擁抱零信任：安全且敏捷的業務轉型策略

AWS 規範性指導

AWS 規範性指導: 擁抱零信任：安全且敏捷的業務轉型策略

Table of Contents

擁抱零信任：安全且敏捷的業務轉型策略

Greg Goden，Amazon Web Services (AWS)

2023 年 12 月 (文件歷史記錄)

如今，組織比以往任何時候都更聚焦於將安全性作為關鍵要務。這會產生各式各樣的好處，例如維持客戶的信任、改善人力流動性，或解鎖全新數位商機。在他們這麼做的時候，就會持續問一個老問題：「什麼是能確保系統和資料安全性正確等級和可用性的最佳模式？」「零信任」一詞已越來越常用來說明此問題的現代答案。

零信任架構 (ZTA) 是一組概念模型和一系列相關聯的機制，著重於為數位資產提供安全控制項，且這些機制並非僅根據傳統的網路控制項或網路邊界運作，或完全不基於此類措施運作。而是透過身分識別、裝置、行為和其他豐富的背景資訊和訊號來增強網路控制，以做出更精細、更有智慧、更具適應性且持續的存取決策。透過實作 ZTA 模型，您便能隨著網路安全和深度防禦概念持續發展成熟的過程，實現有意義的下一次迭代。

決策程序

實作 ZTA 策略需要仔細的規劃和決策，其中包含評估各種因素，並將其與組織目標保持一致。展開 ZTA 之旅的關鍵決策程序包括：

1. 利害關係人的參與 – 務必與其他高階主管、副總和資深經理互動，以了解他們對組織安全狀態的優先順序、疑慮和願景。若從一開始就將關鍵利害關係人納入其中，您便能將 ZTA 實作與整體策略目標保持一致，並取得必要的支持和資源。
2. 風險評估 – 進行全面的風險評估有助於識別問題、過大的受攻擊面積和關鍵資產，以便讓您針對安全控制項和投資做出明智的決策。評估組織現有的安全狀態、找出潛在弱點，並根據您產業和營運環境的特定風險格局，排定改善領域的優先順序。
3. 技術評估 – 評估組織現有的技術全貌並識別缺口，有助於選擇符合 ZTA 原則的適當工具和解決方案。這項評估應包括對以下項目的徹底分析：
    - 網路架構
    - 身分識別和存取管理系統
    - 身分驗證和授權機制
    - 統一端點管理
    - 資源擁有權工具和程序
    - 加密技術

- 監控和日誌功能
- 選擇正確的技術堆疊，對於建置堅實的 ZTA 模型至關重要。

4. 變更管理 – 認知到採用 ZTA 模型的文化和組織影響至關重要。實作變更管理實務有助於確保整個組織順利進行轉換和接納。其中包含向員工說明 ZTA 的原則和好處、提供有關新安全實務的培訓，以及培養有關安全意識的文化，鼓勵問責制和持續學習。

本規範性指引旨在為高階主管、副總和資深經理提供實作 ZTA 的全方位策略。它會深入探討 ZTA 的關鍵面向，其中包括以下層面：

- 組織準備程度
- 分階段採用方法
- 利害關係人協作
- 實現安全和敏捷業務轉型的最佳實務

透過遵循本指南，您的組織可以在 Amazon Web Services (AWS) Cloud 中瀏覽 ZTA 環境，並在安全旅程中取得成功成果。 AWS 提供各種服務，可用於實作 ZTA，例如 AWS Verified Access、 AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway 和 Amazon GuardDuty。這些服務可協助保護 AWS 資源免於未經授權的存取。

目標業務成果

本節會討論為整個組織定義和實作零信任架構的相關期望結果。

改善安全狀態

您的組織可以透過採用零信任原則，強化安全狀態、降低安全風險，以及保護雲端基礎設施和資料。零信任的基本原則是基於僅知原則授予存取權限，再搭配嚴格的控制項、大幅減少受攻擊面積，以及限制安全事件的潛在影響。這種主動的方法有助於組織勝過新興的安全風險，並協助確保資產的機密性、完整性和可用性。

順暢採用雲端

制定明確定義的零信任架構 (ZTA) 採用計劃，可協助確保順利且成功地轉換至雲端環境。ZTA 原則與雲端安全最佳實務密切配合，為組織提供穩固的基礎，以便安全地獲得雲端運算的好處。若從一開始就整合 ZTA 原則，便有助於組織以安全性為核心元素來設計雲端架構。

合規性和法規一致性

實作 ZTA 實務有助於組織符合業界與法規要求和標準。ZTA 本身就會推動最低權限原則，以及強制執行嚴格的存取控制項。存取控制項通常受下列法規管理：

- 聯邦風險與授權管理計劃 (FedRAMP)
- 美國健康保險流通與責任法案 (HIPAA)
- 支付卡產業資料安全標準 (PCI DSS)。

您的組織可以透過採用零信任架構，表明自身對資料保護、隱私權和法規遵循的承諾，同時大幅降低受罰或聲譽受損的可能性。

加強資料保護

組織可以透過實作資料加密、存取控制項和定期安全評估來保護整個雲端採用程序中的敏感資料。您的組織可以採取下列特定步驟：

- 資料加密 – 資料加密 – 資料加密是透過需要金鑰才能將資料解密回原始純文字格式的方式，將純文字資料加密為密文的程序。這使得未經授權的人員更難以存取敏感資料，即使他們能夠取得資料副本亦然。
- 存取控制項 – 存取控制項會限制可存取敏感資料的人員，以及他們可以使用資料執行哪些事項。這項措施的執行方式可以是指派使用者角色和權限，以及使用多重因素身份驗證或其他方法來驗證使用者身份。
- 定期安全評估 – 定期進行安全評估，有助於組織識別和解決安全問題，並主動進行修復。此類評估可由內部安全團隊或外部安全公司進行。

零信任架構透過實作多種安全措施，對資料保護採取全方位的方法。此類措施包括高強度身分驗證、資料加密和精細的存取控制項。這種方法可大幅降低資料相關安全事件的風險，以及防止敏感資訊遭到未經授權的存取。

高效率事件回應

組織可以在雲端環境中建立監控和事件回應框架，以便更快速有效地偵測及回應安全事件。零信任架構強調持續監控、威脅情報整合，以及即時掌握使用者活動、網路流量和系統行為。安全團隊接著便能主動識別和緩解安全事件。這種方法可以縮短偵測和回應潛在問題的時間，並大幅降低對業務營運的影響。關鍵要點包括以下項目：

- 測試 – 無論組織採用何種事件回應框架或方式，都應該定期測試事件回應計劃。透過桌上演練、模擬和紅隊演練獲得練習機會，在實際的設定中練習事件回應、找出工具和能力的缺口，以及為事件回應人員建立經驗和信心。
- 監控 – 持續監控雲端環境是否出現異常活動的跡象。您可以使用各種工具和技術來完成這這項操作，例如日誌分析、網路監控和漏洞掃描。
- 威脅情報整合 – 將威脅情報整合至監控和事件回應框架。這有助於組織更快速有效地識別威脅並加以回應。
- 即時可見性 – 若要快速識別並回應安全事件，組織必須能即時掌握使用者活動、網路流量和系統行為。
- 主動識別和緩解 – 組織可透過主動識別和緩解安全事件，縮短偵測和回應潛在威脅的時間，大幅降低對業務營運的影響。

提高人力的生產力

現代的人力需要彈性，以便從日益增加的位置、裝置和時間完成工作。您可透過實作 ZTA 為這些需求提供支援，並改善人力流動性、生產力和滿意度，同時維持或改善組織的安全狀態。

達成數位轉型

作為數位轉型的一部分，組織越來越追求在傳統網路邊界之外的裝置、機器、設施、基礎設施和程序之間的互聯。物聯網 (IoT) 和營運技術 (OT，也稱為工業物聯網或 IIoT) 裝置通常會將遙測和預測性維護資訊直接傳輸到雲端。若要保護工作負載，就必須套用超出傳統邊界方法的安全控制項。

章節摘要

您的組織可透過聚焦於這些目標的業務成果，充分發揮 ZTA 的潛力，並強化雲端的安全狀態。務必使這類成果與特定的組織目標保持一致、根據獨特的業務要求量身制訂目標業務成果，以及定期評估有效性以推動持續的改善。

了解零信任原則

零信任架構 (ZTA) 奠基於構成其安全模型基礎的一系列核心原則。如果組織希望有效採用 ZTA 策略，就務必了解這些原則。本節會說明 ZTA 的核心原則。

驗證和身分驗證

驗證和身分驗證原則強調對所有類型的主體（包括使用者、機器和裝置）進行高強度識別和身份驗證的重要性。ZTA 要求在整個工作階段持續驗證身份和身份驗證狀態；理想狀態下，最好能針對每次請求執行。它不僅依賴傳統的網路位置或控制項運作。這包括實作現代高強度多重要素驗證 (MFA)，以及在身分驗證程序期間，評估額外的環境和背景資訊訊號。組織可採用此原則，協助確保以最完善的身份輸入資訊做出資源授權決策。

最低權限存取

最低權限的原則包含授予主體執行任務所需的最低存取層級。組織可採用最低權限存取原則，強制執行精細的存取控制，讓主體只能存取履行其角色和責任的必要資源。其中包括實作即時存取佈建、角色型存取控制項 (RBAC) 以及定期審查存取權限，以大幅減少受攻擊面積和未經授權存取的風險。

微分段

微分段是一種網路安全策略，會將網路分割成較小的隔離區段，以授權特定的流量流程。您可以建立工作負載界限，並在不同區段之間強制執行嚴格的存取控制，以達成微分段。

微分段可以透過網路虛擬化、軟體定義聯網 (SDN)、主機型防火牆、網路存取控制清單 (NACLs) 和 AWS 特定功能實作，例如 Amazon Elastic Compute Cloud (Amazon EC2) 安全群組或 AWS PrivateLink。分段閘道會控制區段之間的流量，以明確授予存取權限。微分段和分段閘道有助於組織限制網路中不必要的路徑，尤其是導向關鍵系統和資料的路徑。

持續監控和分析

持續監控和分析包含在組織環境中收集和分析與安全性相關的事件和資料，並且尋找關聯。您的組織能透過實作堅實的監視和分析工具，以融合的方式評估安全資料和遙測。

此原則強調掌握使用者行為、網路流量和系統活動的重要性，以辨識別異常和潛在的安全事件。安全資訊與事件管理 (SIEM)、使用者和實體行為分析 (UEBA)，以及威脅情報平台等進階技術，在達成持續監控和主動偵測威脅方面扮演要角。

自動化和協同運作

自動化和協同運作可協助組織簡化安全程序、減少人工干預，以及加強回應時間。透過自動執行例行的安全工作並使用協同運作功能，您的組織便能強制執行一致的安全政策，以及迅速回應安全事件。此原則也包括自動化存取佈建和取消佈建程序，以協助確保及時且準確地管理使用者權限。透過採用自動化和協同運作，您的組織便能提高營運效率、減少人為錯誤，同時將資源集中在更具策略性的安全措施上。

授權

在 ZTA 中，每項存取資源的請求都應由閘控強制執行點明確授權。除了驗證身分外，授權政策還必須考慮其他背景資訊，例如裝置健康狀態和安全狀態、行為模式、資源分類和網路因素。授權程序應根據與所存取資源相關的對應存取政策，來評估這項融合式背景資訊。最理想的情況下，機器學習模型可以為宣告式的政策提供動態補充。使用此類模型時，這些模型應僅聚焦於其他限制，且不應授予未明確指定的存取權限。

章節摘要

透過遵守 ZTA 的這些核心原則，組織便能建立符合現代企業環境多樣性的堅實安全模型。若要實作這些原則，必須採用結合技術、程序和人員的全方位方法，才能達成零信任思維，並建立具備恢復能力的安全狀態。

零信任架構的關鍵元件

若要有效地實作零信任架構 (ZTA) 策略，您的組織必須了解組成 ZTA 的關鍵元件。這些元件會共同運作，以便在符合零信任原則的全方位安全模型上持續改進。本節會說明 ZTA 的關鍵元件。

身分識別和存取管理

身分識別和存取管理提供堅實的使用者身分驗證和簡化的存取控制機制，構成 ZTA 的基礎。其中包括單一登入 (SSO)、多重要素驗證 (MFA) 以及身分治理和管理解決方案等技術。身分識別和存取管理會提供高等級的身分驗證保證和重要的背景資訊，這些項目是做出零信任授權決策時不可或缺的部分。同時，ZTA 是一種安全模型，會根據每位使用者、每部裝置和每個工作階段，授予應用程式和資源的存取權限。這有助於保護組織免受未經授權的存取，即便使用者的憑證洩漏亦然。

安全存取服務邊緣

安全存取服務邊緣 (SASE) 是新的網路安全方法，可將網路和安全功能虛擬化、互相結合並分派到以雲端為基礎的單一服務中。無論使用者身在何處，SASE 都能提供安全的應用程式和資源存取。

SASE 包括多種安全功能，例如安全網頁閘道、防火牆即服務，以及零信任網路存取 (ZTNA)。這些功能共同運作以保護組織免受各種威脅的侵害，其中包括惡意軟體、網路釣魚和勒索軟體。

資料外洩防護

資料外洩防護 (DLP) 技術可協助組織保護敏感資料，防止未經授權的披露。DLP 解決方案會監控和控制動態及靜態資料。這有助於組織定義政策並強制執行、預防資料相關的安全事件，以及確保敏感資訊在整個網路中都受到保護。

安全資訊和事件管理

安全資訊和事件管理 (SIEM) 解決方案會收集、彙總和分析來自組織基礎設施中各種來源的安全事件日誌。您可以使用此類資料偵測安全事件、促進事件回應，以及深入了解潛在威脅和漏洞。

對於 ZTA 而言，SIEM 解決方案能夠針對來自不同安全系統的相關遙測找出關聯並加以了解，對於改善偵測和回應異常模式的機制至關重要。

企業資源擁有權目錄

若要正確授予企業資源的存取權限，組織必須具備可靠的系統來分類這些資源，以及更重要的是，擁有這些資源的對象。這項事實來源必須提供工作流程，協助進行存取請求、相關核准決策以及其中的定期認證。隨著時間過去，這項事實來源就會包含「誰能存取哪些項目？」的答案，適用於組織內部。您可以將這些答案用於授權、稽核以及合規性。

統一端點管理

ZTA 除了對使用者進行高強度的身分驗證外，還必須考慮使用者裝置的健康狀態、安全狀態和情況，以便評估公司資料和資源存取是否安全。統一端點管理 (UEM) 平台提供下列功能：

- 裝置佈建
- 持續的組態和修補程式管理
- 安全性基準
- 遙測報告
- 裝置清潔和淘汰

以政策為基礎的強制執行點

在 ZTA 中，各項資源的存取權限應由以閘控政策為基礎的強制執行點明確授權。一開始，這類強制執行點可基於現有網路和身份系統中的現有強制執行點決定。只要將 ZTA 所提供更廣泛的背景資訊和訊號納入考量，便能讓強制執行點的功能逐漸增強。長期來看，您的組織應實作 ZTA 特定的強制執行點，以便在融合脈絡下運作、持續整合訊號提供者、維護全方位的政策集，以及透過結合遙測所收集的情報進行強化。

章節摘要

了解這些關鍵元件對於計劃採用 ZTA 的組織至關重要。透過實作這些元件並將它們整合到同一個緊密結合的安全模型中，您的組織便能根據零信任的原則建立強大的安全狀態。下列各節會探索組織準備程度、分階段採用方法以及最佳實務，協助您在組織內成功實作 ZTA。

評估組織對於採用零信任架構的準備程度

採用新的架構策略是極其重要的任務，因此必須進行仔細的規劃，並將組織因素皆納入考量。本節著重說明為整個企業採用零信任架構時的關鍵組織準備考量要素。處理這些考量要素後，您的組織便能做好準備，迎接更強大、更成功的安全狀態。

領導階層的共識和溝通

若要成功實作零信任架構，領導階層的共識和溝通不可或缺。領導階層必須了解零信任架構的優勢以及所需資源。領導者也必須願意改變組織的文化和程序。若要建立員工的信任並取得他們的贊同，請務必與員工溝通。員工需要了解組織實作零信任的理由、這項措施對他們的意義，以及他們能如何提供協助。溝通應該要保持開放、資訊透明且持續進行。

領導階層的支持和贊同

若要成功實作零信任架構 (ZTA)，請務必確保關鍵的利害關係人和高階主管在該架構的目標、優勢和成效衡量等方面達成共識。分享零信任原則對於強化安全性的重要性，以及若要捨棄傳統的邊界式安全措施，轉為使用更精細、以使用者為中心的方法來實現業務敏捷性，這些原則更是扮演要角。若改用這種方法，您的組織便能更迅速地適應變化和威脅。高階主管的共識會為組織建立基調，有助於克服阻擋變化的潛在阻力。

資訊透明的溝通

在實作零信任架構的過程中，請與員工維持開放且資訊透明的溝通。解釋採用該架構的理由、優勢和預期結果，並迅速解決疑慮。提供有關實作進度的定期更新資訊，這麼做能增加贊同的程度、減少阻力以及建立信任。

技能發展和培訓

在領導階層達成共識並且進行開放的溝通後，請務必協助即將實作零信任架構的員工發展相關技能和知識。其中包括了解零信任原則、如何在工作中實作這些原則，以及如何回應安全事件。請提供培訓和發展機會，協助員工掌握這些技能。

雲端知識和技能

評估組織在雲端技術和零信任原則方面的技能和知識缺口。提供培訓和發展計劃，以提高員工的技能並提供必要的專業知識，讓他們能在以雲端為中心的零信任環境中有效地工作。為了跟上不斷推陳出新的技術和安全實務，請培養持續學習的文化。

安全文化和意識

評估組織的安全文化。評估員工之間的安全意識程度、他們對安全最佳實務的理解，以及他們遵循政策和程序的程度。識別安全知識的任何缺口。不妨考慮進行安全意識培訓計劃，向員工說明零信任架構的重要性，以及他們在維護安全環境方面扮演的角色。

組織結構和角色

請建立有效的組織結構和角色，以便成功實作零信任架構。這包括建立雲端卓越中心 (CCoE)、檢閱和修改安全營運程序，以及針對漏洞管理、事件回應和安全監控等方面指派角色和相應的責任。

雲端卓越中心

建立 CCoE，為雲端營運提供指引、最佳實務和監督。CCoE 是由一個團隊或一組人員組成，負責建立和實作雲端相關的最佳實務、準則和治理政策。CCoE 應包括來自不同業務部門和 IT 團隊的代表，協助確保協作和共識。CCoE 在推動雲端託管工作負載採用零信任原則方面扮演要角。CCoE 也有利於整個組織的知識共享。

安全營運

若要符合零信任環境的需求，請檢閱並修改目前的安全營運組織。若要改善監控、事件回應和威脅情報功能，請考慮實作安全營運中心 (SOC) 或受管安全服務供應商 (MSSP)。針對漏洞管理、事件回應和安全監控建立角色和責任。若要確保能快速偵測輕微安全事件並加以修復，以便中斷一連串的事件，運作良好的事件回應程序至關重要。此程序有助於防止輕微事件發展成更具影響力的事件。

IT 基礎設施和架構

檢查公司的 IT 架構和基礎設施，找出可能會對採用零信任方法造成影響的任何限制或相依性。判斷目前的應用程式和系統是否與必要的零信任架構元件相容。分析是否需要針對基礎設施進行任何改善或調整，以協助成功部署零信任原則。請針對每個應用程式或系統考慮是否最適合實作零信任架構，還是應透過規模更大的現代化工作來進行實作。

風險管理、治理和變更控制

請建立有效的風險管理、治理和變更控制程序，以便成功實作零信任架構。這包括使風險管理與零信任原則保持一致、制定事件回應計劃、與法律和合規部門合作，以及建立變更控制程序。

風險管理

檢查在您公司實施的風險管理策略，並判斷該策略遵守零信任原則的程度。分析現行事件回應系統的效率、安全措施和風險評估程序。判斷哪些區域需要改進，以符合零信任策略。開始開發自動化事件回應系統或持續監控和分析架構，以提高解決速度。

變更控制程序

為了確保所有與雲端相關的修改都遵守安全和合規要求，請建立有效的變更控制方法。建立系統化的變更管理程序，其中包括安全組態分析、風險評估、核准和記錄。經常檢閱和稽核更新內容，以保持零信任架構的完整性。

監控和評估

若要成功實作零信任架構，您的組織必須持續監控並評估其安全狀態。這包括建立關鍵績效指標（KPI）、監控和評估 KPI，以及培養持續改善的文化。組織可以透過遵循這些步驟確保成功實作零信任架構，也確保他們持續致力於提高安全性。

關鍵績效指標

建立相關的關鍵績效指標 (KPI)，以評估零信任部署的成效和效能。這類 KPI 可能會衡量使用者滿意度、裝備和推出進度、降低的成本、合規可觀測性，以及安全事件的數量。為了追蹤整體發展並找出改善的機會，請定期監控和評估這些 KPI。

持續改善

建立系統以吸引利害關係人提出意見和洞察，藉此培養持續改善的文化。鼓勵員工提供想法和建議，以改善雲端環境的安全性、有效性和使用者體驗。使用這些資訊來簡化程序、改善安全措施以及加速創新。

章節摘要

您的組織可透過解決這些組織和文化考量要素，為採用零信任安全模型的雲端建立能提供支援的環境。下節會探討分階段採用的方法，提供指引來說明如何以實用且可管理的方式逐步實作零信任原則。

培養零信任思維

實作零信任不僅限於技術實作。它需要在組織內進行文化轉移。培養零信任思維需要強調下列關鍵層面。

零信任教育和訓練

教育員工零信任架構 (ZTA) 的價值和優勢。透過培訓課程、研討會和其他資源，提供 ZTA 概念和方法的技術和非技術性說明。鼓勵員工了解他們在建立和維護零信任安全範例方面的責任。

協作和通訊

促進參與 ZTA 實作的所有團隊和部門之間的協作和透明度。為了確保每個人都對計畫有徹底的了解，請促進跨部門的溝通、知識分享和資訊交換。建立共同責任的文化，其中每個人都體認到其對業務整體安全所做的貢獻的重要性。

持續學習和改進

在 Zero Trust 的內容中，優先考慮持續學習和改進。鼓勵員工掌握最新的安全趨勢、技術和最佳實務。培養創新和實驗的文化，鼓勵員工探索新的解決方案和方法，以強化組織的安全狀態。

指標和責任

建立明確的指標和責任機制，以衡量零信任策略的有效性。定義符合組織安全目標的關鍵績效指標 (KPIs)，並定期追蹤進度。讓個人和團隊對其對零信任原則的實作和維護的貢獻負責。

章節摘要

透過解決這些層面並培養零信任思維，組織可以為成功採用和實作零信任建立堅實的基礎。這種文化轉移對於協助組織中的每個人了解零信任的重要性，並積極為其成功做出貢獻至關重要。

下節會探討分階段採用的方法，提供指引來說明如何以實用且可管理的方式逐步實作零信任原則。

分階段採用零信任架構的方法

採用零信任架構 (ZTA) 需要進行仔細的規劃和實作。我們建議採用分階段採用方法以順利完成轉換，並將對業務營運的干擾降到最低。本節會針對採用 ZTA 包含的關鍵階段提供指引。

第 1 階段：評估和規劃

零信任實作的第一階段是評估和規劃。這個階段對於整體實作能否成功至關重要，因為此階段包含識別您組織目前安全狀態中的任何缺口，並加以解決。花時間評估目前的狀態並定義安全目標後，您便能為成功實作零信任架構奠定基礎。

同時，也不一定總是能獲得百分百完整且準確的評估結果。為了避免分析癱瘓導致您無法進行後續階段，請準備好透過區隔或其他方式，接受某種程度的不完美。

1. 評估目前的狀態 – 針對現有的安全基礎設施、政策和控制項進行評估。識別潛在漏洞、安全缺口，以及實作零信任原則後有助於改善的領域。
2. 定義安全目標 – 根據目前的狀態評估調查結果，定義符合零信任原則的安全目標。這些安全目標也應符合組織的整體安全策略，並解決已識別的漏洞和缺口。
3. 設計架構 – 開發有助於達成組織安全目標的 ZTA。此架構應包括必要的元件，例如身分識別和存取管理解決方案、網路分段機制，以及持續的監控系統。該架構也應具備可擴展性和適應性，並且能夠適應未來的成長和技術進展。理想情況下，此架構應該以負責實作該架構的團隊能輕易理解的格式來表示，例如 AWS CloudFormation 範本，而不只是文件或圖表。
4. 吸引利害關係人參與 – 納入業務單位、IT 團隊和安全團隊等所有利害關係人，以便取得洞察並使其目標與 ZTA 實作計劃保持一致。鼓勵進行協作和溝通，以便針對零信任方法的好處和要求建立共識。

第 2 階段：試行和實作

零信任實作的第二階段是試行和實作。這個階段包含在小規模且受到控制的環境中測試 ZTA，然後在整個組織中迭代部署。請務必向員工說明新的安全措施，以及他們在維護零信任環境中扮演的角色。

1. 試行部署 – 在小規模且受到控制的環境中測試 ZTA。實作架構設計階段所定義的必要元件和安全控制項。密切監控試行部署、收集意見回饋，並進行任何必要的調整。準備好在此過程的初期保持彈性，也就是當零信任架構從假設性演練轉變為您正在建置的實際體驗的時期。

2. 迭代部署 – 根據試行部署所汲取的經驗，開始在整個組織中迭代部署零信任架構。透過飛輪效應創造動力，無須透過廣泛的行銷活動即可達成關鍵的大規模部署。針對推出過程中較長尾的階段，保留可能需要的領導階層命令或上報機制。
3. 提供使用者培訓並提高意識 – 向員工說明新的安全措施，以及他們在維護零信任環境中扮演的角色。強調安全實務的重要性，例如高強度密碼、多重要素驗證以及定期的安全更新。
4. 管理變更 – 建立全方位的變更管理計劃，以便處理與採用零信任架構相關的組織和文化變更。向員工說明採用該架構的好處和理由，並解決任何疑慮或阻力。提供持續的支援和指引，促進順利轉換。

第 3 階段：監測和持續改善

零信任實作的第三和最終階段是監控和持續改進。這個階段包含建立全方位的監測和分析計劃、制定全面的事件回應計劃，以及定期徵求利害關係人和使用者的意見回饋。

1. 持續監控 – 建立全方位的監控和分析計劃，以持續評估安全狀態並偵測任何潛在的異常。使用進階安全工具和技術來監控使用者行為、網路流量和系統活動。
2. 規劃事件回應和修復 – 建立符合零信任原則的全方位事件回應計劃。建立明確的上報路徑、定義角色和責任，並在可能的情況下實作自動化事件回應機制。定期測試和更新事件回應計劃。
3. 取得意見回饋和評估 – 定期徵求利害關係人和使用者的意見回饋，以收集有關零信任架構 (ZTA) 有效性的洞察。進行定期評定和評估，以衡量對安全狀態、營運效率和使用者體驗的影響。使用意見回饋和評估結果來識別需要改善的領域。預期 ZTA 會隨著時間變化，並考慮開發團隊要如何以最少的努力或在盡量避免干擾的情況下，實作這些更新。

章節摘要

組織可以透過遵循這種分階段採用方法，有效地轉換到 ZTA，同時大幅降低風險和干擾。下節會討論透過零信任實作取得成功的最佳實務，範圍涵蓋高階主管、副總和資深經理的關鍵考量要素和建議。

透過零信任獲致成功的最佳實務

若要成功採用零信任架構 (ZTA)，就必須採用具策略性的方法並遵守最佳實務。本節會介紹一系列最佳實務，引導高階主管、副總和資深經理透過採用零信任獲致成功。您的組織可透過遵循這些建議，建立穩固的安全基礎，並實現零信任方法的好處：

- 定義明確的目標和業務成果 – 明確定義雲端營運的目標和期望的業務成果。將這些目標與零信任的原則保持一致，以建立堅實的安全基礎，同時促進業務成長和創新。
- 進行全面評估 – 針對目前的 IT 基礎設施、應用程式和資料資產執行全面的評估。識別相依性、技術負債和潛在的相容性問題。這項評估會為採用計劃提供資訊，並根據重要性、複雜性和業務影響來排定工作負載的優先順序。
- 制定採用計劃 – 整合詳細的採用計劃，概述將工作負載、應用程式和資料移至雲端的逐步方法。定義採用階段、時間表和相依性。吸引關鍵利害關係人參與其中，並據此分配資源。
- 儘早開始建置 - 只要您開始構建和部署零信任架構 (而不只是分析和談論該架構)，您就越來越能真實展現零信任架構在組織內的樣貌。
- 取得高階主管贊助 – 確保高階主管對於實作零信任架構的贊助和支持。吸引其他高階主管參與，以支持該計劃並分配必要資源。領導階層的承諾對於推動成功實作所需的文化和組織變更至關重要。
- 實作治理框架 – 建立治理框架，為零信任實作定義角色、責任和決策流程。清楚定義安全控制項、風險管理和合規的問責和擁有權。定期檢閱和更新治理框架，以適應持續演進的安全要求。
- 支援跨職能協作 – 鼓勵不同業務單位、IT 團隊和安全團隊之間進行協作和溝通。建立共同責任的文化，促進整個零信任實作程序的一致性和協作。鼓勵頻繁互動、共享知識以及共同解決問題。
- 保護資料和應用程式 – 零信任不僅關於最終使用者存取資源和應用程式的行為；零信任原則也應在工作負載內部和工作負載之間實作。也請一併使用資料中心內所有可用的背景資訊，以便套用相同的技術原則 (高強度身分識別、微分段和授權)。
- 提供深度防禦 – 使用多層安全控制項來實作深度防禦策略。結合多重要素驗證 (MFA)、網路分段、加密和異常偵測等各種安全技術，提供全方位的保護。確保每一層都與其他層相輔相成，以建立強大的防禦系統。
- 需要高強度的身分驗證 – 針對存取所有資源的所有使用者，強制執行 MFA 等高強度的身分驗證機制。理想情況下，請考慮 FIDO2 硬體支援的安全密鑰等現代化 MFA，它能為零信任架構提供高層級的身份驗證保證，且具備各種安全優點（例如，防止網路釣魚）。
- 集中並改善授權 – 特別是在每次嘗試存取時進行授權。根據協議的細節，這應該根據每次連線或每個請求執行。根據每個請求執行最為理想。使用身分識別、裝置、行為和網路資訊等所有可用的背景資訊，進行更精細、具適應性且完善的授權決策。

- 使用最低權限原則 – 實作最低權限原則，授予使用者執行其工作職責所需的最低存取權限。根據工作角色、責任和業務需求，定期檢閱和更新存取權限。實作即時存取佈建。
- 使用特權存取管理 – 實作特權存取管理 (PAM) 解決方案，以保護特權帳戶的安全，以及降低未經授權存取關鍵系統的風險。PAM 解決方案可提供特權存取控制項、工作階段記錄和稽核功能，協助您的組織保護最敏感的資料和系統。
- 使用微分段 – 將網路分割成更小、隔離程度越高的區段。使用微分段功能，根據使用者角色、應用程式或資料敏感度，在區段之間強制執行嚴格的存取控制。努力清除所有不必要的網路路徑，特別是導向資料的路徑。
- 監控和回應安全警告 – 在雲端環境中實作全方位的安全監控和事件回應計劃。使用雲端原生安全工具和服務，即時偵測威脅、分析日誌，以及自動化事件回應。建立清楚的事件回應程序、定期執行安全評估，以及持續監控異常或可疑活動。
- 使用持續監控功能 – 若要快速有效地偵測和回應安全事件，請實作持續監控功能。使用進階安全分析工具來監控使用者行為、網路流量和系統活動。自動進行警告和通知，確保人員能即時回應事件。
- 推動安全和合規文化 – 在整個組織中推動安全和合規的文化。向員工說明安全最佳實務、遵守零信任原則的重要性，以及員工在維護安全雲端環境中所扮演的角色。定期進行安全意識培訓，協助確保員工對社交工程保持警惕，並且了解自己在資料保護和隱私權方面的責任。
- 使用社交工程模擬 – 進行社交工程模擬，以評估使用者對社交工程攻擊的敏感度。使用模擬結果來量身打造培訓計劃，以提高使用者的意識並改善對潛在威脅的因應方式。
- 推動持續教育 – 提供持續的安全培訓和資源，建立持續教育和學習的文化。讓使用者瞭解不斷推陳出新的安全最佳實務。鼓勵使用者保持警惕，以及迅速舉報任何可疑活動。
- 持續評估和最佳化 – 定期評估雲端環境以了解需要改善的領域。使用雲端原生工具監控資源用量和效能，並進行漏洞評估和滲透測試，以識別並解決任何弱點。
- 建立治理和合規性框架 – 制定治理和合規框架，協助確保您的組織符合業界標準和法規要求。在框架中定義政策、程序和控制項，以保護資料和系統免受未經授權的存取、使用、披露、干擾、修改或破壞。實作追蹤和回報合規指標的機制、定期進行稽核，以及迅速解決任何不合規的問題。
- 鼓勵合作和知識共享 – 鼓勵參與 ZTA 採用的團隊之間進行協作和知識共享。若要達成此目的，您可以促進 IT、安全性和業務單位之間的跨職能溝通和協作。您的組織也可以建立論壇、工作坊和知識分享會議，以促進理解、解決挑戰，並分享在整個採用過程中學到的經驗。

關鍵要點

本指南探討了制定成功零信任架構 (ZTA) 策略的重要層面。本節從會已呈現的規範性指引摘錄出關鍵要點：

- 了解零信任原則 – 零信任是一組概念模型和一系列相關聯的機制，著重於為數位資產提供安全控制項，且這些機制並非僅根據傳統的網路控制項或網路邊界運作，或完全不基於此類措施運作。而是透過身分識別、裝置、行為和其他豐富的背景資訊和訊號來增強網路控制，以做出更精細、更有智慧、更具適應性且持續的存取決策。熟悉零信任的核心原則，例如最低權限、微分段、持續的身分驗證以及適應性授權。
- 定義明確的目標 – 明確定義採用 ZTA 的目標和期望的業務成果。將這些目標與零信任的原則保持一致，協助確保穩固的安全基礎，同時促進業務成長和創新。
- 進行全面評估 – 對現有的 IT 基礎設施、應用程式和資料資產執行徹底的評估。識別相依性、技術負債和相容性問題，為您的採用策略提供參考資訊。
- 制定 ZTA 採用計劃 – 建立詳細計劃，列出逐步將工作負載、應用程式和資料移至雲端的方法。考慮合規需求和應用程式現代化等因素。
- 實作堅實的 ZTA – 設計並實作 ZTA，強制執行精細的存取控制項、高強度身分驗證機制以及持續監控。若要更有效率地採用 ZTA，請使用雲端原生零信任服務，例如 AWS Verified Access 和 Amazon VPC Lattice。
- 排定資料和應用程式安全性的優先順序 – 套用零信任原則 (高強度身分識別、微分段和授權)，以提供所有可用的背景資訊。將此背景資訊用於存取系統和資源的使用者，以及後端元件內部和之間的通訊和資料流程。
- 建立監控和事件回應框架 – 在雲端環境中實作堅實的安全監控和事件回應功能。使用雲端原生安全工具進行即時威脅偵測、日誌分析和事件回應自動化，例如 Amazon Inspector AWS Security Hub和 Amazon GuardDuty。
- 培養安全和合規的文化 – 在整個組織中推動安全意識和合規的文化。向員工說明安全最佳實務，以及他們在維護安全雲端環境中扮演的角色。
- 持續評估和最佳化 – 定期評估雲端環境、安全控制項和營運流程。若要收集洞察並針對資源使用率、成本管理和效能進行最佳化，請使用 Amazon CloudWatch 和 AWS Security Hub等雲端原生的分析和監控工具。
- 建立治理和合規框架 – 制定符合業界標準和法規要求的治理和合規框架。定義政策、程序和控制項，以協助確保遵守安全性、隱私權和合規性標準。

後續步驟

採用零信任架構 (ZTA) 是其中一項改善組織安全狀態並降低風險的最安全方法。本規範性指引為您提供實作零信任的全方位藍圖，包括了解原則、評估準備程度，以及實作必要元件。

此工作串流或網域中的後續步驟包含以下項目：

- 實作採用計劃
- 實作 ZTA
- 定期進行安全評估
- 持續最佳化雲端環境和安全控制項

ZTA 是一個持續進行的過程，需要持續的監控、評估和適應，以確保穩固的安全基礎。透過遵循本指南中概述的最佳實務，您的組織便能強化安全狀態、確保遵守法規，以及保護敏感資料。

常見問答集

本節提供有關設計和實作零信任架構 (ZTA) 的常見問題解答。

什麼是零信任？

零信任是一組概念模型和一系列相關聯的機制，著重於為數位資產提供安全控制項，且這些機制並非僅根據傳統的網路控制項或網路邊界運作，或完全不基於此類措施運作。而是透過身分識別、裝置、行為和其他豐富的背景資訊和訊號來增強網路控制，以做出更精細、更有智慧、更具適應性且持續的存取決策。

什麼 AWS 服務 可以協助我實作零信任架構？

AWS 提供多項服務，可協助實作零信任，例如 AWS Identity and Access Management (IAM) AWS Verified Access、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway 和 Amazon GuardDuty。

我如何透過 AWS確保資料安全？

AWS 提供靜態和傳輸中資料加密的 AWS Key Management Service (AWS KMS)、網路隔離的 Amazon Virtual Private Cloud (Amazon VPC)，以及憑證 AWS Secrets Manager 的安全儲存和擷取等服務。

在零信任環境中， 可以 AWS 協助滿足合規要求嗎？

是， AWS 具有合規計劃和服務，可協助滿足各種法規要求。 AWS Artifact 提供 AWS 合規報告的存取權，並 AWS Config 支援持續監控和評估合規。

是否有任何 AWS 工具或服務可在零信任環境中自動化安全性？

AWS 提供 等服務 AWS Security Hub，可集中和自動化安全調查結果，以及定義和強制執行安全政策的 AWS Config 規則。

如何透過 確保在零信任雲端環境中持續監控和回應事件 AWS

AWS 提供 Amazon CloudWatch 等服務，以進行即時監控和 AWS CloudTrail 記錄和分析。如果需要事件回應的最佳實務，可以參考 AWS 《安全事件回應指南》。

資源

參考

- 什麼是卓越雲端中心？您的組織為什麼必須建立該中心？ – 此部落格文章概述了 CCoE 以及如何建立有效 CCoE 的最佳實務等內容。
- 零信任 AWS- 此頁面提供 AWS 環境中零信任安全原則和最佳實務的概觀。
- 零信任架構： AWS 觀點 – 此部落格文章分享零信任實作方式的定義和指導原則 AWS。
- AWS Identity and Access Management (IAM) 使用者指南 – 本指南提供在零信任架構的關鍵元件 IAM 中管理使用者存取和許可的完整文件。
- AWS Security Hub – 了解 Security Hub，這項服務可讓您全面檢視整個 的安全提醒和合規狀態 AWS 帳戶。
- AWS Well-Architected Framework – 探索 Well-Architected Framework，該框架可針對在 AWS上建置安全、高效能、具恢復能力且有效率的架構提供指引。
- AWS 安全事件回應指南 – 本指南概述了回應組織 AWS 雲端 環境中安全事件的基本原則。它概述了雲端安全性和事件回應的概念，以及識別要回應安全問題的客戶可使用的雲端功能、服務和機制。

工具

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- AWS Verified Access

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
新增的更新	已新增資訊至「零信任架構的關鍵元件」一節、在「評估組織採用零信任的準備程度」一節中進行變更、已新增資訊至「最佳實務」一節，以及對「常見問答集」進行變更。	2023 年 12 月 4 日
初次出版	—	2023 年 6 月 19 日

AWS 規範性指導詞彙表

以下是 AWS Prescriptive Guidance 所提供策略、指南和模式的常用術語。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 Oracle 的 Amazon Relational Database Service (Amazon RDS) 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：將內部部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子、一致性、隔離、耐久性。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但需要比主動-被動遷移更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。目標資料庫在遷移期間不接受任何交易。

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，其解決方案具有反效益、無效或效果不如替代方案。

應用程式控制

一種安全方法，允許只使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是產品組合探索和分析程序的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱什麼是人工智慧？

人工智慧操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何在 AWS 遷移策略中使用 AIOps 的詳細資訊，請參閱操作整合指南。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性、一致性、隔離性、耐久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱 AWS Identity and Access Management (IAM) 文件中的 ABAC for AWS。

授權資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將資料從授權資料來源複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

在 內的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並對相同區域中的其他可用區域提供價格低廉的低延遲網路連線。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定有效率且有效的計劃，以成功移至雲端。 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。在此角度上， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織準備好成功採用雲端。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

評估資料庫遷移工作負載、建議遷移策略並提供工作預估的工具。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的行為圖中的資料。

大端序系統

首先儲存最高有效位元組的系統。另請參閱結尾。

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。有些機器人很有用或很有幫助，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。某些其他機器人稱為不良機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到惡意軟體感染且受單一方控制之機器人的網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱關於分支 (GitHub 文件)。

碎片存取

在特殊情況下，以及透過核准的程序，使用者快速存取 AWS 帳戶 他們通常沒有存取許可的 。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作碎片程序指標。

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

版本向最終使用者緩慢且遞增的版本。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。

混亂工程

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) 來執行實驗，以強調 AWS 工作負載並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

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營運模型。

採用雲端階段

組織在遷移到 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 在部落格文章中定義：企業策略部落格上的邁向雲端優先之旅和採用階段。 AWS 雲端 如需有關它們與 AWS 遷移策略之關聯的資訊，請參閱遷移準備指南。

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

很少存取且通常為歷史資料的資料。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???，使用機器學習來分析和擷取數位影像和影片等視覺化格式的資訊。例如， AWS Panorama 提供將 CV 新增至內部部署攝影機網路的裝置，而 Amazon SageMaker AI 則提供 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 區域中或整個組織中的單一實體。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

架構架構架構，提供分散式、分散式的資料擁有權，並具有集中式的管理。

資料最小化

僅收集和處理嚴格必要資料的原則。在 中實作資料最小化 AWS 雲端 可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性防護機制，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個生命週期中追蹤資料的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。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱環境。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS上實作安全控制中的偵測性控制。

開發值串流映射 (DVSM)

一種程序，用於識別並排定限制條件的優先順序，這些限制條件會對軟體開發生命週期中的速度和品質產生負面影響。DVSM 延伸了原本專為精實生產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

在星狀結構描述中，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，其行為與文字相似。這些屬性通常用於查詢限制、篩選和結果集標籤。

災難

防止工作負載或系統在其主要部署位置中實現其業務目標的事件。這些事件可能是自然災難、技術故障或人類動作的結果，例如意外的錯誤組態或惡意軟體攻擊。

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

請參閱資料庫操作語言。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

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 來偵測系統資源的偏離，或者您可以使用 AWS Control Tower 來偵測登陸區域中可能會影響對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縮短回應時間。

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

將純文字資料轉換為人類可讀取的運算程序。

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)

可自動化和管理企業關鍵業務流程 （ 例如會計、MES 和專案管理 ） 的系統。

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 安全性特徵包括身分和存取管理、偵測控制、基礎設施安全性、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：包含量值的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

使用頻繁且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，請參閱使用機器學習模型解譯能力 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。對於需要特定格式設定、推理或網域知識的任務，少數擷取提示非常有效。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，以及以自然語言進行交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可以使用簡單的文字提示來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，而以中繼線為基礎的工作流程是現代、偏好的方法。

金色影像

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、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

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

高可用性 (HA)

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 系統設計為自動容錯移轉、持續提供高品質效能，以及處理不同的負載和故障，且效能影響最小。

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，用於從工廠的各種來源收集和存放資料。

保留資料

從資料集保留的歷史標籤資料的一部分，用於訓練機器學習模型。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如，Microsoft SQL Server 至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱資料

經常存取的資料，例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別，才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性，通常會在典型 DevOps 發行工作流程之外執行修補程式。

超級護理期間

在切換後，遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常，此期間的長度為 1-4 天。在超級護理期間結束時，遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

I

IaC

將基礎設施視為程式碼。

身分型政策

連接至一或多個 IAM 主體的政策，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱工業物聯網。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有基礎設施。與可變基礎設施相比，不可避免的基礎設施本質上更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的使用不可變基礎設施的部署最佳實務。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

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

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

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

工業物聯網 (IIoT)

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

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC，可管理 VPCs （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，請參閱使用機器學習模型解譯能力 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 資訊程式庫。

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、彙整文件、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。另請參閱結尾。

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 可 AWS 操作基礎設施層、作業系統和平台，而且您可以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，將原物料轉換為工廠的成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是一種循環，可在操作時強化和改善自身。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，所有 都是 AWS Organizations。一個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)

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遷移至雲端，並協助抵銷遷移初始成本的 AWS 計劃。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

將工作負載遷移到 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 中的應用程式現代化策略 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 - Unified Architecture。

開放程序通訊 - Unified Architecture (OPC-UA)

工業自動化的machine-to-machine(M2M) 通訊協定。OPC-UA 提供與資料加密、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)。

操作準備度審查 (ORR)

問題及相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作就緒審核 (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 建立的追蹤 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱 CloudTrail 文件中的建立組織追蹤。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

CloudFront 中的增強型選項，用於限制存取以保護 Amazon Simple Storage Service (Amazon S3) 內容。OAC 支援使用 S3 AWS KMS (SSE-KMS) 的所有伺服器端加密中的所有 S3 儲存貯體 AWS 區域，以及對 S3 儲存貯體的動態PUT和DELETE請求。

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作準備度檢閱。

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（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的物件 AWS Organizations（請參閱服務控制政策）。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則

可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱在微服務中啟用資料持久性。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱評估遷移準備程度。

述詞

傳回 `true`或 的查詢條件`false`，通常位於 `WHERE` 子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並提升查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS上實作安全控制中的預防性控制。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中角色術語和概念中的主體。

依設計的隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。如需詳細資訊，請參閱 Route 53 文件中的使用私有託管區域。

主動控制

旨在防止部署不合規資源的安全控制。這些控制項會在佈建資源之前對其進行掃描。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的控制項參考指南，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

從設計、開發和啟動到成長和成熟，再到拒絕和移除，產品整個生命週期的資料和程序管理。

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

使用一個 LLM 提示的輸出做為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

一種模式，可讓微型服務之間的非同步通訊改善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以訂閱的頻道。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、知情 (RACI)。

RAG

請參閱擷取增強型產生。

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、知情 (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)

服務中斷和服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

地理區域中的 AWS 資源集合。每個 AWS 區域 都獨立於其他 ，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用哪些。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 7 個 R。

replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

應用程式抵抗中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

定義所有涉及遷移活動和雲端操作之各方的角色和責任的矩陣。矩陣名稱衍生自矩陣中定義的責任類型：負責人 (R)、責任 (A)、已諮詢 (C) 和知情 (I)。支援 (S) 類型為選用。如果您包含支援，則矩陣稱為 RASCI 矩陣，如果您排除它，則稱為 RACI 矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS上實作安全控制中的回應性控制。

保留

請參閱 7 個 R。

淘汰

請參閱 7 個 R。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的權威資料來源。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 Management Console 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。它由秘密值及其中繼資料組成。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 Secrets Manager 文件中的 Secrets Manager 秘密中的內容？。

依設計的安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：預防性、偵測性、回應性和主動性。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生提醒。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為偵測或回應式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換憑證。

伺服器端加密

由接收資料的 AWS 服務 加密其目的地的資料。

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

一種模型，描述您與 共同 AWS 承擔的雲端安全與合規責任。 AWS 負責雲端的安全，而您則負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件中的故障，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

提供內容、指示或指導方針給 LLM 以指示其行為的技術。系統提示可協助設定內容，並建立與使用者互動的規則。

T

標籤

做為中繼資料的鍵值對，用於組織您的 AWS 資源。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱環境。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可以用於互連 VPC 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的什麼是傳輸閘道。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中執行任務 AWS Organizations ，並在其帳戶中執行任務。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 將 與其他 AWS 服務 AWS Organizations 搭配使用。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

兩個比薩就能吃飽的小型 DevOps 團隊。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱量化深度學習系統的不確定性指南。

未區分的任務

也稱為繁重，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

會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，在與目前記錄在某種程度上相關的資料列群組上執行計算。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

零時差漏洞

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。另請參閱微拍提示。

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。