性規劃。

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「位元順序」。

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。

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)。

防碎玻璃訪問

在特殊情況下，並透過核准的程序，使用者可以快速取得他AWS 帳戶們通常沒有存取權限的存取權。如需詳細資訊，請參閱 AWS Well-Architected 指南中的實作防破玻璃程序指標。

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

咖啡

請參閱AWS雲端採用架構。

CCoE

請參閱雲端卓越中心。

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來測試系統的彈性。您可以使用 AWS Fault Injection Service(AWS FIS) 執行實驗來 stress 您的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，在本機對資料進行加密。

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。雲計算通常連接到邊緣計算技術。

雲端運作模式

在 IT 組織中，這是用來建置、成熟和最佳化一或多個雲端環境的作業模型。如需詳細資訊，請參閱建立您的雲端作業模型。

採用雲端階段

組織遷移至 AWS 雲端時通常會經歷以下四個階段：

- 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 在 AWS 雲端企業策略部落格上的部落格文章邁向雲端優先之旅和採用階段中定義。如需有關其與 AWS 遷移策略如何相關的資訊，請參閱遷移準備程度指南。

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。常見的雲存儲庫包括 GitHub 或AWS CodeCommit。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。查詢此類資料時，通常可以接受慢速查詢。將此資料移至效能較低且成本較低的儲存層或類別可降低成本。

電腦視覺

機器使用的 AI 領域，可以準確識別圖像中的人，地點和事物，在人類水平或以上。它通常使用深度學習模型構建，可以自動從單個圖像或一系列圖像中提取，分析，分類和理解有用的信息。

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

AWS Config 規則和補救措施的集合，您可以將其組合起來以自訂合規和安全檢查。使用 YAML 範本，您可以在 AWS 帳戶 和區域中將一致性套件部署為單一實體，或者跨組織部署。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。

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 中安全支柱的一個組成部分。如需詳細資訊，請參閱資料分類。

資料漂移

生產資料與用來訓練 ML 模型的資料之間有意義的變化，或輸入資料隨著時間的推移有意義的變化。資料漂移可降低 ML 模型預測中的整體品質、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。

資料最小化

僅收集和處理絕對必要的數據的原則。在中執行資料最小化AWS 雲端可降低隱私權風險、成本和分析碳足跡。

資料周長

您AWS環境中的一組預防性護欄，可協助確保只有受信任的身分正在存取來自預期網路的受信任資源。若要取得更多資訊，請參閱〈在上建置資料周長〉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。

數據來源

在整個生命週期中追蹤資料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

正在收集和處理資料的個人。

資料倉儲

支援商業智慧 (例如分析) 的資料管理系統。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。

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。在 AWS 上採用此策略時，可以在 AWS Organizations 結構的不同層上新增多個控制，以協助保護資源。例如，一 defense-in-depth 種方法可能會結合多因素驗證、網路分段和加密。

委派的管理員

在 AWS Organizations 中，相容的服務可以註冊 AWS 成員帳戶，用於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。

發展價值流映射

用於識別限制並排定優先順序，對軟體開發生命週期中的速度和品質產生不利影響的程序。DVSM 擴展了最初為精益生產實踐而設計的價值流映射流程。它著重於創造和通過軟件開發過程中移動價值所需的步驟和團隊。

數字雙胞胎

真實世界系統的虛擬表現法，例如建築物、工廠、工業設備或生產線。數位雙胞胎支援預測性維護、遠端監控和生產最佳化。

維度表

在 star 結構描述中，較小的資料表包含事實資料表中定量資料的相關資料屬性。維度表格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、篩選和結果集標籤。

災難

防止工作負載或系統在其主要部署位置達成其業務目標的事件。這些事件可能是自然災害、技術故障或人為行為造成的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您使用的策略和程序，將因災難造成的停機時間和資料遺失降到最低。如需詳細資訊，請參閱 AWS Well-Architected 的架構中的雲端中的工作負載的災難復原AWS：雲端復原。

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。

博士

請參閱災難復原。

漂移檢測

追蹤基線組態的偏差。例如，您可以用AWS CloudFormation來偵測系統資源中的漂移，也可以用AWS Control Tower來偵測 landing zone 中可能會影響法規遵循治理要求的變更。

DVSM

請參閱開發價值流映射。

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。與雲計算相比，邊緣計算可以減少通信延遲並縮短響應時間。

加密

一種計算過程，將純文本數據（這是人類可讀的）轉換為密文。

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 AWS PrivateLink 建立端點服務並向其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 主體授予許可。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。

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) 文件中的封套加密。

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 Epic 包括身分和存取管理、偵測性控制、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。

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

事實表

星型架構中的中央表格。它存儲有關業務運營的定量數據。事實資料表通常包含兩種類型的資料欄：包含計量的資料欄，以及包含維度表格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減少開發生命週期的理念。這是敏捷方法的關鍵組成部分。

故障隔離邊界

在中AWS 雲端，可用區域、AWS 區域控制平面或資料平面等界限，可限制故障的影響，並協助改善工作負載的彈性。如需詳細資訊，請參閱AWS錯誤隔離邊界。

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。有關詳情，請參閱機器學習模型可解釋性：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

請參閱精細的存取控制。

精細的存取控制 (FGAC)

使用多個條件來允許或拒絕訪問請求。

閃切遷移

一種資料庫移轉方法，透過變更資料擷取使用連續資料複寫，在最短的時間內移轉資料，而不是使用階段化方法。目標是將停機時間降至最低。

G

地理阻塞

請參閱地理限制。

地理限制 (地理封鎖)

在 Amazon 中 CloudFront，防止特定國家/地區的使用者存取內容分發的選項。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 工作流程被認為是遺留的，基於主幹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

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。它們是通過使用AWS Config，Amazon AWS Security Hub GuardDuty，AWS Trusted Advisor亞馬遜檢查 Amazon Inspector 和自定義AWS Lambda檢查來實現的。

H

公頃

查看高可用性。

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，無需干預。HA 系統的設計可自動容錯移轉、持續提供高品質的效能，以及處理不同的負載和故障，並將效能影響降到最低。

歷史學家現代化

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。歷史學家是一種類型的數據庫，用於收集和存儲工廠中的各種來源的數據。

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。

熱數據

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的儲存層或類別，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，hotfix 通常是在典型的 DevOps 發行工作流程之外進行。

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

查看基礎結構即程式碼。

身分型政策

附接至一個或多個 IAM 主體的政策，可在 AWS 雲端 環境內部定義其許可。

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。

不可變基礎設施

為生產工作負載部署新基礎結構的模型，而不是更新、修補或修改現有基礎結構。不可變的基礎架構本質上比可變基礎架構更加一致、可靠且可預測。如需詳細資訊，請參閱 Well-Architected 的架構中的使用不可變基礎結AWS構進行部署最佳作法。

傳入 (輸入) VPC

AWS 多帳戶架構中的 VPC，可接受、檢查和路由來自應用程式外部的網路連線。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。

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

AWS 多帳戶架構中的集中式 VPC，可管理 VPC (在相同或不同 AWS 區域 中)、網際網路和內部部署網路之間的網路流量的檢查。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 AWS 的機器學習模型可解釋性。

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

以標籤為基礎的存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中每個使用者和資料本身都明確指派一個安全性標籤值。使用者安全性標籤與資料安全性標籤之間的交集決定了使用者可以看到哪些列與欄。

登陸區域

登陸區域是一個可擴展且安全的、架構良好的多帳戶 AWS 環境。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

請參閱以標示為基礎的存取控制。

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

見 7 盧比

小端序系統

首先儲存最低有效位元組的系統。另請參閱 「位元順序」。

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。

受管理服務

AWS 服務用於AWS操作基礎架構層、作業系統和平台，並且您可以存取端點以儲存和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也被稱為抽象的服務。

MAP

請參閱 Migration Acceleration Program。

機制

一個完整的過程，您可以在其中創建工具，推動工具的採用，然後檢查結果以進行調整。機制是一個循環，它加強和改善自己，因為它運行。如需詳細資訊，請參閱 AWS Well-Architected 的架構中建置機制。

成員帳戶

管理帳戶之外的所有 AWS 帳戶，屬於 AWS Organizations 中組織的一部分。一個帳戶一次只能是一個組織的成員。

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 AWS 無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 AWS 上實作微服務。

Migration Acceleration Program (MAP)

一個提供諮詢支援、培訓和服務的 AWS 計畫，以協助組織為移至雲端建置強大的營運基礎，並協助抵消遷移的初始成本。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。移轉工廠團隊通常包括營運、業務分析師和擁有者、移轉工程師、開發人員和 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 將遷移重新託管至 Amazon EC2。

遷移組合評定 (MPA)

一種線上工具，提供用於驗證遷移至 AWS 雲端的業務案例的資訊。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) 免費提供給所有 AWS 顧問和 APN 合作夥伴顧問。

遷移準備程度評定 (MRA)

使用 AWS CAF 深入了解組織的雲端準備狀態、識別優缺點並制定動作計畫來彌補已識別差距的程序。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

用於將工作負載遷移至 AWS 雲端的方法。如需詳細資訊，請參閱本詞彙表中的 7 Rs 項目，並參閱動員您的組織以加速大規模移轉。

ML

請參閱機器學習。

MPA

請參閱移轉組合評估。

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 AWS 雲端中應用程式現代化策略。

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，請參閱評估 AWS 雲端中應用程式的現代化準備情況。

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。

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？」

可變的基礎

更新和修改生產工作負載現有基礎結構的模型。為了提高一致性，可靠性和可預測性，AWSWell-Architected 框架建議使用不可變的基礎結構作為最佳實踐。

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

請參閱作業整合。

OLA

請參閱作業層級協定。

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。

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)。

操作準備程度檢討 (ORR)

問題和相關最佳做法的檢查清單，可協助您瞭解、評估、預防或減少事件和可能的故障範圍。如需詳細資訊，請參閱 AWS Well-Architected 的架構中的作業準備檢閱 (ORR)。

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 AWS CloudTrail 建立的追蹤，它會記錄 AWS Organizations 中某個組織的所有 AWS 帳戶 的所有事件。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)

在中 CloudFront，限制存取權限以保護 Amazon Simple Storage Service (Amazon S3) 內容的增強選項。OAC 支援 AWS 區域 中的所有 S3 儲存貯體、具有 AWS KMS (SS-KMS) 的伺服器端加密以及對 S3 儲存貯體的動態 PUT 和 DELETE 請求。

原始存取身分 (OAI)

在中 CloudFront，用於限制存取以保護 Amazon S3 內容的選項。當您使用 OAI 時， CloudFront 會建立 Amazon S3 可用來進行驗證的主體。經驗證的主體只能透過特定散發存取 S3 儲存 CloudFront 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

請參閱作業整備檢閱。

傳出 (輸出) VPC

AWS 多帳戶架構中的 VPC，它可處理從應用程式內部啟動的網路連線。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。

個人識別資訊 (PII)

直接查看或與其他相關數據配對時，可用於合理推斷個人身份的信息。PII 的範例包括姓名、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。

政策

可以定義權限 (請參閱以身分識別為基礎的策略)、指定存取條件 (請參閱以資源為基礎的策略) 或定義組織中所有帳戶的最大權限的物件 AWS Organizations (請參閱服務控制策略)。

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`，通常位於子`WHERE`句中。

謂詞下推

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。這樣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

AWS 中的實體，可以執行動作和存取資源。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。

隱私設計

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

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。這些控制項會在資源佈建之前進行掃描。如果資源不符合控制項，則不會佈建該資源。如需詳細資訊，請參閱AWS Control Tower文件中的控制項參考指南，並參閱實作安全性控制中的主動控制AWS。

生產環境

請參閱環境。

化名化

以預留位置值取代資料集中的個人識別碼的程序。假名化可以幫助保護個人隱私。假名化數據仍被認為是個人數據。

Q

查詢計劃

一系列步驟，如指示，用來存取 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

拉齊矩陣

請參閱負責任，負責，諮詢，通知（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。

拉西矩陣

請參閱負責任，負責，諮詢，通知（RACI）。

RCAC

請參閱列與欄存取控制。

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。

重新建築師

見 7 盧比

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這決定了最後一個恢復點和服務中斷之間可接受的數據丟失。

復原時間目標 (RTO)

服務中斷與恢復服務之間的最大可接受延遲。

重構

見 7 盧比

區域

地理區域中 AWS 資源的集合。每個 AWS 區域 都是獨立的且獨立於其他區域，以提供容錯能力、穩定性和恢復能力。如需詳細資訊，請參閱 AWS 一般參考 中的管理 AWS 區域。

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。

重新主持

見 7 盧比

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

見 7 盧比

再平台

見 7 盧比

買回

見 7 盧比

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

定義移轉活動和雲端作業所有相關方的角色和職責的矩陣。矩陣名稱衍生自矩陣中定義的責任型別：負責 (R)、負責 (A)、諮詢 (C)，以及通知 (I)。支撐（S）類型是可選的。如果您包含支援，則該矩陣稱為 RASCI 矩陣，如果您將其排除，則稱為 R ACI 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

見 7 盧比

退休

見 7 盧比

旋轉

定期更新密碼以使攻擊者更難以存取認證的程序。

資料列與資料行存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 運算式。RCAC 由資料列權限和資料行遮罩所組成。

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

許多身份提供者（IdPs）使用的開放標準。此功能可啟用聯合單一登入 (SSO)，因此使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為組織中的每個人都建立一個 IAM 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。

SCP

請參閱服務控制策略。

秘密

您以加密形式儲存的機密或受限制資訊，例如密碼或使用者認證。AWS Secrets Manager它由秘密值及其中繼資料組成。密碼值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱秘密管理員說明文件中的秘密。

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。安全性控制有四種主要類型：預防性、偵測、回應式和主動式。

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

預先定義且程式化的動作，其設計用來自動回應或修復安全性事件。這些自動化作業可做為偵探或回應式安全控制項，協助您實作AWS安全性最佳實務。自動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

由接收資料的 AWS 服務 對其目的地的資料進行加密。

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

AWS 服務 的進入點 URL。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。

服務等級指示器 (SLI)

對服務效能層面的測量，例如錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務狀況的目標測量結果，由服務層次指示器測量。

共同責任模式

描述您與 AWS 共同承擔責任以確保雲端安全和合規的模型。AWS 負責雲端的安全，而您負責雲端中的安全。如需詳細資訊，請參閱共同責任模式。

暹

請參閱安全性資訊和事件管理系統。

單一故障點 (SPF)

應用程式的單一重要元件發生故障，可能會中斷系統。

SLA

請參閱服務等級協議。

SLI

請參閱服務層級指示器。

SLO

請參閱服務等級目標。

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. AWS 雲端

抽

請參閱單一故障點。

星型綱要

使用一個大型事實資料表來儲存交易或測量資料，並使用一或多個較小的維度表格來儲存資料屬性的資料庫組織結構。這種結構是專為在數據倉庫中使用或用於商業智能目的。

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。

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

以模擬使用者互動以偵測潛在問題或監控效能的方式測試系統。您可以使用 Amazon CloudWatch Synthetics 來創建這些測試。

T

標籤

作為組織AWS資源的中繼資料的索引鍵值配對。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 文件中的傳輸閘道是什麼。

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

准許您指定的服務在 AWS Organizations 中的組織中以及其帳戶中代表您執行任務。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 AWS Organizations 文件中的搭配使用 AWS Organizations 和其他 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 DevOps 團隊，你可以餵兩個比薩餅。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。

無差別的任務

也稱為繁重工作，是創建和操作應用程序所必需的工作，但不能為最終用戶提供直接價值或提供競爭優勢。無差異化作業的範例包括採購、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

會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。

溫暖的數據

不常存取的資料。查詢此類資料時，通常可以接受中度緩慢的查詢。

視窗功能

一種 SQL 函數，可對以某種方式與當前記錄相關的一組行執行計算。視窗函數對於處理工作非常有用，例如計算移動平均值或根據目前列的相對位置存取列的值。

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。

蠕蟲

看到寫一次，多讀。

WQF

請參閱 AWS 工作負載資格架構。

寫一次，多讀（WORM）

一種儲存模型，可單次寫入資料並防止資料遭到刪除或修改。授權用戶可以根據需要多次讀取數據，但無法更改數據。這種數據存儲基礎設施被認為是不可變的。

Z

零日漏洞

一種利用零時差漏洞的攻擊，通常是惡意軟件。

零時差漏洞

生產系統中未緩解的瑕疵或弱點。威脅參與者可以利用這種類型的漏洞攻擊系統。由於攻擊，開發人員經常意識到該漏洞。

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。