AWS 適用於 SaaS 產品的 上的網路連線選項

AWS 方案指引

AWS 方案指引: AWS 適用於 SaaS 產品的 上的網路連線選項

Table of Contents

簡介 1
目標對象 1
目標 1
評估決策 3
了解您的市場 3
了解您的角色 3
產品和商業指標 4
商業模型和市場定位 5
成長和市佔率 5
客戶體驗 6
財務效能 7
合規與風險 8
合作夥伴策略 9
工程指標 9
開發指標 10
卓越營運指標 14
安全與控管指標 15
AWS 網路概觀 17
AWS 服務 17
AWS PrivateLink 17
Amazon VPC Lattice 17
VPC 對等互連 17
AWS Transit Gateway 18
AWS Site-to-Site VPN 18
AWS Direct Connect 18
功能 18
安全性功能 19
評估選項 22
指標 22
擁有權總成本 23
VPC 互連成本 24
AWS PrivateLink 成本 24
Amazon VPC Lattice 成本 24
AWS Transit Gateway 成本 24

AWS Site-to-Site VPN 成本 25
AWS Direct Connect 成本 25
公有網際網路存取成本 25
值映射 25
網路案例 27
在 上操作 AWS 27
AWS PrivateLink 29
Amazon VPC Lattice 30
VPC 對等互連 32
AWS Transit Gateway 33
在內部部署操作 36
AWS Site-to-Site VPN 38
AWS Direct Connect 41
傳輸 VPC 架構 42
公有網際網路 45
在其他 CSPs 上操作 46
支援混合環境 48
進階聯網案例 50
雙向通訊 50
TCP、UDP 和專屬通訊協定 50
反面模式 52
可用區域與 不相符 AWS PrivateLink 52
AWS Site-to-Site VPN 之間的連線 AWS 帳戶 54
後續步驟 55
評估 55
市場分析 55
策略一致性 56
標準化 56
控管 56
重複 57
資源 58
AWS 文件 58
其他 AWS 資源 58
文件歷史紀錄 59
詞彙表 60
..... 60

A 60
B 63
C 65
D 67
E 71
F 72
G 74
H 75
I 76
L 78
M 79
O 83
P 85
Q 87
R 87
S 90
T 93
U 94
V 95
W 95
Z 96
..... xcvii

AWS 適用於 SaaS 產品的 上的網路連線選項

Tomas Sykora 和 Luca Schumann，Amazon Web Services

2025 年 9 月 (文件歷史記錄)

本指南探討將消費者應用程式連接到軟體即服務 (SaaS) 供應商的常見案例。它討論如何連接到內部部署、 、 AWS 雲端其他雲端服務提供者 (CSP) 雲端或混合架構中的資源。這些案例包括下列項目：

- 透過 HTTPS 公開 Web 服務
- 公開 TCP 型服務
- 使用 AWS AppSync實作發佈訂閱 (Pub/Sub) 和 GraphQL APIs
- 使用 AWS 資源公開即時應用程式的 WebSockets
- 啟用互動式服務通訊的雙向存取

透過與本指南涵蓋的最佳實務保持一致，SaaS 供應商可以推動客戶信任，並支援可擴展、安全和彈性存取 SaaS 產品。

本指南也包含自我評定條件，協助您評估如何成功滿足 SaaS 產品的消費者聯網需求。除了連線模式之外，您還可以找到 AWS 聯網服務的完整比較、各種部署案例的高階架構圖，以及如何根據您的特定商業環境選擇正確方法的實際指導。本指南探索每個聯網選項的安全考量、討論要避免的常見陷阱，並提供實作建議，以平衡技術需求與營運效率。此外，您還可以找到策略架構，讓您的聯網決策與您的商業模型、成長目標和法規合規需求保持一致。

目標對象

本指南適用於 SaaS 供應商。它可協助設計、實作和最佳化 中 SaaS 產品的網路連線能力的雲端架構師、產品經理和網路工程師 AWS 雲端。若要了解本指南中的概念和建議，您應該熟悉 AWS 基本概念、核心 SaaS 概念和高階聯網原則。

目標

本指南討論網路架構選項和經過欄位測試的最佳實務，可協助消費者最佳化對 SaaS 產品的存取。實作本指南中的建議可支援下列項目：

- 易於整合 – 提供從加入到生產的簡單客戶旅程，以便您可以加快客戶實現價值的時間並縮短收入確認週期。

- 適應性 – 透過適應客戶不斷變化的需求，無縫整合客戶的現有網路基礎設施。這可增強產品的價值主張。
- 總擁有成本 – 標準化網路存取，以減少變更成本和每個租用戶的成本。透過改善部署一致性，您也可以縮短執行根本原因分析或修復的時間。
- 相依性管理 – 了解不同網路存取選項的相依性、長期影響和權衡。這有助於產品領導者做出明智的產品決策。
- 可編譯性和可擴展性 – 將核心功能的開發與操作基礎設施分離。這有助於開發團隊更快地移動，並專注於為客戶創造價值。
- 推動信任 – 透過提供彈性、容錯、安全且可擴展的 SaaS 產品存取，您可以降低法規風險，並取得支援客戶成長能力的信任。

評估 SaaS 產品的網路存取決策

了解您的市場

您現在對聯網所做的決策會決定 SaaS 產品的價值主張是否可以交付給客戶。雖然這些決策的策略重要性，但提供對 SaaS 產品的存取通常被視為純技術主題。此感知帶來的風險包括延長收入辨識週期、營運效率低下，以及與業務策略不一致。例如，如果快速擴展是策略業務目標，則決策過程的引導因素應該是您考慮的解決方案是否可擴展且足夠靈活以支援擴展。即使您成功發展業務，營運開銷也不得成為未來成長的障礙，而且不一致的成本結構可能會消耗您的所有利潤。

例如，考慮以下市場考量因素如何影響產品的技術層面，例如聯網：

- 如果您的商業模型是以訂閱為基礎，您的客戶可能會偏好具有可預測、經常性成本的解決方案，而不是大型的前期投資。
- 如果您的商業策略以高價值的企業級客戶為目標，則安全、控管和法規合規標準會決定是否甚至考慮您的 SaaS 產品。
- 如果您的目標市場大多是新創公司，則易於整合、價值實現時間和適應性可能是重要因素。新創公司通常會優先考慮速度和敏捷性。由於他們需要建立品牌並快速產生利潤，他們可能偏好快速且易於整合的解決方案，可以經濟實惠地擴展、減少對專家的依賴，並且不會綁定寶貴的週期。
- 有些企業需要穩定、高輸送量和低延遲的存取。這包括娛樂和媒體產業、製造和金融交易處理。如果這些是您的目標客戶，可靠性是他們的首要考量。

在所有這些情況下，如果聯網存取不順暢，客戶可能會感知到運作狀態良好的 SaaS 產品。如果聯網成為障礙，則不支援您的商業案例。如果您的客戶無法可靠地存取您提供的服務，則 SaaS 產品的價值主張為 nil。

了解您的角色

您在支援業務目標中的角色取決於您是誰、您的特定個人和團隊目標，以及您的客戶是誰，以及對他們的重要性。即使您不是通常與客戶互動的團隊的一部分，您也需要關心他們是誰以及他們需要什麼。工程和開發團隊也必須關心他們的內部客戶，尤其是他們定期與之互動的客戶。一般而言，這些是操作和客戶成功團隊。

如果您是銷售組織的一部分，請務必與產品和工程團隊溝通聯網，即使這是一個看似純的技術主題。分享有關目標市場結構的洞見。傳達您現有和潛在客戶和合作夥伴的困擾點和需求。分享有關錯過機會、

每個客群的預測增長和事件的資料和軼事。提出挑戰組織支援業務成長能力的問題。這會增加機會的數量，並改善業務的長期獲利能力。最終，這有助於您的組織為未來的擴展和開發提供資金。

如果您是工程組織的一部分，請先了解組織的商業策略，再嘗試草擬解決方案。與業務策略保持一致可協助您選擇正確的指標，以評估不同的網路存取選項。隨著組織的成長，它也可以防止昂貴、大規模的網路重新設計。業務一致性可協助您的團隊保護並保留未來挑戰所需的資源。您團隊的員工人數、專業開發預算或對尖端技術的存取，將取決於您展現業務一致性的能力。理想情況下，您可以展示決策如何為組織的業務成功做出貢獻。因此，我們建議您擷取決策程序，包括指標選擇條件。定期檢閱您的指標，以確認其符合業務目標。這可協助您的團隊取得他們應得的點數。定期審查也有助於驗證您的團隊不會根據假設或過時的歷史原因做出決策。

下列各節中的指標清單與聯網存取相關：

- 產品和商業指標
- 影響聯網決策的工程指標

本指南使用這些指標的子集，協助您識別 SaaS 產品的最佳網路存取方法。選擇與您的業務最重要且相關的指標，然後根據這些指標評估方法。

影響聯網決策的產品和商業指標

產品和商業團隊使用成功條件來評估他們是否符合業務目標。本節說明產品或商業指標，這些指標可能會受到組織所做聯網存取決策的正面或負面影響。

使用這些指標和自我評估問題來評估您的網路存取方法如何與您的業務定位和市場策略保持一致。此評估可協助您判斷目前的聯網決策是否支援公司的市場差異化、競爭優勢和目標受眾需求。

本節包含下列主題的指標和自我評估問題：

- 商業模型和市場定位
- 可定址市場總數、新的用戶端取得率、成長和可擴展性
- 客戶體驗和保留
- 效率和財務效能
- 法規合規和風險管理
- 合作夥伴策略

商業模型和市場定位

這些指標與貴公司在市場中的地位有關，包括競爭差異化、市場觸角和品牌感知。您必須評估網路存取方法與商業模型之間的一致性。無論評估是以訂閱為基礎、以用量為基礎、免費、分層、市集、API 優先或白標籤，執行評估。確定模型支援組織的目標和客戶的目標。

高分數條件

網路存取方法與商業模式無縫一致。它可簡化服務的採用和交付。它支援商業模型的長期財務可行性，而且成本結構與預期的成長相容。它可最大限度地減少客戶或合作夥伴採用產品時的任何摩擦。這可增強使用者體驗，並鼓勵更廣泛的服務使用。

低分數指標

選取的網路存取方法與其應支援的商業模式不相符。部署的成本結構和前置時間代表目標市場採用的封鎖程式。持續的基礎設施和營運成本會抑制任何潛在的利潤。這可防止業務成長，並使操作難以達到預期的規模。或者，由於法規原因，網路存取方法的屬性可能會讓客戶無法考慮該服務。

自我評定問題

- 所選網路存取方法在初始部署和持續交付方面的成本影響是什麼？ 方法的固定和可變成本是多少？
- 網路存取方法是否可以有效擴展，以滿足商業模型的成長需求？ 考慮個別租用戶大小和已加入租用戶的數量。
- 網路存取方法是否會施加任何技術或操作限制，以限制商業模型的彈性或適應性？
- 對於網路存取方法，部署前置時間如何與業務模型所需的上市速度保持一致？

可定址市場總數、新的用戶端取得率、成長和可擴展性

請務必評估聯網決策對組織擴展到新市場的能力的影響、有效地吸引客戶，以及維持營運可擴展性。這些因素會影響轉換率。它們也會影響網路存取方法是否支援擴展到重要的市場客群，或限制您只服務特定的客戶類型。

高分數條件

網路存取方法可協助組織達到目標市場的重要部分，也可以與其他網路方法有效結合，以擴展市場觸角。這種方法應該需要最少的額外整合工作。此方法支援部署、快速進入市場和擴展的短前置時間。它允許大量的平行部署。整合對客戶來說很簡單，可降低採用的障礙並增強客戶體驗。此方法可將營運開銷降至最低、保留營運容量，並支援成長預測。

低分數指標

網路存取方法僅支援目標市場的一小部分，或主要適用於業務策略中未排定優先順序的利基客群。它無法有效地補充其他已支援的網路存取方法。部署延遲市場需求的前置時間，會限制市場擴展和新客戶開發。部署模型是循序的，這會隨著需求增加而增加服務瓶頸的風險。複雜的整合程序會阻止潛在的用戶端，這會對取得率和轉換率造成負面影響。大量的營運開銷會降低組織的營運容量。這將成為預測成長的封鎖程式。

對於這些指標，評估引入新的網路存取方法是否有助於組織實現其策略業務目標。考慮新的網路存取方法是否可能建立新的產品相依性或耗用操作資源，而不交付所需的結果。

自我評定問題

- 目前的方法是否有任何差距，使您無法到達目標市場的較大客群？
- 您應該支援以涵蓋目標市場 70–90% 的網路存取方法的最低非重疊、標準化清單為何？
- 每個網路存取方法可實現什麼範圍，以及重要指標的相關增加，例如基礎設施成本、營運週期和對專家的依賴性？
- 網路基礎設施的部署功能和服務限制如何與目標市場中的成長期望保持一致？
- 網路整合是否為新客戶建立進入的任何障礙？ 如何解決這些問題以改善轉換率？
- 管理網路的操作開銷如何影響您的成長和可擴展性容量？
- 您可以實作哪些策略來縮短網路部署的前置時間，並改善市場擴展和客戶開發？
- 是否有任何對專家資源的相依性會延遲部署或與客戶生態系統整合？

客戶體驗和保留

本節中的指標可協助您了解組織取得和最重要的保留客戶的能力。了解聯網存取方法與客戶滿意度之間的關係，有助於產品和工程團隊做出由資料告知的決策。

高分數條件

網路存取方法可靠且易於管理。它有助於提高客戶滿意度 (CSAT) 和淨推薦分數 (NPS) 結果。這些分數代表強大的品牌評價和客戶忠誠度。由於與客戶現有生態系統的無縫整合，採用摩擦很低，而且對專家的依賴性也很低。您的組織始終符合服務水準協議 (SLAs)，這可強化客戶信任和合約義務。由於客戶喜歡穩定且可靠的服務，因此您的客戶保留率很高。

低分數指標

難以整合和不一致的服務存取通常會導致客戶沮喪和負面意見回饋。這會損害品牌評價。由於依賴於專家或由於長時間的加入和整合時間，新客戶無法從免費或試用計劃轉換為付費服務。經常不符合 SLAs 會導致財務處罰和失去可信度，從而可能降低客戶保留率。

自我評定問題

- 網路效能（例如速度、運作時間和延遲）如何直接影響 CSAT 和 NPS 結果？ 哪些特定的網路改進可以提高這些分數？
- 目前的網路延遲和執行時間指標如何影響初始使用者體驗和採用率？ 最佳化這些指標需要哪些特定的網路效能改善？
- 網路組態或安全設定中是否有任何經常性問題會使新客戶的整合複雜化？ 如何簡化這些程序？
- 設定網路存取的便利性如何影響新使用者的加入體驗？ 是否有可以最佳化的特定網路存取點或前置時間，以增強初始使用者印象？
- 自動化新用戶端的網路服務佈建有哪些挑戰。如何調整此程序以改善可擴展性和可靠性？
- 分析最近 SLA 違規的根本原因。它們是否與網路組態、容量規劃或外部廠商問題有關？
- 網路問題導致您錯過 SLA 承諾的頻率為何？ 最常見的網路相關故障有哪些？
- 哪些網路效能改善已顯示過去對客戶滿意度的最重要正面影響？

效率和財務效能

此類別會評估業務的財務運作狀態和獲利能力方面，例如成本效益、長期可行性、獲利能力、投資報酬率 (ROI) 和總體擁有成本 (TCO)。透過標準化簡化網路操作，您可以降低操作開銷和維護成本。這可支援組織的成長目標。

高分數條件

網路存取方法的成本結構與商業模型一致。它支援永續成長，以及您實現提高獲利能力的顯著成本節省。高效率的網路存取可讓快速加入客戶，縮短交付價值的時間並加速市場滲透。這會直接縮短收入辨識週期。

低分數指標

客戶正轉向您的競爭，以加速交付其應用程式和服務。您的組織已增加與複雜和各種網路組態相關的營運成本，以及延長的前置時間。成本結構和商業模型不一致，這可能會導致訂閱型服務的預付成本很高。繁瑣的加入程序可減少市場滲透率並延遲收入確認。

自我評定問題

- 新服務部署目前的前置時間為何，以及它們如何影響上市時間和收入確認？
- 標準化網路操作如何有效地降低開銷和維護成本？
- 成功完成初始整合、每日操作、疑難排解問題或實作變更時，是否需要專家資源？
- 在技術進展方面，目前的網路投資永續性如何？ 您是否正在投資符合預計市場開發的未來技術？
- 您配置和追蹤個別租戶網路流量和用量相關成本的效果如何？

法規合規和風險管理

從根本上來說，驗證是否符合網路相關法規非常重要。這可確認您以合法的方式營運，並可維持客戶的信任。跨網路操作的標準化可簡化合規程序，並提升各種司法管轄區和地理區域的一致性。這些措施可協助您擴展服務。

高分數條件

網路操作一致地遵守法律標準，沒有複雜性，這有助於市場擴展、減少採用摩擦，並增強客戶信任。已證明符合重要的法規架構，例如數位營運恢復法案 (DORA) 和國家標準技術研究所 (NIST)，可協助您贏得對法規合規敏感的客戶。持續查看合規狀態可縮短完成稽核所需的時間。

低分數指標

網路合規中的差距會導致高度採用摩擦、服務啟動延遲、法律挑戰和潛在的罰款。這些挑戰會導致擴展到新市場的計劃延遲或取消。在不同司法管轄區之間維護標準合規實務並不容易，這會影響營運效率和市場評價。

自我評定問題

- 您的網路操作是否符合適用的法規或產業準則？ 您最近的合規稽核必須揭露什麼？
- 您如何遵守數位和網路安全領域中新興的法規？
- 您的文件和報告程序在滿足不同監管機構的要求方面的效果如何？
- 在造成法律挑戰之前，您有哪些風險管理策略可以識別和解決潛在的合規風險？
- 您的網路管理團隊需要哪些層級的合規訓練和意識來支援您的網路存取方法？

合作夥伴策略

評估網路存取方法與公認合作夥伴、平台和市場生態系統的一致性。這是必要的，特別是如果您的成長策略取決於合作夥伴的擴展。

高分數條件

網路存取方法已與您的合作夥伴生態系統整合。其成本結構與您的主要合作夥伴的商業模式非常一致。合作夥伴擁有必要的聯網技能，可無縫整合 SaaS 產品，而且可以提供持續的存取和功能。

低分數指標

選取的網路存取方法需要極少或難以取得的專業技能、資源或設備。它與平台和市場常用的標準網路存取通訊協定不同。這會導致難以預測的成本結構難以協調。網路存取方法與您主要合作夥伴的商業模式不一致。

自我評定問題

- 合作夥伴的網路存取方法的成本影響是什麼。這些成本如何與其商業模型保持一致？ 整合的哪一端承擔了大量成本，以及必須投資多少個操作週期？
- 對於網路存取方法，整合或維護是否有任何可能影響合作夥伴關係或生態系統可擴展性的障礙？
- 如何最佳化網路存取方法，以增強整個生態系統的相容性和整合方便性？

影響聯網決策的工程指標

與產品和商業團隊一樣，工程團隊也會使用成功條件來評估他們是否符合業務目標。但是，這些指標不同，它們著重於團隊開發、操作和滿足安全和合規要求的能力。本節說明工程指標，這些指標可能會受到您組織所做聯網存取決策的正面或負面影響。

使用這些指標和自我評估問題，根據您的業務需求和技術功能評估您目前的網路存取方法。此評估可協助您識別架構中的差距，並優先考慮符合您策略目標的改進。透過定期檢閱這些條件，您可以確保您的網路存取策略持續支援客戶的需求和組織的成長計畫。

本節包含下列類別和主題的指標和自我評估問題：

- 開發指標
  - 部署頻率、部署時間和衝刺速度
  - 彈性和功能交付

    - 變更失敗率
    - 程式碼品質和工程團隊效能
    - 技術債務減少
    - 可擴展性、容量和效能
- 卓越營運指標
    - 操作彈性和災難復原
    - 服務和應用程式效能監控
- 安全與控管指標
    - 安全性、合規性和漏洞管理

與 SaaS 產品網路存取相關的開發指標

本節包含下列指標：

- 部署頻率、部署時間和衝刺速度
- 彈性和功能交付
- 變更失敗率
- 程式碼品質和工程團隊效能
- 技術債務減少
- 可擴展性、容量和效能

部署頻率、部署時間和衝刺速度

若要最佳化開發週期的效率，您必須了解網路堆疊佈建對衝刺速度的影響。

高分數條件

網路堆疊佈建已簡化且自動化，且需要最少的手動介入。它不會顯著影響衝刺速度。網路堆疊佈建和重新部署可由任何團隊成員執行。這可減少特殊資源的瓶頸和相依性。

低分數指標

佈建網路堆疊需要大量的案例點。這表示一個複雜且耗時的程序，會減損新功能的開發。網路堆疊頻繁重新部署會產生大量時間和成本額外負荷。網路佈建任務需要專門的工程專業知識，這會產生瓶頸並減緩開發週期。

自我評定問題

- 部署程序涉及哪些手動步驟。它們如何影響部署頻率和時間？
- 部署失敗時如何處理轉返。它們對部署頻率和復原時間有何影響？
- 當您設定新環境時，佈建網路堆疊需要多少個故事點？
- 在開發過程中，經常重新部署網路堆疊會產生多少額外的成本和時間額外負荷？
- 佈建網路堆疊取決於專業工程專業知識，還是可由任何團隊成員管理的任務？

彈性和功能交付

網路存取方法可能會影響工程團隊有效率地創新和部署新功能的能力。

高分數條件

網路存取方法提供快速無縫功能部署所需的彈性。它支援各種通訊協定、單向和雙向通訊，以及訊息大小。它不會對開發程序或創新施加重大限制。

低分數指標

網路存取方法會限制團隊推出新功能的能力，因為缺乏支援的通訊協定、訊息大小的靈活性，或對特定技術和相關專家資源的依賴性。這可能會導致開發週期變慢，並阻礙服務的演變。

自我評定問題

- 網路存取方法如何影響團隊在開發和部署新功能的敏捷性？
- 網路存取方法中是否有限制某些通訊協定或技術的支援？
- 該方法如何促進或限制將新技術和創新整合到服務中？
- 網路存取方法如何影響開發時間表和產品藍圖？

變更失敗率

您選擇的網路存取方法可能會影響部署新服務或功能時的變更失敗率。更高的控制通常意味著更大的靈活性，但也會增加組態錯誤的可能性，例如在管理複雜的路由設定時。

高分數條件

您可以對網路堆疊實作變更，並將失敗風險降至最低。存在足夠的測試機制、有效率的復原機制，而有效的監控可協助您快速識別和解決問題。

低分數指標

網路存取方法在變更期間容易失敗。測試選項有限、部署策略複雜，或監控和故障診斷功能不足。需要多個方才能參與故障診斷工作階段。這可能會導致停機時間增加，並減少 SaaS 產品的可用性。

自我評定問題

- 有哪些措施可在更新網路堆疊時降低變更失敗的風險？
- 是否有完整的測試和驗證程序？
- 系統從失敗的變更中復原的速度有多快？ 是否有有效的轉返程序？
- 是否有主動監控和提醒系統，可在網路堆疊變更期間和之後快速偵測和解決問題？
- 網路堆疊部署的歷史變更失敗率是多少。從過去的事件中學到了哪些教訓？
- 網路存取方法如何促進或限制變更實作。該方法是否將服務中斷降至最低？
- 當您部署涉及網路存取方法的變更時，影響生產環境中 SaaS 產品可用性的風險為何？

程式碼品質和工程團隊效能

網路存取方法可能會間接影響 SaaS 產品的程式碼品質。網路存取缺乏標準化可能會迫使工程團隊支援多種整合方法，這可能會導致程式碼庫膨脹。這反過來會阻礙團隊開發深度和控制程式碼品質的能力，這對於維護高效能工程團隊來說是必要的。

高分數條件

由於受支援網路存取方法的程式碼模組化和可重複使用性，工程團隊會保持專注。網路存取方法與現有的部署管道和自動化測試策略相容。

低分數指標

工程團隊效能會因為與整合和維護過多網路存取方法相關聯的額外負荷而降低。有些方法會大幅增加複雜性、產生技術負債，或需要開發解決遺失或功能不足的解決方法。

自我評定問題

- 網路存取方法如何管理網路變異性？
- 您需要開發額外的程式碼來處理連線中斷嗎？
- 新的網路存取方法是否與現有方法無縫整合，還是需要大量的自訂開發？
- 採用新的網路存取方法所需的變更程度為何？ 現有的程式碼庫和自動化測試可以有效地使用嗎？

- 使用選取的網路存取方法部署或重新部署服務有多容易或多困難？ 這可以經常完成嗎？ 專家資源是否有任何相依性？
- 網路存取方法是否有助於或複雜地遵守編碼標準和最佳實務？
- 該方法如何影響新功能或修正的time-to-market？

技術債務減少

評估網路存取方法對技術負債的影響時，應考慮其可擴展性、可觀測性和安全性功能。

高分數條件

隨著客戶群的擴展，此方法可有效簡化基礎設施管理。它提供out-of-the-box強大可觀測性功能。這可提升高效的監控和維護。

低分數指標

網路存取方法不足以保護通訊管道，且缺少足夠的工具進行定性指標觀察。隨著客戶群的增加，它也可能需要額外的基礎設施管理開發，或者可能需要可靠性問題的解決方法。

自我評定問題

- 網路存取方法如何影響基礎設施的長期可擴展性？ 它是否以最少的額外投資促進無縫成長？
- 隨附的可觀測性工具有多全面？ 它們是否允許主動監控和問題解決？
- 網路存取方法隨著時間對程式碼庫的維護和演變的預期影響是什麼？
- 該方法是否與現有和規劃的基礎設施完美整合。是否需要重大變更或新增？

可擴展性、容量和效能

若要判斷 SaaS 產品網路存取方法的適用性，請務必分析它如何隨著需求增加維持最佳效能。

高分數條件

網路存取方法可順暢地促進擴展。它會在請求處理期間維持低延遲，並有效率地處理流量尖峰。無論流量增加，它都能提供一致的效能，也不會對成長施加操作限制。

低分數指標

網路存取方法無法有效擴展，可能是因為固有頻寬限制或基礎設施容量不足。資源佈建和管理會增加複雜性或建立相依性。由於延遲、抖動和輸送量變化增加，尤其是在擁塞的網路條件下，服務效能會降低。

自我評定問題

- 網路存取方法如何容納越來越多的租戶及其資料磁碟區？
- 是否本質上可擴展以滿足未來需求？
- 採取哪些措施來確保效能一致，即使在尖峰流量期間或快速擴展事件？
- 該方法如何處理網路延遲和抖動？ 是否有機制可最佳化資料輸送量並將延遲降至最低？
- 網路存取方法是否可以適應不同的網路條件？ 它可以為每個客戶提供單一租戶體驗嗎？
- 網路存取方法對基礎基礎設施有何影響？ 是否需要對現有系統進行重大升級或變更？

與 SaaS 產品網路存取相關的卓越營運指標

本節包含下列指標：

- 操作彈性和災難復原
- 服務和應用程式效能監控

操作彈性和災難復原

網路存取方法應可協助 SaaS 產品承受各種類型的中斷，並快速從任何災難中復原。

高分數條件

建立和測試的災難復原計劃一致地顯示網路存取方法符合災難復原要求。網路存取方法支援高可用性組態，並支援自動、快速且可靠的容錯移轉機制。

低分數指標

網路存取方法使得難以建立一致的災難復原策略。您會在中斷後觀察到較長的復原時間。網路基礎設施的頻繁操作失敗正在影響服務交付。

自我評定問題

- 上次災難復原演練是什麼時候，結果是什麼？
- 中斷後需要多長時間才能復原關鍵服務？ 網路基礎設施的哪個部分需要重新部署？
- 可以對網路基礎設施進行哪些改善，以簡化災難復原計劃？
- 是否有針對最關鍵的網路元件進行備援？
- 在重大中斷之後，您是否已自動化網路基礎設施的潛在重新部署？

- 網路存取方法如何支援容錯能力和可靠性？ 是否有內建機制來處理網路中斷和維護資料完整性？

服務和應用程式效能監控

網路存取方法可能會影響用於驗證最佳操作和服務執行時間的效能監控工具。視服務而定，您可能可以存取低階指標（例如封包捨棄率）或更高層級指標（例如工作階段持續時間）。低階指標提供網路行為的詳細技術洞見，但可能難以解釋。相反地，更高層級的指標通常提供更直接、更簡單的方法來衡量整體使用者體驗。這是因為它們將基礎網路條件的影響彙總為明確的服務品質指標。

高分數條件

提供近乎即時洞見的全方位監控工具隨時可用。您有可解決效能問題的自動警示和回應系統。您可以預測潛在的服務瓶頸或故障，然後再影響使用者。

低分數指標

經常發生服務中斷或效能問題，而未受到觀察或採取行動。缺乏對服務效能的可見性會導致對效能瓶頸的回應緩慢。需要多方團隊來疑難排解網路基礎設施問題。

自我評定問題

- 目前有哪些監控工具和網路基礎設施指標可用？ 它們偵測服務異常的效果如何？
- 您可以多快識別和解決效能問題？
- 您是否有可預測潛在效能問題的機制？
- 您可以進行哪些改善來增強可觀測性功能？

與 SaaS 產品網路存取相關的安全與控管指標

本節包含下列指標：

- 安全性、合規性和漏洞管理

安全性、合規性和漏洞管理

您必須評估網路存取方法的安全層面，包括遵守安全標準和管理漏洞。

高分數條件

網路存取方法可協助您的團隊遵守安全架構，例如國際標準化組織 (ISO) 27001、系統和組織控制 2 (SOC 2) 或 NIST。它可讓您輕鬆執行定期安全稽核。有強大的加密和身分驗證機制。網路是隔離的，

只有必要的資源才會公開給客戶的基礎設施。您可以近乎即時地發現聯網異常，而不會產生過多的額外負荷。

低分數指標

網路存取方法容易發生重複的安全漏洞或漏洞，而且不符合關鍵安全標準。您經常觀察到安全事件的延遲偵測和回應。

自我評定問題

- 是否有任何最近與所選網路存取方法相關的安全漏洞，以及我們從中學到了什麼？
- 您的網路存取方法如何符合全球安全標準？
- 偵測和回應安全威脅需要多長時間？ 網路存取如何協助或限制此能力？
- 對網路存取方法進行安全評估的頻率為何？ 您可以使用常用工具來評估網路存取方法的安全性，還是需要專門的軟體？
- 網路存取方法固有的安全層級為何，以及如何符合產業最佳實務和法規要求？

SaaS 產品 AWS 聯網服務概觀

本節討論本指南中參考的 AWS 聯網服務。它也會比較其功能，並說明每個服務的安全考量。

本節包含下列主題：

- AWS 聯網服務
- 比較服務功能
- 安全功能和考量事項

AWS 聯網服務

以下是本指南中一致討論 AWS 服務 的 。

AWS PrivateLink

AWS PrivateLink 是一項雲端原生服務，可在您的客戶已在 中操作時提供存取您的 SaaS 產品 AWS 雲端。您的客戶會透過介面 VPC 端點連線至 SaaS 產品。這是在客戶 的一或多個子網路中佈建的端點網路介面 AWS 帳戶。在本指南的案例中，流量會通過界面 VPC 端點，並到達您帳戶中的 Network Load Balancer。Network Load Balancer 會將流量轉送至您已註冊為端點服務的 SaaS 應用程式。透過資源 VPC 端點， AWS PrivateLink 也可以協助您存取其他資源，例如資料庫。

Amazon VPC Lattice

Amazon VPC Lattice 是一種應用程式聯網服務，可協助 SaaS 供應商安全有效地將其服務提供給跨多個 VPCs 和 操作的客戶 AWS 帳戶。客戶透過 VPC Lattice 存取您的 SaaS 產品，可提供一致的網路連線、強大的存取控制和進階流量管理。在這些情況下，流量會透過 VPC Lattice 流向已註冊的應用程式服務。無論您使用哪種運算服務，它都能提供可擴展且安全的通訊。

VPC 對等互連

VPC 對等互連是兩個虛擬私有雲端 (VPCs) 之間的網路連線，透過使用私有 IPv4 地址或 IPv6 地址路由它們之間的流量。VPC 對等互連通常會在信任的實體之間使用，就像同一組織內的實體一樣。您的客戶會建立對等請求給其中一個 VPCs。當您接受它時，流量可以在兩個 VPCs之間雙向流動。這種連線方法因其唯一性而突出，因為它涉及兩個 VPCs之間的直接通訊，而不需要管理任何中介服務或基礎設施。

AWS Transit Gateway

AWS Transit Gateway 是集中式網路傳輸中樞，可連接 VPCs、虛擬私有網路 (VPN) 連線、AWS Direct Connect 閘道、VPC 中的第三方虛擬設備，以及其他傳輸閘道。傳輸閘道的每個附件可以有不同的路由表。這可提供最大的路由彈性，並可協助您隔離網路。它通常用於將許多 VPCs連接在一起或進行集中式檢查。

AWS Site-to-Site VPN

AWS Site-to-Site VPN 可以使用網際網路通訊協定安全 (IPsec) 技術，在內部部署網路、遠端辦公室、工廠、其他雲端供應商和 AWS 全球網路之間建立連線。連線是從 中 VPC 中的虛擬私有閘道或傳輸閘道 AWS 雲端 建立到實體或軟體型客戶閘道，該閘道可以位於 AWS 雲端、內部部署或其他 CSP 雲端。連線可以透過網際網路或實體 AWS Direct Connect 連線。也可以使用 進行加速Site-to-Site連接 AWS Global Accelerator。加速連線會將流量路由到 AWS 節點，並降低延遲並改善效能。

AWS Direct Connect

AWS Direct Connect 在內部部署資料中心和 之間建立高速的私有連線 AWS 雲端。透過繞過公有網際網路， Direct Connect 提供更可靠、安全且一致的低延遲連線給 AWS 雲端。客戶連線到其中一個Direct Connect 位置，然後選擇託管或專用連線 AWS。雖然這是 SaaS 產品不常見的架構選擇，但它非常適合只有少數但大型企業消費者的 SaaS 供應商。

比較服務功能

下表概述本指南中 AWS 服務 討論的 支援的功能。以下是此表格中包含的功能說明：

- 重疊 CIDR 範圍 – 可以連接具有相同或重疊 CIDR 範圍的兩個或多個網路
- 雙向通訊 – 可支援雙向通訊管道，讓 SaaS 取用者可以向 SaaS 供應商公開內部資源，例如資料庫
- IPv6 – 可支援 IPv6，無論是單一或雙堆疊
- 巨型訊框 – 可支援巨型訊框，訊框大小上限為 8，500 個 位元組
- 混合雲端 – 可支援與內部部署網路的連線
- 多雲端 – 可支援不同雲端服務供應商上網路之間的連線

服務或方法	重疊 CIDR 範圍	雙向通訊	IPv6	巨型訊框	混合雲端	多雲端

VPC 對等互連	否	是	是	是[5]	否	否
AWS PrivateLink	是	是[1]	是	是	No[6]	No[6]
Amazon VPC Lattice	是	是[1]	是	是	No[6]	No[6]
AWS Transit Gateway	否	是	是	是	是[3]	是[3]
AWS Site-to-Site VPN	否	是	是	否	是	是
AWS Direct Connect	否	是	是	是[2]	是	是
公有網際網路存取[4]	不適用	否	是	是	是	是

1. 使用 Amazon VPC Lattice 中的 VPC 資源
2. 僅適用於私有和傳輸虛擬介面
3. 使用Site-to-Site或 AWS Direct Connect 附件
4. 做為讓應用程式可公開存取之 AWS 資源的一般術語，例如 Application Load Balancer
5. 僅適用於一個 內的對等連線 AWS 區域
6. 可透過環境之間預先存在的第 3 層連線來實現

安全功能和考量事項

下表概述本指南中 AWS 服務 討論的 安全功能。

- 身分驗證的方法 – 如何確保只有客戶可以連線到您的服務。傳入請求的另一層級身分驗證通常是必要的，尤其是在共用租用戶環境中。
- 傳輸中加密 – 描述是否預設提供傳輸中加密。原生加密描述為 VPCs、VPC VPCs 或資料中心內的所有流量 AWS 提供的加密。補充加密說明您控制且可由個別 服務停止的加密。

服務或方法	身分驗證的方法	傳輸中加密
VPC 對等互連	您對客戶的 AWS 帳戶 和 VPC 啟動對等請求，或接受他們啟動的請求。請參閱接受或拒絕 VPC 對等互連。	僅限原生加密
AWS PrivateLink	您可以選擇 AWS 帳戶 允許哪些 為您的服務建立端點。這些帳戶稱為允許的主體。請參閱接受或拒絕連線請求。	僅限原生加密
Amazon VPC Lattice	您與客戶的 共用 VPC Lattice 服務或服務網路 AWS 帳戶。請參閱共用您的 VPC Lattice 實體。	原生加密和補充 TLS 加密
AWS Transit Gateway	您的客戶從他們的 建立對等連接請求 AWS 帳戶，或者您啟動請求。請參閱 Amazon VPC Transit Gateways 中的傳輸閘道對等互連附件。	使用 VPN 連接進行原生加密和補充 IPsec 加密
AWS Site-to-Site VPN	您可以在客戶的裝置上使用 IPsec 預先共用金鑰或私有憑證。請參閱AWS Site-to-Site VPN 通道身分驗證選項。	補充 IPsec 加密
AWS Direct Connect	您的客戶從 建立虛擬介面請求 AWS 帳戶。請參閱Direct Connect 虛擬介面和託管虛擬介面。	可在所選站點進行補充第 2 層加密。請參閱Direct Connect 位置。

公有網際網路存取[1]	需要自訂身分驗證。	可能的補充 TLS 加密

1. 做為讓應用程式可公開存取之 AWS 資源的一般術語，例如 Application Load Balancer

評估 SaaS 產品的網路存取選項

對組織重要的指標取決於您的客戶是誰、您的商業策略和您的組織目標。本指南提供可用來選擇聯網存取方法的指標，但您應該優先考慮符合使用案例獨特需求的指標。

本節包含下列主題：

- 評估指標
- 擁有權總成本
- 網路值映射

評估指標

有些指標在組織和使用案例之間是一致的，而這些指標是我們可以協助您評分的指標。以下是這些指標：

- 易於整合 – 您可以輕鬆快速地加入新客戶？
- 總體擁有成本 (TCO) – 成本結構是什麼？ 除了固定和可變基礎設施成本之外，還有與營運開銷、專家相依性、實作變更的成本和合規相關的主要額外成本考量。如需詳細資訊，請參閱 擁有權總成本 一節。
- 可擴展性 – 您的網路存取方法是否能夠擴展以支援公司的成長？ 擴展您的客戶群有重要的架構和組織考量。考慮如何擴展以容納您目前支援的 5-100 倍客戶。
- 適應性 – 您可以輕鬆實作變更嗎？ 變更可能包括新的應用程式、新的功能、不同的平台或不同的網路。
- 網路隔離 – 您會向客戶公開多少網路基礎設施？ 您是否提供恰到好處的存取，或是公開整個網路？ 如果您提早隔離網路資源，稍後可以更輕鬆地提供安全、隱私權和合規保證。
- 可觀測性 – 您偵測服務故障或降級的能力為何？ 識別問題有多簡單快速？ 您可以協助客戶了解故障點並協助他們解決故障問題的速度（以及額外負荷）有多快？
- 修復時間 – 偵測服務故障或降級與恢復操作之間的前置時間為何？ 影響此能力的因素有哪些？

其他指標對於您的組織或產品來說是唯一的，因為它們與您的業務營運、策略或目標相關。只有您可以為這些指標評分。以下是這些指標：

- 商業模式一致性 – 您的商業模式是什麼，以及個別存取方法與商業模式的一致性如何？

- 總可定址市場 (TAM) – 您目前和未來的市場是什麼，以及網路存取方法的涵蓋程度如何？
- 投資報酬率 (ROI) – 您預期在獲利能力和利潤方面有哪些改善？ 預期的經濟效益是否足以滿足您的適應性和彈性服務存取需求？
- 法規遵循 – 哪些類型的法規要求適用，以及哪些市場適用？
- 服務層級協議 (SLAs) – 客戶是否需要高度可用的 SaaS 產品？ 您在合約上必須維護哪些類型的承諾？

擁有權總成本

本節探討總體擁有成本 (TCO)，這是用來比較網路存取方法的其中一個評估指標。TCO 是一個複合指標，由固定和可變基礎設施成本、營運開銷、專家相依性、變更成本和合規成本組成。

每個網路存取方法的 TCO 評分可能會因您的使用案例而有所不同。例如，具有簡單 Web 服務的 SaaS 提供者和五個租用戶的變更成本與具有複雜、互連產品組合和數百或數千個租用戶的 SaaS 提供者不同。此外，並非所有元件都有相同的權重。例如，聘請聯網專家通常比支援服務個別部署的基礎設施成本更昂貴。針對初始方向使用下表中的值，並做為進一步討論的參考點。

存取方法	固定基礎設施成本	可變基礎設施成本	營運開銷	專家相依性	變更成本	合規成本
VPC 對等互連	無	無	高	低	高	中
AWS PrivateLink	低	低	低	無	低	低
Amazon VPC Lattice	中	中	低	低	低	低
AWS Transit Gateway	中	中	低	低	低	中
AWS Site-to-Site VPN	中	高	高	中	中	低

AWS Direct Connect	高	中	中	高	高	低
公有網際網路存取	低	高	中	低	低	高

VPC 互連成本

VPC 互連連線沒有相關的直接基礎設施成本。當流量保持在相同的可用區域內時，無需支付資料傳輸費用。不過，營運開銷可能很大，因為管理與複雜性會隨著每個額外的對等互連而呈指數成長。對聯網的一些基本了解足以設定對等連線，但網路上的變更很難使用少量對等連線實作。合規成本略高，因為雙方會互相公開整個 VPC，而不是個別服務。

AWS PrivateLink 成本

AWS PrivateLink 通常是一種經濟實惠的解決方案，操作開銷很小。這是因為 SaaS 供應商必須僅管理 Network Load Balancer，而消費者必須僅管理 VPC 端點。您可以透明地對兩側進行變更，從而減少昂貴和資源密集的跨組織協作。合規成本通常很低，因為 SaaS 供應商只公開他們想要的服務，而不是整個網路。

Amazon VPC Lattice 成本

Amazon VPC Lattice 提供平衡的成本結構，具有中等的固定和可變基礎設施成本。作為全受管服務網路，它可透過自動化跨多個 VPCs 的服務探索、流量管理和存取控制，大幅降低營運開銷。相較於手動聯網組態，這可簡化初始部署和持續管理。您可以透過以政策為基礎的控制項實作變更，無需複雜的路由更新，從而減少對聯網專家的依賴。合規成本通常低於傳統的聯網方法，因為 VPC Lattice 透過內建的監控和記錄功能提供精細的存取控制和全面的可見性。這可讓您更輕鬆地示範法規合規。

AWS Transit Gateway 成本

AWS Transit Gateway 每小時和資料處理費用比 高 AWS PrivateLink，但其營運開銷類似。您必須對上的 AWS Transit Gateway 服務和路由有更深入的了解， AWS 才能正確設定所有路由表。基礎設施變更可能需要路由或 DNS 更新。合規成本類似於 VPC 對等互連，因為雙方可能彼此暴露子網路或整個 VPCs。 AWS Transit Gateway 路由表也需要謹慎處理，因為它們是由多個消費者共用，而且您不允許它們之間的任何流量。

AWS Site-to-Site VPN 成本

由於Site-to-Site VPN 基本上會將流量傳送至網際網路，因此由於資料傳輸費用，因此相較於 ，可變成本最高。雖然它是受管虛擬私有網路 (VPN) 服務，但它具有大量的營運開銷，尤其是在客戶閘道上。佈建和操作需要進階的聯網知識，而變更通常需要雙方採取動作。合規成本通常很低，因為安全團隊通常會預先核准 IPsec 通道，無需額外審核。

AWS Direct Connect 成本

AWS Direct Connect 隨附最大的固定基礎設施成本，因為它是直接連至 的私有實體連線 AWS 雲端。設定和操作邊界閘道協定 (BGP) 工作階段 （ 如果需要 ）、操作 VPN 連接和執行流量工程需要專家知識。此服務可減少安全團隊的工作量，因為它將私有連線與額外具有媒體存取控制安全性 (MACsec) 和 IPsec 加密的選項混合。

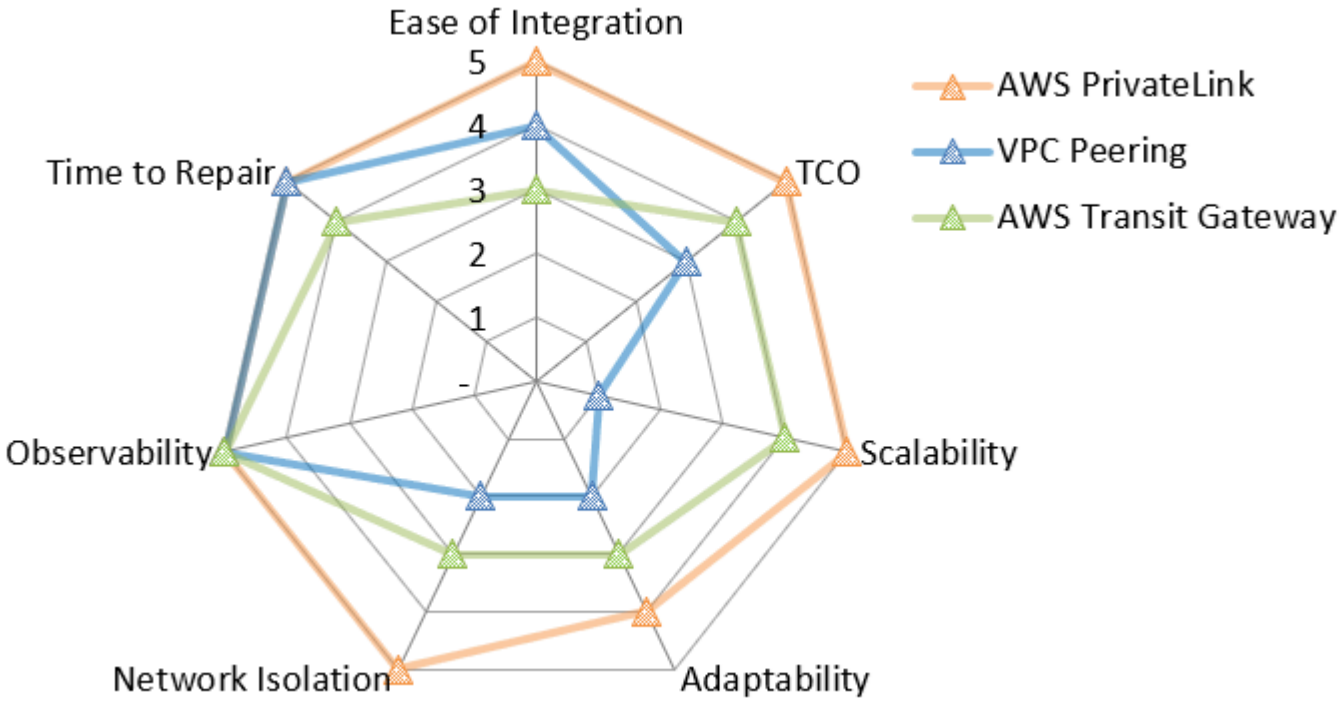
公有網際網路存取成本

公有網際網路存取是指可用來公開存取應用程式 AWS 的資源，例如 Application Load Balancer。對於此方法，提供存取您服務所連結的可變成本，包括將資料傳輸至網際網路的費用。營運開銷和合規成本可能很大，因為您將服務暴露於網際網路，並且需要額外的安全和身分驗證機制。不過，沒有涉及複雜的路由，而且任一方都不必知道彼此基礎設施的詳細資訊。

網路值映射

為了協助您了解全局並做出明智的決策，本指南包含每個案例的聯網值映射。由於評分因案例而異，因此兩個案例的相同服務分數可能不同。值映射是雷達圖，其中假設性完美分數在所有類別中為 5。

例如，下圖顯示範例雷達圖。它只包含我們可以協助評估的指標。我們建議您建立自己的值映射，其中包含只有您可以評估的其他指標。


Ease of Integration
5
4
3
2
1
-
TCO
Scalability
Adaptability
Network Isolation
Observability
Time to Repair
AWS PrivateLink
VPC Peering
AWS Transit Gateway

中的 SaaS 產品聯網存取案例 AWS 雲端

本節涵蓋 中 SaaS 產品的不同網路存取選項 AWS 雲端。它從消費者的角度討論方法，消費者在 內 AWS 雲端、內部部署資料中心或其他雲端服務提供者 (CSPs) 可能有連線需求。此外，您可能需要支援從多種類型的消費者環境進行存取。

了解這些不同環境中的網路連線需求對於建立全面的存取策略至關重要。您的架構決策必須考量各種安全模型、效能期望和技術限制，同時維持營運效率。正確的方法提供安全、可靠的連線能力，可隨業務成長而擴展，並將實作複雜性和持續的管理開銷降到最低。

評估網路存取選項時，請考慮每種方法如何影響您的總體擁有成本，包括基礎設施成本，以及營運開銷和合規要求。有些方法在可擴展性方面表現卓越，但可能會帶來複雜性，而有些方法則優先考慮易於整合，而犧牲網路隔離。您消費者的技術功能和資源在決定最適當的解決方案方面也扮演重要角色。

對於 上的消費者 AWS 雲端， 等服務在安全性和可擴展性方面 AWS PrivateLink 提供了顯著的優勢。內部部署消費者可能受益於 AWS Direct Connect ，以獲得一致的效能，或受益於 Site-to-Site VPN，以實現經濟實惠的連線能力。多雲端案例通常需要仔細考慮互通性挑戰，而且您可以使用傳輸 VPC 架構來標準化存取模式。在所有情況下，您的設計都應該預測未來的消費者和流量成長，以便您的網路架構隨著 SaaS 產品發展而保持彈性和適應性。

本節包含下列案例：

- 在 上操作的 SaaS 消費者 AWS
- 在內部部署操作的服務消費者
- 在其他雲端服務供應商上運作的 SaaS 消費者
- 支援混合環境

在 上操作的 SaaS 消費者 AWS

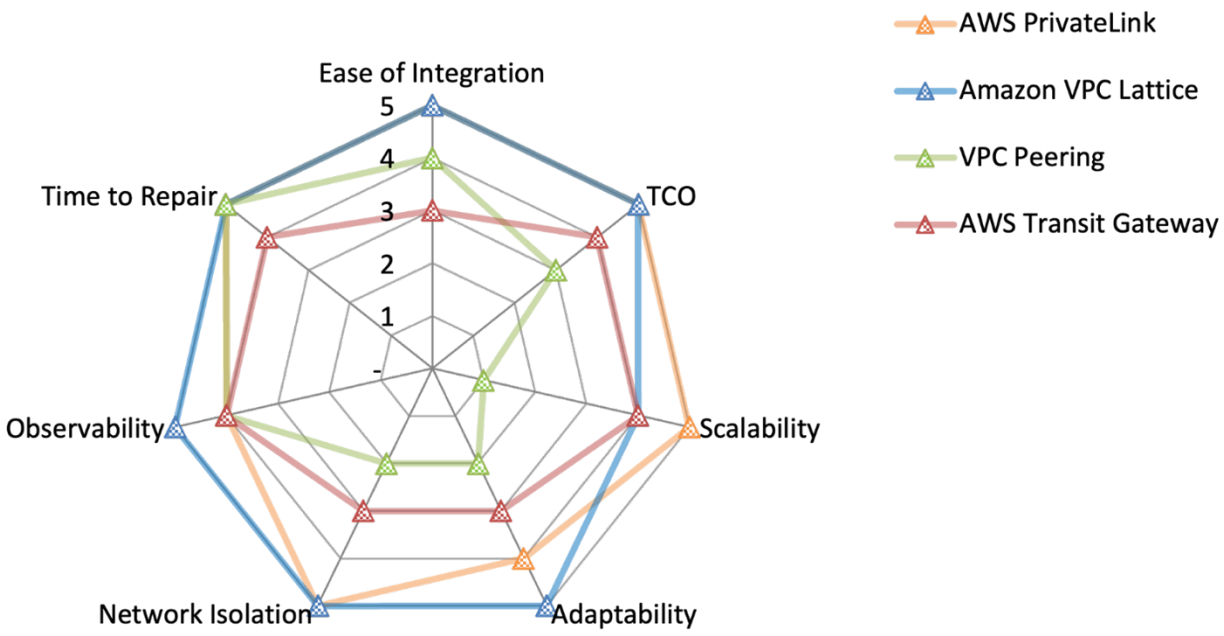
如果您和您的消費者都在 中操作，本節會討論連線選項 AWS 雲端。此案例提供最大的彈性，因為許多 AWS 服務 原生整合 和 ，因為雙方都可以存取整個 AWS 服務 產品組合。

本節討論下列網路存取方法：

- 與 整合 AWS PrivateLink
- 共用 Amazon VPC Lattice 服務
- 建立 VPC 對等互連

- 使用 VPCs AWS Transit Gateway

下列聯網值映射摘要說明每個評估指標的這些選項分數。如需評估指標的詳細資訊，請參閱本指南中的評估指標。在地圖中，5 代表最佳分數，例如最低 TCO、最佳網路隔離或最低修復時間。如需如何讀取此雷達圖的詳細資訊，請參閱本指南網路值映射中的 。



雷達圖顯示下列值。

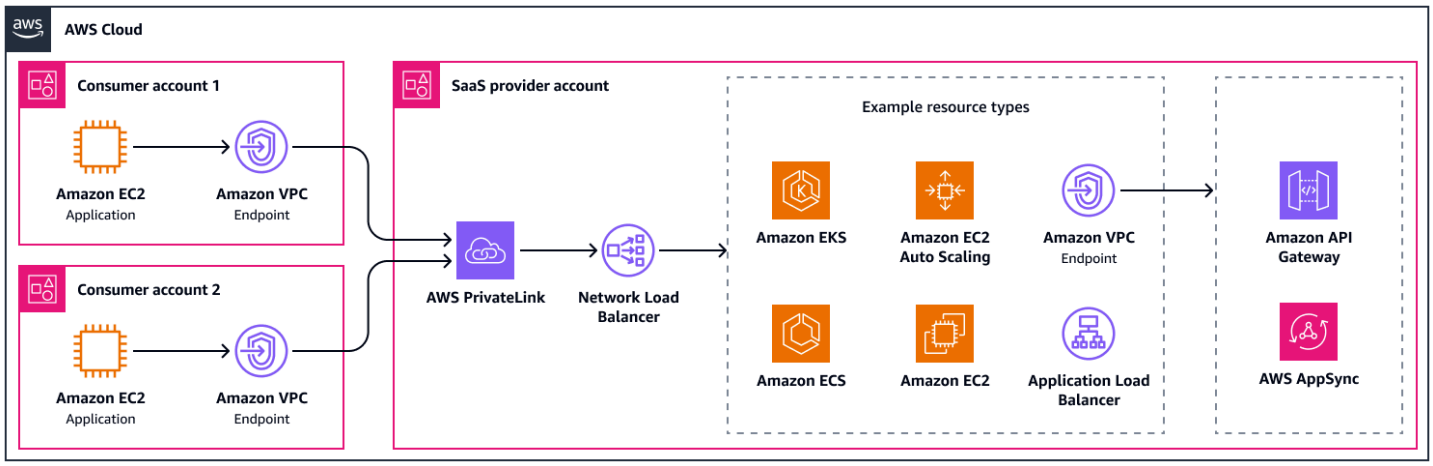
評估指標	AWS PrivateLink	Amazon VPC Lattice	VPC 對等互連	AWS Transit Gateway
易於整合	5	5	4	3
TCO	5	5	3	4
可擴展性	5	4	1	4
適應性	4	5	2	3
網路隔離	5	5	2	3
可觀測性	4	5	4	4

評估指標	AWS PrivateLink	Amazon VPC Lattice	VPC 對等互連	AWS Transit Gateway
修復時間	5	5	5	4

與 整合 AWS PrivateLink

AWS PrivateLink 是整合 SaaS 產品最雲端原生的方式。SaaS 供應商可以在 Network Load Balancer 後方託管其應用程式。Network Load Balancer 會直接與 Application Load Balancer、Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS) 和 Auto Scaling 群組整合。您也可以將流量從 Network Load Balancer 路由到 SaaS 供應商帳戶中的 VPC 端點。這可協助您使用 API 來連接應用程式，例如透過 Amazon API Gateway 或 AWS AppSync。如果您的應用程式需要存取客戶環境中未平衡負載的資源，例如資料庫，您可以使用資源 VPC 端點。

AWS PrivateLink 支援每個可用區域高達 100 Gbps 的頻寬。下圖顯示具有一些可能整合的基本組態。它透過 將兩個消費者帳戶連接到 SaaS 提供者帳戶 AWS PrivateLink。消費者帳戶中有服務端點，SaaS 供應商帳戶中有 Network Load Balancer。



以下是此方法的優點：

- 易於整合：不需要變更路由表
- 易於整合：您可以透過 提供端點服務 AWS Marketplace
- 易於整合：VPC 端點支援易記的 DNS 名稱
- 可擴展性：它可以擴展到數千個 SaaS 消費者
- 適應性：支援重疊 CIDR 範圍
- 適應性：支援 IPv6

- 適應性：跨區域支援
- TCO： AWS PrivateLink 是全受管服務，因此需要的營運工作較少
- 網路隔離：SaaS 消費者的安全優勢，因為流量無法從 SaaS 供應商啟動
- 網路隔離：SaaS 供應商的安全優勢，因為它們不會暴露整個子網路或 VPC

以下是此方法的缺點：

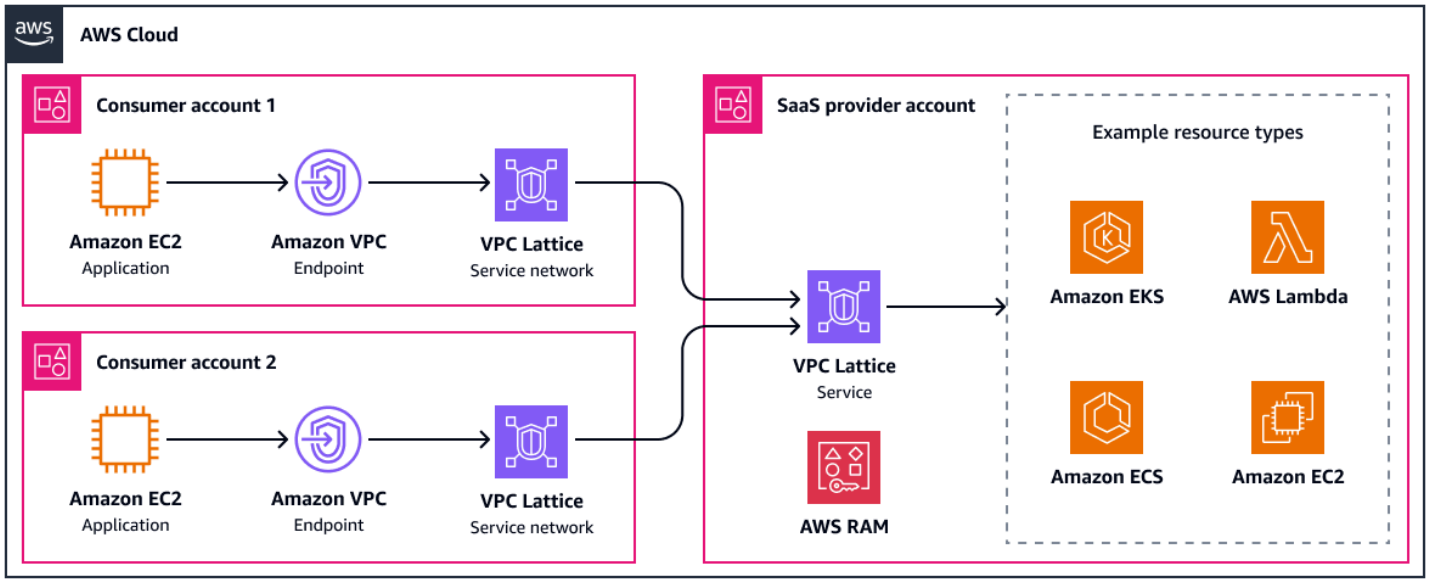
- 適應性：SaaS 供應商必須使用與消費者相同的可用區域
- 適應性：僅支援用戶端起始的連線，服務起始的通訊需要資源 VPC 端點
- 適應性：Network Load Balancer 是 的唯一直接整合 AWS PrivateLink

共用 Amazon VPC Lattice 服務

若要使用 Amazon VPC Lattice 做為 SaaS 應用程式的連線選項，您必須先建立一或多個代表 SaaS 應用程式元件的 VPC Lattice 服務。您可以設定接聽程式和路由規則，將流量導向後端目標，例如 Amazon EC2 執行個體、容器或 AWS Lambda 函數。如需詳細資訊，請參閱在 VPC Lattice 服務網路中連接 Saas 服務 (AWS 部落格文章）。就概念而言，這幾乎與設定 Application Load Balancer 相同。然後，您可以使用 AWS Resource Access Manager (AWS RAM) 指定他們擁有的許可，安全地與客戶 AWS 帳戶 或組織共用 SaaS 服務。客戶接受資源共享後，可以將 SaaS 服務與其現有或新建立的 VPC Lattice 服務網路建立關聯，以啟用service-to-service通訊。

每個 VPC Lattice 服務每秒每個可用區域最多可支援 10 Gbps 和 10，000 個請求。透過實作身分驗證政策，您的客戶可以精細控制哪些 服務和資源可以存取 SaaS 應用程式。您可以使用資源閘道來存取需要 TCP 連線的資源。例如，這可能是您管理的 Amazon EKS 叢集，也可能是應用程式需要存取的客戶受管資源。如需針對 SaaS 產品使用資源閘道的詳細資訊，請參閱AWS 帳戶 使用 VPC 資源 AWS PrivateLink 支援將 SaaS 功能延伸到 (AWS 部落格文章）。

下圖顯示具有一些範例整合的高階 VPC Lattice 組態。它使用客戶管理的服務網路來存取 SaaS 應用程式。



以下是此方法的優點：

- 易於整合：不需要變更路由表
- 易於整合：開箱即用的 服務探索
- 可擴展性：它可以擴展到數千個 SaaS 消費者
- 適應性：支援重疊 CIDR 範圍
- 適應性：支援 IPv6
- 適應性：整合任何 AWS 運算服務做為 VPC Lattice 服務
- TCO：VPC Lattice 是全受管服務，因此需要的營運工作較少
- TCO：具有進階流量路由的內建負載平衡
- 網路隔離：具有身分驗證政策的精細授權
- 網路隔離：SaaS 消費者的安全優勢，因為流量無法從 SaaS 供應商啟動
- 網路隔離：SaaS 供應商的安全優勢，因為您未公開整個子網路或 VPC

以下是此方法的缺點：

- 適應性：僅支援用戶端起始的連線，服務起始的通訊需要資源閘道
- 適應性：無跨區域支援

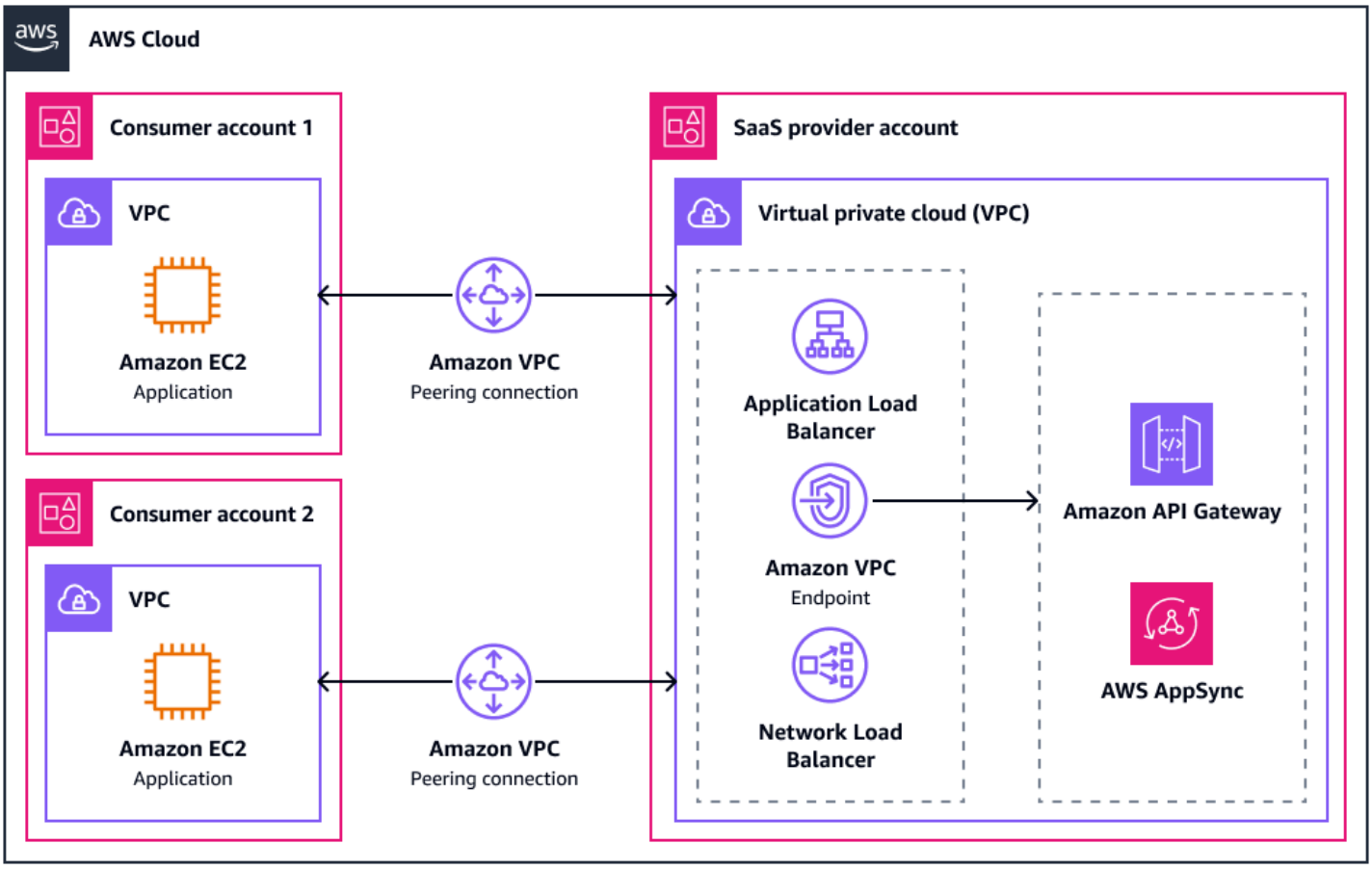
建立 VPC 對等互連

當您使用 VPC 對等互連將 SaaS 提供者的 VPC 連接到消費者的 VPC 時，雙方都可以啟動連線。這需要兩個帳戶中安全群組、防火牆和網路存取控制清單 (NACLs的適當組態。否則，不需要的流量可能會透過對等連線進入網路。您可以使用安全群組來參考對等 VPCs的安全群組。這可協助您控制對應用程式的存取，因為相較於允許列出 IP 地址，允許列出安全群組可提供更明確且精細的存取控制。

使用 VPC 對等互連，可透過 VPC 中部署的服務或資源來存取 SaaS 產品。大多數 SaaS 應用程式都位於 Application Load Balancer 或 Network Load Balancer 後方。AWS AppSync 私有 APIs 或 Amazon API Gateway 私有 APIs 是 SaaS 應用程式的其他常見進入點，因為它們可以透過介面 VPC 端點透過對等連線成為目標。

建立對等連線後，您必須更新兩個帳戶中 VPCs的路由表，將對等連線定義為個別 CIDR 範圍的下一個躍點。此解決方案建議僅適用於擁有幾個消費者的 SaaS 提供者，因為管理多個互連連線很快就會變得太複雜。

下圖顯示具有一些可能整合的基本組態。兩個消費者帳戶中VPCs 與 SaaS 提供者帳戶中的 VPC 具有對等連線。



以下是此方法的優點：

- 修復時間：沒有單一通訊失敗點
- 可擴展性：VPC 對等互連沒有頻寬限制
- TCO：對等連線或相同可用區域內對等連線的流量不收取費用
- TCO：無需管理基礎設施
- 適應性：支援 IPv6
- 適應性：支援區域間對等互連

以下是此方法的缺點：

- 適應性：不支援暫時性路由
- 適應性：不支援重疊的 CIDR 範圍
- 可擴展性：可擴展性有限（每個 VPC 最多 125 個互連連線）
- TCO：透過每個額外的互連連線，複雜性呈指數增長
- TCO：管理路由表、對等連線本身、安全群組規則和流量檢查的開銷
- 網路隔離：由於雙方的整個 VPCs 都公開，因此需要嚴格的安全控制

使用 VPCs AWS Transit Gateway

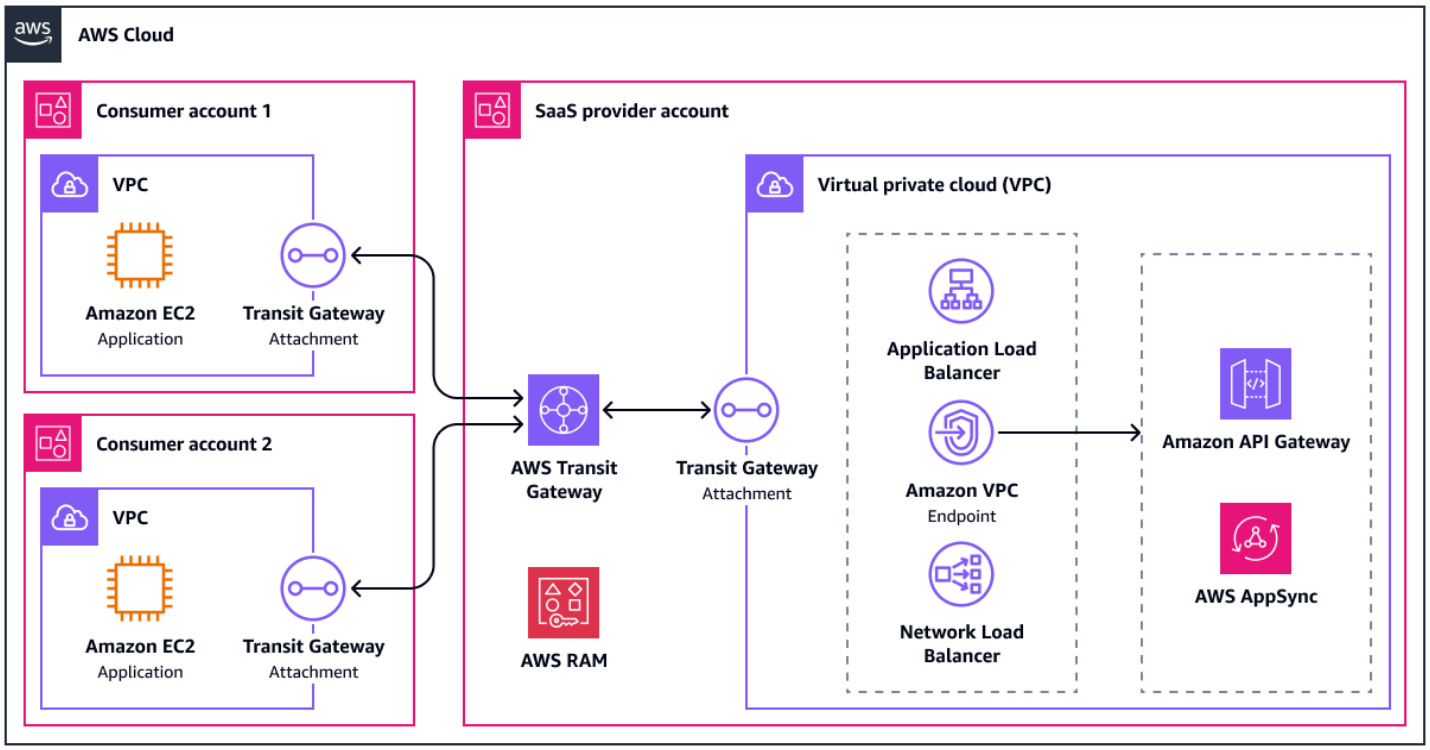
當您透過 連接 VPCs 時AWS Transit Gateway，它會建立 VPC 連接，並在每個可用區域的子網路中部署網路介面，該子網路應路由往返 VPC 的流量。建議在 VPC 連接的每個可用區域中都有專用/28子網路。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 設計最佳實務。VPCs 需要更新的路由表，才能透過部署的網路界面傳送流量，且 Transit Gateway 路由表需要相應地更新。在多租戶組態中，您希望 SaaS 提供者的 VPC 路由到所有消費者的 VPCs。消費者的 VPCs 應該只有通往 SaaS 提供者 VPC 的路由。

Transit Gateway 透過設計提供高可用性。它支援使用 VPC 流量日誌進行監控，傳輸閘道連接的最大頻寬為每個可用區域 100 Gbps。如同 VPC 對等互連，此方法可啟用跨 VPC 安全群組參考，簡化環境之間的存取控制。

使用 Transit Gateway 將消費者連線至您的 SaaS 產品有兩個主要選項。

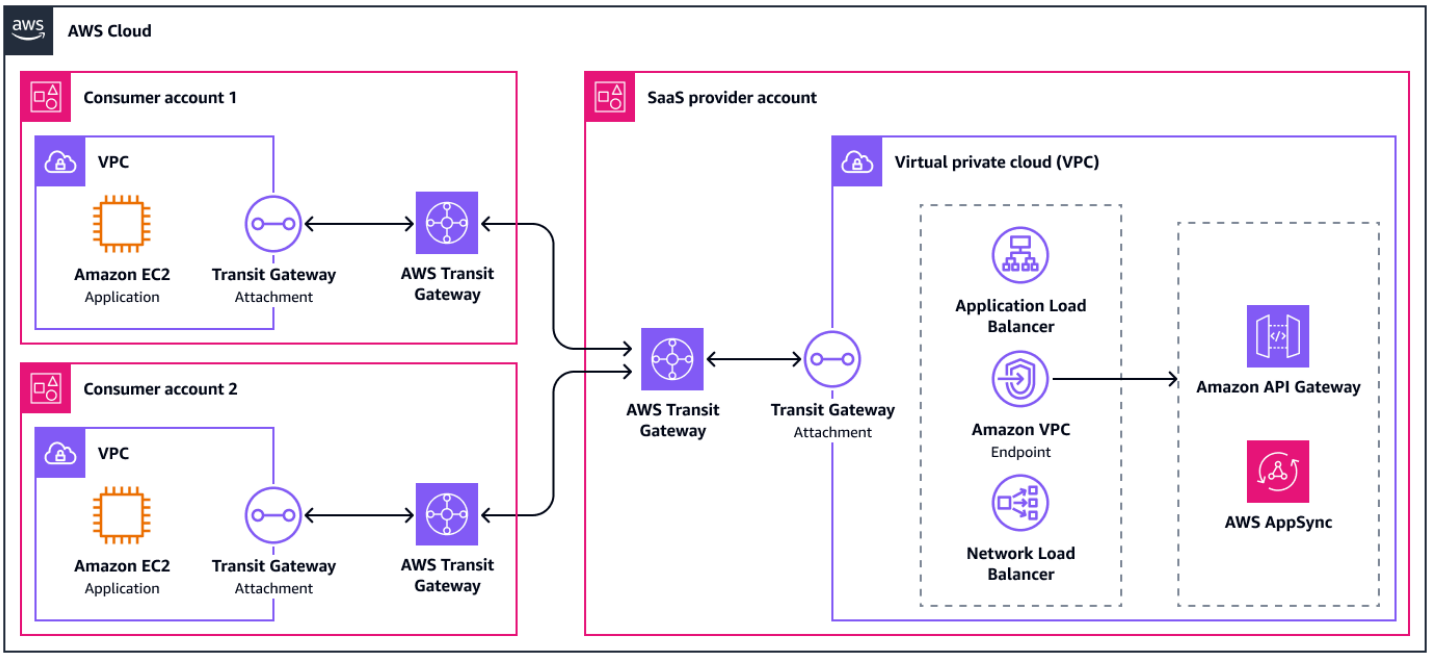
選項 1：使用 RAM

在第一個選項中，服務提供者會使用 () 與消費者共用 Transit Gateway。 AWS Resource Access ManagerAWS RAM這可讓消費者在自己的帳戶中部署 VPC 連接。下圖顯示此選項的高層級。



選項 2：對等傳輸閘道

第二個選項是將傳輸閘道與消費者帳戶中的傳輸閘道對等。這可讓消費者更具彈性，因為他們現在可以完全控制其傳輸閘道內的路由表。例如，他們可以在服務與其工作負載之間設定集中式檢查。此選項的缺點是僅支援傳輸閘道之間的靜態路由。下圖顯示此選項的高層級。



以下是此方法的優點：

- 可擴展性：支援最多 5，000 個附件
- 可擴展性：管理和監控所有連線 VPCs單一位置
- 適應性：傳輸閘道也可以連接到 VPNs、 Direct Connect 閘道和第三方 SD-WAN 設備
- 適應性：彈性架構，例如新增檢查 VPC
- 適應性：支援可轉移路由
- 適應性：可以對等區域內和區域間傳輸閘道
- 適應性：支援 IPv6
- TCO： AWS Transit Gateway 是全受管服務，因此需要的營運工作較少
- TCO：隨著每個額外的傳輸閘道連接，TCO 會線性成長

以下是此方法的缺點：

- 易於整合：路由組態需要進階聯網知識
- 適應性：不支援重疊的 CIDR 範圍
- TCO：管理路由表項目、安全群組規則和流量檢查的額外負荷
- 安全性：由於雙方的整個 VPCs 都公開，因此需要嚴格的安全控制

在內部部署操作的服務消費者

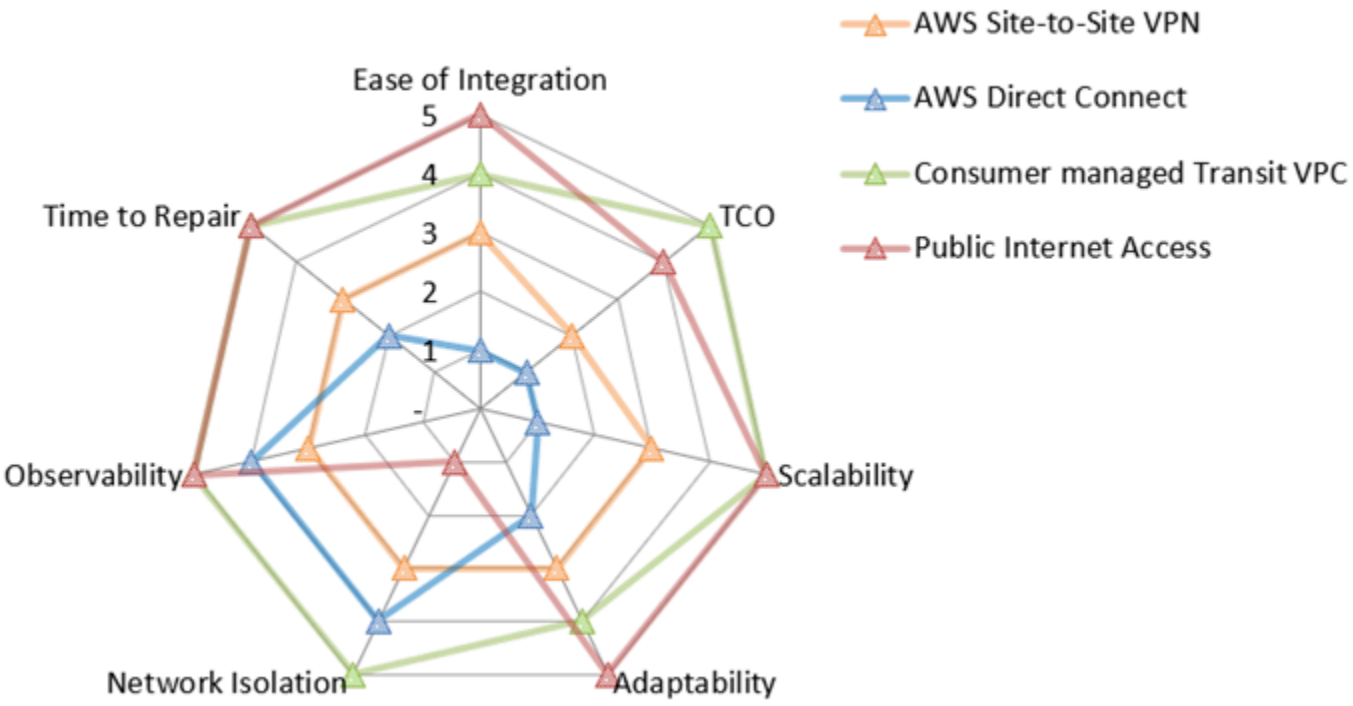
本節討論 中的 SaaS AWS 雲端 工作負載與內部部署資料中心之間的連線選項。許多具有內部部署需求的消費者，特別是在企業層級，將雲端視為實體網路的延伸，而且他們想要在架構中反映這一點。這表示透過邏輯通道或甚至是私有實體連線，在雲端中私有連線至 SaaS 產品。其他消費者將透過公有網際網路接受連線，本節也討論此部分。

本節討論下列網路存取方法：

- 使用 連線 AWS Site-to-Site VPN
- 使用 連線 AWS Direct Connect
- 與傳輸 VPC 架構連線
- 透過公有網際網路連線

下列聯網值映射摘要說明每個評估指標的這些選項分數。如需評估指標的詳細資訊，請參閱本指南中的評估指標。在地圖中，五代表最佳分數，例如最低 TCO、最佳網路隔離或最低修復時間。如需如何讀取此雷達圖的詳細資訊，請參閱本指南網路值映射中的 。

> **Note**
>
> 供應商管理的傳輸 VPC 選項會被排除，因為分數很大程度上取決於正在操作的服務。



雷達圖顯示下列值。

評估指標	AWS Site-to-Site VPN	AWS Direct Connect	消費者受管傳輸 VPC	公有網際網路存取
易於整合	3	1	4	5
TCO	2	1	5	4
可擴展性	3	1	5	5
適應性	3	2	4	5
網路隔離	3	4	5	1
可觀測性	3	4	5	5
修復時間	3	2	5	5

使用 連線 AWS Site-to-Site VPN

AWS Site-to-Site VPN 連線可以在虛擬私有閘道或傳輸閘道上終止。虛擬私有閘道是站台對站台 VPN 連接 AWS 端的 VPN 端點，可連接到單一 VPC。 Site-to-Site 傳輸閘道是一種傳輸中樞，可用於互連多個 VPCs 和內部部署網路。它也可以用作站台對站台 VPN 連接端 AWS 的 VPN 端點。 Site-to-Site 本節討論這兩個選項。

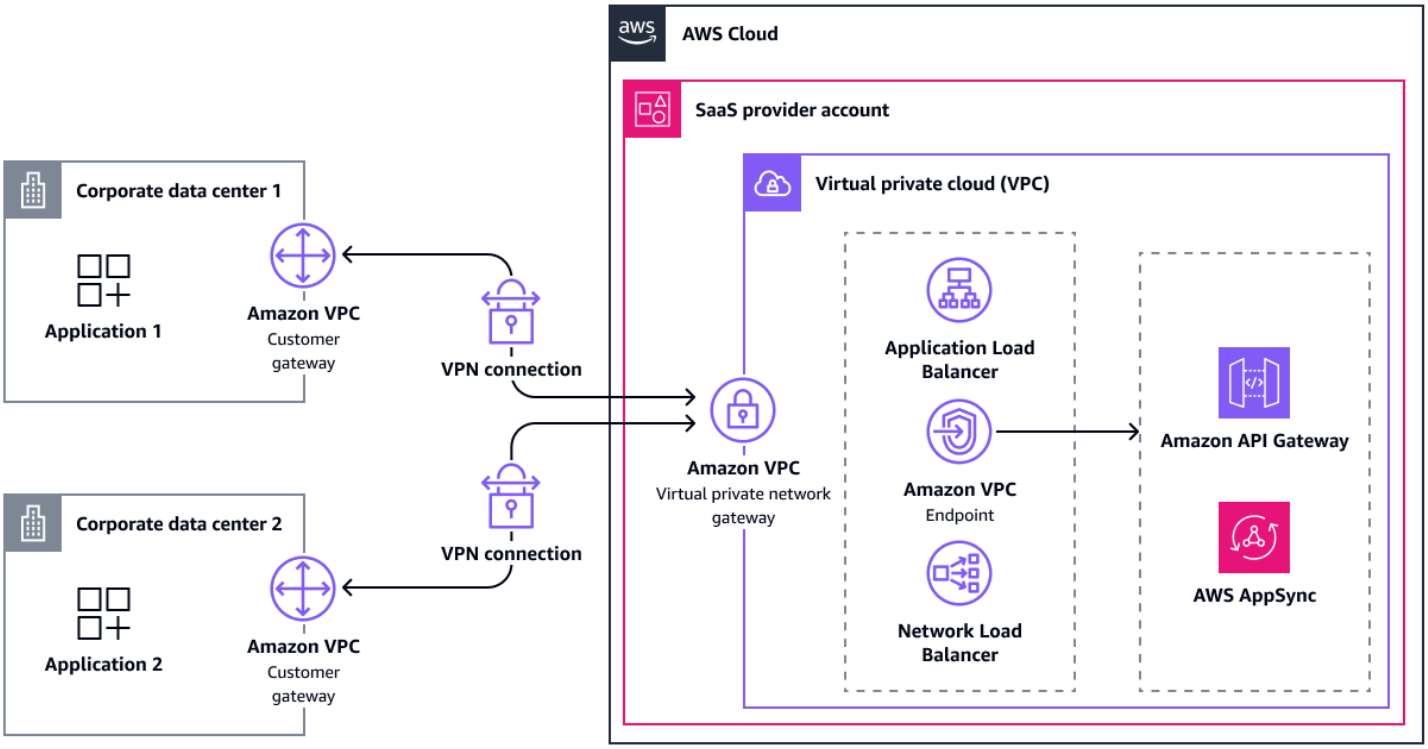
透過虛擬私有閘道的連線

建立虛擬私有閘道之後，您可以將它連接到包含 SaaS 產品的 VPC。然後，您可以啟用路由傳播，將 VPN 路由傳播到 VPC 路由表。這些路由可以是靜態或 BGP 公告的動態路由。

為了實現高可用性，Site-to-Site連接有兩個 VPN 通道，其終止於 AWS 側面的兩個可用區域中。如果無法使用，第二個通道可以接管。單一通道允許最大頻寬 1.25 Gbps。由於虛擬私有閘道不支援等成本多路徑路由 (ECMP)，因此您一次只能使用一個通道。

若要提高容錯能力，您可以設定第二個實體客戶閘道的 VPN 連接。建立連線後，消費者可以連接 SaaS 提供者 VPC 中的資源。

下圖顯示此架構。



以下是此方法的優點：

- 修復時間：受管容錯移轉至次要 VPN 通道
- 可觀測性：使用 Network Synthetic Monitor 整合受管主動監控
- 易於整合：透過 BGP 的動態路由支援
- 適應性：與大多數內部部署聯網設備的相容性
- 適應性：IPv6 支援
- TCO： AWS Site-to-Site VPN 是全受管服務，因此需要的營運工作較少
- TCO：虛擬閘道不收取費用，但每個閘道上的兩個公有 IPv4 地址都會收費
- 網路隔離：透過網際網路啟用安全的私有通訊

以下是此方法的缺點：

- 易於整合：消費者必須設定其客戶閘道
- 可擴展性：缺少 ECMP 支援會將頻寬限制為每個虛擬閘道 1.25 Gbps
- 可擴展性：由於網路複雜性和營運開銷增加，擴展受限
- 適應性：IPv6 僅支援 VPN 通道的內部 IP 地址
- 適應性：無暫時性路由
- TCO：維護、管理和設定 SaaS 供應商許多 VPN 連線的操作額外負荷

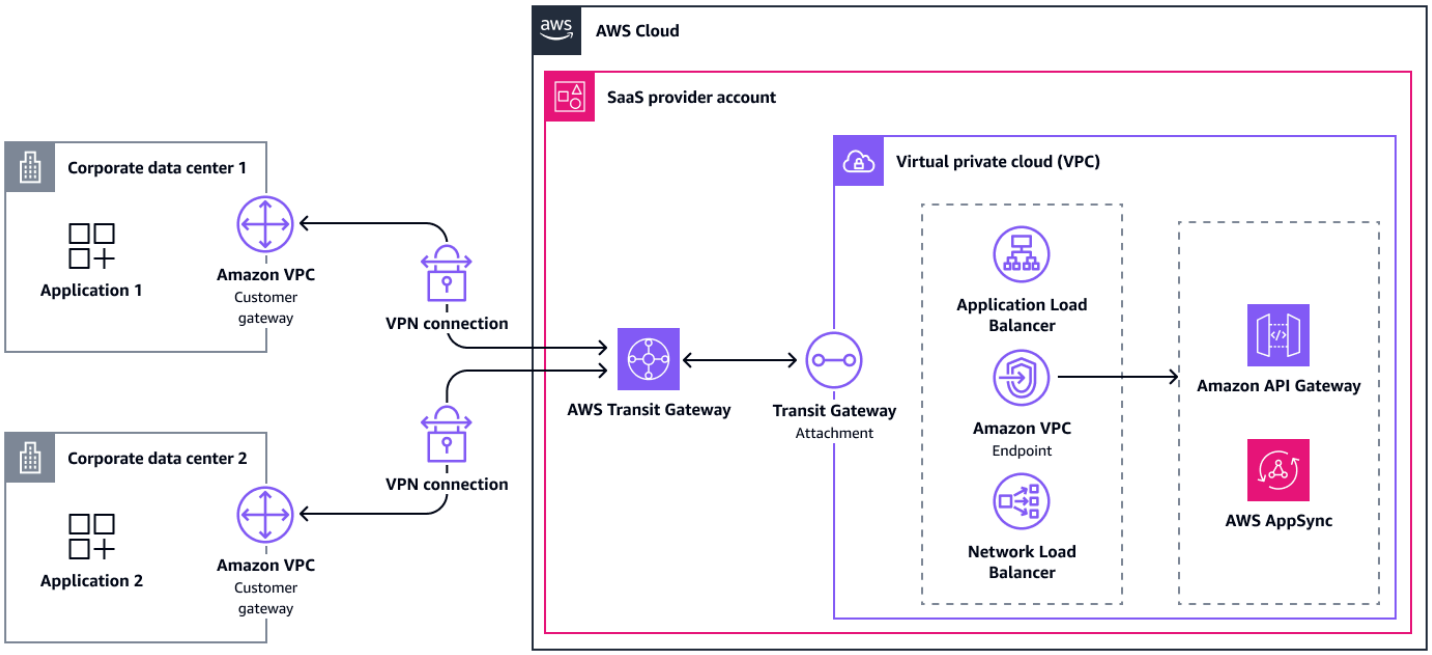
透過傳輸閘道的連線

透過傳輸閘道的連線類似於虛擬閘道。不過，需要記住一些差異。

首先，VPN 連接的路由可以在傳輸閘道路由表中自動傳播，但您必須手動將路由新增至連接的 VPCs。

與虛擬閘道相比，Transit Gateway 支援 ECMP。如果客戶閘道支援 ECMP，則可以使用兩個通道來達到 2.5 Gbps 的總輸送量上限。您可以在相同的內部部署網路與傳輸閘道之間建立多個連線。使用此方法，您可以為每個連線增加高達 2.5 Gbps 的最大頻寬。

下圖顯示此架構。



以下是此方法的優點：

- 修復時間：受管容錯移轉至次要 VPN 通道
- 可觀測性：使用 Network Synthetic Monitor 整合受管主動監控
- 易於整合：透過 BGP 的動態路由支援
- 可擴展性：ECMP 支援允許擴展 VPN 輸送量以滿足大型頻寬需求
- 可擴展性：單一傳輸閘道支援的大量 VPN 連線 （最多近 5，000 個）
- 可擴展性：管理和監控所有 VPN 連線的一處
- 適應性：與大多數內部部署聯網設備的相容性
- 適應性：IPv6 支援
- 適應性： 的繼承彈性 AWS Transit Gateway
- TCO： AWS Transit Gateway 是全受管服務，因此需要的營運工作較少
- TCO：虛擬閘道不收取費用，但每個閘道上的兩個公有 IPv4 地址都會收費
- 網路隔離：透過網際網路啟用安全的私有通訊

以下是此方法的缺點：

- 易於整合：消費者必須設定其客戶閘道
- 可擴展性：由於網路複雜性和營運開銷增加，擴展受限

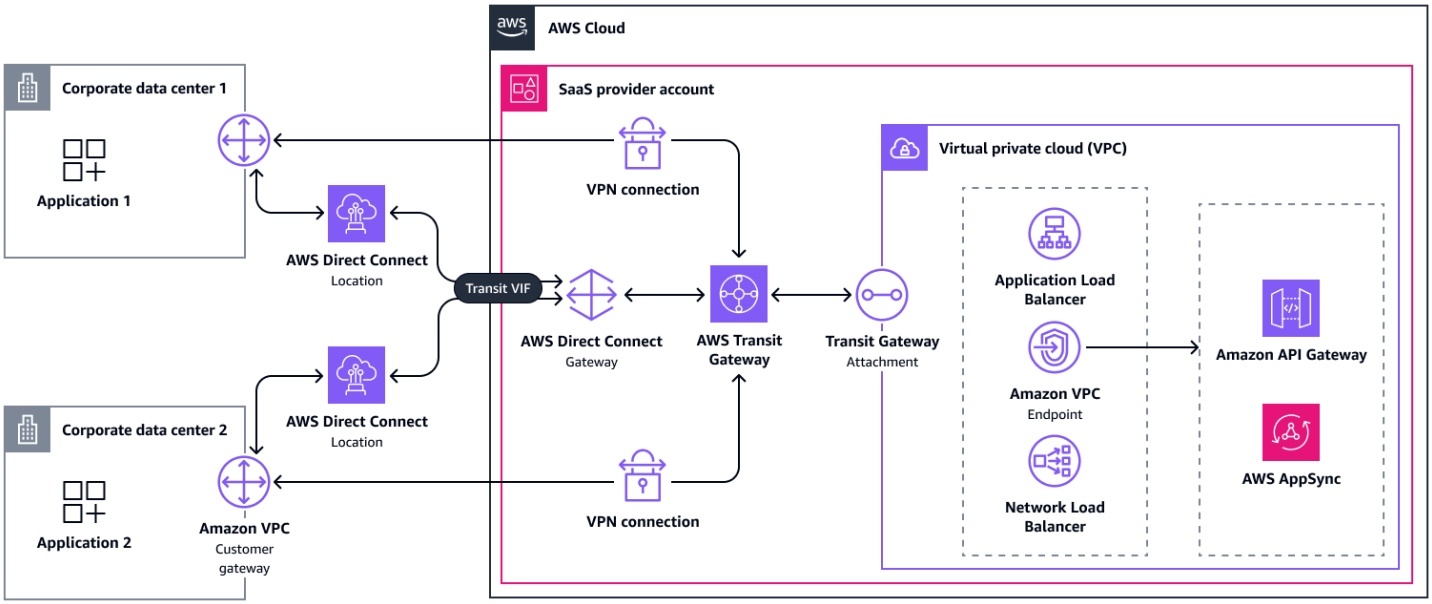
- 適應性：IPv6 僅支援 VPN 通道的內部 IP 地址
- TCO：維護、管理和設定 SaaS 供應商許多 VPN 連線的操作額外負荷
- TCO：使用 的額外費用 AWS Transit Gateway
- TCO：管理傳輸閘道路由表的額外複雜性

使用 連線 AWS Direct Connect

AWS Direct Connect 會透過標準乙太網路光纖纜線將您的內部網路連結至某個 Direct Connect 位置。與其他架構選項不同，無法在幾分鐘內建立專用連線。相反地，如果符合所有要求，此程序最多可能需要幾天的時間。如果沒有，則可能需要更長的時間。因此，我們建議您聯絡您的 AWS 客戶團隊或 AWS 支援 取得此方法的協助。或者，您可以選擇由 AWS 合作夥伴提供並與其他客戶共用的託管連線。無論如何，架構都是相同的。您可以選擇 Direct Connect ，因為它可以減少延遲、改善頻寬或符合法規要求。

若要使用 Direct Connect 連線，消費者必須建立公有、私有或傳輸虛擬介面。有不同的架構選項可用。將多個現場部署位置連接到 最靈活的 AWS 雲端 是連接到 Direct Connect 閘道的傳輸虛擬介面。Direct Connect 閘道是全域邏輯元件，可讓服務供應商最多連接六個傳輸閘道。此外，您最多可以將 30 個虛擬介面連接到閘道。對於擴展，您可以建立其他 Direct Connect 閘道。在 SaaS 提供者帳戶中，傳輸閘道接著會連接至 VPCs，如先前所述。

消費者可以使用一到四個來自一或兩個Direct Connect 位置的 Direct Connect 連線進行連線，具體取決於所需的彈性層級。如需詳細資訊，請參閱設定 Direct Connect 以取得最大彈性。透過網際網路的 AWS Site-to-Site VPN 連線也可以做為 Direct Connect 連線成本較低的備份路徑。支援的 Direct Connect 專用連線可以使用 MACsec 來加密 Direct Connect 位置與資料中心之間的第 2 層連結。通常會有Site-to-Site連線，以便對資料進行額外的機密性。Site-to-Site VPN 連接可以使用正常的 VPN 連接在傳輸閘道上終止。下圖顯示此架構。



以下是此方法的優點：

- 可觀測性：使用 Network Synthetic Monitor 整合受管主動監控
- 可擴展性：支援增加頻寬輸送量
- 適應性：IPv6 支援
- TCO：可能減少資料傳輸
- TCO：一致的網路體驗
- 網路隔離：可滿足法規要求的私有連線

以下是此方法的缺點：

- 易於整合：設定時間和手動工作
- 可擴展性：超過數十個 Direct Connect 連線的可擴展性有限，因為有多個要追蹤的配額
- 適應性：組態選項取決於可用的 Direct Connect 位置
- TCO：排定的 Direct Connect 維護可能會導致需要採取動作的停機時間

與傳輸 VPC 架構連線

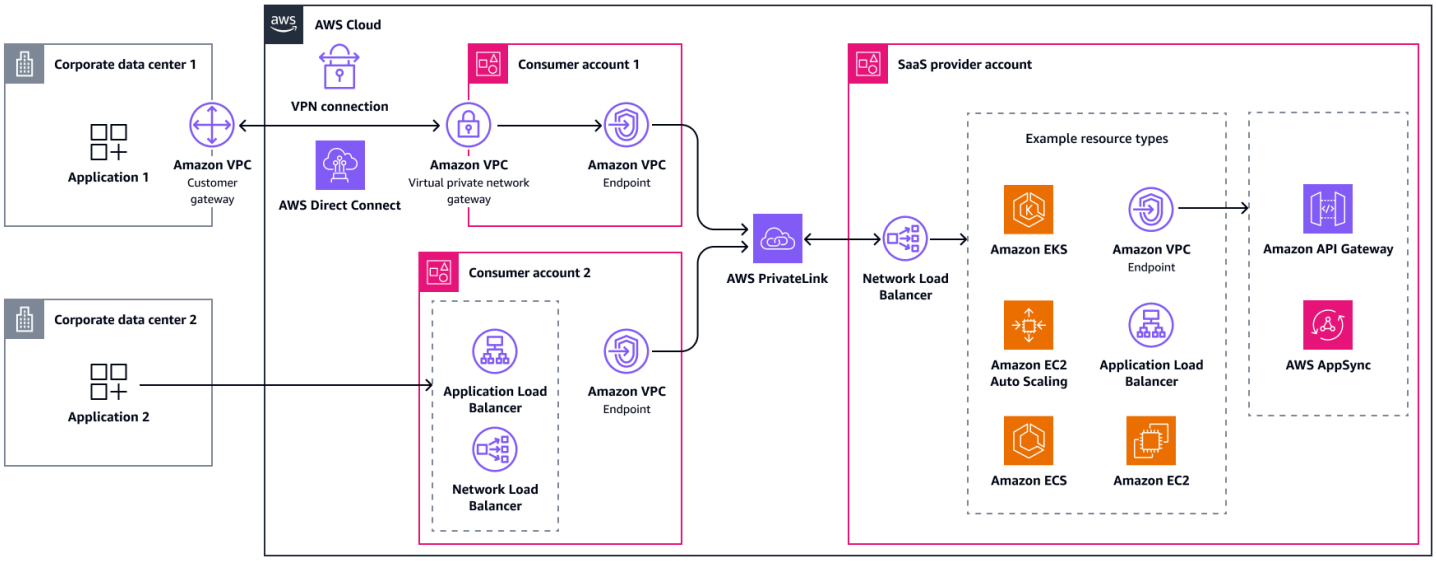
Transit VPC 是一種架構選項，可為消費者提供連線彈性 AWS，並允許 SaaS 供應商透過 統一存取其服務。 AWS PrivateLink消費者從現場部署連線到僅包含進入點（例如虛擬私有閘道） 和介面 VPC 端

點的傳輸 VPC，這是 AWS PrivateLink 資源。傳輸 VPCs 應由 SaaS 提供者或消費者擁有。本節討論這兩個選項。

您可以使用與現場部署資料中心相容的 CIDR 範圍來建立傳輸 VPC 和子網路。如果需要私有連線，消費者可以透過 AWS Direct Connect 或 連線到該 VPC AWS Site-to-Site VPN。您也可以使用指向 VPC 端點的 Application Load Balancer 或 Network Load Balancer，設定從公有網際網路對傳輸帳戶的存取。

消費者受管傳輸 VPC

在此方法中，SaaS 提供者會將傳輸 VPCs 的管理留給消費者。從技術角度來看，SaaS 提供者的架構與透過 AWS 雲端 連線至消費者時相同 AWS PrivateLink。從銷售和產品的觀點來看，這是額外的努力，因為有些消費者 AWS 帳戶 還沒有。他們可能會對開立和操作帳戶感到遲疑。SaaS 提供者應該為消費者提供有關如何建立 AWS 帳戶 和連接現場部署資料中心的指導。下圖顯示公有和私有存取的混合，其中消費者擁有傳輸 VPCs。



以下是此方法的優點：

- 修復時間：營運開銷主要卸載至 SaaS 消費者
- 適應性：SaaS 消費者可以從不同的存取選項中選擇
- 適應性：即使使用Site-to-Site或 Direct Connect
- 所有指標：服務供應商繼承 AWS PrivateLink 利益

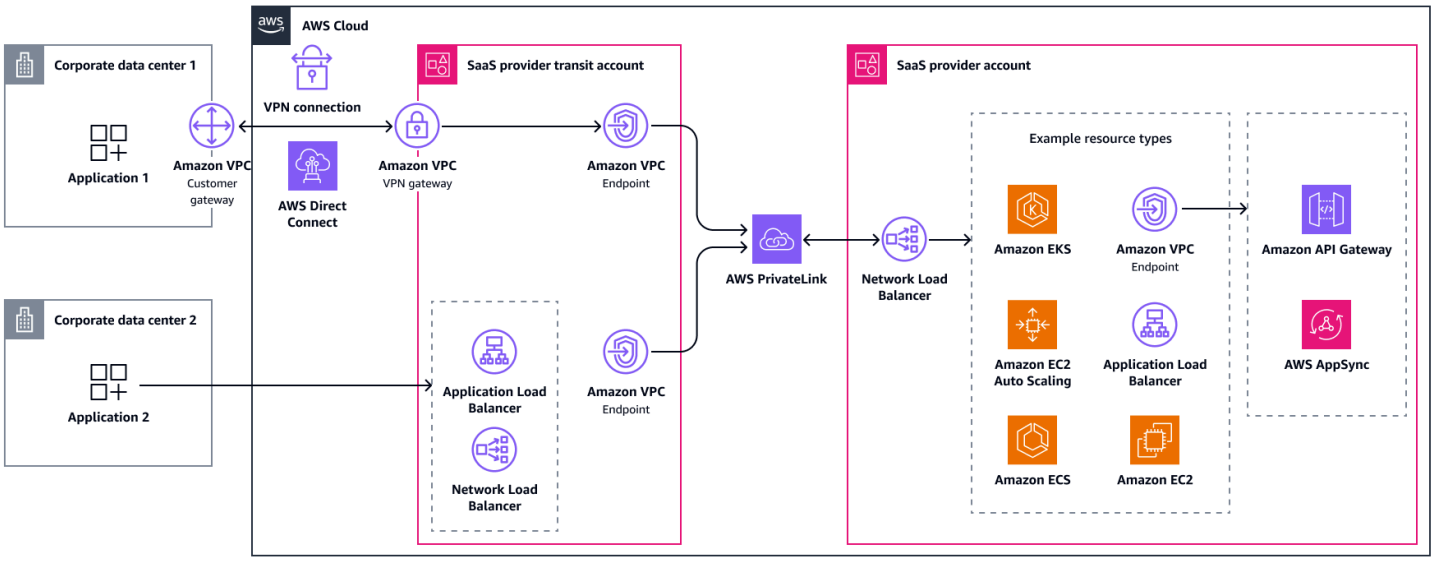
以下是此方法的缺點：

- 易於整合：SaaS 消費者至少需要一個 AWS 帳戶

- TCO：傳輸 VPC 是一種架構，而不是全受管服務，因此需要更多的操作工作

供應商受管傳輸 VPC

這種方法使用相同的技術，但帳戶界限和責任會變更。在這裡，SaaS 供應商擁有傳輸 VPCs，最好是在與 SaaS 產品不同的帳戶中。此解耦可降低成本、降低風險，並允許傳輸帳戶獨立擴展。對於需要高度隔離的環境，您可以使用子網路或為每個消費者建立單獨的傳輸 VPC，在租用戶之間建立額外的分隔。然後，消費者可以選擇如何連接到傳輸 VPC。這種方法提供更多選項來擴展總可定址市場，但由於需要操作和監控其他架構元件，因此 SaaS 供應商擁有更高的 TCO。



以下是此方法的優點：

- 適應性：SaaS 消費者可以從不同的存取選項中選擇
- 適應性：SaaS 消費者不需要擁有 AWS 帳戶
- 適應性：即使使用Site-to-Site或 Direct Connect

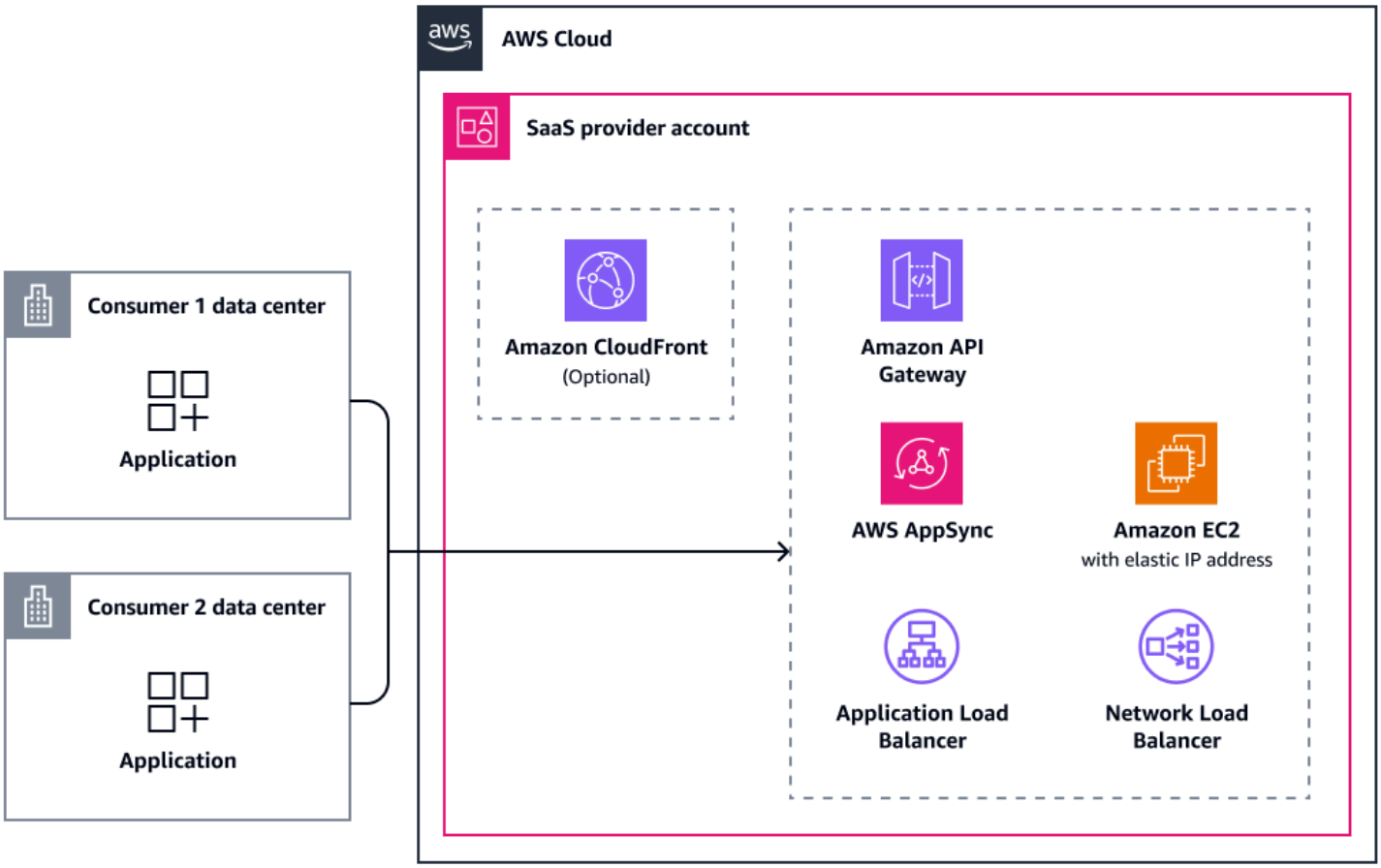
以下是此方法的缺點：

- TCO：傳輸 VPC 是一種架構，而不是全受管服務，因此需要更多的操作工作
- TCO：SaaS 供應商需要操作和監控其他架構元件

透過公有網際網路連線

公有網際網路存取也是提供 SaaS 產品存取權的有效選項，雖然傳統上不提供私有連線。有些消費者可能仍然偏好公開存取方法，因為其與 SaaS 供應商之間不需要額外的聯網基礎設施。它可降低複雜性、成本和整合時間，以換取增加的攻擊面。強大的身分驗證和授權機制有助於緩解增加的威脅層級，您應該一律加密流量。在此案例中，仍建議您多加一層安全性，例如使用 AWS WAF。

此案例中的架構非常簡單。消費者透過網際網路連線至公有主機 (SaaS 供應商）。應用程式可以直接託管在具有彈性 IP 地址的公有 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上。偏好的選項是在 Application Load Balancer 或類似服務後方託管它。為了獲得更好的效能和快取靜態資產，您可以使用內容交付網路，例如 Amazon CloudFront。若要為具有兩個全域靜態 Anycast IP 地址之最低延遲的應用程式提供服務，您可以將 AWS Global Accelerator 放置在 Amazon EC2 執行個體、Network Load Balancer 或 Application Load Balancer 前面。此外，CloudFront AWS AppSync、Application Load Balancer 和 Amazon API Gateway 全都與 整合 AWS WAF。下圖提供公有網際網路存取連線選項的概觀。



下表說明此案例支援的通訊協定和整合。

服務或資源	IPv6	AWS WAF 整合	可以是 Global Accelerator 端點
Amazon CloudFront	支援	支援	不支援
Amazon API Gateway	支援	支援	不支援
AWS AppSync	部分支援	支援	不支援
具有彈性 IP 地址的 Amazon EC2	支援	不支援	支援
Application Load Balancer	支援	支援	支援
Network Load Balancer	支援	不支援	支援

以下是此方法的優點：

- 易於整合：簡易性和可存取性
- 可擴展性：無限制擴展
- 適應性：不可能發生 CIDR 範圍衝突
- 適應性：CloudFront 支援

以下是此方法的缺點：

- 網路隔離：無私有連線
- 網路隔離：需要強大的安全措施

視您選擇的服務而定，適用其他優點和缺點。

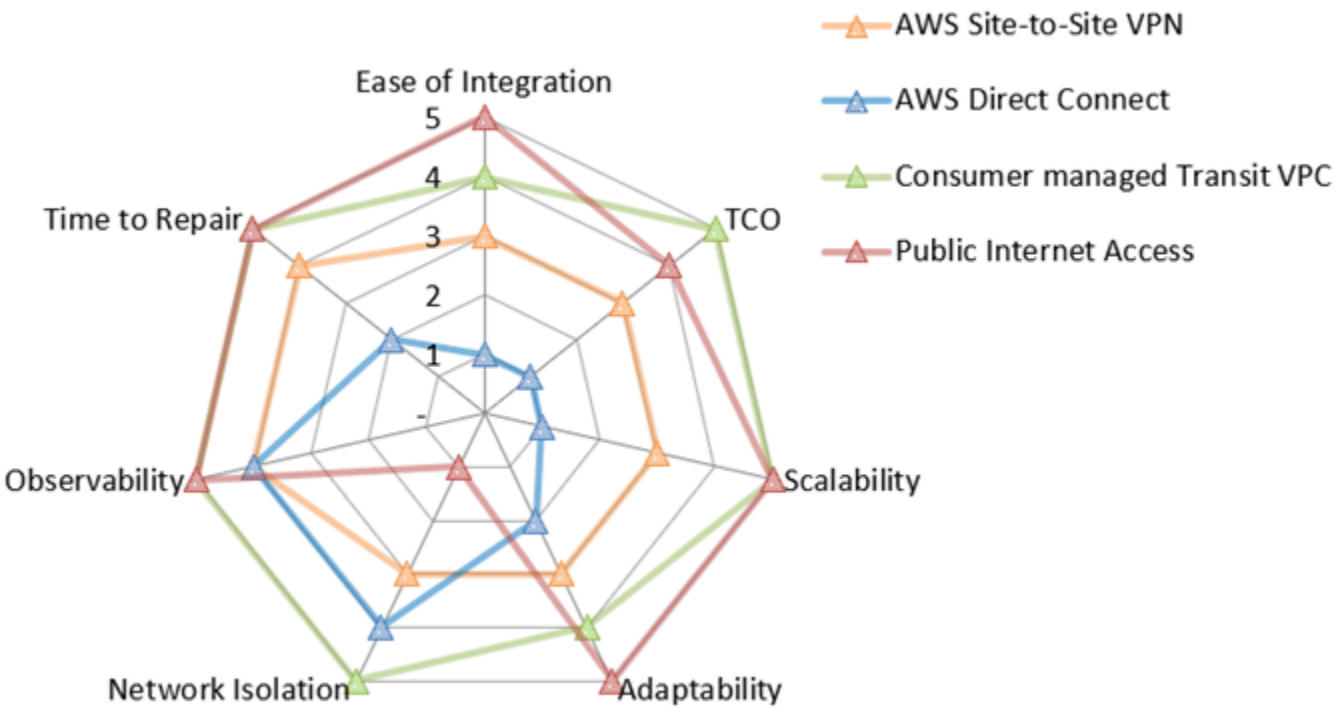
在其他雲端服務供應商上運作的 SaaS 消費者

此案例說明其他雲端服務提供者 (CSPs) 上消費者的解決方案。此案例與內部部署資料中心的連線有一些共同點。事實上，內部部署環境的所有連線選項對其他 CSPs上的消費者同樣有效，即使某些 CSPs

AWS Direct Connect 可以與 進行私有連線。大多數 CSPs提供有關如何 AWS 雲端 透過 AWS Site-to-Site VPN 或 連接到 的文件和支援 AWS Direct Connect。

選擇Site-to-Site時，消費者可以從各自 CSP 的受管閘道或類似資源中受益。消費者不必像現場部署案例一樣自行設定。這會影響Site-to-Site VPN 的一些指標，例如改善修復時間和可觀測性。這是因為現在會管理連線的兩端。

下列聯網值映射摘要說明每個評估指標的這些選項分數。它非常類似於現場部署連線的網路值映射，雖然Site-to-Site的值不同。如需評估指標的詳細資訊，請參閱本指南評估指標中的 。在地圖中，五代表最佳分數，例如最低 TCO、最佳網路隔離或最低修復時間。如需如何讀取此雷達圖的詳細資訊，請參閱本指南網路值映射中的 。



雷達圖顯示下列值。

評估指標	AWS Site-to-Site VPN	AWS Direct Connect	消費者受管傳輸 VPC	公有網際網路存取
易於整合	3	1	4	5
TCO	3	1	5	4
可擴展性	3	1	5	5

適應性	3	2	4	5
網路隔離	3	4	5	1
可觀測性	4	4	5	5
修復時間	4	2	5	5

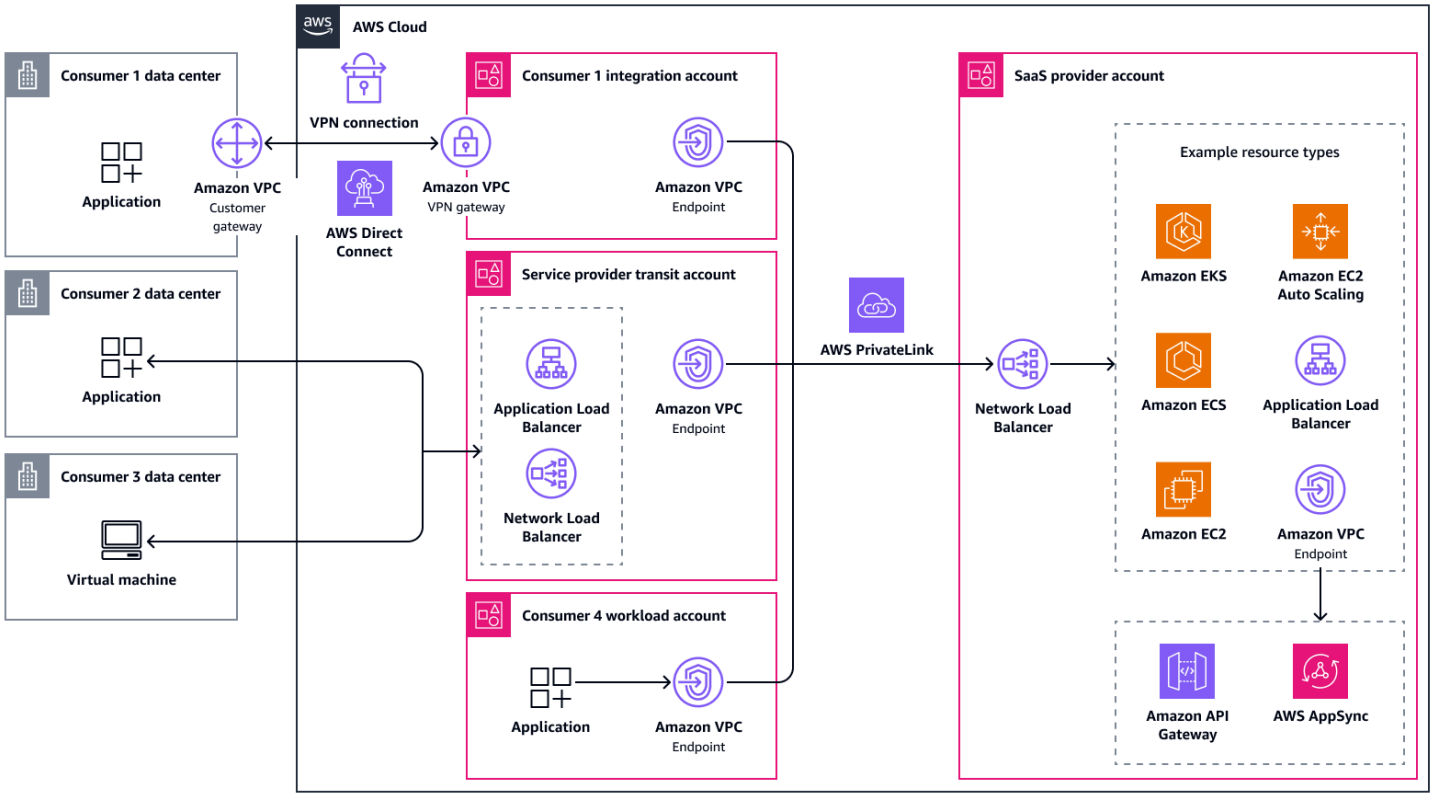
支援混合環境

消費者通常來自不同的環境，每個環境都有自己的技術和安全限制。有些客戶可能完全從需要透過網際網路或透過專用網路連結進行安全連線的內部部署資料中心操作。其他 可能已在 內執行工作負載，AWS 並預期低延遲的私有網路路徑。第三個群組可能會依賴其他 CSPs，其中連線必須橋接不同的雲端網路。

無論如何，您應該以標準化網路存取 SaaS 應用程式為目標，以簡化架構並降低操作複雜性。先前介紹的兩種方法 - 公有網際網路存取和傳輸 VPCs - 適用於這些案例。公有網際網路存取可為您的客戶提供最快的加入路徑，且設定最少。傳輸 VPCs提供更受控制的私有存取，通常使用 AWS PrivateLink。

設計 SaaS 產品時，您可以採用單一網路存取模型，或將多種方法結合到分層產品中。例如，您可以為優先考慮輕鬆連線和快速入門的客戶提供公有存取部署層，也可以為具有嚴格合規或安全控制要求的客戶提供私有存取部署層。這些層具有不同的成本、效能和風險設定檔。您也可以將這兩種方法合併為單一架構。在這種情況下，請確保您有強大的安全措施，以便公有和私有路徑保持隔離。

下圖顯示混合存取方法，消費者可以選擇從其資料中心或 CSP 私下、公開或直接透過 進行連線 AWS PrivateLink （ 如果他們在 中有工作負載 AWS 雲端)。


AWS Cloud
Consumer 1 data center
Application
Amazon VPC
Customer gateway
VPN connection
Amazon VPC
VPN gateway
AWS Direct Connect
Consumer 1 integration account
Amazon VPC
Endpoint
Consumer 2 data center
Application
Consumer 3 data center
Virtual machine
Service provider transit account
Application Load Balancer
Network Load Balancer
Amazon VPC
Endpoint
Consumer 4 workload account
Application
Amazon VPC
Endpoint
AWS PrivateLink
SaaS provider account
Network Load Balancer
Example resource types
Amazon EKS
Amazon EC2 Auto Scaling
Amazon ECS
Application Load Balancer
Amazon EC2
Amazon VPC
Endpoint
Amazon API Gateway
AWS AppSync

中的 SaaS 產品的進階聯網存取案例 AWS 雲端

中的 SaaS 產品聯網存取案例 AWS 雲端 一節中討論的架構應可協助您尋找大多數使用案例的解決方案。不過，有些案例有特定的技術需求。許多 超出本指南的範圍。

本節討論下列進階技術需求和考量事項：

- 雙向通訊
- TCP、UDP 和專屬通訊協定

雙向通訊

在某些情況下，應用程式需要雙向流量，才能如預期般運作。常見的使用案例是 Webhook 或通知服務。一般而言，您可以在伺服器與用戶端之間建立 WebSocket 連線來達成此目的。此連線會保持 TCP 工作階段開啟，並允許兩個參與者透過連線傳送流量。本指南中討論的大多數服務原生支援 WebSocket，包括 Network Load Balancer、Application Load Balancer、Amazon API Gateway AWS PrivateLink和 AWS AppSync （ 透過私有即時端點)。

在其他情況下，SaaS 供應商端的應用程式可能需要存取取用者端的資源，例如資料庫。當您透過雙向管道連線時，例如 AWS Site-to-Site VPN 連線，這不是問題。

另一方面， AWS PrivateLink 和 Elastic Load Balancing 僅支援單向流量。如果您使用這些服務，則必須為從 SaaS 產品啟動的流量設定另一個網路路徑。例如，這可能是往反方向的額外 AWS PrivateLink 連線。

TCP、UDP 和專屬通訊協定

許多應用程式是透過 HTTP 或 HTTPS 提供，但並非全部。有些 可能會在 TCP 上使用其他第 7 層通訊協定，例如訊息佇列遙測支援 (MQTT)。其他人甚至可能使用 UDP 為消費者提供服務。在極少數情況下， 服務會使用必須在封包 （ 第 3 層 ） 內傳輸的專屬通訊協定。對於這些案例，請務必了解哪些服務支援您的 SaaS 產品。

對於 Layer 3 服務，您可以使用 AWS PrivateLink 和 Network Load Balancer，這兩者都支援所有 TCP 和 UDP 流量。

對於 Layer 7 服務，Application Load Balancer 和 Amazon CloudFront 支援 HTTP、HTTPS、WebSocket 和 Google 遠端程序呼叫 (gRPC)。同樣地，Amazon API Gateway 和

AWS AppSync 每個 都支援 HTTP、HTTPS 和 WebSocket。Amazon CloudFront 是目前唯一支援 HTTP/3 的服務。

您可以使用 Amazon VPC Lattice 來連接 Layer 7 應用程式和 Layer 3 資源。它支援 HTTP、HTTPS、gRPC、TCP 和 TLS 傳遞。

如果應用程式只能透過第 3 層提供流量，請務必使用核心 AWS 聯網服務 AWS Transit Gateway，例如 AWS Direct Connect AWS Site-to-Site VPN， 和 VPC 對等互連。然後，流量應該直接從 SaaS 取用者路由到 SaaS 產品的運算層。

中的網路存取反模式 AWS 雲端

反模式是經常性問題的常用解決方案，其解決方案具有反生產力、無效或效果不如替代方案。本節中提到的設計選項通常有效，但具有重大缺點。如果可能，應該避免它們，因為有更好的替代方案可用。

本節討論下列反模式和挑戰：

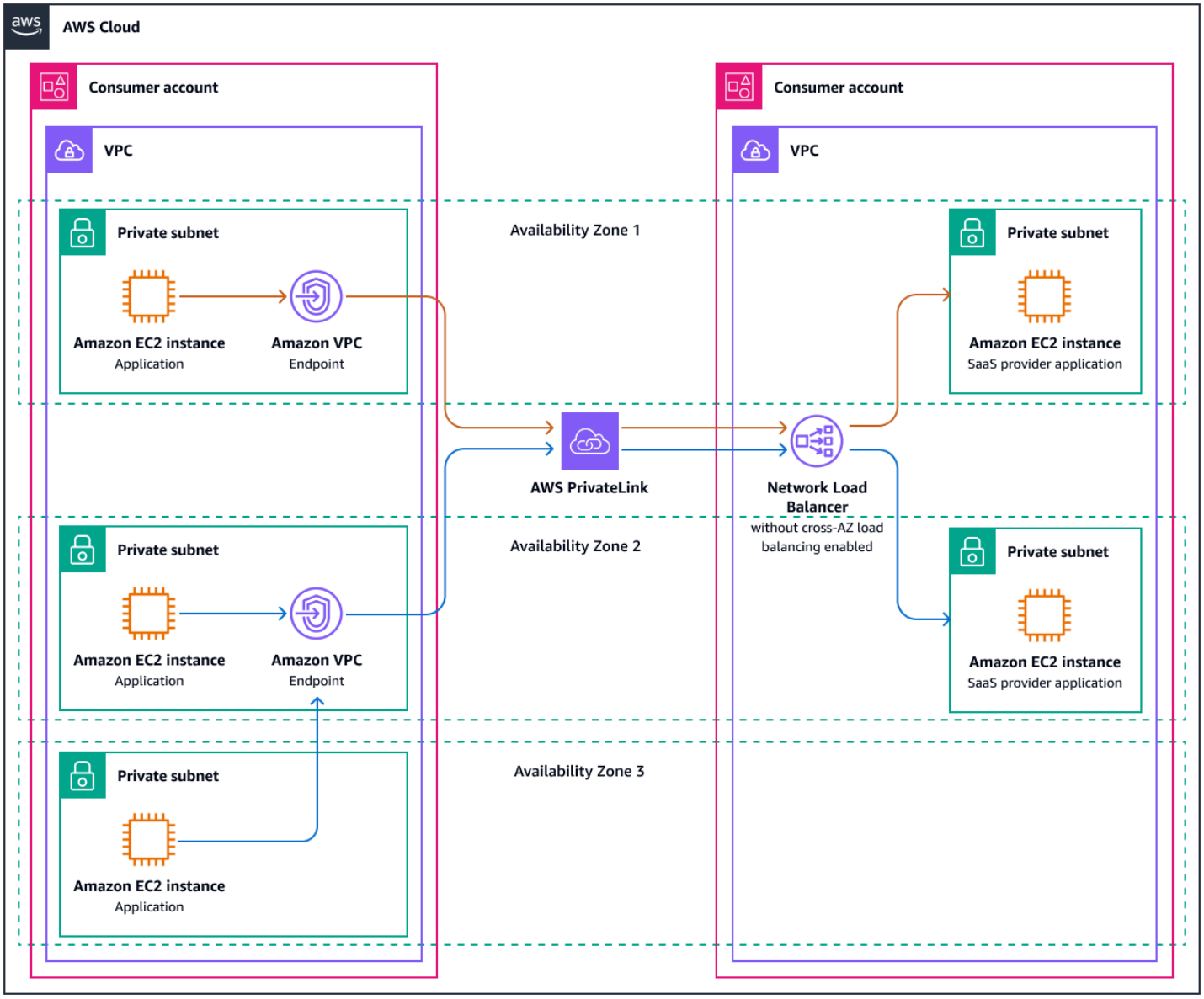
- 可用區域與 不相符 AWS PrivateLink
- AWS Site-to-Site VPN 之間的連線 AWS 帳戶

可用區域與 不相符 AWS PrivateLink

透過 提供應用程式存取權時 AWS PrivateLink，SaaS 取用者只能在部署應用程式的可用區域中建立介面 VPC 端點。例如，如果應用程式部署在 use1-az1和 中use1-az2，消費者就無法在 中部署 VPC 端點use1-az3。建議您在每個可用區域中部署 SaaS 產品。大多數 AWS 區域 有三個可用區域，但有些有更多可用區域。如需完整清單，請參閱區域和可用區域。選擇 時，請考慮可用區域的數量 AWS 區域。

> **Note**
>
> 可用區域名稱與可用區域 IDs不同。如需詳細資訊，請參閱 AWS 資源的可用區域 IDs。

如果 SaaS 供應商選擇不在所有可用區域中部署，則會產生一些後果。假設 SaaS 產品已部署在 use1-az1和 中use1-az2，但消費者正在使用所有三個可用區域，包括 use1-az3。介面 VPC 端點部署在 use1-az1和 的取用者端use1-az2，現在 中的應用程式use1-az3需要存取其中一個端點。首先，必須允許從不相符可用區域中的子網路到個別 VPC 端點的流量。消費者可以決定使用區域 AWS PrivateLink DNS 名稱，此名稱可以解析為任一 VPC 端點，並在兩者之間平均分配流量。或者，消費者可以選擇將流量直接傳送到端點，例如 use1-az2。這會導致 67% 的流量到達 中的提供者端use1-az2，以及 中的 33%use1-az1。下圖說明此案例。



由於大量消費者和流量分佈不均，工作負載可能會遇到一個可用區域中的容量問題，並在另一個可用區域中的容量不足。為了解決此問題，SaaS 提供者可以在 Network Load Balancer 上啟用跨區域負載平衡，以決定平均地平衡其端的流量。這會產生額外費用。

如果服務提供者只比對一個可用區域，則所有流量將透過單一端點進入。這會產生更大的不平衡。因此，消費者不再高度使用 SaaS 產品。對於消費者而言，應用程式是否透過他們自己未使用的其他可用區域提供並不重要。在最壞的情況下，SaaS 供應商可能無法為未使用任何相同可用區域的消費者提供服務。

在極少數情況下，SaaS 提供者無法透過所有可用區域佈建其應用程式，也可以僅在缺少的可用區域中建立子網路，然後將服務延伸至這些空的可用區域。跨區域負載平衡接著可以將傳入流量分配到其他可用區域中的實際應用程式端點。

AWS Site-to-Site VPN 之間的連線 AWS 帳戶

從內部部署環境遷移到雲端的公司有時會嘗試提升和轉移整個網路。這可能會導致問題，因為內部部署和雲端聯網實務之間存在重大差異。如果沒有發生這種思維轉移，可能會發生像是從一個 VPC 到另一個 VPC 的 AWS Site-to-Site VPN 連線。此方法無法利用 中的專用聯網服務 AWS 雲端，可簡化管理並改善效能。適應雲端原生設計有助於降低營運開銷，並在 VPCs連線能力。

如果您考慮以 SaaS 提供者身分提供此連線選項，請詢問自己或消費者為什麼 AWS Site-to-Site VPN 應該使用。然後，從這些要求向後工作，尋找更好的連線選項。本指南的比較服務功能區段包含一個矩陣，您可以用來協助識別選項。然後，您可以完成本指南的相關章節，尋找解決您的使用案例的架構方法。

後續步驟

本指南說明不同案例的各種網路存取方法，並說明每個架構的優點和缺點。您應該了解為什麼選擇網路存取方法不應只是技術討論。商業和技術之間的一致性至關重要。下列後續步驟和建議可協助您透過評估目前功能、分析市場需求和實作控管控制，來評估和標準化網路架構策略。

本節包含下列主題：

- 評估目前的架構和功能
- 市場和客戶分析
- 策略一致性
- 標準化
- 控管
- 重複

評估目前的架構和功能

根據相關資料來源檢閱目前的網路架構，例如本指南中的自我評估架構、目前的法規要求，以及目前的市場狀態（包括您的客戶和競爭分析）。例如，請考慮使用 AWS Well-Architected Framework，這是基於在 中大規模執行生產系統數十年的經驗 AWS 雲端。

檢閱任何潛在的例外狀況、一次性和歷史產品決策。保持好奇、挑戰它們，並且不要自動假設其有效性。多年前的客戶要求可能不再有效。挑戰假設可創造簡化和降低架構複雜性的機會。

簡單來說，請記錄觀察結果，以便組織中的不同角色可以存取和了解這些觀察結果。擷取目前狀態與目標狀態不同的位置、目標狀態、影響，以及進行觀察的時間。記錄此資訊有助於您的組織根據新資料做出決策。

市場和客戶分析

收集市場趨勢的洞見。消費者目前偏好的 SaaS 產品存取方式是什麼？ 您仍在與客戶會面嗎？ 客戶群組或行為是否變更？ 您的高階主管是否將船舶轉向新市場、具有特定法規要求的地理位置或新客戶層？ 您的業務或營運模式是否有所變更？ 例如，您是否正在考慮將服務標示為白標籤？ 您的成長計畫是否包括與合作夥伴合作，以便在客戶與這些合作夥伴連線時，提供這些服務？

策略一致性

當您了解目前的功能、目前的架構、市場和客戶時，請呼叫策略一致性會議。使用相關的產品、業務和技術利益相關者，挑戰哪些要求仍然有效，以及哪些新要求需要考慮。透過捨棄不再需要的要求，尋找降低複雜性的機會。這不是委員會的設計；工程團隊需要準備並擁有實際的架構和實作詳細資訊。不過，此會議應釐清為什麼這是一組要求，可最大限度地為您的客戶和組織帶來好處。

標準化

為了吸引客戶，讓每個客戶自由選擇如何連接到您的服務可能會很有吸引力。畢竟，任何解決方案在技術上都可以運作，而且您可能也具備管理及操作所有解決方案的專業知識和資源。這可以在特定時間點上正常運作，但隨著您的業務擴展，很難管理。您的可觀測性堆疊需要支援來自多個解決方案的指標，而您的站點可靠性工程師也需要能夠了解這些指標。您需要每種連線方法up-to-date文件。您應用程式的主要變更需要針對您提供的每個存取方法進行評估。您需要為每個存取方法撰寫和維護自動化和基礎設施作為程式碼 (IaC)。未標準化服務存取的額外額外負荷，必須權衡您想要提供給客戶的彈性。

如果您需要北星來引導您的決策制定，我們建議標準化。標準化您的客戶如何與您提供的服務互動，通常是您可以採取的最有影響力行動，以改善整個組織的許多成功指標。標準化可讓產品團隊更輕鬆地了解服務的成本結構，並做出資料驅動型產品決策。在根據預先定義的標準開發、推出和操作的環境中，操作團隊可以更輕鬆地對問題進行故障診斷，並自動化部分故障診斷程序。它可協助您偵測惡意演員的異常、意外行為或動作。標準化也可減少技術負債。工程團隊需要較少的週期來測試和推展生產變更。它也可以加快您的上市速度、改善自助服務上線成功，並降低法規風險。

因此，我們建議您也檢閱目前可能已就緒的任何一次性項目。量化您用來支援現有客戶的操作週期數量。將您的結果與歷史資料進行比較，並評估您目前的方法是否在未來幾年內擴展。每當需要轉移標準時，請挑戰這些請求背後的需求。評估影響，並平衡立即利益與長期承諾。

如果自訂是不可避免的，但與您的標準衝突，請考慮共同的責任模型。在此模型中，您的產品在很大程度上會受到請求變更的保護，而自訂會在最少的專用環境中進行。如需範例，請參閱 與傳輸 VPC 架構連線一節。

控管

為了符合法規要求和您自己的內部標準，控管至關重要。透過適當的控管，您可以控制強制執行標準的位置和方式。您也可以建立 來控制 ，以偵測與標準的差異，並通知資源擁有者必要的修正動作。AWS Organizations、AWS CloudTrail、 AWS Config和 AWS Control Tower是其中一些 AWS 服務 可協助您管理和控管 中工作負載 AWS 雲端。

重複

使用您最初工作的學習，設定輕量且可重複的程序，以在未來保持一致。定義您需要輸入的角色、頻率、資料需要的準確度、資料如何共用，以及誰將對其採取行動。

資源

AWS 文件

- 在 中整合第三方服務 AWS 雲端(AWS 方案指引）
- 多租戶 SaaS 授權和 API 存取控制 (AWS 規範指引）
- 在單一控制平面上跨多個 SaaS 產品管理租用戶 (AWS 方案指引）
- 什麼是 AWS Direct Connect？(Direct Connect 文件）
- 什麼是 AWS PrivateLink？ (Amazon VPC 文件）
- 什麼是 AWS Site-to-Site VPN？ (AWS Site-to-Site VPN 文件）
- 什麼是 AWS Transit Gateway？ (Amazon VPC 文件）
- 什麼是 VPC 對等互連？ (Amazon VPC 文件）

其他 AWS 資源

- Amazon Virtual Private Cloud Connectivity Options (AWS 白皮書）
- AWS re：Invent 2021 - 如何為您的 AWS 工作負載選擇正確的負載平衡器 (YouTube)
- 什麼是 SaaS？(AWS 網站）
- AWS SaaS Factory Program (AWS Partner 程式）
- 上的多租戶架構指南 AWS(AWS 解決方案程式庫）

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 12 日

AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的內部部署 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護欄，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 延伸了原本專為精簡製造實務設計的價值串流映射程序。它著重於在軟體開發過程中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 中的在 雲端中復原工作負載的災難 AWS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)

組織之間商業文件的自動交換。如需詳細資訊，請參閱什麼是電子資料交換。

加密

將人類可讀取的純文字資料轉換為加密文字的運算程序。

加密金鑰

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

端序

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

端點

請參閱 服務端點。

端點服務

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

企業資源規劃 (ERP)

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

信封加密

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

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

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

epic

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

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

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

F

事實資料表

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

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等邊界會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱AWS 故障隔離界限。

功能分支

請參閱分支。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

少量擷取提示

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

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過變更資料擷取使用連續資料複寫，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已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，以及自然語言的交談。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)

安全機制可篩選、驗證和限制代理程式輸入和輸出，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)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，並處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

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

保留資料

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

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

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

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

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC，可管理 VPCs 之間 （在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱什麼是 IoT？

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM 提供了基礎。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需有關將雲端操作與 ITSM 工具整合的資訊，請參閱操作整合指南。

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會獲得明確指派的安全標籤值。使用者安全標籤和資料安全標籤之間的交集會決定使用者可以看到哪些資料列和資料欄。

登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱設定安全且可擴展的多帳戶 AWS 環境。

大型語言模型 (LLM)

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

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的套用最低權限許可。

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱機器學習。

主要分支

請參閱分支。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊，或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬程式、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。

MCP

請參閱模型內容通訊協定。

模型內容通訊協定 (MCP)

適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

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。

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，通常可接受中等速度的查詢。

視窗函數

SQL 函數，對與目前記錄在某種程度上相關的資料列群組執行計算。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，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。