在 上實作機器人控制策略 AWS

AWS 方案指引

AWS 方案指引: 在 上實作機器人控制策略 AWS

Table of Contents

實作機器人控制策略 AWS

Amazon Web Services（貢獻者）

2024 年 2 月 (文件歷史記錄)

我們所知，如果沒有機器人，互聯網是不可能的。機器人在互聯網上運行自動化任務，並模擬人類活動或互動。它們使企業能夠為流程和任務提高效率。有用的漫遊器，例如網絡爬蟲，互聯網上的索引信息，並幫助我們快速找到與我們的搜索查詢最相關的信息。機器人是改善業務並為公司提供價值的良好機制。但是，隨著時間的推移，不良行為者開始使用機器人作為以新的創造性方式濫用現有系統和應用程序的手段。

殭屍網絡是擴展機器人及其影響的最著名機制。殭屍網絡是受惡意軟件感染的機器人網絡，並由單一方（稱為機器人牧民者或機器人操作員）的控制。從一個中心點開始，操作員可以命令殭屍網絡上的每台計算機同時執行協調操作，這就是為什麼殭屍網絡也被稱為 command-and-control（C2）系統的原因。

殭屍網絡的規模可以是數以百萬計的機器人。殭屍網絡可幫助運營商執行大規模操作。由於殭屍網絡仍然由遠程操作員控制，因此受感染的計算機可以接收更新並即時更改其行為。因此，為了獲得顯著的財務收益，C2 系統可以在黑市上租用對其殭屍網絡細分市場的訪問權限。

殭屍網絡的流行率持續增長。專家認為它是壞演員最喜歡的工具。未來是最大的殭屍網絡之一。它於 2016 年出現，仍在運行，估計已經感染了 35 萬個物聯網（IoT）設備。該殭屍網絡已被改編並用於許多類型的活動，包括分佈式拒絕服務（DDoS）攻擊。最近，不良行為者試圖通過使用住宅代理服務獲取 IP 地址來進一步混淆他們的活動並獲取流量。這將創建一個合法的相互連接的 peer-to-peer 系統，該系統可以增加活動的複雜性，並使其更具挑戰性的檢測和緩解。

本文件著重於機器人環境、其對應用程式的影響，以及可用的策略和緩解選項。此規範指引及其最佳做法可協助您瞭解並減輕不同類型的機器人攻擊。此外，本指南還說明支援機器人緩解策略的 AWS 服務和功能，以及每種策略如何協助您保護應用程式。其中也包含機器人監控的概觀，以及最佳化解決方案成本的最佳做法。

了解機器人威脅和操作

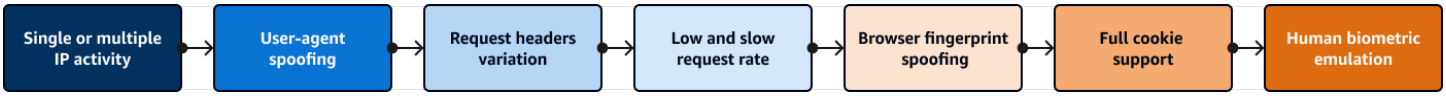
根據 Security Today，網際網路上超過 47% 的流量是由機器人所造成。這包括機器人的實用部分，也就是可自我識別並提供價值的部分。大約 30% 的機器人流量是執行惡意活動的無法識別機器人，例如 DDoS 攻擊、票證清理、庫存湊集或碎片。Securitymaster 報告 2023 年上半年容積 DDoS 事件增加 300%。這使得此主題更具相關性，而且更重要的是了解可用的預防性和保護性工具和技術。

下表會分類不同類型的機器人活動，以及每個機器人活動對業務的影響。這並非廣泛清單，而是最常見的機器人活動的摘要。它強調了監控和緩解控制的重要性。如需機器人威脅的廣泛清單，請造訪 OWASP 自動化應用程式威脅手冊 (OWASP 網站）。

機器人活動類型	Description	潛在影響
內容抓取	複製專屬內容供第三方網站使用	由於內容重複、品牌影響和攻擊性抓取器造成的效能問題，對您的 SEO 造成的影響
登入資料填充	測試您網站中遭竊的登入資料資料庫，以取得存取權或驗證資訊	使用者的問題，例如詐騙和帳戶鎖定，可增加支援查詢並降低品牌信任
卡片破解	測試遭竊信用卡資料的資料庫，以驗證或補充遺漏的資訊	使用者的問題，例如身分盜竊和詐騙，以及詐騙分數受損
拒絕服務	增加特定網站的流量，以減慢回應速度或使其無法供合法流量使用	收入損失和聲譽受損
帳戶建立	建立多個以濫用或財務收益為目的的帳戶	阻礙成長和行銷分析扭曲
擴展	取得有限的可用商品、經常門票，而不是真正的消費者	使用者的收入損失和問題，例如無法存取正在銷售的貨物

殭屍網路的運作方式

殭屍網路運算子的策略、技術和程序 (TTP) 已隨著時間大幅演進。他們必須跟上公司開發的偵測和緩解技術。下圖顯示此演變。殭屍網路從使用 IP 地址作為操作方式開始，最終發展為使用複雜的人類生物識別模擬。這種複雜性非常昂貴，而且並非所有殭屍網路都使用最先進的工具。網際網路中混合了運算子，他們可能會評估任務的最佳工具，以提供良好的投資回報。機器人防禦的一個目標是讓殭屍網路活動昂貴，讓目標不再可行。



一般而言，機器人會分類為常見或目標：

- 常見機器人 – 這些機器人會自我識別，不會嘗試模擬瀏覽器。其中許多機器人會執行有用的任務，例如內容爬取、搜尋引擎最佳化 (SEO) 或彙總。請務必識別並了解哪些常見機器人會進入您的網站，以及它們對您的流量和效能的影響。
- 目標機器人 – 這些機器人嘗試透過模擬瀏覽器來逃避偵測。他們使用瀏覽器技術，例如無頭瀏覽器，或是仿造瀏覽器指紋。他們能夠執行 JavaScript 並支援 Cookie。他們的意圖並不總是明確的，他們產生的流量可能看起來像正常的使用者流量。

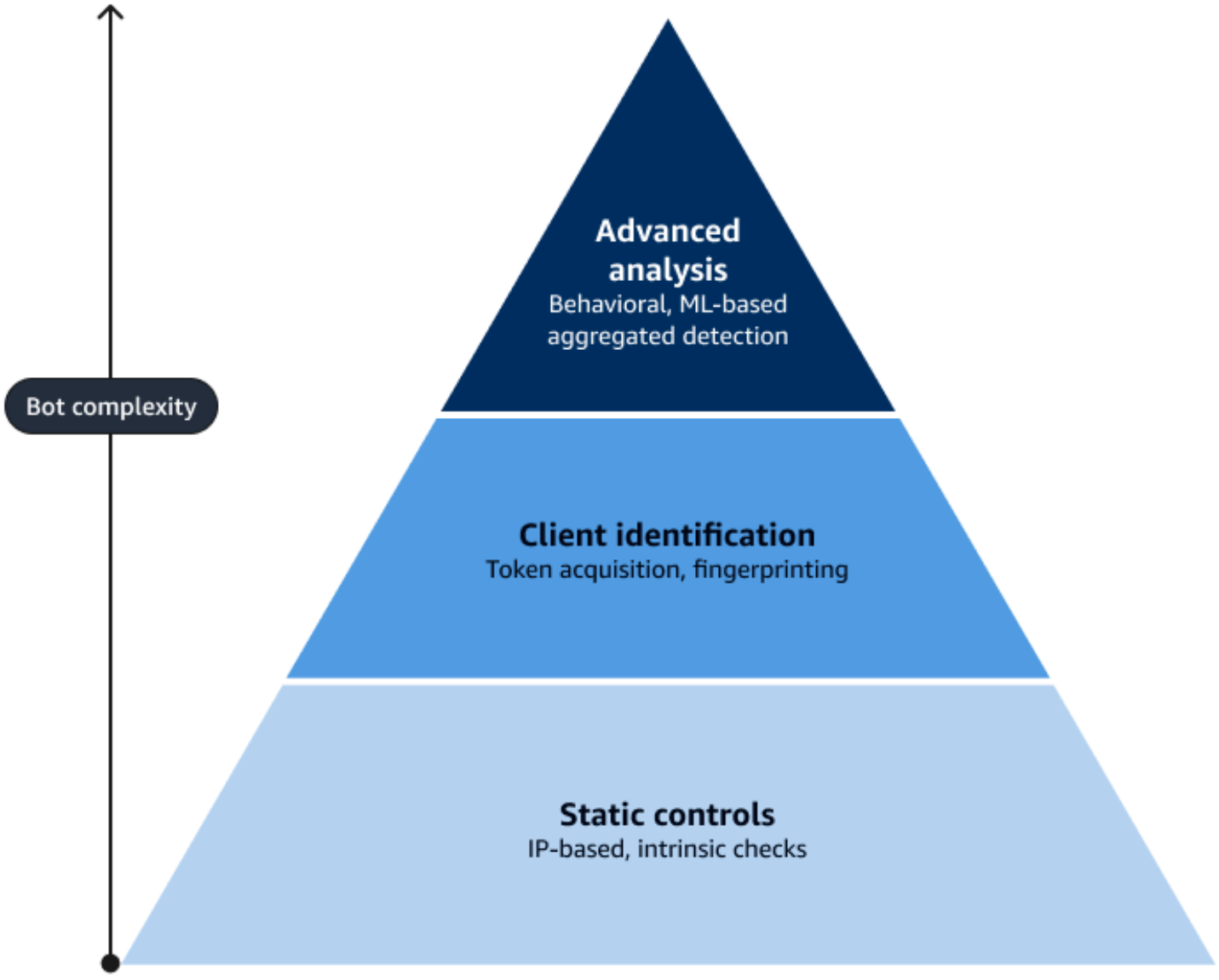
最先進且持久的目標機器人透過產生類似人類的滑鼠動作並在網站上按一下來模擬人類行為。它們是最複雜且難以偵測的，但也是最昂貴的操作。

通常，運算子會結合這些技術。這會建立持續追求的遊戲，您必須經常變更保護和緩解方法，以適應運算子的最新技術。這些機器人被視為進階持久性威脅 (APT)。如需詳細資訊，請參閱 NIST 資源中心的進階持久性威脅。

機器人控制的技巧

機器人緩解的主要目標是限制自動化機器人活動對組織網站、服務和應用程式的負面影響。使用的技術和技術取決於您要防禦的流量或活動類型。了解應用程式及其流量是達成此目標的關鍵。如需從何處開始的詳細資訊，請參閱本指南中的監控機器人控制策略的準則一節。

一般而言，機器人緩解解決方案提供的控制項可以分為下列高階類別：靜態、用戶端識別和進階分析。下圖顯示可用的不同技術，以及根據機器人活動複雜性如何使用這些技術。這強調了如何透過使用靜態控制項取得基礎或最廣泛的緩解措施，例如允許列出和內部檢查。機器人的最小部分始終是最進階的部分，而針對這些機器人的緩解需要更進階的技術和控制組合。



接下來，本指南會探索每個類別及其技術。它還描述了 中可用於AWS WAF實作這些控制項的選項：

管理機器人的靜態控制

若要採取動作，靜態控制項會評估來自 HTTP(S) 請求的靜態資訊，例如其 IP 地址或其標頭。這些控制對於低複雜度的不良機器人活動或需要驗證和管理的預期有益機器人流量非常有用。靜態控制技術包括：允許列出、以 IP 為基礎的控制和內部檢查。

允許列出

允許列出是允許透過現有機器人緩解控制識別的易記流量的控制項。有各種方式可以達成此目標。最簡單的是使用符合一組 IP 地址或類似相符條件的規則。當請求符合設定為 `Allow`動作的規則時，後續規則不會評估該請求。在某些情況下，您只需要防止某些規則受到處理；換句話說，您需要允許一個規則的清單，但並非所有規則。這是處理規則誤報的常見案例。允許清單視為廣範圍規則。為了降低誤報的可能性，建議您將其與另一個更精細的選項配對，例如路徑或標頭比對。

IP 型控制

單一 IP 地址區塊

緩解機器人影響的常用工具是限制來自單一請求者的請求。最簡單的範例是，如果流量的請求是惡意或大量，則封鎖流量的來源 IP 地址。這會使用 AWS WAF IP 集比對規則來實作 IP 型區塊。這些規則符合 IP 地址，並套用 `Block`、 `Challenge`或 的動作CAPTCHA。您可以透過查看內容交付網路 (CDN)、Web 應用程式防火牆或應用程式和服務日誌，來判斷來自 IP 地址的請求是否太多。不過，在大多數情況下，如果沒有自動化，此控制是不切實際的。

在 中自動化 IP 地址區塊清單 AWS WAF 通常使用以速率為基礎的規則來完成。如需詳細資訊，請參閱本指南中的 速率為基礎的規則。您也可以實作 解決方案的安全自動化 AWS WAF。此解決方案會自動更新要封鎖的 IP 地址清單，且 AWS WAF 規則會拒絕符合這些 IP 地址的請求。

識別機器人攻擊的一種方法是，如果來自相同 IP 地址的大量請求專注於少量網頁。這表示機器人正在淘汰價格，或重複嘗試以高百分比失敗的登入。您可以建立可立即辨識此模式的自動化。自動化會封鎖 IP 地址，透過快速識別和緩解來降低攻擊的有效性。當攻擊者擁有大量 IP 地址來啟動攻擊，或攻擊行為難以辨識並與正常流量分開時，封鎖特定 IP 地址會較不有效。

IP 地址評價

IP 評價服務提供的智慧有助於評估 IP 地址的可信度。此智慧通常衍生自從該 IP 地址彙總過去活動的 IP 相關資訊。先前的活動有助於指出 IP 地址產生惡意請求的可能性。資料會新增至追蹤 IP 地址行為的受管清單。

匿名 IP 地址是 IP 地址評價的特殊案例。來源 IP 地址來自易取得 IP 地址的已知來源，例如雲端虛擬機器，或來自代理，例如已知 VPN 提供者或 Tor 節點。 AWS WAF Amazon IP 評價清單和匿名 IP 清單受管規則群組會使用 Amazon 內部威脅情報來協助識別這些 IP 地址。

這些受管清單提供的智慧可協助您對從這些來源識別的活動採取行動。根據此智慧，您可以建立直接封鎖流量的規則，或限制請求數量的規則（例如以速率為基礎的規則）。您也可以使用此智慧，在 COUNT 模式中使用規則來評估流量的來源。這會檢查比對條件，並套用可用來建立自訂規則的標籤。

速率為基礎的規則

對於某些案例而言，以速率為基礎的規則可能是寶貴的工具。例如，與敏感統一資源識別符 (URIs) 中的使用者相比，當機器人流量達到高磁碟區，或流量開始影響正常操作時，速率型規則是有效的。速率限制可將請求保持在可管理層級，並限制和控制存取。 AWS WAF 可以使用以速率為基礎的規則陳述式，在 Web 存取控制清單 (Web ACL) 中實作速率限制規則。 https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html使用速率型規則的建議方法是包含涵蓋整個網站、URI 特定規則和 IP 評價型規則的括住規則。IP 評價率型規則結合了 IP 地址評價的智慧與速率限制功能。

對於整個網站，以空白 IP 評價率為基礎的規則會建立上限，以防止不複雜的機器人從少量 IPs 淹沒網站。特別建議將速率限制用於保護具有高成本或影響URIs，例如登入或帳戶建立頁面。

速率限制規則可提供具成本效益的第一層防禦。您可以使用更進階的規則來保護敏感URIs。URI 特定速率型規則可以限制對關鍵頁面或影響後端APIs 的影響，例如資料庫存取。保護本指南稍後討論的特定 URIs的進階緩解措施通常會產生額外費用，而這些 URI 特定速率型規則可協助您控制成本。如需常用建議速率型規則的詳細資訊，請參閱 安全部落格中的三個最重要的 AWS WAF 速率型規則。 AWS 在某些情況下，限制以速率為基礎的規則評估的請求類型會很有用。您可以使用縮小範圍陳述式，例如，依來源 IP 地址的地理區域限制以速率為基礎的規則。

AWS WAF 透過使用彙總金鑰為以速率為基礎的規則提供進階功能。透過此功能，您可以設定速率型規則，以使用來源 IP 地址以外的各種其他彙總金鑰和金鑰組合。例如，作為單一組合，您可以根據轉送的 IP 地址、HTTP 方法和查詢引數彙總請求。這可協助您為複雜的容積流量緩解設定更精細的規則。

內部檢查

內部檢查是系統或程序內各種類型的內部或固有驗證或驗證。對於機器人控制， AWS WAF 驗證請求中傳送的資訊是否符合系統訊號，以執行內部檢查。例如，它會執行反向 DNS 查詢和其他系統驗證。有些自動化請求是必要的，例如 SEO 相關請求。允許列出是允許良好、預期的機器人通過的方法。但有時候，惡意機器人會模擬良好的機器人，而將它們分開可能很困難。 AWS WAF 提供透過受管AWS WAF 機器人控制規則群組達成此目標的方法。此群組中的規則可驗證自我識別的機器人是他們所說的身分。 會根據該機器人的已知模式 AWS WAF 檢查請求的詳細資訊，也會執行反向 DNS 查詢和其他目標驗證。

用於管理機器人的用戶端識別控制項

如果無法透過靜態屬性輕鬆識別與攻擊相關的流量，則偵測需要能夠準確識別提出請求的用戶端。例如，當限制速率的屬性是應用程式特定的，例如 Cookie 或權杖時，速率型規則通常會更有效率且更難逸出。使用與工作階段繫結的 Cookie 可防止殭屍網路運算子跨多個機器人複製類似的請求流程。

字符獲取通常用於用戶端識別。針對權杖取得，JavaScript 程式碼會收集資訊，以產生在伺服器端評估的權杖。評估的範圍可以從驗證用戶端上執行 JavaScript 到收集裝置資訊以進行指紋。權杖取得需要將 JavaScript 開發套件整合到網站或應用程式中，或者需要服務提供者動態執行注入。

需要 JavaScript 支援為嘗試模擬瀏覽器的機器人新增額外的障礙。涉及 SDK 時，例如在行動應用程式中，權杖擷取會驗證 SDK 實作，並防止機器人模擬應用程式的請求。

權杖取得需要使用在連線用戶端實作的 SDKs。下列 AWS WAF 功能提供適用於瀏覽器的 JavaScript 型 SDK 和適用於行動裝置的應用程式型 SDK：機器人控制、詐騙控制帳戶接管預防 (ATP) 和詐騙控制帳戶建立詐騙預防 (ACFP)。

用戶端識別的技術包括 CAPTCHA、瀏覽器分析、裝置指紋和 TLS 指紋。

CAPTCHA

完全自動化的公有 Turing 測試，用於區分電腦和人類 (CAPTCHA)，以區分機器人和人類訪客，並防止 Web 抓取、憑證填充和垃圾郵件。有各種實作，但它們通常涉及人類可以解決的拼圖。CAPTCHAs 為常見機器人提供額外的防禦層，並可減少機器人偵測中的誤判。

AWS WAF 允許規則針對符合規則檢查條件的 Web 請求執行 CAPTCHA 動作。此動作是評估 service. AWS WAF rules 收集的用戶端識別資訊的結果。rules 可能需要解決 CAPTCHA 挑戰，以解決經常由機器人鎖定的特定資源，例如登入、搜尋和表單提交。 AWS WAF 可以透過間質方式或使用 SDK 在用戶端處理 CAPTCHA。如需詳細資訊，請參閱 CAPTCHA 和 Challenge in AWS WAF。

瀏覽器分析

瀏覽器分析是一種收集和評估瀏覽器特性的方法，作為字符獲取的一部分，用於使用互動式瀏覽器區分真實人類和分散式機器人活動。您可以透過瀏覽器運作方式固有之請求的標頭、標頭順序和其他特性，被動地執行瀏覽器分析。

您也可以使用字符擷取在程式碼中執行瀏覽器分析。透過使用 JavaScript 進行瀏覽器分析，您可以快速判斷用戶端是否支援 JavaScript。這可協助您偵測不支援它的簡單機器人。瀏覽器分析檢查不只是 HTTP 標頭和 JavaScript 支援；瀏覽器分析讓機器人難以完全模擬 Web 瀏覽器。兩個瀏覽器分析選項都有相同的目標：尋找瀏覽器設定檔中的模式，指出與實際瀏覽器的行為不一致。

AWS WAF 目標機器人的機器人控制提供指示，指出瀏覽器是否顯示自動化的證據或不一致的訊號。AWS WAF 會標記請求，以採取規則中指定的動作。如需詳細資訊，請參閱 AWS 安全部落格中的偵測和封鎖進階機器人流量。

裝置指紋

裝置指紋類似於瀏覽器分析，但並不限於瀏覽器。在裝置上執行的程式碼 （ 可以是行動裝置或 Web 瀏覽器 ） 會收集裝置的詳細資訊，並向後端伺服器回報。詳細資訊可以包含系統屬性，例如記憶體、CPU 類型、作業系統 (OS) 核心類型、作業系統版本和虛擬化。

您可以使用裝置指紋辨識機器人是否模擬環境，或是否有使用自動化的直接跡象。除此之外，裝置指紋也可以用來辨識來自相同裝置的重複請求。

識別來自相同裝置的重複請求，即使裝置嘗試變更請求的某些特性， 也允許後端系統強制執行速率限制規則。以裝置指紋為基礎的速率限制規則通常比以 IP 地址為基礎的速率限制規則更有效。這可協助您減少在 VPNs 或代理之間輪換，但來自少量裝置的機器人流量。

與應用程式整合 SDKs 搭配使用時，目標 AWS WAF 機器人的機器人控制可以 彙總用戶端工作階段請求行為。這可協助您偵測並區隔合法用戶端工作階段與惡意用戶端工作階段，即使兩者都來自相同的 IP 地址。如需目標 AWS WAF 機器人的機器人控制詳細資訊，請參閱 AWS 安全部落格中的偵測和封鎖進階機器人流量。

TLS 指紋

當機器人來自許多 IP 地址，但具有類似的特性時，通常會使用 TLS 指紋，也稱為以簽章為基礎的規則。使用 HTTPS 時，用戶端和伺服器端會交換訊息，以互相確認和驗證。它們會建立密碼編譯演算法和工作階段金鑰。這稱為 TLS 交握。如何實作 TLS 交握是一種簽章，通常對於識別分散在許多 IP 地址的大型攻擊很有價值。

TLS 指紋可讓 Web 伺服器以高準確度判斷 Web 用戶端的身分。在進行任何應用程式資料交換之前，它只需要第一個封包連線中的參數。在此情況下，Web 用戶端是指起始請求的應用程式，可能是瀏覽器、CLI 工具、指令碼 （機器人）、原生應用程式或其他用戶端。

SSL 和 TLS 指紋方法之一是 JA3 指紋。JA3 會根據 SSL 或 TLS 交握的 Client Hello 訊息中的欄位對用戶端連線進行指紋。它可協助您跨不同的來源 IP 地址、連接埠和 X.509 憑證來描述特定的 SSL 和 TLS 用戶端。

Amazon CloudFront 支援將 JA3 標頭新增至請求。`CloudFront-Viewer-JA3-Fingerprint` 標頭包含傳入檢視器請求之 TLS Client Hello 封包的 32 個字元雜湊指紋。指紋會封裝用戶端通訊方式的相關資訊。此資訊可用於描述共用相同模式的用戶端。您可以將 `CloudFront-Viewer-JA3-Fingerprint`標頭新增至原始伺服器請求政策，並將政策連接至 CloudFront 分佈。然後，您可以在原始伺服器應用程式或 Lambda@Edge 和 CloudFront Functions 中檢查標頭值。您可以比較標頭值與已知惡意軟體指紋清單，以封鎖惡意用戶端。您也可以將標頭值與預期的指紋清單進行比較，以僅允許來自已知用戶端的請求。

用於管理機器人的進階分析控制項

有些機器人使用進階欺騙工具來主動逃避偵測。這些機器人模擬人類行為，以執行特定活動，例如剪影。這些機器人具有用途，通常與大貨幣獎勵相關聯。

這些進階、持久性機器人使用混合技術來逃避偵測，或與一般流量混合。反之，這還需要混合不同的偵測技術，才能準確識別和緩解惡意流量。

針對性使用案例

使用案例資料可提供機器人偵測機會。詐騙偵測是需要特殊緩解的特殊使用案例。例如，為了協助防止帳戶接管，您可以將遭入侵的帳戶使用者名稱和密碼清單與登入或帳戶建立請求進行比較。這有助於網站擁有者偵測使用遭入侵登入資料的登入嘗試。使用洩露的登入資料可能表示機器人嘗試接管帳戶，或者可能是不知道其登入資料洩露的使用者。在此使用案例中，網站擁有者可以採取其他步驟來驗證使用者，然後協助他們變更密碼。 為此使用案例 AWS WAF 提供詐騙控制帳戶接管預防 (ATP) 受管規則。

應用程式層級或彙總機器人偵測

有些使用案例需要結合來自內容交付網路 (CDN) 請求的資料 AWS WAF，以及應用程式或服務的後端。有時，您甚至需要整合第三方智慧，才能對機器人做出高可信度的決策。

Amazon CloudFront 和 中的功能 AWS WAF 可以將訊號傳送至後端基礎設施，或者它們隨後可以透過標頭和標籤彙總規則。CloudFront 公開 JA3 指紋標頭，如前所述。這是 CloudFront 透過標頭提供此類

資料的範例。當符合規則時， AWS WAF 可以傳送標籤。後續規則可以使用這些標籤，對機器人做出更好的決策。合併多個規則時，您可以實作高度精細的控制項。常見的使用案例是透過標籤比對受管規則的部分， 然後將其與其他請求資料合併。如需詳細資訊，請參閱 AWS WAF 文件中的標籤比對範例。

機器學習分析

機器傾斜 (ML) 是處理機器人的強大技術。ML 可以適應不斷變化的詳細資訊，而且當 與其他工具結合時， 提供最強大且完整的方法，以最少的誤判來緩解機器人。兩種最常見的 ML 技術是行為分析和異常偵測。透過行為分析，系統（在用戶端、伺服器或兩者中） 會監控使用者與應用程式或網站的互動方式。它會監控滑鼠移動模式或點選和觸控互動的頻率。接著會使用 ML 模型分析行為，以辨識機器人。異常偵測類似。它著重於偵測與應用程式或網站所定義基準明顯不同的行為或模式。

AWS WAF 機器人的目標控制項提供預測性 ML 技術。此技術有助於防禦由旨在逃避偵測的機器人進行的分散式代理型攻擊。受管 AWS WAF Bot Control 規則群組使用網站流量統計資料的自動化 ML 分析，來偵測指示分散式協調機器人活動的異常行為。

部署和實作您的機器人控制策略

規劃機器人控制部署策略時，需要考慮多個因素。除了 Web 應用程式的獨特特性之外，環境大小、開發程序和組織結構也會影響部署策略。根據您的環境和應用程式特性，可以使用集中式或分散式部署策略：

- 集中式部署策略 – 當您想要嚴格強制執行機器人控制時，集中式方法可實現更高程度的控制。如果應用程式團隊偏好卸載管理，則這種方法非常適合。當 Web 應用程式具有類似的特性時，集中式方法最有效。在這種情況下，應用程式受益於一組常見的機器人控制規則和機器人緩解動作。
- 分散式部署策略 – 分散式方法為應用程式團隊提供自主性，以獨立定義和實作機器人控制組態。這種方法在較小的環境或應用程式團隊需要保留對其機器人控制政策的控制時很常見。由於許多 Web 應用程式的性質，通常需要維護針對唯一應用程式特性量身打造的獨立機器人控制政策，進而產生分散式方法。
- 合併策略 – 這兩種方法的組合適用於混合 Web 應用程式。例如，這可能需要一組適用於所有 Web ACLs 的基本規則，同時將更具體的機器人控制政策的管理委派給應用程式團隊。

您可以使用 來AWS Firewall Manager集中和自動化定義機器人控制政策的 AWS WAF Web ACLs 部署。使用 Firewall Manager 時，請考慮集中機器人控制政策是否適當，包括是否應委派給應用程式團隊。透過 Firewall Manager，您可以使用標記來允許應用程式團隊選擇加入 AWS WAF 政策。這提供 AWS WAF 智慧型威脅緩解功能。您也可以為應用程式和安全性操作啟用集中式 AWS WAF 記錄。

無論使用的部署策略為何，建議透過基礎設施即程式碼 (IaC) 型架構定義和管理加入程序，例如 AWS CloudFormation 或 AWS Cloud Development Kit (AWS CDK)。這可協助您設定來源控制來存放 和版本組態物件。如需詳細資訊，請參閱 AWS CDK(GitHub) 和 CloudFormation (AWS 文件） 的 AWS WAF 組態範例。

實作策略

選取部署策略之後，即可開始實作。部署策略會定義規則如何推展到不同的應用程式。在實作策略中，重點是新增控制項、測試、持續監控，然後評估其效果的反覆程序。

了解流量模式

若要真正了解流量模式，請務必熟悉應用程式的業務功能和預期的屬性，例如使用模式、金鑰資源和使用者角色。針對應用程式納入測試期間產生的生產流量和流量，以建立評估基準。請確定時間範圍包含足以代表多個用量峰值的流量資料。

使用您偏好的工具，檢閱代表性用量期間的流量日誌和指標。透過篩選 AWS WAF headers（例如，User-Agent和 Referer)、 和 等日誌欄位，分析異常請求的日誌資料clientIp。 country請記下統一資源識別符 (URIs) 及其存取頻率。將流量分類，例如識別良好的機器人。例如，允許存取有益的機器人，例如搜尋引擎爬蟲程式和監視器。

在 AWS WAF 主控台的機器人控制儀表板上，機器人活動範例可用於任何作用中的 Web ACL。雖然這提供了常見機器人請求磁碟區的初始觀點，但請執行進一步的組態和分析，以進一步了解機器人活動。

為了有效實作，您必須充分了解機器人流量、其效果，以及哪些機器人請求對惡意有益。這有助於下一個階段、選取控制項，並協助您平行評估機器人流量。

選取和新增控制項

初始流量分析有助於判斷要使用哪些機器人控制項，以及要為每個機器人選取哪些動作。您也可以選擇記錄和監控潛在未來動作的活動。初始流量分析可協助您選取管理流量的最佳控制項。如需可用控制項的詳細資訊，請參閱本指南機器人控制的技巧中的 。

考慮在此步驟中包含其他 SDK 實作。這可協助您在所有必要的應用程式中測試和完成 SDK 實作。AWS WAF 機器人控制和詐騙控制規則可在實作 JavaScript SDK 或行動 SDK 時提供完整的字符評估效益。如需詳細資訊，請參閱 AWS WAF 文件中的為什麼您應該使用應用程式整合 SDKs搭配 Bot Control。

我們建議針對不同的應用程式類型實作權杖擷取，如下所示：

- 單頁應用程式 (SPA) – JavaScript SDK （無重新導向）
- 行動瀏覽器 – JavaScript SDK 或規則動作 (CAPTCHA 或挑戰）
- Web 檢視 – JavaScript SDK 或規則動作 (CAPTCHA 或挑戰）
- 原生應用程式 – Mobile SDK
- iFrames – JavaScript SDK

如需如何實作 SDKs的詳細資訊，請參閱 AWS WAF 文件中的AWS WAF 用戶端應用程式整合。

測試和部署至生產環境

控制項一開始應該部署在非生產環境中，您可以在其中執行測試，以確認保留預期的 Web 應用程式功能。在生產部署之前，請務必在測試環境中執行 徹底的驗證。

在非生產環境中測試和驗證之後，生產版本可以繼續。選取預期使用者流量最低的日期和時間。在部署之前，應用程式和安全團隊應該檢閱操作準備程度、討論如何復原變更，以及檢閱儀表板，以確保已設定所有必要的指標和警示。

透過 Amazon CloudFront 持續部署，您可以將少量流量傳送至已特別為機器人控制評估設定的 AWS WAF Web ACL 預備分佈。 AWS WAF 提供任何新受管規則或更新受管規則的版本管理，以便在開始評估生產流量之前測試和核准變更。

評估和調校控制項

實作的控制項可以提供對流量活動和模式的進一步洞察和可見性。經常監控和分析應用程式流量，以新增或調整安全控制。通常有一個調校階段來緩解潛在的誤報和誤報。偽陰性是您的控制項未攔截的攻擊，要求您強化規則。誤報代表未正確識別為攻擊並因此封鎖的合法請求。

分析和調校可以手動完成，或藉助 工具完成。安全資訊和事件管理 (SIEM) 系統是一種常見工具，可協助提供指標和智慧型監控。有許多不同程度的複雜度，但它們都提供了良好的起點來取得流量洞察。

定義網站和應用程式的重要關鍵績效指標 (KPIs)，可協助您更快速地識別物件未如預期運作的時間。例如，您可以使用信用卡退款、每個帳戶的銷售額或轉換率，做為機器人可能產生的業務異常指標。定義和了解哪些指標和 KPIs值得監控，甚至比監控行為更重要。

了解如何從機器人控制解決方案取得正確的指標和日誌，與識別要監控的指標一樣重要。下一節監控機器人控制策略的準則詳細說明要考慮的監控和可見性選項。

監控機器人控制策略的準則

對於機器人流量和 Web 應用程序流量而言，監控和可見性非常重要。它可協助您排定活動的優先順序以及安全性作業。如果無法進行詳細記錄或使用 SIEM 系統，那麼一個很好的起點就是監視您選取的解決方案或廠商提供的基本指標。

此可見性對於威脅情報、強化規則、疑難排解誤報以及回應事件非常有用。有多個可用的監視選項 AWS WAF。若要進行高階監控，請在中 AWS WAF 提供流量概觀資訊 AWS 管理主控台。當您的 Web ACL 中啟用了機器人控制規則群組時，此功能可用於所有流量以及機器人流量的詳細檢視。

AWS WAF 提供不同的選項來詳細記錄 Web ACL 流量。您也可以將標籤新增至請求，以便進行記錄分析和設定機器人評估規則。透過整合 Amazon CloudWatch 日誌洞見，您可以查詢 AWS WAF 日誌並將結果視覺化。

如果您開啟詳細記錄，則會 AWS WAF 提供預先設定的機器人控制儀表板以外的其他可見性。使用 AWS WAF 記錄檔將流量視覺化以及臨機操作調查，可深入瞭解 Web 應用程式的流量模式和緩解選項。

您可以將日 AWS WAF 誌數據與 Amazon CloudWatch 日誌，Amazon Simple Storage Service (Amazon S3) 或 Amazon 數據 Firehose 集成。如需詳細資訊，請參閱開啟 AWS WAF 記錄功能並將日誌傳送到 CloudWatch Amazon S3 或 Amazon 資料 Firehose。您也可以將日誌傳送到各種目標進行分析，包括到 Amazon OpenSearch 服務或AWS Marketplace解決方案。如需詳細資訊，請參閱 Firehose 文件中的目的地設定。如果使用多個記錄來源，建議使用集中式記錄解決方案來關聯來源。

接下來，本指南提供有關如何使用 Amazon 開始監控機器人流量並獲得可見度的建議 CloudWatch。

追蹤熱門規則

跟踪命中最高的規則可以突出趨勢和潛在的異常活動。提高特定規則的比率可能表示您應該調查的潛在誤判或鎖定目標活動。最常見的追蹤規則是IP 型控制地理封鎖規則 (這裡的尖峰可以顯示來自不尋常國家/地區的流量，這可能不會自動封鎖)，以及速率為基礎的規則。這些規則將始終具有固有的變化，但流量模式的異常可能表示機器人活動。如果您要手動設定閾值，請考慮這一點。

追蹤頂端標籤和命名空間

透過使用 CloudWatch 指標追蹤最常用的標籤，您可以查看經常叫用哪些 AWS WAF 規則。這有助於您檢測異常情況，例如抓取活動增加，來自可疑來源的流量，或嘗試濫用應用程序登錄頁面或 API。

以下是可能感興趣的範例標籤：

- awswaf:managed:aws:bot-control:signal:non_browser_user_agent
- awswaf:managed:aws:bot-control:bot:category:http_library
- awswaf:managed:aws:bot-control:bot:name:curl
- awswaf:managed:aws:atp:signal:credential_compromised
- awswaf:managed:aws:core-rule-set:NoUserAgent_Header
- awswaf:managed:token:rejected

以下是可能感興趣的範例標籤命名空間：

- awswaf:managed:aws:bot-control:
- awswaf:managed:aws:atp:
- awswaf:managed:aws:anonymous-ip-list:

建立數學運算式

在 Amazon 中 CloudWatch，您可以為任何或所有規則建立數學運算式。如果您在數學運算式上設定警示，系統會通知您有關特定量度的比率 (而非數量) 異常。這是減少警報疲勞的重要工具。

建立以數學運算式建置的自訂量度。查看規則的相對費率，從對應用程序的請求的總數。以下是常見的數學運算式：

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

此數學運算式提供百分比，讓您可以追蹤特定規則並視覺化其隨時間變化的趨勢。

使用異常偵測

在任何 CloudWatch 量度上使用CloudWatch異常偵測可以針對異常低或高趨勢提供警示，而無需手動設定實際閾值。 這些演算法會持續分析系統和應用程式的指標、判斷一般基準線，並以最少的使用者介入來顯示異常情況。 CloudWatch 在其異常偵測功能中套用統計和 ML 演算法。

使用 Amazon CloudWatch 指標

AWS WAF 處理流量並將標籤新增至符合 Web ACL 中定義的規則的請求。每個標籤都會在中建立一個度量 CloudWatch。同時，每個 Web ACL 規則也會為每個可能的動作建立量度。使用這些標籤和動

作指標，深入瞭解機器人流量。這是一種具有成本效益的方法來視覺化趨勢。如需詳細資訊，請參閱 CloudWatch 文件中的檢視可用量度和繪製圖形化指標。

CloudWatch 提供將資料傳送至記錄收集器或彙總工具的選項，無論是第三方解決方案 AWS 服務 還是協力廠商解決方案。從中擷取資料 CloudWatch 可提供更整合的安全觀察性體驗，您可以在其中將來自多個來源的資料建立關聯。這可協助您調查、檢視或設定警示和安全自動化。

建立儀表板

確定要跟踪的重要指標後，創建一個包含最相關指標的儀表板。在單個玻璃窗格下顯示它們 side-by-side可以提供額外的可見性和控制。

最好為異常量度值設定警示和自動化規則。不要依賴人類通過查看儀表板來識別異常情況。但是，在收到警示之後，儀表板可用於調查目的。

最佳化機器人控制策略的成本

Web 流量的性質是動態的。這表示用於緩解威脅的技術和服務可能會隨著時間而變化和調校。這是考慮機器人控制策略及其所包含的控制項時的關鍵。隨著時間的推移進行最佳化是需要記住的主要原則，它來自 AWS Well-Architected Framework 的成本最佳化支柱。

AWS WAF Web ACLs可以是動態的，特別是在發行新功能或您嘗試緩解新威脅時。留意您的成本需要了解 AWS WAF 服務的成本維度，以及每個維度如何影響您的最終支出。主要駕駛成本是 服務評估的請求數量。如果您使用 Bot Control 和帳戶接管預防 (ATP) 受管規則群組，或使用進階動作，例如 CAPTCHA 或挑戰，則需支付額外費用。

由於特殊化機器人控制的成本很高，因此主要成本最佳化目標是減少這些進階控制項檢查的請求數量。適用的技術包括分隔高價值內容、先套用成本較低的量值、縮小評估區域，以及將機器人保護與其他類型的控制項結合。成本監控技術可為您的組織提供額外的可見性。

分隔動態和靜態內容

一種成本降低技術是從動態應用程式隔離靜態內容。對典型 Web 應用程式的大多數請求都是對靜態物件的請求。減少應用程式伺服器上負載的常見方法是將靜態內容移至自己的 URL，例如 `static.example.com`。 這通常是透過使用針對靜態內容最佳化的快取組態建立唯一的內容交付分佈來實現。如果靜態內容不常以網站或應用程式為目標，則 這項技術也有助於降低機器人控制成本。將靜態內容與動態應用程式 分開，可以更精確地套用進階機器人控制。

先套用成本較低的規則

另一個技巧是套用低成本的基準規則，在使用更昂貴的進階控制項之前篩選掉不需要的流量。 實際上，這通常意味著將機器人控制緩解措施作為最後一層防禦，並使用先前的控制來篩選掉不需要機器人控制的技巧的流量。本指南先前討論過 這種金字塔方法。主要目標是使用這些成本較低的選項來停止不需要的流量，從而減少 進階、成本較高的緩解技術所處理的請求數量。

縮小評估區域

AWS WAF 縮小範圍陳述式提供強大的技術，可減少進階規則檢查的請求數量。 如果無法實作將靜態內容分隔為自己的 URL，則縮小範圍陳述式是篩選不需要進階緩解技術之請求的另一種方法。這可以透過定義特定應用程式路徑、HTTP 方法 （ 例如 POST) 或類似的組合來完成。

將機器人保護與其他控制項結合

保護應用程式免受多個威脅以及不必要的機器人流量時，應審查額外的成本控制考量。 例如，防止分散式阻斷服務 (DDoS) 攻擊和帳戶接管，需要額外的組態來影響成本。建議 Shield Advanced 協助保護應用程式免受 DDoS 攻擊。 特別是，其應用程式層緩解措施可以自動解決請求洪水，因此在將規則置於評估順序之前時，減少機器人控制規則群組可能處理的 AWS WAF 請求數量。Shield Advanced 具有額外優勢；標準受管和自訂 AWS WAF 規則對於 Shield Advanced 保護的資源無需額外費用。 請注意，智慧型威脅緩解規則群組，包括 Bot Control，即使對於 Shield Advanced 保護的資源，也會產生額外的成本。

需要帳戶接管預防的應用程式可以使用 AWS WAF Fraud Control 帳戶接管預防 (ATP) 規則群組。 ATP 規則群組的每次請求檢查成本高於 Bot Control 規則群組。 這種較高的成本使得盡可能精確地套用 ATP 規則群組至關重要。搭配 ATP 使用 Bot Control 規則群組有助於實現此目標。Bot Control 規則群組應放置在 Web ACL 中的 ATP 前面，以篩選出機器人請求，並減少 ATP 檢查的請求數量。

為了持續最佳化，最重要的活動是監控與 Bot Control 規則群組相關聯的 CloudWatch 指標。隨著時間的推移，目標是將 Bot Control 規則群組評估的請求數量減少為僅以您需要的資源為目標，以防止不必要的機器人活動為目標的請求數量。 建置 CloudWatch 儀表板可提供應用程式最關鍵指標的可見性，包括 AWS WAF 成本和用量。

監控成本

AWS Cost Explorer 是一個可讓您檢視和分析成本與用量的工具。Cost Explorer 有助於成本分析 AWS ，包括產生的 AWS WAF 成本。此工具提供最近 12 個月的成本資訊，並預測未來 12 個月的未來支出。

AWS 成本異常偵測是另一種成本管理控制工具，可用於監控 AWS WAF 成本。它使用進階 ML 技術來識別異常支出和根本原因。這可協助您在成本意外增加時快速採取行動或接收提醒。若要在達到特定成本閾值時收到提醒，AWS Budgets 可以提供該追蹤和監控功能。

資源

AWS 文件

- AWS WAF 開發者指南
- AWS DDoS 彈性的最佳做法 (AWS 白皮書)
- 實施指引 AWS WAF (AWS 白皮書)

其他 AWS 資源

- 分析 Amazon AWS WAF 日誌中的 CloudWatch 日誌 (AWS 部落格文章)
- AWS WAF 以最小的努力部署儀表板 (部AWS 落格文章)
- AWS WAF(AWS 解決方案程式庫) 的安全自動化
- 三個最重要的 AWS WAF 基於速率的規則 (AWS 博客文章)
- 使用 Amazon CloudWatch 儀表板將 AWS WAF 日誌視覺化 (AWS 部落格文章)

貢獻者

撰寫

- 戴安娜·阿爾瓦拉多，高級解決方案架構師 AWS
- 卡梅倫·沃雷爾，企業建築師， AWS
- 吉里·舍勒，解決方案架構師， AWS
- Tzoori Tamam，首席解決方案建築師， AWS

檢閱

- 傑西伊曾, 高級軟件開發工程師, AWS
- 帕塔克, 高級產品經理, AWS
- 維克拉馬迪蒂亞·巴特納加爾, 高級安全顧問, AWS

技術寫作

- 莉莉 AbouHarb，高級技術作家， AWS

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	—	2024年2月21 日

AWS 規範性指引詞彙表

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

數字

7 R

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

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的內部部署 Oracle 資料庫 遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將您的內部部署 Oracle 資料庫 遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統 遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫 遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式 遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

A2A Agent-to-Agent)

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

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

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

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。目標資料庫在遷移期間不接受任何交易。

客服人員

一種 AI 系統，可使用工具自動推理、規劃和採取行動來實現目標。

客服人員操作

在生產環境中大規模建置、測試、部署和執行 AI 代理器的操作實務。

彙總函數

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

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

永久刪除資料集中個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常用於重複性問題的解決方案，其中解決方案具有反效益、無效或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

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

人工智慧 (AI)

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

人工智慧操作 (AIOps)

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

非對稱加密

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

原子性、一致性、隔離性、耐久性 (ACID)

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

屬性型存取控制 (ABAC)

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

授權資料來源

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

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針整理成六個重點領域：業務、人員、治理、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

一種工具，可評估資料庫遷移工作負載、建議遷移策略，並提供工作預估值。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

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

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 （藍色） 中執行目前的應用程式版本，並在另一個環境 （綠色） 中執行新的應用程式版本。此策略可協助您快速復原，並將影響降至最低。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上編製資訊索引的 Web 爬蟲程式。某些其他機器人稱為惡意機器人，旨在中斷或傷害個人或組織。

殭屍網路

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

分支

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

碎片存取

在特殊情況下，並透過核准的程序，讓使用者快速取得他們通常無權存取 AWS 帳戶 之 的存取權。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 AWS上執行容器化微服務白皮書的圍繞業務能力進行組織部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

版本對最終使用者的緩慢和增量版本。當您有信心時，您可以部署新版本並完全取代目前的版本。

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，為您的 AWS 工作負載帶來壓力，並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

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

公民開發人員

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

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

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

雲端運算

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

雲端操作模型

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

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

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

這些階段由 Stephen Orban 在部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub或 Bitbucket Cloud。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

AI 欄位???，使用機器學習從數位影像和影片等視覺化格式分析和擷取資訊。例如，Amazon SageMaker AI 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或整個組織的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的一致性套件。

持續整合和持續交付 (CI/CD)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱持續交付的優點。CD 也可表示持續部署。如需詳細資訊，請參閱持續交付與持續部署。

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

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

資料周邊

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

資料預先處理

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

資料來源

在整個資料生命週期中追蹤資料的來源和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如 分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重要素驗證、網路分割和加密。

委派的管理員

在 中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶，以管理組織的帳戶和管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的可搭配 AWS Organizations運作的服務。

deployment

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

開發環境

請參閱 環境。

偵測性控制

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

開發值串流映射 (DVSM)

一種程序，用於識別對軟體開發生命週期中的速度和品質造成負面影響的限制並排定優先順序。DVSM 擴展了最初專為精簡製造實務設計的價值串流映射程序。它著重於透過軟體開發程序建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬呈現，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在星星結構描述中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

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

災難復原 (DR)

您用來將災難造成的停機時間和資料遺失降至最低的策略和程序。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 上工作負載的災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

領域驅動的設計

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

DR

請參閱災難復原。

偏離偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源中的偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲端運算相比，邊緣運算可以減少通訊延遲並改善回應時間。

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

加密金鑰

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

端序

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

端點

請參閱 服務端點。

端點服務

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

企業資源規劃 (ERP)

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

信封加密

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

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

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

epic

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

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

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

F

事實資料表

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

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

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

功能分支

請參閱分支。

特徵

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

功能重要性

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

特徵轉換

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

少量擷取提示

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

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

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

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及以自然語言交談。如需詳細資訊，請參閱什麼是基礎模型。

FM 閘道

集中式中介，可控制和標準化對基礎模型的存取。也稱為 LLM 閘道。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的限制內容的地理分佈。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於改善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)

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

歷史現代化

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

保留資料

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

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

屬於組織一部分的管理帳戶 AWS 帳戶 以外的所有 AWS Organizations。帳戶一次只能是一個組織的成員。

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

根據發佈/訂閱模式的輕量型machine-to-machine(M2M) 通訊協定，適用於資源受限的 IoT 裝置。

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用無 AWS 伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱在 上實作微服務 AWS。

Migration Acceleration Program (MAP)

一種 AWS 計畫，提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 AWS 遷移策略的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的遷移工廠的討論和雲端遷移工廠指南。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。MPA 工具 （需要登入） 可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移準備程度評定 (MRA)

使用 AWS CAF 取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱《》中的現代化應用程式的策略 AWS 雲端。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱《》中的評估應用程式的現代化準備 AWS 雲端程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱將單一體系分解為微服務。

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」 或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性， AWS Well-Architected Framework 建議使用不可變的基礎設施作為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

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

OPC-UA

請參閱開放程序通訊 - 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 中的操作準備度審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造中，OT 和資訊技術 (IT) 系統的整合是工業 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、使用 AWS KMS (SSE-KMS) 的伺服器端加密 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)

當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

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

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以提高可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強生成。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

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

迴歸

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

重新託管

請參閱 7 Rs。

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 Rs。

Replatform

請參閱 7 Rs。

回購

請參閱 7 Rs。

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

回應性控制

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

保留

請參閱 7 個 R。

淘汰

請參閱 7 個 R。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者 (IdP) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，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？ Secrets Manager 文件中的 。

設計安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

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

安全強化

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

安全資訊與事件管理 (SIEM) 系統

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

安全回應自動化

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

伺服器端加密

由 AWS 服務 接收資料的 在其目的地加密資料。

服務控制政策 (SCP)

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

服務端點

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

服務水準協議 (SLA)

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

服務層級指標 (SLI)

服務效能方面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

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

陰影 AI

在組織內受管頻道之外建置或使用的未授權 AI 應用程式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱 中的階段式應用程式現代化方法 AWS 雲端。

SPOF

請參閱單一故障點。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構旨在用於資料倉儲或商業智慧用途。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 Amazon CloudWatch Synthetics 來建立這些測試。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

T

標籤

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

目標變數

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

任務清單

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

測試環境

請參閱 環境。

訓練

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

tool

代理程式可以叫用以在外部系統中執行操作的函數或 API。

傳輸閘道

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

主幹型工作流程

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

受信任的存取權

將許可授予您指定的服務，以代表您在組織中 AWS Organizations 及其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 文件中的 AWS Organizations 搭配使用 AWS Organizations 與其他 AWS 服務。

調校

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

雙比薩團隊

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

U

不確定性

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

未區分的任務

也稱為繁重工作，這是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危害系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等緩慢的查詢。

視窗函數

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

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

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

WORM

請參閱寫入一次，讀取許多。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

儲存模型，可一次性寫入資料，並防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為不可變。

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的缺陷或漏洞。威脅行為者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。