aws

經過實證的多雲端策略開發實務

AWS 方案指引

AWS 方案指引: 經過實證的多雲端策略開發實務

Table of Contents

經過實證的多雲端策略開發實務

Tom Godden 和 Ellie Tamari，Amazon Web Services

2025 年 9 月 (文件歷史記錄)

組織現在面臨有關多雲端採用的衝突訊息。有些建議完全不要這麼做，有些則聲稱每個人都要切換到多雲端環境。這些極端情況之間的事實：多重雲端策略和多重雲端策略存在合法原因，成功取決於平衡潛在商業價值與固有複雜性和風險。

在 AWS，我們對互通性的承諾是許多客戶選擇平台的關鍵原因。我們相信，您可以自由地創新工作負載，並讓您能夠選擇最符合您需求的技術。在 AWS，我們一直處於開發解決方案的最前線，讓您能夠在任何環境中建置和部署應用程式。這種以客戶為中心的方法是 的基礎 AWS 雲端，受到全球數百萬客戶的信任。

我們了解客戶需要可順暢搭配現有工具和未來技術選擇的雲端平台。當您從其他供應商新增功能時，應該不需要重建所有項目。您的雲端應可協助您跨環境連線、保護和管理工作負載，而不必強制您成為每個平台的專家。 會將連線點直接 AWS 建置到其服務中，以協助您有效運作，無論您的策略是 AWS 專門使用 ，還是遵循選擇性的多雲端方法。

我們了解每個組織都有獨特的業務需求，以推動其雲端策略決策。無論您是主要在 上執行工作負載 AWS、跨多個雲端執行工作負載，還是使用 AWS 作為更廣泛的多雲端架構的一部分，我們都致力於協助您取得成功。 AWS 提供工具和功能的深度和廣度，以協助您更輕鬆快速地建置、遷移和操作工作負載。 AWS 工具可簡化跨供應商的管理，同時最大化雲端投資的效能和價值。

本文著重於多雲端策略取得成功的實證原則，包括多雲端方法的合理時機和位置，以及 如何 AWS 協助企業使用多雲端策略取得成功。它提供規範性指引，協助高階主管做出與多雲端採用相關的明智策略和決策選擇。本白皮書不提供多雲端實作的技術性深入討論。如需特定挑戰的技術實作支援和協助，建議您與 AWS 解決方案架構師合作。

本白皮書根據我們對 AWS 企業客戶的體驗，為多雲端的成功提供了九項經過驗證的原則。每個原則都解決了多雲端策略的關鍵層面，從調整業務目標到安全實作。透過套用這些原則，組織可以放心地導覽多雲端複雜性。

Tenet 1. 將多雲端目標與您的策略保持一致

根據「Gartner 的研究」和產業趨勢顯示，組織越來越採用多雲端方法來解決特定的業務需求。下列案例示範多雲端基礎設施在策略上何時具有優勢。

合併和收購

合併和收購 (M&A) 會建立雲端策略的立即決策。雖然操作多個雲端可能會增加成本和複雜性，但快速整合可能會延遲整合價值並中斷業務營運。您的雲端決策會成為實現 M&A 優勢的核心。

整合規劃應考量完整的技術環境。每個工作負載都需要在整合時間表和業務優先順序的範圍內進行評估。

我們的指引：

- 制定業務驅動的合併策略，在即時整合需求與長期營運效率之間取得平衡。在雜湊合併可能會中斷關鍵業務營運或延遲 M&A 價值實現的情況下，一開始會維護多個雲端。
- 建立符合整合時間表的明確工作負載置放條件。優先考慮產生營收的應用程式和核心業務流程，同時考慮技術相依性和營運需求。

希望利用另一個 CSP 的長期差異化功能

擔心遺失，促使某些公司想要一些每個雲端。工作負載置放決策會影響整個組織，從工程團隊到財務，再到安全操作。

因此，組織需要檢查其追求多個雲端的原因。有人認為，每個工作負載應該存在於最符合其需求的雲端服務提供者 (CSP) 上。不過，個別工作負載最佳化必須平衡更廣泛的組織影響。每個額外的雲端供應商都會面臨營運複雜性增加、建立新的人才需求，以及引入影響整個技術組織的安全考量。

我們的指引：

- 遵循 80/20 方法：為大多數工作負載選取主要供應商，並僅針對特定、高價值的使用案例考慮其他供應商。此策略可最大化效率和人才保留，同時降低複雜性。
- 考慮跨雲端操作的總成本。在分析中包含安全工具、控管產品、財務管理系統和營運開銷。
- 評估每個工作負載的相依性和互動。工作負載很少單獨運作；它們共用資料、安全控制和操作程序。
- 跨供應商進行徹底的價格效能分析。不僅比較直接成本，還比較管理多個環境的額外負荷。

持有公司的多雲端和營運公司或業務單位的主要雲端

私有股票公司和持有公司面臨獨特的雲端策略考量。他們的產品組合公司通常會維持獨立的雲端策略，通常是由過去的 M&A 活動所產生。此結構可降低通常與多雲端操作相關聯的複雜性，因為每個業務單位都會獨立運作。不過，這種獨立性可能會限制利用整個企業數量折扣和購買獎勵的機會。

持有公司層級的雲端策略有效性取決於產品組合公司的自主權及其個別技術需求。雖然合併可能會建立購買槓桿，但可能會與持有公司和私募資產產品組合的典型獨立操作模型發生衝突。

我們的指引：

- 了解 CSP 磁碟區折扣結構。每個供應商都提供從企業協議新增或移除子公司，以及將業務單位分割成個別實體的機制。這些代表雙向大門決策。
- 仔細規劃雲端購買承諾。儘早與 CSP 的帳戶團隊互動，或聯絡 AWS Partner 具備 AWS Cloud Operations 能力的 尋求協助。
- 平衡獨立性與效率。考慮共用服務或購買協議，讓產品組合公司受益，而不會限制其營運。
- 首先專注於業務目標。開發技術策略來支援您的操作模型，而不是為了自己的緣故而追求多雲端策略。
- 透過產品組合管理的角度評估雲端策略。考慮雲端選擇如何影響潛在的剝離或未來的收購。

Tenet 2. 請注意多雲端誤解

當您開發多雲端策略時，請避免下列各節討論的常見誤解。

每個人都採用多雲端策略

諮詢公司和媒體公司繪製了多雲端採用的複雜情況。研究顯示對多雲端方法有廣泛的興趣，但花費模式通常會說不同的故事。實際上，許多企業會維護單一雲端環境或明確的主要/次要 CSP 關係。此中斷連線強調了超越頭條新聞的重要性，並專注於組織的特定需求。

我們的指引：

- 根據您的特定業務需求做出雲端決策，而不是遵循產業趨勢。專注於組織的可衡量成本和風險。
- 在您的產業環境中檢查多雲端使用案例。適用於消費者技術公司的雲端策略可能不會轉換為金融服務、製造或遊戲環境。
- 將資料重力視為工作負載置放決策的主要因素。資料的位置和移動通常會決定最有效的雲端架構。
- 超越採用統計資料，以了解支出模式。高報告的多雲端採用率通常會掩蓋實際支出模式。
- 承諾多雲端環境之前，請評估技術限制條件。有些工作負載會在其元件保留在單一雲端環境中時發揮最佳效能。

多雲端可降低廠商鎖定的風險

廠商彈性是雲端策略開發的合法考量。Organizations 重視隨著業務需求發展而調整其技術選擇的能力。此問題反映了傳統 IT 投資的先前經驗，這些投資建立了具約束力的長期承諾。 雲端服務提供有關提供者彈性的不同動態。 AWS 提供開放原始碼相容的服務和資料可攜性選項，可減少遷移的技術障礙。不過，彈性與營運效率之間的權衡仍然很重要。組織必須權衡維護供應商選項的商業價值，以及與主要供應商的專業服務深度整合的技術優勢。

有些客戶嘗試透過工程設計使用容器的雲端獨立解決方案來避免鎖定。這種方法通常會將它們限制為基本運算和儲存服務，並繞過進階雲端功能的優勢。我們的經驗顯示，相較於使用原生 服務，此策略會因為所需的開發時間和資源增加而增加相當複雜度。

我們的指引：

- 考慮雲端無關架構的完整成本。額外的工程開銷可能不會證明可攜性優勢。
- 使用雲端原生功能取得最大值。單獨使用基本運算和儲存服務通常會犧牲安全性、可擴展性和創新的顯著優勢。

- 根據業務需求規劃雲端策略。當多雲端實作新增了明確的價值，例如能夠在多個平台上為使用者提供服務時，額外的工程投資就會變得值得。
- 評估逼真的退出案例和成本。比較變更供應商的可能性和費用，以及使用整組 的好處 AWS 服務。
- 在 Amazon Relational Database Service (Amazon RDS) 等 AWS AWS 受管服務的開放原始碼基礎上建置，可為您提供彈性和卓越營運，並支援您目前使用的資料庫引擎。
- 利用 提供的完整遷移工具 AWS。如果您離開 AWS 使用其他供應商，我們會協助您將工作負載朝任何方向移動，並提供免費的資料輸出。如需詳細資訊，請參閱 AWS 部落格文章 移出時免費資料傳輸至網際網路 AWS。

多雲端可改善可用性和彈性

對雲端供應商在中斷期間無縫切換工作負載的信心，推動了某些組織實現多雲端策略。這種思維會建立雲端基礎設施彈性的過度簡化檢視，忽略基本的技術現實。

根據與多雲端客戶合作多年的經驗 AWS，我們發現在供應商之間維持完整的工作負載可攜性通常會產生巨大的複雜性，而不會帶來所有預期的好處。由於資料重力限制，資料密集型應用程式面臨無法克服的挑戰。事實上，在我們看來，組織幾乎不可能成功實作真正無縫的多雲端容錯移轉，以處理資料繁重的工作負載。

在社交媒體文章中，Gartner 的傑出副總裁分析師 Lydia Leong 強調了這個觀點：「多雲端容錯移轉非常複雜且成本高昂，幾乎幾乎總是不切實際，而且這不是解決雲端恢復風險特別有效的方法。」 網路、儲存、資料庫、機器學習和安全性供應商之間的固有差異，使得真正的可攜性幾乎是不可能的。跨供應商分散工作負載可能會增加風險，因為任一環境中的故障都可能觸發所有環境的中斷。

我們的指引：

- 專注於個別工作負載的掌握 AWS 功能，而不是追求複雜的多雲端架構。
- 透過 AWS 區域 和可用區域建置彈性，而不是嘗試跨供應商容錯移轉。如需深入了解 AWS 如何在實體資料中心之間自動容錯移轉工作負載的技術，請參閱 AWS 部落格文章「區域自動轉移」：當我們偵測到潛在問題時，自動將流量移離可用區域。
- 以策略方式將工作負載遷移到 AWS，並一次專注於一個應用程式，以最大限度地取得成功。

多雲端提供更好的定價

價格競爭性可能是多雲端環境中所有 最弱的引數。組織使用複雜、昂貴的軟體或資料中心合約的經驗，將它們鎖定在多年協議中，讓他們在採購 IT 服務時保持警惕。傳統的採購方法尚未適應pay-as-

you-go購買、數量折扣或雲端中價格競爭的實際情況。（截至 2025 年 1 月， 自成立以來 AWS 已降價 151 次。）

降低成本的最大單一驅動因素是妥善管理和最佳化的雲端環境。一家公司主要與供應商合作，其服務提供價格效能優勢（例如以 AWS Graviton 等自訂設計的晶片為基礎的運算執行個體），並擁有卓越的雲端財務管理解決方案，從而獲得更好的成本最佳化。根據 2022 年 Hackett Group 對超過 1，000 個組織的研究，相較於多雲端組織， AWS 客戶的基礎設施支出佔總 IT 支出的百分比降低了 20%。

我們的經驗顯示，公司預期在多個雲端中營運的成本和複雜性不會增加，也不會適當權衡此成本與head-to-head採購業務中感知的收益。

我們的指引：

- 在 AWS Well-Architected Framework 成本最佳化支柱上建置您的成本最佳化策略。有五個設計原則：
  - 實作雲端財務管理：為了在雲端中取得財務成功並加速商業價值實現，您必須投資雲端財務管理。您的組織必須投入必要的時間和資源，以打造這個新的技術與使用管理領域的能力。如同您的安全或操作功能，您需要透過知識建置、計劃、資源和程序來擴展功能，以協助成為具成本效益的組織。
  - 採行取用模式：僅為您消耗的運算資源付費，依照業務需求增減用量。例如，在工作週期間，開發和測試環境通常每天只會使用八小時。您可以在資源未使用時停止這些資源，以節省 75% 的潛在成本 (40 小時相較於 168 小時）。
  - 測量整體效率：測量工作負載的業務輸出，以及與交付相關的成本。使用此資料以了解您透過增加輸出、增加功能及降低成本所獲得的增益。
  - 停止在未區分的繁重工作上花費金錢：CSPs 會繁重處理資料中心操作，例如機架、堆疊和驅動伺服器。它們也會消除使用 受管服務管理作業系統和應用程式的操作負擔。這可讓您專注於客戶和商業專案，而不是 IT 基礎設施。
  - 分析和歸因支出：採雲端式能更容易準確識別工作負載的用量和成本，繼而允許將 IT 成本透明化地歸因至收入流和個別工作負載擁有者。如此有助於測量投資報酬率 (ROI)，並且讓工作負載擁有者有機會優化資源和降低成本。
- 考慮到不同供應商之間營運的財務開銷，我們會引導客戶大量投資於自動化和成本最佳化工具。每個 CSP 都會在此區域提供廣泛的原生工具，例如 AWS 成本最佳化中心。大多數原生工具為雲端環境中的客戶提供卓越的功能。不過，若要了解跨多個 CSPs 的支出，您可以從一組豐富的 ISV 和軟體即服務 (SaaS) 產品中進行選擇，這些產品可延伸這些功能，以提供成本最佳化的單一體驗。
- 透過支出公平策略來排除購買力不會產生商業價值。它可能會破壞潛在的數量折扣，並可能破壞技術設計。使用雲端服務最有效率的方式是使用主要供應商進行大量操作，並僅在增加商業價值時使用其他 CSPs。

Tenet 3. 擁有明確的策略和控管來支援它

決定追求多雲端策略並不足夠；您必須建立實現目標的策略，包括明確控管哪些工作負載將前往何處及其原因。應使用評估條件來最佳化工作負載及其相依性。如果評估保留給個人，則跨 CSPs 的不協調擴展可能會侵蝕多雲端策略的值。我們建議您定期評估 CSP 工作負載效能，並使用評估做為 CSP 選擇、條件和未來用量的關鍵輸入。

有效的控管策略需要了解整個企業使用的服務、應用程式和元件總數。整合到此是強大的標記策略，可跨越 CSPs，並為所有部署的資源建立明確的擁有權、用量和環境（例如開發、QA、預備和生產）。所有內容都應標記給擁有者；如果未標記或無法識別擁有者，則應將其移除。我們與主要金融服務組織緊密合作，該組織會自動尋找和移除任何未標記的資源，並認為這是最佳實務，無論它對開發團隊造成的不便為何。此標記方法會編纂控管規則，並自動化強制執行，而不是建立要繼續的區塊（即實作護欄，而不是閘道）。成本、操作和安全性必須以相同的方式進行追蹤、監控和操作，並在 CSPs 之間具有相同的資料深度和透明度。

當您實作多雲端策略時，跨雲端提供者建立清楚且一致的帳戶結構，對於維護營運控制和安全性至關重要。我們建議採用hub-and-spoke模型，您可以在其中 AWS 帳戶 為不同的業務單位建立個別的模型。這些由兩個關鍵的中央帳戶錨定：用於合併合規和安全監控的安全/稽核帳戶，以及用於管理互連性的中央聯網帳戶。（此方法在 的設計中編AWS Control Tower纂。 不過，最低權限和職責分離的原則同樣適用於其他雲端。 AWS Well-Architected 架構詳細討論了這些概念，強烈建議技術對象使用。）此基礎方法應鏡像到雲端提供者，以維持控管和操作的一致性。工作負載帳戶應依環境（開發、預備、生產）或 函數組織，並建立明確的帳戶建立和刪除程序。

我們的指引：

- 實作全面的標記策略，在所有雲端資源中維持明確的擁有權和使用模式。透過一致的標記政策追蹤環境、成本中心、應用程式和業務單位。移除缺少適當標籤的資源，以強制執行控管標準並保持環境清晰度。
- 建立統一的合規架構，以映射多雲端環境中的法規要求。維護明確文件，說明每個雲端供應商的控制和認證如何支援您的合規義務。
- 透過自動化自動執行控管，而不是使用手動核准程序。將您的控管規則編碼為自動化系統，防止政策違規發生。這可移除人為錯誤，同時維持開發速度。
- 使用集中式安全和聯網控制，在hub-and-spoke模型中建構帳戶。建立安全稽核和網路管理的專用帳戶，以集中關鍵功能。此基礎可在整個組織中實現一致的安全政策和網路連線。
- 若要維持操作界限，請為不同的環境和函數建立單獨的帳戶、訂閱或專案（取決於您的 CSP 命名法）。依開發、預備和生產環境分割工作負載。此區隔可防止安全事件分散，並維持明確的操作網域。

- 透過整個環境的一致指標來監控成本、操作和安全性。針對資源使用率、安全事件和花費模式實作統一監控。使用此資料可最佳化工作負載配置和資源配置決策。
- 透過組織政策和自動化控制，防止未經授權的雲端使用。定義明確的帳戶建立和資源佈建程序。實作服務控制政策 SCPs)，在所有帳戶中強制遵循組織標準。
- 建立偵測和預防性控制，以防止影子 IT 透過未經授權的提供者帳戶產生。透過費用報告和網路流量監控未經授權的雲端使用情況。封鎖未經授權的供應商存取，同時維護核准的創新路徑。

Tenet 4. 請勿將連續工作負載分散到雲端

在多個雲端提供者之間分散連續工作負載會造成不必要的複雜性、風險和成本。當處理和分析資料的工作負載跨越多個供應商時，組織會面臨資料移動、同步和一致性的挑戰。團隊必須為每個供應商導覽不同的 APIs、管理介面、安全模型和操作程序，這會增加發生錯誤的可能性並增加操作開銷。這種複雜性會增加錯誤和操作負荷的機會，並可能阻礙敏捷性和可擴展性。

不過，在某些實際案例中，由於特定的商業或技術需求，組織可能需要在雲端之間分配連續工作負載。在這些情況下，我們建議您建立明確的標準和指導原則來評估權衡，並確保方法符合您組織的整體多雲端策略。

當組織選擇將工作負載分散到多個雲端時，採用以簡訊和鬆散耦合為中心的架構可以緩解許多相關的挑戰。這是在雲端之間分隔問題的最佳方式，並在供應商受損時減少影響範圍。最有時間限制的操作，例如金融交易，最好保留在單一環境中。不應允許某個環境中的中斷危及另一個環境中的工作負載。

我們的指引：

- 為營運獨立性設計雲端工作負載，將供應商之間的即時相依性降至最低。需要工作負載分佈時，請實作高效的大量資料傳輸機制，而不是維持持續的跨雲端連線。
- 根據明確的業務條件評估每個提議的分散式工作負載。同時考慮 分佈帶來的策略優勢和操作複雜性。

Tenet 5. 擁有長期整合策略

當您在不同雲端的應用程式之間移動大量資料時，請小心，特別是當您的運算資源和應用程式部署在一個 CSP 中，而您的資料儲存資源部署在另一個 CSP 中時。這種情況可能會增加複雜性和延遲，進而抵銷感知的好處。我們會與許多客戶交談，這些客戶在一個雲端上有資料湖，但想要使用來自另一個 CSP 的工具執行機器學習 (ML) 或分析。決定將工作負載放置在多雲端環境中的位置，是組織面臨的最關鍵決策之一，通常是最具挑戰性的決策之一。我們建議您透過三個關鍵維度來評估每個工作負載配置決策：技術需求、業務需求和供應商優勢。

透過映射每個工作負載的基本特性來開始技術評估：運算能力、資料操作、回應時間需求和成長需求。應用程式自然會在接近資料時發揮最佳效能。將應用程式移離資料來源會造成不必要的技術障礙，並降低效能。

商業決策必須考量供應商定價、資料落地要求和廠商合約。每個工作負載置放都會影響整個組織的操作、安全性和生產力。獨立查看工作負載會導致決策不佳。

我們的指引：

- 在雲端之間實作大量資料傳輸，而不是即時存取。使用高效的大量操作來排程定期資料重新整理，而不是在雲端之間使用持續的 API 呼叫。這種方法可降低成本、改善可靠性，並維持一致的效能。例如，匯出摘要每日銷售資料，而不是查詢跨雲端的個別交易。
- 設計工作負載置放時，請考慮資料重力。讓應用程式靠近其主要資料來源，以維持效能並降低成本。ML 模型、分析引擎和交易處理系統都受益於直接存取其資料。將這些工作負載移離其資料會導致不必要的網路延遲和複雜性。
- 在完整雲端策略的環境中評估工作負載決策，而不是單獨檢閱。考慮每個置放選擇如何影響整個組織的操作程序、安全控制和團隊功能。整體檢視時，似乎最適合單一工作負載的決策可能會使監控複雜化或增加安全風險。
- 定義明確的資料擁有權和管理政策，以指定不同類型的資料可以存放的位置。建立資料分類架構，以推動有關跨雲端提供者放置資料的一致決策。

Tenet 6. 以策略方式使用容器

容器在支援多雲端策略方面可以發揮重要作用，但識別其限制也很重要。對於任何現代的雲端原生應用程式來說，使用容器通常是個好主意，因為它們可為不同環境的可攜性和一致性提供優勢。容器與平台無關，這表示它們可以在支援容器化技術的任何雲端平台或基礎設施上執行，例如 Kubernetes。使用容器的組織可以開發和封裝其應用程式一次，然後將它們一致地部署到多個雲端提供者或內部部署環境，而無需進行重大修改。透過封裝容器內的應用程式程式碼、相依性和執行時間環境，您可以實現高度的可攜性，這可讓您在雲端提供者之間或在雲端和內部部署資料中心之間無縫移動工作負載。

不過，容器可能無法解決每個使用案例，也無法消除組織在採用多雲端策略時可能面臨的所有挑戰。容器最適合用於現代的微服務型架構，但可能不太適合大型的單一應用程式。此外，雖然容器可以解決某些可攜性方面的問題，例如應用程式執行期，但它們不會自動解決資料管理、安全政策和其他跨雲端相依性的問題。組織仍需要仔細規劃和架構其多雲端解決方案，以確保一致的資料管理、統一的安全控制，以及雲端託管和內部部署元件之間的無縫整合。

我們的指引：

- 使用每個雲端供應商的原生容器管理功能，將商業價值最大化並加速交付。這種方法可確保最佳效能，同時避免建立很少提供有意義的傳回的雲端無關解決方案的複雜性。
- 開發容器策略，以解決完整的營運狀況，包括資料管理、安全性和跨雲端相依性。當您做出容器架構決策時，專注於業務成果。

Tenet 7. 擁有單一 CCoE，但擅長其中

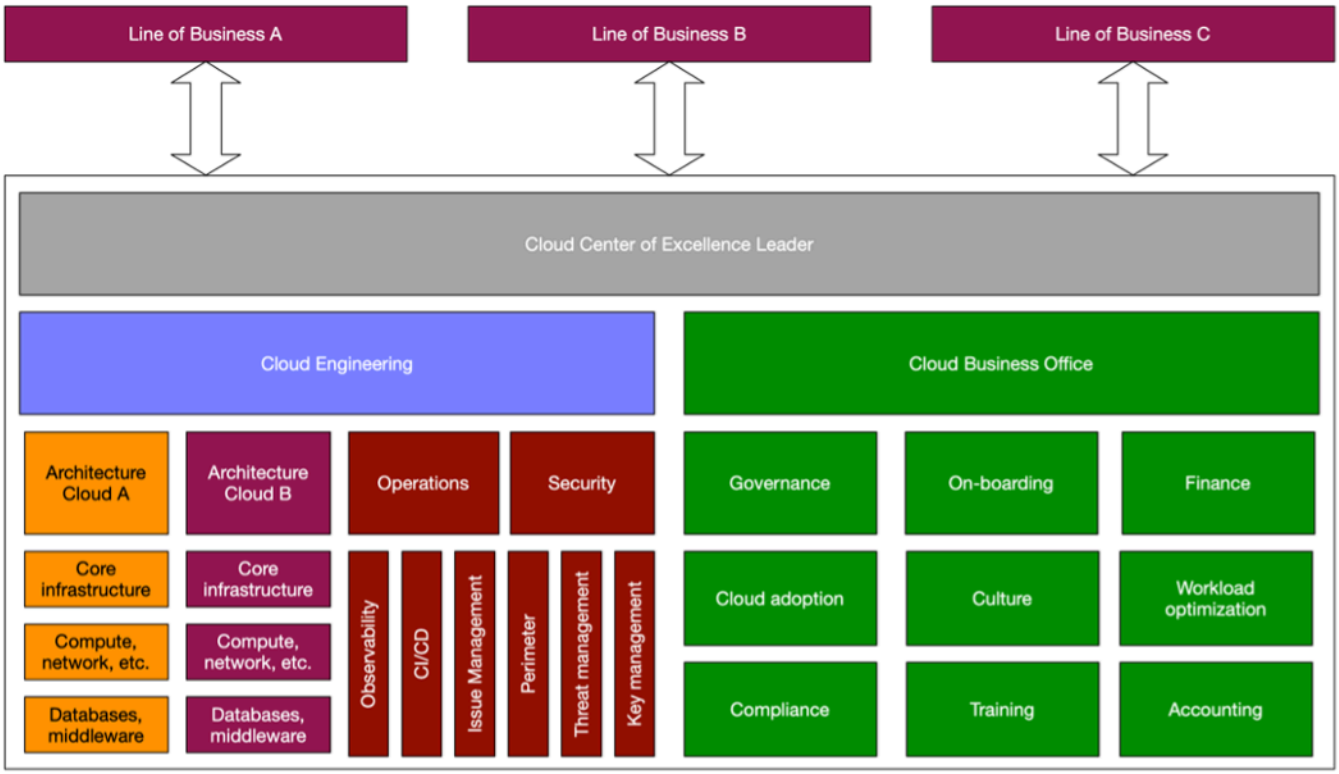
在我們建議許多 AWS 客戶時，您應該在組織內建置 Cloud Center of Excellence (CCoE)，以提供雲端之旅的領導力、標準化和加速。談到多雲端環境，我們發現最成功的公司對其 CCoE 採取平衡的方法。

我們建議您使用單一、統一CCoEs 來監督組織的多雲端策略，而不是為每個 CSP 建立單獨的 CCoE。這有助於確保協調一致的方法，而不是孤立的工作，這可能會導致差異、重新設計和浪費。請確定您單一 CCoE 中的團隊具有組織使用的每個 CSP 所需的專業技能、工具和機制。這項專業知識可讓 CCoE 有效地控管、支援和加速使用不同的雲端平台。

例如，CCoE 應該擁有 AWS特定專家，這些專家可以深入了解 AWS 雲端、 服務和最佳實務，以及其他 CSPs 專家，這些專家可以指導組織使用這些雲端技術。單一 CCoE 中的這種專業知識可協助您的組織從集中式方法的協調和標準化中受益，同時確保以最佳方式使用每個雲端平台。

單一 CCoE 應做為中央管理機構，為組織的多雲端策略建立標準、政策和最佳實務。雲端工作負載和專案的實際實作可以分發給專業團隊或業務單位，同時 CCOE 提供監督、支援和協調。這種平衡的方法有助於確保具有一致性的多雲端策略，同時在組織內提供必要的靈活性和自主性。

下圖說明 CCoE 如何跨多業務線 (LOBs)、雲端工程團隊和雲端商業辦公室 (CBO) 團隊提供集中式方法和管理。



我們的指引：

- 建構 CCoE 以維持策略監督，同時內嵌每個雲端供應商的專業知識。專注於在個別雲端平台中招聘深入的專業知識，而不是尋求罕見的多雲端專家，並培養內部知識共享以建立組織能力。
- 讓您的 CCoE 能夠為安全性和可觀測性等交叉切入問題建立全企業標準，同時透過使用雲端原生工具和服務，為個別團隊提供在這些準則內執行的自主性。
- 制定全面的人才策略，在主要雲端平台的深厚專業知識與更廣泛的架構知識之間取得平衡。專注於建置結合強大、雲端特定技能與企業架構體驗的團隊。

Tenet 8. 確保安全始終是首要任務

多雲端方法會提高未經授權的存取風險，讓您更難確保安全性，因為您的安全狀態必須考慮更多的攻擊面。多雲端策略通常會強制公司在身分管理、網路安全、資產管理和稽核記錄等領域跨 CSPs 處理多個安全模型。這種複雜性風險會使透明度更加困難、增加安全團隊的負擔，並提高風險。

安全自動化在多雲端環境中至關重要。身分管理必須順暢地跨環境運作；它必須連接現有的身分提供者，同時保持一致的存取政策。安全性需要跨資料、網路和端點層的整合保護。資料分類、加密和生命週期管理構成了基礎。網路安全是以標準化設計和連線模式為基礎。端點保護透過一致的修補程式管理和主機型控制來完成架構。

這些基本元素對於成功和安全地採用多個雲端供應商至關重要，而且必須在任何多雲端策略規劃中儘早考慮。

我們的指引：

- 在您的多雲端環境中實作整合的安全架構，著重於三個核心元素：透過標準化分類和加密進行資料保護、透過一致的設計模式進行網路安全，以及透過系統控制和修補程式管理進行端點保護。
- 建立統一的安全操作模型，利用每個雲端供應商的原生安全功能，同時透過標準化工具和程序維持集中的可見性和控制。
- 使用 Amazon Security Lake 集中收集和分析安全資料。此平台會將來自其他雲端提供者 AWS、SaaS 應用程式和內部部署系統的安全資訊彙總為單一檢視。它支援開放式網路安全結構描述架構 (OCSF)，並啟用跨混合多雲端環境的標準化分析。這種集中式方法可改善威脅偵測和回應，同時簡化安全操作。
- 部署每個供應商的原生安全工具，以增強您的保護功能。這些專用服務可解決提供者特定的功能，同時將資料饋回集中式安全平台。結合原生工具和集中式可見性，有助於在整個基礎設施中提供全面的安全涵蓋範圍。
- 實作統一的可觀測性策略，讓您從頭開始全面掌握整個雲端環境，包括營運和安全資料。標準化業界領先的監控方法，無論業務服務在何處營運，都能持續追蹤業務服務。
- 為營運資料收集和視覺化建立全企業標準，以便在多雲端環境中快速識別和解決問題。專注於為同時為技術和業務利益相關者提供服務的操作洞察建立單一事實來源。

Tenet 9. 接受 80/20 方法而非相等分佈

您如何在供應商之間分配工作負載，從根本上決定您的多雲端成功。許多組織在雲端分佈中錯誤地追求平等，並嘗試將工作負載平均分散到各個供應商。這種方法會增加複雜性，而不會提供成比例的好處。相等分佈會分割您的技術功能、縮減您的購買能力，並產生不必要的營運開銷。當團隊被迫同時維持跨多個平台的能力時，很難開發深入的專業知識。

80/20 方法提供明顯優於跨雲端平均分佈的結果。將 80% 的投資集中在一家主要供應商，同時選擇性地將其他供應商用於特定功能，可建立降低成本和複雜性的平衡策略。這種集中的方法可加速創新，因為您的團隊可以使用主要平台的進階服務開發深入的專業知識。您的技術人員可以在一個架構中成為專家，而不是在多個環境中保持表面層級知識。當工程師主控一個平台時，他們會更有效率地建置、更快地進行故障診斷，並實作更複雜的解決方案。

遵循 80/20 方法的公司通常會報告更好的人才保留，因為他們的團隊開發了有價值、可銷售的專業知識，而不是在多種技術之間進行延伸。這種集中策略還透過限制跨供應商的不同安全模型的複雜性，協助簡化安全管理。主要雲端會接收您對安全工具、監控解決方案和操作程序的大部分投資。這建立了比平均分割資源可能更強大的安全基礎。

我們的指引：

- 選擇符合您大多數業務和技術需求的主要雲端供應商。此供應商應支援至少 80% 的工作負載，並成為雲端策略的基礎。將您的訓練投資、架構標準和操作程序專注於從此主要平台最大化價值。
- 針對需要放置在次要雲端上的工作負載，制定明確的條件。這些條件應著重於無法在主要供應商上實現的特定商業價值。僅為了維持提供者之間的支出公平或人工平衡，而拒絕將工作負載放置在次要雲端上。
- 組織您的企業協議，以反映您的 80/20 方法。根據集中支出與主要供應商商量折扣，並針對特定使用案例與次要供應商保持靈活性。這種方法可最大化您的購買利用率，通常比平均分配您的支出獲得更好的整體定價。
- 將您的人才策略與您的 80/20 方法保持一致。投資於使用主要供應商的服務開發深入的專業知識，同時保持對次要平台的足夠知識，以支援特定工作負載。這種專注的人才策略可提高生產力、加速交付，並降低關鍵技能差距的風險。
- 定期測量多雲端策略的業務成果。追蹤顯示從每個提供者取得之值的指標，並視需要調整您的分佈。目標是不完全避免多雲端，而是以策略方式實作它，其中特定工作負載真正受益於其他供應商獨有的功能。

結論

本文概述了開發有效多雲端策略的九個關鍵原則。組織透過主要雲端方法獲得最大成功，並策略性地使用特定業務需求的其他供應商。我們描述的 80/20 方法在重點與靈活性之間取得平衡，並使組織能夠開發更深入的專業知識、維持更強大的供應商關係，並培養更有價值的人才，同時仍然滿足合法的多雲端需求。

成功的多雲端實作需要明確評估業務需求，而不是遵循產業趨勢。公司必須建立強大的控管、維持安全為第一要務、避免將連線工作負載分散到各個供應商、將應用程式與其交易資料一起保存、辨識容器限制，以及維護統一但專門的雲端卓越中心。

雲端 AWS 的方法基本上是以客戶選擇和互通性為基礎。我們設計的工具和服務可無縫跨環境運作，因為我們了解您的業務需求通常超出單一供應商。從混合連線解決方案到跨越環境的容器協同運作，AWS 提供可協助您在技術環境中有效運作的功能。

您可以透過直覺式工具和一致性界面， AWS 簡化多雲端管理，而不是強制您成為多個平台的專家。我們專注於消除複雜性，以便您可以專注於創新。這些功能可協助您根據自己的條件實作多雲端策略，這表示 AWS 只使用 ，或是 AWS 服務 搭配其他環境使用特定 。

雲端應該授權您的商業策略，而不是限制它。透過套用本文概述的原則並利用 AWS 互通性功能，您可以建置雲端方法，將價值最大化、將不必要的複雜性降至最低，並讓您的組織在現今的動態商業環境中獲得長期成功。

若要進一步了解可協助簡化混合多雲端環境管理 AWS 的解決方案，請參閱AWS 多雲端的解決方案。

資源

參考

- 使用雲端卓越中心 (CCOE) 轉換整個企業 (AWS 部落格文章）
- AWS Well-Architected 架構
- 使用 Cost Optimization Hub 識別機會 (AWS Cost Management 文件）
- 遷移至 Amazon Web Services 的商業價值 (Hackett Group，2022 年 2 月）
- 移出時免費將資料傳輸到網際網路 AWS(AWS 部落格文章）

工具

- 區域自動轉移 – 偵測到潛在問題時，自動將流量移離可用區域 (AWS 部落格文章）
- AWS 多雲端解決方案

AWS 合作夥伴

- AWS 雲端 操作能力

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 9 月 3 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 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

A2A Agent-to-Agent)

支援任務委派和狀態轉移的agent-to-agent協同合作的狀態通訊協定。

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。

客服人員

一種 AI 系統，可使用工具自動推理、規劃和採取行動來實現目標。

客服人員操作

在生產環境中大規模建置、測試、部署和執行 AI 代理器的操作實務。

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效益、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。

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 將指導方針整理成六個重點領域：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。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，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。

公民開發人員

在沒有專業技術技能的情況下，使用無程式碼/低程式碼平台建立 AI 應用程式的商業使用者。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

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

雲端運算

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

雲端操作模型

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

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

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

這些階段由 Stephen Orban 在部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略關聯的資訊，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 成員帳戶來管理組織的帳戶，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。

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

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

加密金鑰

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

端序

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

端點

請參閱 服務端點。

端點服務

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

企業資源規劃 (ERP)

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

信封加密

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

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

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

epic

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

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

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

F

事實資料表

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

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等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。

FM 閘道

集中式中介，可控制和標準化對基礎模型的存取。也稱為 LLM 閘道。

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。

護欄 (AI)

可篩選、驗證和限制代理程式輸入和輸出的安全機制，以協助確保負責任且安全的 AI 行為。

H

HA

請參閱高可用性。

異質資料庫遷移

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

高可用性 (HA)

工作負載在遇到挑戰或災難時持續運作的能力，無需介入。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，並處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

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

保留資料

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

human-in-the-loop (HitL)

一種工作流程模式，其中代理程式執行會在關鍵決策點暫停進行人工審核和核准。

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 Rs。

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。

MCP

請參閱模型內容通訊協定。

模型內容通訊協定 (MCP)

用於代理程式對工具通訊的無狀態通訊協定。

MCP 伺服器

透過模型內容通訊協定公開一或多個工具的服務。

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

屬於組織一部分的管理帳戶 AWS 帳戶 以外的所有 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 建議使用不可變基礎設施做為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

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

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

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

操作水準協議 (OLA)

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

操作整備審查 (ORR)

問題和相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作準備審查 (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。

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

以預留位置值取代資料集中個人識別符的程序。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)、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。

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

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。它包含秘密值及其中繼資料。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？ Secrets Manager 文件中的 。

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

由接收資料的 AWS 服務 在其目的地加密資料。

服務控制政策 (SCP)

為 AWS Organizations中的組織的所有帳戶提供集中控制許可的政策。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制政策。

服務端點

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

服務水準協議 (SLA)

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

服務層級指標 (SLI)

服務效能方面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

描述您與 共同 AWS 承擔雲端安全與合規責任的模型。 AWS 負責雲端的安全，而 負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

陰影 AI

在組織內受管管道之外建置或使用的未授權 AI 應用程式。

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。

tool

代理程式可以叫用以在外部系統中執行操作的函數或 API。

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，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。