將 AWS Well-Architected 架構套用至 Amazon WorkSpaces 應用程式

AWS 方案指引

AWS 方案指引: 將 AWS Well-Architected 架構套用至 Amazon WorkSpaces 應用程式

Table of Contents

將 AWS Well-Architected 架構套用至 Amazon WorkSpaces 應用程式

Mohamed Wali，Amazon Web Services

2025 年 7 月 (文件歷史記錄)

本指南涵蓋當您使用 Amazon WorkSpaces 應用程式時套用 AWS Well-Architected Framework 的最佳實務。WorkSpaces 應用程式是一種全受管應用程式串流服務，可讓您將桌面應用程式串流給使用者，而無需重寫。

AWS Well-Architected Framework 可協助雲端架構師為各種應用程式和工作負載建置安全、高效能、彈性且高效率的基礎設施。它也為使用者和 AWS 合作夥伴提供一致的方法來評估架構並實作可擴展的設計。

AWS Well-Architected 架構是以六個支柱為基礎：

- 卓越營運
- 安全
- 可靠性
- 效能效率
- 成本最佳化
- 永續性

本指南討論這些支柱和最佳實務如何適用於使用 WorkSpaces 應用程式。

目標對象

本指南適用於：

- 設計和實作 WorkSpaces 應用程式解決方案的雲端架構師和工程師，需要確保其架構遵循 AWS Well-Architected Framework 最佳實務。
- 管理和維護 WorkSpaces 應用程式環境、處理機群管理、擴展和監控，以及需要最佳化成本和效能的 IT 營運團隊。
- 正在考慮或已經在使用 WorkSpaces 應用程式的組織或企業，想要將桌面應用程式串流至其使用者，並且需要建置安全、高效能、彈性和高效的基礎設施。

目標

遵循本指南中的最佳實務可協助您：

- 在 中為串流桌面應用程式建置安全、高效能、彈性且高效率的基礎設施 AWS 雲端。
- 在評估 WorkSpaces 應用程式架構和實作可擴展設計時，套用一致的方法。

卓越營運支柱

卓越營運 (OE) 代表致力於打造持續符合並超越使用者期望的高品質軟體解決方案。 AWS Well-Architected Framework 的卓越營運支柱包含經過驗證的有效團隊組織策略、強大的工作負載設計、高效的大規模操作，以及隨著時間的推移無縫適應不斷變化的需求。透過遵守這些原則，組織可以確保其系統保持彈性、高效能，並符合不斷變化的業務需求。

將此支柱套用至 WorkSpaces 應用程式串流環境的主要重點領域：

- 監控與可觀測性
- 自動化和 DevOps
- 操作程序和文件
- 支援和事件管理

根據業務成果組織團隊

建立具有強大領導承諾的雲端一致營運模式，其中業務目標和關鍵績效指標 (KPIs) 透過最佳化的人員、流程和技術推動組織轉型。

- 團隊結構。建立符合應用程式串流結果的專用團隊。例如：
  - 映像管理團隊負責應用程式封裝和映像最佳化。
  - 機群營運團隊管理容量、效能和擴展。
  - 使用者體驗團隊會處理最終使用者支援和滿意度。
- KPIs和指標。定義和追蹤符合業務的指標，例如：
  - 應用程式可用性費率
  - 部署新應用程式的時間
  - 每個應用程式串流小時的成本
- 操作模型。為下列項目建立明確的程序：
  - 應用程式加入和更新
  - 機群容量管理
  - 使用者存取佈建
  - 事件回應和解決方案

實作可觀測性以取得可行的洞見

實作全面的監控和可觀測性，以追蹤 KPIs和工作負載運作狀態。此原則可啟用資料驅動型決策，並主動改善效能、可靠性和成本。

- 實作效能監控。將 Amazon CloudWatch 設定為：
  - 確保有足夠的容量來滿足需求。例如，您可以使用下列指標：
    - `AvailableCapacity` 監控可用的串流執行個體
    - `InUseCapacity` 追蹤目前使用的執行個體
    - `CapacityUtilization` 監控機群用量的百分比
  - 監控使用者體驗和效能。
  - 立即識別和解決服務問題。
- 追蹤和分析 WorkSpaces 應用程式用量報告。
- 擷取和分析應用程式日誌。如需詳細資訊，請參閱 AWS 部落格文章：使用適用於 Linux 的 Kinesis 代理程式串流 WorkSpaces 應用程式中的應用程式日誌，以及使用適用於 Microsoft Windows 的 Kinesis 代理程式存放 WorkSpaces 應用程式 Windows 事件日誌。
- 透過聊天通知監控 WorkSpaces 應用程式指標和事件。如需詳細資訊，請參閱 AWS 部落格文章 Monitor，並使用 Chatbot 自動化 AWS 最終使用者運算 (EUC) AWS。
- 透過視覺化提示啟用主動工作階段管理。如需詳細資訊，請參閱 AWS 部落格文章顯示工作階段過期和 Amazon WorkSpaces 應用程式中的倒數計時器。
- 建立使用模式和趨勢的視覺化效果。如需詳細資訊，請參閱 AWS 部落格文章擷取和視覺化 Amazon OpenSearch Service 中的 Amazon WorkSpaces 應用程式用量報告 OpenSearch。
- 利用 EUC 工具組來監控作用中工作階段、追蹤機群庫存，以及產生工作階段報告 (CSV 匯出）。如需詳細資訊，請參閱 AWS 部落格文章使用 EUC Toolkit 管理 Amazon WorkSpaces 應用程式和 Amazon WorkSpaces。

盡可能安全地自動化

將基礎設施套用為程式碼 (IaC) 原則，以自動化工作負載操作的所有層面。使用護欄協助確保安全且一致的執行，同時減少手動介入。

- 使用映像助理 CLI 自動化 WorkSpaces 應用程式映像的建立和組態。如需詳細資訊，請參閱 Amazon WorkSpaces 應用程式文件中的映像助理 CLI 操作，以程式設計方式建立 Amazon WorkSpaces 應用程式映像。

    - 應用程式安裝：使用映像助理 CLI 在映像建立期間自動安裝應用程式。
    - 映像建立：使用映像助理 CLI 命令，以程式設計方式建立 WorkSpaces 應用程式映像。
    - 組態管理：自動化預設應用程式設定和啟動參數的組態。
- 自動化 WorkSpaces 應用程式映像的自訂。如需詳細資訊，請參閱 AWS 部落格文章自動建立自訂的 WorkSpaces 應用程式 Windows 映像。
- 套用 IaC 來部署 WorkSpaces 應用程式的基礎設施和應用程式元件。如需詳細資訊，請參閱 AWS 部落格文章使用 Terraform 自動化 Amazon WorkSpaces 應用程式的基礎設施和應用程式部署。
- 實作機群管理的自動化程序，包括：
    - 機群會根據需求進行擴展。設定自動擴展政策，根據使用率指標自動調整機群容量。如需詳細資訊，請參閱 AWS 部落格文章使用 AWS Lambda 來調整 Amazon WorkSpaces 應用程式的擴展步驟和閾值。
    - 基礎映像更新。受益於 提供的 WorkSpaces 應用程式基礎映像的自動更新 AWS。
    - 容量最佳化。設定自動擴展閾值，根據需求模式最佳化資源用量。
- 設定護欄以自動化安全控制：
    - 機群大小上限。設定機群容量的上限，以防止過度佈建。
    - 擴展政策組態。使用適當的閾值實作步驟擴展或目標追蹤擴展政策。
    - 服務配額。使用 AWS 服務配額做為內建限制，以防止資源配置過多。
    - 縮減保護。設定縮減保護，以防止在擴展事件期間移除作用中的執行個體。
- 執行測試和驗證，包括映像建置器、機群和整合測試。
    - 映像建置器測試：
        - 直接在映像建置器界面中測試應用程式。
        - 驗證應用程式啟動和功能。
        - 測試使用者設定和組態。
        - 驗證應用程式相容性。
    - 機群測試：
        - 測試來自不同用戶端裝置的串流工作階段。
        - 驗證使用者權利和存取權。
        - 驗證應用程式效能。
        - 測試使用者體驗的元素和操作，例如剪貼簿、檔案傳輸和列印。
    - 整合測試：
        - 測試 Active Directory 或 SAML 2.0 型身分驗證。

    - 測試主資料夾和持久性儲存。
    - 測試應用程式權利。
    - 測試 USB 裝置重新導向 （ 如果已設定 ）。
- 使用 WorkSpaces 應用程式管理員來自動化應用程式封裝和部署。如需詳細資訊，請參閱 AWS 部落格文章 Amazon WorkSpaces 應用程式的應用程式管理員簡化應用程式加入。
- 使用持續整合和持續交付 (CI/CD) 管道，自動化新應用程式版本的部署。如需詳細資訊，請參閱 AWS 部落格文章篩選精靈：最佳化 CI/CD 和 Amazon WorkSpaces 應用程式中的最終使用者體驗。Amazon WorkSpaces

進行頻繁、小型、可逆的變更

建置鬆散耦合、可擴展的工作負載，以最小風險和輕鬆復原功能啟用頻繁的小型自動化部署。

- 對於映像更新，請使用版本控制的映像建立和增量更新。
    - 版本化映像建立：
        - 使用映像建置器為每組變更建立新的映像。
        - 維護多個映像版本以支援回復案例。
        - 使用AWS 標記策略來追蹤映像版本和屬性。
    - 增量更新：
        - 對應用程式或組態進行小型的增量變更。
        - 在建立新映像之前，在映像建置器中徹底測試更新。
        - 記錄您在每個新映像版本中所做的所有變更。
- 對於控制機群更新：
    - 使用更新的映像建立新機群進行測試。
    - 修改現有的機群屬性，而不會中斷作用中的工作階段。
- 建立文件、測試通訊協定、核准工作流程和監控程序的變更管理程序。
    - 文件：
        - 維護所有映像和機群更新的詳細變更日誌。
        - 記錄每個變更的測試程序和結果。
        - 使用 AWS CloudTrail 追蹤和稽核組態變更。
    - 測試通訊協定：
        - 為所有變更建立全面的測試程序。

    - 包括應用程式功能、效能和使用者體驗測試。
    - 在建立新映像之前，在映像建置器中進行測試。
    - 在完全部署之前，對非生產機群執行其他測試。
- 核准工作流程：
    - 實作生產環境變更的核准程序。
    - 定義需要核准與標準更新之變更的條件。
    - 為變更核准建立角色和責任。
- 監控和驗證：
    - 使用 Amazon CloudWatch 在變更後監控機群和應用程式效能。
    - 設定關鍵指標的提醒，以在更新後快速識別問題。
    - 執行實作後審查，以驗證變革成功並收集學習成果。

經常精簡操作程序

透過定期審查、更新和團隊參與持續改善營運程序，讓所有利益相關者隨時掌握最新情況並符合最佳實務。

- 文件管理。在中央位置維護 WorkSpaces 應用程式程序的目前版本控制文件，以確保團隊之間的操作一致性和知識共享。
    - 必要文件：維護關鍵 WorkSpaces 應用程式操作up-to-date文件，以進行映像建立和管理、機群操作和故障診斷。
    - 營運審查：監控和審查關鍵營運層面，包括效能指標和事件管理。
- 持續改進。透過將 AWS 服務 更新、操作指標和學到的最佳實務整合到標準程序中，系統性地增強 WorkSpaces 應用程式操作。
    - 服務更新：監控 WorkSpaces 應用程式的新功能、服務改進、安全性更新和區域可用性的版本備註。
    - 最佳實務：檢閱並整合 AWS Well-Architected Framework 更新、WorkSpaces 應用程式最佳實務、 AWS 參考架構和安全性 AWS 建議。
    - 知識管理：維護和更新標準操作程序、執行手冊、故障診斷指南和使用者支援文件。

預期失敗

定期執行失敗案例測試，以了解風險、驗證回應程序，並改善團隊處理真實事件的準備程度。

- 失敗測試。定期模擬和測試故障，例如機群容量耗盡、應用程式啟動失敗和網路連線問題。
  - 機群容量耗盡：
    - 在接近容量限制時監控和測試機群擴展行為。
    - 設定 CapacityUtilization和 AvailableCapacity指標的 CloudWatch 警示。
    - 實作在尖峰用量期間處理容量限制的程序。
  - 應用程式啟動失敗：
    - 在串流執行個體上測試應用程式啟動行為。
    - 驗證不同機群組態的應用程式存取和效能。
  - 網路連線問題：
    - 測試不同網路條件下的串流工作階段效能。
    - 監控StreamingSessionLatency連線品質問題。
    - 確保 VPC 設定和安全群組的正確組態。
- 復原程序。開發和測試下列程序：
  - 介於兩者之間的機群容錯移轉 AWS 可用區域。此外，用於擴展機群容量、管理機群更新以及回應執行個體運作狀態問題的文件程序。
  - 使用者資料管理：
    - 在 Amazon Simple Storage Service (Amazon S3) 中為 Windows 機群的主資料夾設定和測試應用程式設定持續性和儲存解決方案，並在 Amazon Elastic File System (Amazon EFS) 中為 Linux 機群設定和測試共用檔案系統。
    - 驗證工作階段之間的資料同步。
  - 服務持續性。維護建立新機群執行個體、管理映像更新和處理工作階段中斷連線的程序。
- 風險管理。識別和緩解：
  - 透過設定適當的機群最小容量、根據需求模式設定自動擴展政策，以及使用 CapacityUtilization、 InUseCapacity和 等 CloudWatch 指標來監控機群使用率趨勢，來限制容量AvailableCapacity。
  - 透過追蹤關鍵指標，例如StreamingSessionLatency並設定適當的 CloudWatch 警示，來產生效能瓶頸。

從所有操作事件和指標中學習

透過在整個組織中分享從營運事件和故障中學到的經驗，培養持續改進的文化。強調它們對業務成果的影響。

- 事件分析。記錄和分析服務中斷、效能降級、使用者投訴和容量問題。
- 指標檢閱。定期分析用量模式、效能趨勢、成本指標和使用者滿意度資料。
- 知識分享。建立團隊學習工作階段、最佳實務文件、跨團隊知識轉移和事件回顧的流程。

使用 受管服務

使用 AWS 受管服務並建置標準化程序，將營運開銷降至最低。與下列 AWS 受管服務整合：

- AWS Systems Manager 用於自動化
- 用於監控的 Amazon CloudWatch
- 存取控制的 AWS Identity and Access Management (IAM)
- Windows 機群使用者儲存的 Amazon S3
- Linux 機群使用者儲存的 Amazon EFS
- AWS Directory Service 用於使用者身分驗證

安全支柱

AWS Well-Architected Framework 的安全支柱著重於利用雲端功能，協助為您的資訊、基礎設施和資源建立強大的保護機制。這些原則有助於增強您的整體安全狀態，同時實現創新。

將此支柱套用至 WorkSpaces 應用程式串流環境的主要重點領域：

- 資料完整性和機密性
- 管理使用者許可
- 建立控制以偵測安全事件

實作強大的身分基礎

使用最低必要許可來存取 AWS 資源，同時集中身分管理和避免長期登入資料。

- 授予 WorkSpaces 應用程式資源的最低權限許可：
  - 為 WorkSpaces 應用程式機群建立具有最少必要許可的特定 IAM 角色。
  - 為映像建置器設定有限的 IAM 許可。
  - 限制對 WorkSpaces 應用程式管理函數的管理存取。
  - 定義堆疊和機群管理的精細許可。
- 實作適當的使用者身分驗證機制：
  - 為企業身分提供者整合設定 SAML 2.0 聯合。
  - 設定 AWS IAM Identity Center以進行使用者管理。
  - 僅在特定身分驗證案例需要時使用自訂身分代理程式。
  - 在支援的情況下實作多重要素驗證 (MFA)。
- 控制使用者對應用程式的存取：
  - 設定應用程式權利以限制對特定應用程式的存取。
  - 根據使用者角色建立應用程式指派群組。
  - 透過堆疊許可管理應用程式存取。
  - 實作工作階段政策來控制應用程式行為。
- 使用適當的控制項保護使用者工作階段：
  - 設定工作階段逾時政策。

  - 設定中斷連線逾時動作。
  - 實作工作階段持續性要求。
  - 控制檔案系統重新導向許可。
- 設定 WorkSpaces 應用程式的憑證型身分驗證。如需詳細資訊，請參閱 AWS 部落格文章：使用 AWS 私有 CA Connector for Active Directory 簡化 WorkSpaces 應用程式和 WorkSpaces 的憑證型身分驗證。
- 使用工作階段標籤來實作精細存取控制。如需詳細資訊，請參閱 AWS 部落格文章使用工作階段標籤來簡化 WorkSpaces 應用程式許可。

維持可追蹤性

針對所有環境變更和活動實作即時監控和自動化回應系統。

- 設定應用程式日誌的 CloudWatch 記錄，以監控應用程式特定的事件，包括應用程式啟動、當機和錯誤。設定工作階段日誌以追蹤串流工作階段資訊，包括工作階段開始、停止和使用者連線事件。
- 啟用 CloudTrail 以記錄所有 WorkSpaces 應用程式 API 呼叫，並追蹤管理事件，例如機群建立和修改、映像建置器操作、堆疊組態和使用者管理活動。
- 監控 WorkSpaces 應用程式執行個體活動：
  - 設定執行個體記錄以擷取系統層級事件。
  - 追蹤應用程式啟動和失敗。
  - 監控系統資源用量和效能。
- 追蹤使用者活動：
  - 監控使用者身分驗證嘗試和失敗。使用 CloudWatch 指標和 CloudWatch Logs 來追蹤使用者登入嘗試、工作階段開始和結束時間，以及工作階段中斷連線事件。
  - 追蹤應用程式用量模式。啟用 WorkSpaces 應用程式用量報告，以擷取工作階段持續時間、開始和結束時間、使用的執行個體類型和存取的應用程式等資訊。
  - 透過已啟用的主資料夾記錄檔案系統活動。
  - 設定剪貼簿設定和列印操作，以實現防止資料遺失的目標。
- 針對安全相關指標設定 CloudWatch 警示，例如使用者身分驗證失敗、不尋常的工作階段模式，以及資源存取違規。
- 使用 EUC 工具組追蹤作用中工作階段和狀態、監控使用中工作階段的 IP 地址，以及匯出工作階段資料以進行稽核。如需詳細資訊，請參閱 AWS 部落格文章使用 EUC 工具組來管理 Amazon WorkSpaces 應用程式和 Amazon WorkSpaces。

在所有層套用安全性

從網路邊緣到應用程式程式碼，跨基礎設施的所有元件實作多層安全控制。

- 設定網路層安全性：
  - 實作嚴格的安全群組規則。
  - 將 WorkSpaces 應用程式機群執行個體放置在沒有直接網際網路存取的私有子網路中。透過 NAT 裝置控制網際網路存取。
  - 使用虛擬私有雲端 (VPC) 端點來存取支援的 AWS 服務 （ 例如 Amazon S3)。
  - 實作網路存取控制清單 ACLs) 作為額外的網路安全層。
  - 限制串流連接埠 (TCP 8443 for HTTPS and WebSocket Secure) 對特定 IP 範圍的存取。
- 設定存取層安全性：
  - 實作工作階段逾時政策，以自動中斷非作用中的使用者連線。
  - 使用工作階段標籤實作屬性型存取控制。如需詳細資訊，請參閱 AWS 部落格文章使用工作階段標籤來簡化 WorkSpaces 應用程式許可。
- 設定應用程式層安全性：
  - 設定應用程式權利，以控制哪些使用者可以存取特定應用程式。
  - 啟用檔案系統重新導向控制，以限制對本機磁碟機的存取。
  - 根據安全需求設定剪貼簿、檔案傳輸和列印許可。
  - 根據安全政策設定 USB 裝置存取控制。
- 設定映像層安全性：
  - 建立和維護符合安全需求的強化基礎映像。
  - 使用最新的安全修補程式來保持基礎映像的更新。
  - 在基礎映像中設定 Windows 安全設定。
  - 在基礎映像中停用不必要的 Windows 服務和功能。

自動化安全最佳實務

在版本控制範本中使用自動化的程式碼定義安全控制，以啟用安全且可擴展的基礎設施部署。

- 透過使用 等服務來使用基礎設施做為程式碼 (IaC) AWS CloudFormation ，在所有機群部署中實作一致的安全組態。如需詳細資訊，請參閱 AWS 部落格文章自動將其他安全群組連接至 Amazon WorkSpaces 應用程式和 Amazon WorkSpaces。

- 使用映像助理 CLI 自動化映像建立安全程序。
- 使用 Amazon CloudWatch 警示、Amazon EventBridge 規則和自動回應的 AWS Lambda 函數，設定超過容量使用率閾值的自動回應、未經授權的存取嘗試和安全群組變更。

讓人員遠離資料

自動化資料處理程序，將直接人工存取降至最低，並降低錯誤或處理不當的風險。

- 設定應用程式權利，以控制哪些使用者可以存取特定應用程式。
- 使用動態應用程式架構來建置動態應用程式提供者，以根據使用者屬性動態提供應用程式。
- 設定檔案系統重新導向，以控制使用者可以存取的本機磁碟機、限制對特定資料夾的存取，以及管理本機和串流工作階段之間的檔案傳輸許可。
- 實作剪貼簿限制，以停用本機和串流工作階段之間的剪貼簿共用、視需要啟用單向剪貼簿流程，並防止未經授權的資料複製。
- 設定應用程式設定持續性，以自動儲存和還原應用程式組態、消除手動組態需求，以及維持一致的使用者體驗。

準備安全事件

使用自動化工具從安全事件中快速偵測、調查和復原，以制定和練習事件回應計劃。

- 針對失敗的身分驗證嘗試、機群安全群組的變更、映像組態的修改，以及不尋常的串流工作階段模式，設定 CloudWatch 警示。
- 常見 WorkSpaces 應用程式安全案例的文件回應程序，例如：
  - 未經授權的存取嘗試
    - 偵測：監控身分驗證失敗。
    - 回應：撤銷使用者權利、檢閱工作階段日誌和更新存取政策。
  - 遭入侵的串流執行個體
    - 偵測：監控執行個體行為。
    - 回應：終止受影響的工作階段、取代機群執行個體，以及檢閱安全群組組態。
  - 資料外洩嘗試
    - 偵測：監控檔案傳輸活動。
    - 回應：檢閱剪貼簿和檔案傳輸日誌、調整檔案傳輸許可，以及更新資料保護政策。

- 實作機群執行個體替換、安全群組還原、使用者存取重新設定和應用程式設定復原的自動化復原程序。
- 使用 AWS 服務 進行安全管理，例如 AWS Security Hub CSPM 用於安全調查結果和用於威脅偵測的 Amazon GuardDuty。

可靠性支柱

AWS Well-Architected Framework 的可靠性支柱可解決系統在其整個生命週期的預期操作期間維持其預期功能和效能等級的情況。它提供在 上建置和維護可靠系統的完整指導方針 AWS，包括跨工作負載生命週期所有階段進行測試和驗證的策略。

將此支柱套用至 WorkSpaces 應用程式串流環境的主要重點領域：

- 機群管理和擴展
- 工作階段可靠性
- 應用程式可用性
- 復原程序

從失敗中自動復原

監控業務價值KPIs，以觸發自動化回應，在故障影響操作之前預測、防止或復原故障。

- 請確定您的 IP 子網路配置考慮了擴展和可用性。
- 監控關鍵 CloudWatch 指標以確保服務可用性和效能，包括機群容量指標，例如 `AvailableCapacity`和 `InUseCapacity`，以及串流品質指標，例如 `StreamingSessionLatency`。
- 設定容量閾值、工作階段運作狀態指標、效能降級和機群運作狀態變更的提醒。
- 使用內建的 WorkSpaces 應用程式自動擴展功能來：
  - 設定最小和最大機群容量。
  - 根據容量使用率設定擴展政策。
  - 根據使用者體驗指標和業務需求來定義向外擴展和向內擴展閾值，而不只是技術指標。
- 為您的 WorkSpaces 應用程式環境建置災難復原環境。如需詳細資訊，請參閱 AWS 部落格文章 Amazon WorkSpaces 應用程式災難復原考量事項。

測試復原程序

雲端環境可自動測試故障案例和復原程序。這些功能可協助您在實際故障發生之前識別和修正漏洞。

- 機群復原測試。在多個案例中實作全面的機群復原測試：

  - 模擬執行個體終止以驗證自動擴展回應。
  - 驗證機群最小容量維護。
  - 測試執行個體替換時機和使用者重新導向。
  - 驗證擴展政策有效性。
  - 測試機群容量限制和溢位處理。
- 工作階段復原測試。實作工作階段復原驗證程序：
  - 測試中斷連線和重新連線案例。
  - 驗證應用程式狀態保留。
  - 測試各種網路中斷案例。
  - 驗證工作階段逾時行為。
  - 驗證使用者身分驗證持續性。
  - 驗證暫時儲存處理。

水平擴展以增加彙總工作負載可用性

將工作負載分散到多個較小的資源，將個別故障的影響降至最低，並消除單一故障點。

- 跨多個可用區域部署機群執行個體。
- 設定適當的最小機群容量。
- 設定機群的自動擴展，並設定適當的擴展閾值。
- 監控整個機群的容量使用率。
- 跨多個區域部署 WorkSpaces 應用程式堆疊。如需詳細資訊，請參閱 AWS 部落格文章 最佳化 Amazon WorkSpaces 應用程式的延遲型路由使用者體驗。

停止猜測容量

使用雲端的自動擴展功能，根據需求動態調整資源。這有助於防止資源飽和，同時保持最佳效率。

- 監控 `CapacityUtilization`、 `AvailableCapacity`和 等關鍵指標`InUseCapacity`，以了解容量需求。
- 追蹤不同時段的機群使用率趨勢。監控每日模式、每週變化、每月趨勢和季節性峰值。
- 設定擴展政策並設定擴展閾值。
- 確保目前配額與最大用量之間存在足夠的間隙，以適應容錯移轉。

- 透過架構因應固定的服務配額和限制。

透過自動化管理變更

透過自動化實作基礎設施變更，包括自動化程式碼本身的版本控制變更。

- 使用 IaC 進行機群組態。
- 實作一致的擴展政策。
- 使用影像助理 CLI 建立一致的影像。

效能效率支柱

AWS Well-Architected Framework 的效能效率支柱著重於最佳化雲端資源的使用，以達到或超過效能目標，同時確保適應不斷變化的需求和新興技術。它強調持續微調系統在動態雲端環境中維持尖峰效率的重要性。

將此支柱套用至 WorkSpaces 應用程式串流環境的主要重點領域：

- 執行個體類型選擇和最佳化
- 串流效能最佳化
- 機群容量管理

普及進階技術

利用雲端廠商管理的複雜技術服務，讓您的團隊可以專注於產品開發，而不是基礎設施管理。

- 根據應用程式需求設定適當的執行個體類型：
  - 選取圖形密集型應用程式的 GPU 執行個體。
  - 根據應用程式需求選擇適當的 GPU 系列（例如 Graphics G4dn 或 Graphics G5)。
- 選擇並設定下列其中一種身分驗證方法：
  - 設定與 SAML 2.0 型身分提供者的整合。
  - 設定使用者集區設定。
  - 與 整合AWS Directory Service。
- 根據使用者需求啟用和設定儲存選項：
  - 在 Amazon S3 for Windows 型機群中設定主資料夾。
  - 在 Amazon EFS 中為 Linux 型機群設定共用檔案系統。
  - 設定持久性儲存許可。
  - 啟用應用程式設定持續性。

在幾分鐘內全球化

使用多區域部署，透過減少延遲來改善全球使用者體驗。

- 在為每個區域建立個別堆疊時，在最接近使用者的區域中部署機群， AWS 區域 以設定多個 中的機群。
- 實作跨區域重新導向，以自動將 WorkSpaces 應用程式使用者重新導向至最接近其目前位置的 AppStream 堆疊。
- 如果您使用 WorkSpaces 應用程式中的任何選用功能，例如應用程式設定持久性、主資料夾或彈性機群，則需要為 Windows 型機群的使用者資料設定 Amazon S3 跨區域複寫，並為 Linux 型機群設定跨區域複寫。
- 跨區域複寫映像。如需詳細資訊，請參閱 AWS 文件AWS 區域 中的將您所擁有的映像複製到 Amazon WorkSpaces 應用程式中的另一個映像。
- 對於加入網域的機群，請確定 Active Directory 基礎設施，包括 Active Directory Federation Services (AD FS)（除非您使用 SAML 2.0 和 Amazon Cognito 作為替代方案）已在其他區域中正確設定，而且您AWS Directory Service for Microsoft Active Directory用於多區域複寫功能。
- 將使用者導向最低延遲的 WorkSpaces 應用程式端點。如需詳細資訊，請參閱 AWS 部落格文章最佳化 Amazon WorkSpaces 應用程式的延遲型路由使用者體驗。

使用無伺服器架構

無伺服器架構使用雲端管理服務進行運算函數，可消除伺服器管理開銷並降低成本。

使用無 AWS 伺服器服務，例如：

- AWS Lambda 自動化任務，並透過事件驅動函數整合自訂邏輯
- Amazon S3 為 WorkSpaces 應用程式使用者資料、應用程式檔案和工作階段成品提供可擴展的儲存體
- Amazon CloudWatch 可監控、記錄和提醒 WorkSpaces 應用程式效能和用量指標
- Amazon Cognito 可促進 WorkSpaces 應用程式的使用者身分驗證和存取控制
- Amazon API Gateway 可建立 RESTful APIs，以連接 WorkSpaces 應用程式與其他 服務或自訂應用程式

更頻繁的實驗

雲端基礎設施可快速測試各種資源組態，以最佳化效能和成本。

- 測試不同的執行個體類型，以最佳化效能和成本：
  - 比較不同執行個體系列的串流效能。

  - 評估圖形應用程式的 GPU 與非 GPU 執行個體。
  - 針對記憶體密集型應用程式測試記憶體最佳化執行個體。
- 使用 Image Builder 測試應用程式組態：
  - 使用不同的應用程式組態建立測試映像。
  - 在部署之前驗證應用程式效能。
  - 測試應用程式與不同執行個體類型的相容性。
- 使用機群容量組態測試機群設定，例如最小和最大容量、擴展政策、工作階段設定，例如最大工作階段持續時間，以及中斷連線逾時設定。

考慮機械同情

根據工作負載的特定需求和使用模式選擇雲端服務，以確保最佳效能和效率。

- 針對圖形密集型應用程式、需要 DirectX、OpenGL、OpenCL 或 3D 視覺化軟體的應用程式，選擇圖形 G5 執行個體。
- 選取商業應用程式、網頁瀏覽器和光線圖形應用程式的`stream.standard`執行個體
- 根據 CloudWatch 指標監控和調整串流通訊協定，例如 `StreamingSessionLatency`。
- 在最接近您使用者的 VPCs中設定 WorkSpaces 應用程式，並根據您的應用程式需求使用適當的網路頻寬。
- 根據應用程式行為選擇適當的機群類型。例如，為需要專用資源的應用程式選擇單一工作階段機群，為可有效率地共用資源的應用程式選擇多工作階段機群。
- 考慮應用程式與多工作階段環境的相容性。
- 使用檔案系統重新導向功能來處理遠端和本機應用程式之間的互動。如需詳細資訊，請參閱 AWS 部落格文章從 Amazon WorkSpaces 應用程式串流工作階段啟動本機應用程式。

成本最佳化支柱

AWS Well-Architected Framework 的成本最佳化支柱著重於將商業價值最大化，同時將支出降至最低。它有助於確保您在雲端資源上花費的每一美元都有助於實現您的組織目標。

將此支柱套用至 WorkSpaces 應用程式串流環境的主要重點領域：

- 機群容量管理和執行個體類型選擇
- 擴展和排程最佳化
- 監控和分析用量模式
- 成本分配和追蹤

實作雲端財務管理

透過結構化計劃和程序，在雲端財務管理和成本最佳化中建立專用組織能力，以最大限度地提高雲端價值和效率。

- 使用 AWS Cost Explorer和 用量報告來追蹤串流時數用量、分析機群執行個體成本，以及監控區域成本分佈，以監控 WorkSpaces 應用程式成本。
- 使用 來規劃和設定成本控制AWS Budgets，以設定整體 WorkSpaces 應用程式服務成本的提醒、建立服務的預算閾值，並根據預算金額監控實際支出。如需詳細資訊，請參閱 AWS 部落格文章如何使用自動化來最佳化和控制 Amazon WorkSpaces 應用程式的成本。

新增耗用模型

根據實際使用模式擴展運算資源和成本。例如，您可以在非上班時間關閉非生產環境，以最佳化支出。

- 選擇適當的定價模型。例如，針對可變工作負載，使用永遠在線的機群以取得一致的用量和隨需機群。
- 選取最佳執行個體類型。例如，針對一般應用程式使用 `stream.standard` 執行個體，並僅在需要時使用圖形執行個體 (G4dn)。

測量整體效率

計算和追蹤cost-per-unit成本的業務輸出，以量化效率改善並引導最佳化工作。

- 追蹤工作階段效率。
- 使用下列 CloudWatch 指標監控機群使用率：
  - `AvailableCapacity` 追蹤未使用的容量
  - `InUseCapacity` 測量實際用量
- 計算和追蹤每個工作階段的成本，例如每個串流小時的成本、每個使用者的成本，以及每個應用程式的成本。
- 實作 WorkSpaces 應用程式的成本最佳化工具來監控您的建置器。
- 比較機群類型之間的成本。例如，比較：
  - 單一工作階段和多工作階段的授權成本
  - 資源使用率
  - 每個執行個體的使用者密度
- 使用程序追蹤資料來識別未充分利用或不必要的應用程式。如需詳細資訊，請參閱 AWS 部落格文章在 Amazon WorkSpaces 應用程式工作階段中追蹤使用者程序。

停止在未區分的繁重項目上花費金錢

AWS 管理基礎設施操作並提供受管服務，讓您的組織可以專注於業務目標，而不是 IT 維護。

- 使用 Image Builder 封裝應用程式、設定應用程式設定和測試應用程式相容性，以建立和維護應用程式映像。
- 透過選取適當的執行個體類型和定義擴展閾值，以及設定所需的容量限制，來設定機群規格。
- 在 Amazon S3 for Windows 型機群中設定主資料夾，以及在 Amazon EFS for Linux 型機群中設定共用檔案系統，以設定持久性儲存選項。設定儲存許可並定義保留政策。

分析和屬性支出

雲端可精確追蹤每個工作負載的資源用量和成本，進而提供準確的投資報酬率 (ROI) 測量和目標最佳化機會。

- 針對成本分配的機群、資產追蹤的映像、環境指定的影像建置器，以及組織分組的堆疊，實作全面的標記策略。
- 使用AWS 成本和用量報告 (AWS CUR) 依標記的資源細分 WorkSpaces 應用程式成本，並分析每個機群、堆疊和映像的成本。

- 使用 AWS Cost Explorer 視覺化 WorkSpaces 應用程式支出趨勢，並比較區域和執行個體類型等不同維度的成本。
- 依應用程式監控和分析機群使用率、執行個體類型效率和串流時數。
- 追蹤未使用的預留容量、未充分利用的機群或堆疊，以及機群用量的閒置期間。
- 計算和追蹤每個應用程式每位使用者的成本、每個應用程式的串流時數，以及串流應用程式的使用者採用率。
- 透過設定 WorkSpaces 應用程式用量報告、使用 Amazon Athena 查詢用量資料，以及在 Amazon Quick 中建立視覺化以取得成本和用量洞察，來設定詳細的用量分析。
- 與每個裝置授權相比，評估 Windows Server 授權、應用程式授權模型和每個使用者授權等總成本考量。
- 使用 Amazon Athena 依使用者查詢和分析主資料夾儲存成本和用量模式。如需詳細資訊，請參閱 AWS 部落格文章如何報告 Amazon WorkSpaces 應用程式主資料夾與 Amazon Athena 搭配使用。

永續性支柱

AWS Well-Architected Framework 的永續性支柱強調將環境足跡降至最低，並最佳化能源使用量和效率。它引導架構師在其系統設計和資源配置策略中做出具有環境意識的決策。

將此支柱套用至 WorkSpaces 應用程式串流環境的主要重點領域：

- 了解和最佳化資源配置以符合實際需求，並將串流環境中的浪費降至最低
- 分析和調整使用者取用模式，以提高應用程式交付和串流工作階段的效率
- 選取並使用適當的硬體組態來最大化能源效率，同時符合效能需求
- 使用 AWS 受管服務功能受益於這些服務提供的規模經濟和內建效率功能

了解您的影響

透過測量每個輸出單位的資源效率和排放量，監控和最佳化工作負載的環境影響。使用此資料來建立 KPIs並引導永續性改進。

- 監控機群使用率模式。
- 追蹤每個使用者的串流時數。
- 分析機群容量用量趨勢。

建立永續性目標

為每個符合組織目標的工作負載設定可衡量的永續性目標。當您擴展時，專注於降低每筆交易的資源強度。

- 設定機群使用率、執行個體類型效率和串流時數最佳化的目標。
- 根據實際用量模式規劃容量。

最大化使用率

透過適當調整資源大小並最大化使用率來最佳化工作負載效率。減少閒置容量，將能源消耗降至最低並改善永續性。

- 設定自動擴展以符合實際需求。

- 根據用量模式調整合適的機群容量。
- 實作適當的最小和最大容量限制。
- 為工作負載選擇適當的執行個體類型。
- 監控和最佳化串流工作階段密度。
- 在離峰時間減少閒置容量。

預期並採用新的、更有效率的硬體和軟體產品

隨時掌握並快速採用合作夥伴和供應商的新高效技術，以持續改善工作負載的環境影響。

- 使用最新一代的執行個體類型。
- 可用時升級至較新的執行個體類型。
- 最佳化應用程式串流設定。
- 設定適當的串流通訊協定。
- 更新至最新的 WorkSpaces 應用程式功能。

已使用的受管服務

利用共用雲端服務和受管解決方案，將資源使用效率最大化，同時透過自動化擴展和生命週期管理將環境影響降至最低。

- 將 Amazon S3 用於 Windows 型機群的使用者儲存，將 Amazon EFS 用於 Linux 型機群的共用檔案系統。
- 實作 CloudWatch 進行監控。
- 設定 IAM 以進行存取管理。

減少雲端工作負載的下游影響

設計 服務以將用戶端資源需求降至最低，減少能源消耗並延長使用者的裝置生命週期。

- 調整工作階段持續時間上限，以防止不必要的資源消耗。
- 設定適當的工作階段逾時。
- 設定中斷連線逾時政策。
- 視需要實作工作階段持續性政策。

Resources

AWS 文件

- AWS Well-Architected 架構
- Amazon WorkSpaces 應用程式管理指南
- 《Amazon CloudWatch 使用者指南》https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
- Amazon EFSS 使用者指南
- Amazon S3 使用者指南
- IAM 使用者指南

AWS 部落格文章

- Active Directory 群組成員資格型 WorkSpaces 應用程式目標
- 使用 Azure AD 為所有 Amazon WorkSpaces 應用程式堆疊建立單一身分提供者
- 為 Amazon WorkSpaces 和 Amazon WorkSpaces 應用程式設定 Windows 遠端協助
- 建立 AS2TrustedDomains DNS TXT 記錄，將 Amazon WorkSpaces 應用程式原生用戶端重新導向至第三方身分提供者
- 在 Amazon WorkSpaces 應用程式中建立自訂記錄和 Amazon CloudWatch 提醒 Amazon WorkSpaces
- 使用 Geo Targetly 和 Amazon WorkSpaces 應用程式進行跨區域重新導向
- 跨帳戶資源和 Amazon WorkSpaces 應用程式
- 使用 Bio-key PortalGuard 和 Amazon WorkSpaces 應用程式啟用聯合
- 使用 SimpleSAMLphp 和 Amazon WorkSpaces 應用程式啟用聯合
- 使用 Duo Single Sign-On 和 Amazon WorkSpaces 應用程式啟用聯合身分
- 使用 Shibboleth 和 Amazon WorkSpaces 應用程式啟用聯合身分
- 使用 Amazon 最終使用者運算進行內部部署 VDI 的容錯移轉策略
- Amazon 如何使用 Amazon WorkSpaces 應用程式為資料科學家和分析師提供敏感資料的存取權
- 如何設定 Amazon WorkSpaces 應用程式的憑證型身分驗證
- 如何將 Okta 宣告與 Amazon WorkSpaces 應用程式的應用程式權利搭配使用

- 使用開放原始碼虛擬應用程式管理在 Amazon WorkSpaces 應用程式上管理電腦實驗室
- 將 WorkSpaces 應用程式成本分配給業務單位的方法
- 使用 Amazon OpenSearch Service 和 Amazon Kinesis Data Firehose 監控 Amazon WorkSpaces 應用程式 OpenSearch Amazon Kinesis Data Firehose
- 使用 Amazon WorkSpaces、Amazon WorkSpaces 應用程式和 Amazon Macie 進行網路分離和資料清理
- 使用 Amazon WorkSpaces 應用程式的 OneLogin SSO
- 使用 Amazon WorkSpaces 應用程式最佳化 Amazon Connect 呼叫音訊路徑 Amazon WorkSpaces
- Amazon Elastic File System 上 Amazon WorkSpaces 應用程式 Linux 機群的持久性儲存 Amazon Elastic File System
- 將 Okta SAML 應用程式重新導向至 Amazon WorkSpaces 應用程式原生用戶端
- 使用應用程式遮罩簡化 Amazon WorkSpaces 應用程式映像管理
- 使用 Amazon WorkSpaces 應用程式彈性機群和 Linux 相容性，以較低的成本串流應用程式
- 使用 WorkSpaces 應用程式從受管制環境的介面 VPC 端點進行串流
- 搭配 Azure AD 使用 Amazon WorkSpaces 應用程式權利
- Amazon WorkSpaces 應用程式的使用者問題報告程式
- 搭配 Google Workspace 使用 Amazon WorkSpaces 應用程式權利
- 在 Amazon WorkSpaces 應用程式上使用 Auth0 搭配 Microsoft Active Directory
- 使用 Microsoft AppLocker 管理 Amazon WorkSpaces 應用程式上的應用程式體驗
- 使用 Python 為 WorkSpaces 應用程式提供支援 Linux 影像助理 GUI
- WorkSpaces 應用程式用戶端的 Web 應用程式重新導向選項

文件歷史紀錄

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

變更	描述	日期
初次出版	—	2025 年 7 月 23 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

經常用於經常性問題的解決方案，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

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、低延遲網路連線能力。

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，例如在網際網路上編製資訊索引的 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，並透過核准的程序，讓使用者快速取得他們通常無權存取 AWS 帳戶 之 的存取權。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) 執行試驗，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。

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 () 文件中的信封加密。 AWS Key Management Service AWS KMS

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給 LLM。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，已在廣義和未標記資料的大量資料集上進行訓練。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 系統旨在自動容錯移轉、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

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

由 Klaus Schwab 於 2016 年推出的術語，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、特洛伊木馬程式、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)

此 AWS 計畫提供諮詢支援、訓練和服務，以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，請參閱本詞彙表中的 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 建議使用不可變的基礎設施作為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

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

OPC-UA

請參閱開啟程序通訊 - 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

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 支援使用 S3 AWS KMS (SSE-KMS) 的所有伺服器端加密中的所有 S3 儲存貯體 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。

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。

重新放置

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，定義所有參與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 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)，AWS 管理主控台 讓使用者可以登入 或呼叫 AWS API 操作，而不必為組織中的每個人在 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。

斯卡達

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

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 秘密中的內容？ 在 Secrets Manager 文件中。

設計安全性

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。

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，多次讀取。

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缺陷或漏洞。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。