採用 IoT 裝置製造商的事項標準

AWS 方案指引

AWS 方案指引: 採用 IoT 裝置製造商的事項標準

Table of Contents

IoT 設備製造商採用物聯網標準

圖莎·帕特爾，維傑·烏賈因和大衛·沃爾特斯，Amazon Web Services（ ）AWS

2024 年 2 月 (文件歷史記錄)

根據 S tatista 的數據，到 2028 年，全球智能家居家庭的數量預計將達到 7.8 億。這種快速增長在運營和管理方面帶來了挑戰。從消費者的角度來看，每個設備供應商都有不同的方法，可以通過該設備供應商特定的應用程序將智能家居設備上載到家庭網絡上。這使得管理來自不同供應商的各種不同類型的設備變得具有挑戰性。同樣，從設備製造商的角度來看，通過各種生態系統認證其智能家居產品會增加其業務流程的成本和複雜性。例如，對於相同的裝置型號，這可能需要不同的 SKU。維護引人注目的用戶體驗應用程序並提供定期更新，從而使資源遠離構建和交付更好的產品，這是一個額外的開銷。消費者和設備製造商都將受益於通用的智能家居互操作性標準。該標準允許來自多個供應商的設備以無縫，安全和可靠的方式相互操作。

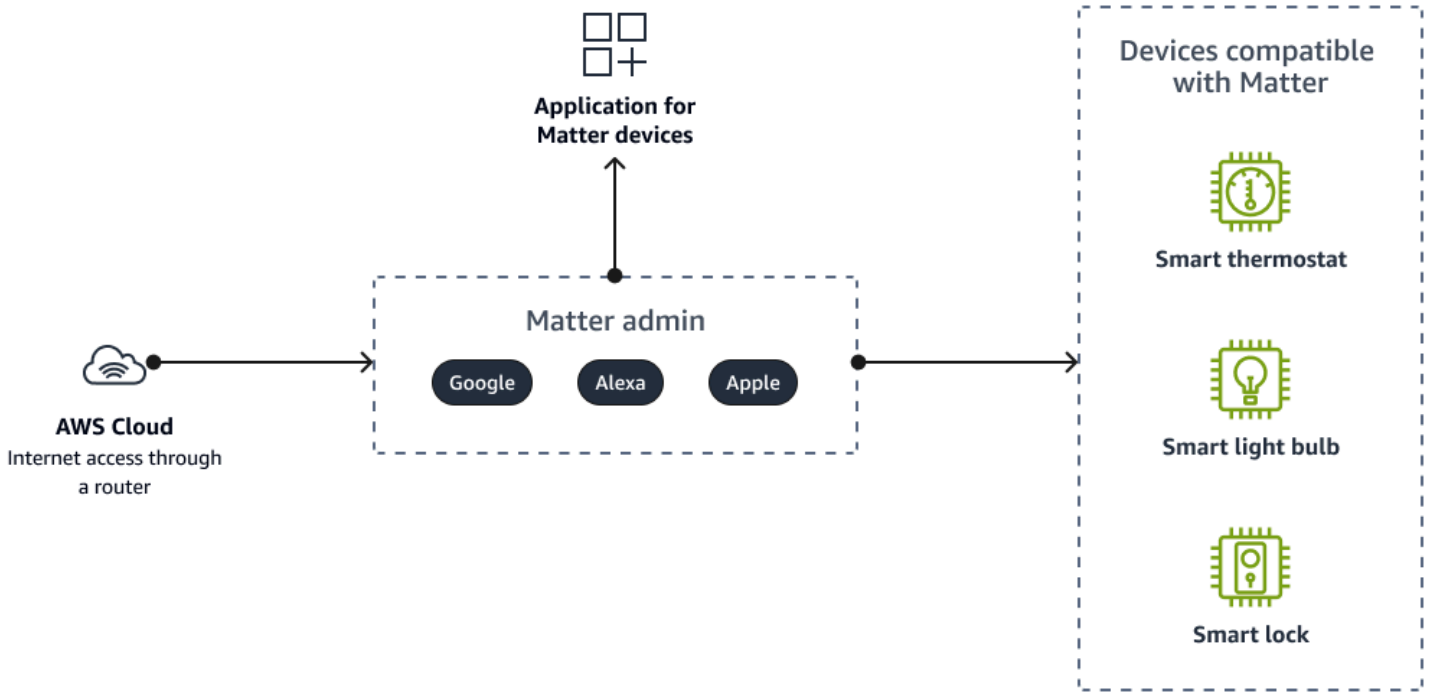
新的 Met ter 標準為智慧家庭領域的物聯網 (IoT) 裝置製造商提供了令人興奮的機會。該標準旨在提高不同製造商設備之間的兼容性和互操作性。Matter 是一種開放式的智慧家庭連線通訊協定，可在 IoT 裝置、行動應用程式和雲端服務之間進行通訊。

目標

將 Matter 標準整合到其產品中時，IoT 裝置製造商必須在開始開發之前應對數個挑戰。相較於專有的 IoT 通訊協定，Matter 具有許多優勢，包括裝置的互通性、安全性、簡易性、可靠性和面向未來的需求。但是，將 Matter 整合到新的和現有的 IoT 部署中需要仔細的規劃和策略。製造商需要有關物質合規性流程的指導，以便在充分利用效益的同時避免陷阱。本指南為 IoT 裝置製造商提供有關 Matter 採用的全面指引。它包括從策略到實施的清晰路線圖。本指南簡化了向 Matter 的過渡，幫助您構建安全、可互操作且符合未來需求的產品，在智慧家庭生態系統中蓬勃發展。透過正確的策略方法，組織可以克服 Matter 採用的障礙，並開發採用開放標準的創新 IoT 裝置。

本指南為裝置製造商提供 Matter 的全面概觀，以及符合 Matter 標準所需的步驟。它概述了計劃 Matter 採用策略的利弊。該指南還提出了利用 Matter 的最佳實踐，同時繼續分階段支持現有的無線協議。對於探索智慧家庭解決方案的 IoT 裝置製造商而言，本指南可以為您提供連線策略。

了解物質標準



物质协议

Matter 是一種開放的智慧家庭連線通訊協定，可在裝置、行動應用程式和雲端服務之間進行通訊。Matter 由連接標準聯盟（CSA）開發，為消費者和製造商簡化了連接性和互操作性。物質支持廣泛的智能家居類別。對於消費者而言，Matter 在整個生態系統中提供入職、統一管理和控制。對製造商而言，Matter 透過單一認證和應用程式開發，降低開發和支援成本。許多大公司，如 Amazon，蘋果和谷歌，正在推動物質的採用。CSA 根據組織的參與程度提供四個會員級別-推廣員，參與者，採用者和同事。憑藉強大的行業支持，Matter 旨在為消費者提供跨品牌的無縫連接，並簡化製造商的開發。

物質如何工作的概述

Matter 是一種基於 IP 的應用程序級協議，適用於跨供應商生態系統的智能家居設備。它適用於使用 IPv6 的設備。從概念上講，物質被組織為網絡節點，這是物質端點的集合。以下是問題術語的簡要摘要：

- 物質設備是智能家居產品，例如燈泡，開關，恆溫器或鎖。

- 物質結構是所有設備都連接在其上的虛擬網絡。所有裝置都共用相同的受信任根目錄。光纖形成星狀網路拓撲結構。
- Matter 管理員會為網狀架構上的所有裝置建立、維護及管理安全性和權限。管理員可以是中樞或應用程式。Matter 具有多管理功能，其中 Matter 設備可以同時成為多個網狀架構的一部分。例如，Amazon Alexa 裝置和 Google 主頁裝置都可以管理單一問題裝置，兩者都可以是同一個實體網路上的物質管理員。
- 「事項專員」是一種將新物件裝置委託 (或在機上) 到結構中的裝置。這可能是手機上的應用程序，智能家居網關或 Matter 管理員。
- 物質橋接器會將非 IP 通訊協定裝置連接至 Matter 結構。

有關硬件和軟件可以在 Matter 中承擔的不同角色的信息，請參閱在您的事情智能家居的引擎下偷看（CSA 博客文章）。

與物質認證的優勢

Matter 的引入有望為智能家居消費者和為他們服務的製造商提供顯著優勢。Matter 透過為智慧型裝置建立通用語言，旨在透過簡化的設定、跨平台統一管理，以及擴展語音控制的選擇和靈活性來解開當今零散的市場。

對於消費者而言，這種統一的體驗應該使智能家居的構建和擴展顯著減少複雜和艱鉅。裝置製造商也能透過簡化的認證、降低開發成本和簡化的客戶支援，獲得有意義的優勢。由於 Matter 推動了更大的互操作性並降低了智能家居採用的障礙，這兩個團體都受益 總體而言，Matter 標準的認證有望通過解決迄今為止阻礙它的問題來加速智能家居市場的增長。

主題

物質認證對智慧家庭消費者的好處

Matter 的引入有望為消費者帶來顯著的好處。Matter 為智能家居設備提供了一種通用語言，以便在主要平台上無縫協作。通過使用 Matter 認證設備，消費者可以期望更簡單的智能家居設置和管理，並在控制設備方面獲得更大的靈活性和選擇。

簡化設定與統一管理

消費者面臨的最大挫折之一是操作不同的智能家居設備並使他們協同工作所需的複雜設置和入職過程。每個設備可能需要自己的專有應用程序和單獨的帳戶。為了解決此問題，Matter 會啟用認證裝置的 plug-and-play 功能。入職 Matter 認證的裝置非常簡單，只要將裝置連接到本機家庭網路，然後使用 Matter 管理員 (例如 Alexa 應用程式) 讀取裝置上的 QR 碼即可。

透過單一應用程式提供統一的設定體驗，讓消費者不再需要處理多個不同的應用程式來管理不同品牌的裝置。他們可以通過單個界面查看和控制所有經過 Matter 認證的燈光，鎖，傳感器等。蘋果 HomeKit，Amazon Alexa 和谷歌助理用戶都受益於能夠發現和控制 Metter 設備，而無需下載單獨的製造商應用程序。透過統一的系統簡化智慧家庭裝置管理，可降低消費者的複雜性，並使建置和擴充設定變得不那麼艱鉅。

改善語音控制的選擇與彈性

語音控制已成為消費者與智慧家庭裝置互動的熱門方式。但是，今天語音助手的選擇通常決定了您可以通過語音控制哪些品牌的設備。問題通過在生態系統中啟用語音控制來改變這一點。

消費者可以靈活選擇最適合其需求的語音助理生態系統，而無需擔心設備兼容性。使用 Google 助理的用戶可以通過語音控制其經過 Matter 認證的設備，即使這些設備最初是為 Alexa 或 HomeKit 市場製造的。

語音控制的這種交叉兼容性創造了一個更開放的環境，為用戶提供了更多選擇。他們可以根據功能和價格挑選設備，而不是與單個生態系統的兼容性。如果使用者 future 想要變更語音助理，他們現有的智慧家庭設定可以輕鬆移動，因為所有裝置都會使用通用的 Mature 語言。

物質認證對設備製造商的好處

除了幫助消費者之外，Matter 認證還為智能設備製造商提供了有意義的好處。通過採用 Matter 標準，組織可以獲得降低成本並擴大客戶覆蓋範圍的優勢。

跨生態系統的單一認證

目前，為了確保 Alexa HomeKit 和 Google Home 等生態系統之間的兼容性，製造商需要與每個組織進行多個冗長且昂貴的認證流程。問題通過建立一個通用認證來改變這一點。

設備製造商只需要對其產品進行一次認證，以便與所有主要的智能家居生態系統和語音助手兼容。與現狀相比，這可簡化開發並大幅降低認證成本。隨著產品的更新，資源不再需要花費在維護單獨的認證上。單一物質認證還可以面向未來的產品，即使在新的生態系統出現時也能確保兼容性。

降低開發成本

Matter 也有助於降低製造商的開發成本。通過採用通用的連接和安全標準，組織可以從共享基礎架構組件中受益，這些組織對整個 Matter 項目有貢獻

例如，製造商不再需要在產品中包含自己專有的 Thread 邊界路由器，從而將此責任卸載給集線器製造商。共用的開放原始碼驅動程式和程式庫可進一步減少冗餘的工程 常見的服務發現和設備設置機制意味著需要較少的定制應用程序開發。這些基礎設施和應用程序開發成本的降低可以通過更經濟實惠的智能家居設備的形式傳遞給消費者。

簡化客戶支援

當前智能家居市場的碎片化導致製造商的高客戶支持負擔。消費者經常遇到連線、設定和相容性問題，需要疑難排解。Matter 旨在通過標準化核心功能來減少這些問題。

當問題確實發生時，常見的基礎問題協議意味著公司可以更輕鬆地診斷和解決連接問題，而無需考慮多個生態系統。這簡化了支持過程。透過單一應用程式和通用的語音相容性，客戶也可以更輕鬆地學習使

用裝置，在許多情況下減少支援的需求。Matter 提供簡化的客戶體驗與疑難排解，有助於降低製造商的長期支援成本。

物質認證策略的注意事項

Matter 實現了不同智能家居設備和平台之間的互操作性。但是，對於設備製造商而言，通過 Matter 進行認證可能並不總是最佳選擇。根據裝置類型和使用案例的不同，實施和認證的成本可能不具有實際或財務意義。本節將探討製造商選擇不使用 Matter 認證某些裝置的一些主要原因。

儘管 Matter 標準旨在簡化開發並實現通用兼容性，但某些類型的智能家居設備可能面臨實際障礙，這些認證超過了利益。對於物質中具有嚴格限制、非 IP 協議、受限對象或未定義的設備類型的產品，最初追求 Mate 認證可能不是最佳策略。這可能是製造商可能避免採用物質的原因。但是，Matter 確實允許啟用 IP 的閘道裝置代理非 IP 端點。對於某些舊式裝置，閘道方法可以成為 Matter 相容性的可行途徑，同時避免完整的裝置重新設計。

隨著 Matter 標準的發展，其範圍擴大以涵蓋更多使用案例，認證案例可能會隨著時間的推移而增強，即使對於這些產品類別也是如此。設備製造商需要評估他們的具體情況和藍圖，以確定有關 Metter 合規性的最佳方法。在許多情況下，至少暫時可能存在合理的技術或業務原因，選擇退出認證。

非 IP 連接協議

為了採用物質標準，設備必須在 IP 網絡上運行，例如 Wi-Fi，以太網和線程。非 IP 無線協議，如 Zigbee，Z-Wave 和藍牙 LE，通常用於低帶寬設備。這些通訊協定需要額外的非 IP 至 IP 通訊協定轉換器，才能與 Matter 相容。升級通訊模組或引入翻譯閘道通常會增加裝置的硬體成本。

新增 IP 堆疊支援意味著為網路處理配置更多記憶體和處理能力。這可能超過極低成本和低功率設備的能力。增加額外的記憶體或快閃記憶體來支援 IP 也會增加製造成本並縮短電池續航力。對於需要開啟和關閉電源或感測器資料的使用案例，非 IP 通訊協定可提供有效的解決方案。

Matment 基本上排除了認證任何依賴專有、非 IP 無線標準的設備。這可能會限制想要為其低端產品使用替代連接方法的製造商。雖然基於 IP 的協議（如 Wi-Fi 和乙太網絡）對於連接不同的生態系統是必要的，但非 IP 標準仍然具有某些應用中傳感器和交換器的基本連接性的優勢。

硬體限制

另一個挑戰是，Matter 需要最低級別的設備上處理能力和內存來支持必要的軟件堆棧。但是，由於成本和尺寸的限制，最基本的智能家居設備的嵌入式芯片功能通常非常有限。

例如，一個簡單的門窗感測器可能只包含一個小於 100 KB 快閃記憶體和 10 KB RAM 的微控制器。這並不能為完整的 Matter 實作提供足夠的儲存空間和處理預留空間。添加更強大和昂貴的矽將顯著提高材料清單。

在成本和規模是首要任務的情況下，製造商可能會發現 Matter 需求與其硬件預算不一致。使用 Matter 認證非常基本的感測器、開關或控制器，可能會強制不必要的硬體升級，進而影響可負擔性。

客戶生態系統

另一個要考慮的因素是製造商的目標客戶群是否使用與 Matter 兼容的智能家居平台。如果該區段中的大多數消費者不使用 Matter 控制器或啟用 Matter 的中樞和應用程式，則認證產品的動機可能很少。

例如，專注於服務老年使用者需求的公司，可能會發現他們的客戶在沒有 Matty 管理員的情況下擁有簡單的設定 或者 do-it-yourself （DIY）家庭自動化愛好者可能更喜歡定制解決方案，並且不需要 Matter 跨品牌的 plug-and-play 經驗。

在目標人口統計與 Matter 基礎架構無關的情況下，認證會增加複雜性，而沒有明確的收益。資源可能會更好地花在相關平台中優化用戶體驗，而不是將努力轉移到 Metter 合規性上。

尚未定義裝置類型

Matter 目前僅定義常見智慧家居類別的裝置設定檔和規格，例如照明、HVAC、鎖、百葉窗和娛樂。在這些已定義區域之外的任何利基產品類型都必須使用自訂描述檔，直到裝置類型標準化為止。列出垂直行業以外的設備類別，例如灌溉控制器，游泳池設備和利基設備，尚無法使用 Matter。

如果公司開發的獨特裝置類型並未涵蓋在現有的 Matter 設定檔中，則除非草擬新的描述檔，否則無法進行認證。這可能會延遲新產品的推出，同時等待 Matter 擴大其範圍。

一些製造商可能更喜歡通過專有手段更快地將利基解決方案推向市場，而不是擱置發布創新。在相關配置文件成熟後，稍後認證仍然是一種選擇。對於先發者的優勢，在某些情 direct-to-consumer 況下，無物質可能更好。

替代方法：在閘道上進行代理

如果端點裝置具有無法直接認證的限制，則另一種方法是在閘道上代理裝置的「物件」功能。閘道可做為端點的本機無線通訊協定與以 IP 為基礎的 Matty 通訊協定之間進行轉換的橋接器。

例如，通過專有無線電標準進行通信的基本溫度傳感器仍然可以顯示為 Matter 設備給 Matter 管理員。閘道在非 IP 介面上接收感應器資料，但會將透過 IP 代表該資料的虛擬物件實體公開給控制器。這可讓您使用現有的硬體，並透過閘道取得一些互通性優勢。

當然，這會增加開發人員的複雜性，並且需要閘道來支援必要的翻譯層。但是，如果直接認證對設備本身來說太具挑戰性，這可能是一個可行的折衷方案。代理可以幫助低功耗或利基解決方案參與 Metter 生態系統，而無需進行完整的硬件大修。

與物件的雲端連線

儘管 Matter 可實現基本的本機裝置互通性，但需要額外的雲端連線能力才能提供強大的 over-the-air 更新、遙測資料、遠端管理，以及與專屬廠商服務的整合 裝置製造商提供多種選擇，例如運送 Matter 閘道中樞、使用家用的 Matter 認證中樞，或將直接雲端連線整合至端點。M atter-to-cloud 連接的標準正在出現，但製造商仍然需要將其他連接軟件堆疊整合到 Metter 設備中。在診斷和新功能更新等領域提供智慧家用裝置的全部價值，要求 Metter 製造商必須考慮雲端整合，而不是基本的本機作業。

透過雲端連線，為物質端點啟用進階裝置功能

Matter 標準承諾透過共同的通訊協定統一來自不同廠商的 IoT 裝置。它指定智慧家庭裝置如何透過使用以 IP 為基礎的網路技術 (例如乙太網路、Wi-Fi 和執行緒) 在區域網路上相互探索、通訊和互通。這種本地互通性使得來自不同供應商的 Matter 認證設備能夠無縫協同運作，以進行自動場景和語音控制等活動。但是，Matter 不會為裝置端點定義雲端介面或需要網際網路連線。

如今，許多智能設備依賴額外的雲連接來獲得關鍵功能，例如 over-the-air （OTA）更新，遠端訪問以及與製造商平台的集成。設備製造商希望打造符合 Matter 標準的產品，同時保留高級功能，在使用雲端連接補充 Matter 方面面臨一些設計考量 雖然基本的本機控制和語音助理整合可用於簡單的 Metter 裝置，但需要額外的雲端連線才能啟用更進階的功能。

需要雲端連線的使用案例

儘管 Matter 可以處理本地設備的互操作性，但額外的雲連接能力可實現多種重要的智能家

- O ver-the-air (OTA) 更新 — 透過網際網路提供韌體和軟體更新，可讓廠商輕鬆增強已部署的裝置。如果沒有 OTA，更新將被手動處理。儘管 Matter 標準描述了如何處理 OTA 更新並將其傳遞到 Matter 認證的端點，但它取決於端點所連接的 Metter Hub 支持的功能。此外，提供給端點的更新也有限制。例如，當端點要求更新時，只會提供可用的最新更新。所有相同類型的設備都提供了一次更新。沒有選項可以進行順序更新，甚至無法進行 OTA 回滾或刪除更新。在端點上啟用雲連接可以減輕 OTA 更新的精細管理缺乏的問題。
- 遠端存取和控制 — 從家用網路外部遠端存取和控制裝置需要雲端端點。正如目前所定義的物件，僅支援本機存取。雖然 Matter 端點可以透過區域網路內的使用者應用程式進行控制，但只有在 Matty Hub 支援的情況下，才能使用遠端控制。即使如此，通常情況下，只有基本的遙控器可用。
- 遙測和診斷 — 在雲端彙總現場資料，例如錯誤日誌和感應器串流，可讓廠商監控裝置健康狀況並識別問題。儘管 Matter 透過一般診斷叢集支援無線電和通訊協定相關的診斷，但任何特定於裝置的詳細診斷都需要雲端連線，以便製造商可以從裝置擷取資料。

- 供應商特定的整合 — 任何未在問題規範中定義的自訂功能和資料類型都需要連線至供應商雲端平台。
- 外部集成 — 鏈接到第三方服務，例如不在 Matter 生態系統上的語音助理或第三方支付網關（根據用例需要）需要在 Matter 管理員之外的互聯網連接。

有了這些仰賴雲端連線能力的關鍵功能，Metter 端點通常需要額外的網際網路存取選項。

啟用雲端連線的架構

對於 Matter 設備，有三種通用方法可以在滿足本地操作規範的同時提供必要的雲端連接。

內置網關的智能家居集線器

一些設備製造商可能會選擇運送專有的家庭中樞，該中樞結合了 Matter 管理員和其雲端服務的閘道。這個家庭中樞可以根據標準在本地管理連接的 Matment 端點，同時還促進了高級功能的雲連接。該集線器可以支持 OTA 更新，遠程訪問和端點的遙測收集。

將雲端連線卸載到現有的 Matty 中樞

而不是捆綁一個自定義集線器, 設備可以被設計為與物質集線器，如 Amazon 迴聲或谷歌主頁連接互聯網連接. 在這種情況下，現有的 Matty Hub 會根據標準處理本機裝置通訊，並且還為需要它的端點提供通往雲端的閘道。這利用了消費者可能已經擁有的基礎結構。但是，這種方法取決於 Matter Hub 針對標準中未指定為標準中心規範的功能所提供的支援層級。

端點中的直接雲端連線

具有直接互聯網連接的設備（例如 Wi-Fi）可以為 Matter 本地網絡和供應商雲服務集成單獨的連接。這可讓裝置充當自己通往雲端的閘道。但是，對於依賴通訊協定 (例如 Thread) 的非 Wi-Fi 端點，則需要解決方案。這使得設備可以獨立連接到雲，但對於簡單，低成本，電池供電的設備可能不可行。

橋接物質與製造商雲端平台

儘管 Matter 簡化了本地互通性，但需要額外的努力才能順利連接 Matter 管理系統和製造商的雲平台諸如連接標準聯盟（CSA）之類的 Organizations 正在努力將 Matter 設備與雲端連接的方式標準化，以獲得 OTA 更新等功能。廣泛採用這種雲連接標準將使設備製造商的開發變得容易。

最佳路徑取決於特定產品的使用案例、價格點和商業模式。顯然，對雲服務的強大訪問是必要的，以釋放智能家居消費者所期望的完整功能-即使是專注於本地互操作性的 Matter 兼容設備也是如此。設備製造商有機會使用 Matter 進行互操作性，同時仍通過精心設計的雲連接提供高級功能。

安全

設計上的安全性是在設備設計階段整合安全功能的做法，而不是在後期開發階段作為事後的考慮。加密通信和 over-the-air （OTA）更新是安全性設計的示例。Matter 透過從值得信賴、安全的製造設施開始實施安全性，為智慧家庭裝置提供堅實的基礎。物質裝置只能由已知、受信任的產品證明授權單位 (PAA) 憑證授權單位 (CA) 的擁有者製造和佈建。

裝置驗證

物質裝置必須先對彼此和控制器進行驗證，才能進行通訊。只有經過授權的裝置才能連接至 Matter 結構。在製造過程中，裝置會佈建唯一識別碼和 X.509 憑證，稱為「裝置驗證憑證」(DAC)。當裝置第一次嘗試連線至 Matter 結構時，專員裝置會檢查 DAC 的有效性，並由已知且受信任的產品驗證中間 (PAI) CA 簽署。專員設備還會檢查嘗試連接到網絡的設備是否遵守 Matter 的規格，協議和安全標準。只有在所有檢查都成功時，才會授與裝置存取 Matter 網狀架構。

加密通訊

在授與裝置存取 Matter 網狀架構之後，裝置之間傳送的所有資料都會受到強大的加密保護。使用多層方法可保留資料完整性。事項專員使用 ECC-256 秒 256r1 曲線執行金鑰交換和簽名驗證。交換金鑰之後，Matty 裝置會使用 AES-256 加密傳輸中的資料。對於每個消息，設備使用 SHA-256 算法來驗證數據在傳輸過程中沒有被篡改。

O ver-the-air 更新

Matter 標準還要求設備為 over-the-air （OTA）更新實施強大的安全狀態。OTA 是智能家居生態系統的關鍵組成部分，因此設備可以接收安全更新以及新功能。Matter 裝置的每個韌體更新都必須由製造商的私密金鑰簽署。該設備通過使用相應的非對稱公鑰驗證有效負載簽名。驗證有效負載的簽名後，設備可以將映像提交到其引導加載程序並重置。在開機程序期間，裝置必須再次驗證映像檔以確保其未遭竄改，而且裝置也會驗證其執行的是最新的已知版本。

物質發展

使用

Amazon 為物質開發提供了一套全面的工具。這些工具為建立與所有主要生態系統相容且可與 Amazon Alexa 無縫協作的 Matter 產品提供快速途徑。

程序:工作與 Alexa

該程序可確保您連接 Alexa 的設備提供出色的客戶體驗。與 Alexa 合作 (WWA) 徽章可增加客戶信心，協助推動您認證裝置的偏好。如需詳細資訊，請參閱宣布事項啟動和與 Alexa 合作 (WWA) 適用於物質裝置的作品 (Amazon 部落格文章)。

SDK: 使用 Alexa 開發問題

此 SDK 可讓您將本機 Metter 連線新增至裝置，同時包括受管理的雲端連線、商業智慧和 OTA 支援。如需詳細資訊，請參閱使用 Alexa 充分利用問題。

套件：Alexa 環境家庭開發套件

該套件可幫助您跨協議與設備集成，以便使用 Alexa 構建環境和統一的智能家居。有關更多信息，請參閱 Amazon Alexa。

端點：佣金端點

對於技能連接的問題裝置，可佣金端點 API 可建立與 Alexa 裝置之間的本機、基於事項的連線，而無需客戶在獲得其許可的情況下執行任何步驟。有關更多信息，請參閱亞歷克薩斯。可佣金界面 1.0（Alexa 技能套件）。

AWS 私有 CA 對事項的支持

AWS Private Certificate Authority (AWS 私有 CA) 提供使用「物質」標準的指引。

用於物質的 DAC

事項需要裝置證明憑證 (DAC)，該憑證必須由符合「物質公開金鑰基礎架構 (PKI)」憑證原則 (CP) 的裝置證明 CA 核發。裝置廠商可以用 AWS 私有 CA 來執行下列動作：

- 主控產品證明授權單位 (PAA) 憑證授權單位 (CA)

- 主控產品證明中繼 (PAI) CA
- 發出、簽署和維護每個裝置的 DAC

如需詳細資訊，請參閱 AWS 安全性部落格中的「用 AWS Private Certificate Authority 於核發物件的裝置驗證憑證」。

物質基礎設施

AWS 提供範例，示範如何為 M AWS Cloud Development Kit (AWS CDK)atter 設定 PKI 基礎結構。您可 AWS 私有 CA 以使用來滿足事項 PKI CP 的要求。如需詳細資訊，請參閱上的事項 PKI CDK 專案。 GitHub

爪哇範例

AWS 私有 CA 提供 Java 範例，用於建立符合 Matter 標準的產品證明授權單位 (PAA) 憑證、產品證明中繼 (PAI) 憑證，以及裝置驗證憑證 (DAC)。如需詳細資訊，請參閱 AWS Private Certificate Authority 文件中的使用 AWS 私有 CA API 實作問題標準 (Java 範例)。

PKI 合規性事項指南

此事項 PKI 合規性指南說明如何實作並展示符合 CSA 事項 PKI CP 要求。它提供有關如何用來 AWS 私有 CA 建立和操作符合 Matter 標準的憑證授權單位 (CA) 的資訊。

常見問答集

Mature 的會員等級是什麼？

截至 2023 年 1 月，事項具有以下四個級別的會員資格。

會員類型	年會費 (美元)	描述
主持人	105,000 美元	領導聯盟，並獲得所有標準的最終批准，擁有董事會席位，並參加董事會委員會
參與者	二萬元	為標準做出貢獻並取得草案規格，加快上市速度
採納者	七千元	使用已核准的規格來建置和認證產品
助理	0 元 *	透過認證轉移計劃標示認證產品

* 對於白標或重新品牌產品的經銷會員，每件產品的初始費用為 2,500 美元（美元），每項產品每年的持續費用為 500 美元。

您選擇的會員級別取決於您對產品認證（採用者）或在標準（參與者）中定義產品類型的興趣。如需有關會員資格等級的詳細資訊，請參閱 CSA 網站上 IoT 的未來影響。

智能家居消費者如何從物質中受益？

消費者通過以下方式從物質中受益：

- 在家中簡化 Metter 裝置的上線作業
- 通過單個應用程序統一管理所有智能家居設備
- 從不同生態系統的一個或多個語音助理進行設備控制

如需詳細資訊，請參閱本指南中的 物質認證對智慧家庭消費者的好處。

設備製造商如何從 Matter 中受益？

設備製造商通過以下方式從 Matter 中受益：

- 一個設備的單一認證，而不是每個生態系統的多個認證, 如 Amazon Alexa, 或谷歌主頁.
- 不再需要開發應用程序
- 由於不需要運送基礎架構元件 (例如執行緒邊界路由器)，可降低材料成本
- 降低支援有基礎架構和連線問題的客戶的成本

如需詳細資訊，請參閱本指南中的 物質認證對設備製造商的好處。

物質是否取代 Wi-Fi，藍牙或線程？

否，Metter 是在 IP 網路上執行的應用程式層級通訊協定。使用 Wi-Fi，以太網或線程進行連接的設備可以通過 Metter 認證。下表總結了物質與 Wi-Fi，藍牙和線程的對比。

功能	物質	Wi-Fi	藍牙	Thread
用途	智慧家庭通訊	網際網路存取與資料傳輸	短距離無線通訊	低功耗無線網狀網路
範圍	根據基礎協議而異	最遠可達 300 英尺	最大可達 30 英尺	最遠可達 300 英尺
頻寬	根據基礎協議而異	高達每秒 10 千兆位元	每秒最多 2 兆位元	高達每秒 250 千位元
耗電量	根據基礎協議而異	相對較高	相對較低	非常低
安全	根據基礎協議而異	WPA2, WPA3	AES、BLE 安全連線	AES
費用	根據設備而異	相對便宜	相對便宜	相對昂貴

什麼是供應商 ID 和產品 ID？

CSA 會員可以申請將其識別為供應商的廠商 ID。此後，公司的產品將被分配給此 ID，並且可以追溯到其來源。此外，他們還會收到唯一的產品 ID。16 位數的數字代碼伴隨著護照號碼等產品，並使其成為供應商的明確無誤。

哪些設備需要通過 Metter 認證？

任何需要進行身份驗證並成為 Matter 結構一部分的設備都需要獲得 Matter 認證。但是，那些設計為僅通過非標準（專有）協議與供應商指定的集線器進行交互的設備不會受益於 Matter 認證過程。例如，智能家居安全系統集線器必須通過認證為物質投訴，但與集線器通信的門窗傳感器不需要被認證為 Metter 兼容。獲得 Matter 產品認證的選擇主要由此考慮驅動。

我的產品類型目前未在「物質」中定義。我應該預算哪些額外任務來獲得 Matter 認證的產品？

物質規格不支持所有類型的設備。如果您的裝置類型不受支援，第一步是以參與者的身分加入 CSA。這需要您對 CSA 的財務和時間投資。身為參與者的成員，您可以領導裝置類型的定義，並可存取草案規格，以實現更快的 go-to-market 策略。如需有關會員資格等級的詳細資訊，請參閱 CSA 網站上 IoT 的未來影響。

我的一些設備直接連接到家庭 Wi-Fi 網絡。這些設備是否需要通過 Metter 認證？

物質認證可以使直接連接到智慧家庭網路的裝置受益，因為它們可以連接到 Matter 網狀架構。這可讓消費者透過同一個 Matter 網狀架構上的虛擬助理來控制裝置。但是，消費者必須將特定於設備的應用程序用於特定於供應商且未在 Matter 規範中定義的任何操作。

資源

AWS 資源

- 使用 Alexa 充分利用物質
- 宣布與 Alexa（WWA）用於物質設備的物質啟動和介紹合作（Amazon Alexa 博客）

IoT 連接標準聯盟 (CSA)

- 美安官方網站
- CSA 認證程序概觀
- CSA 授權測試提供商
- 物質規格

文件歷史記錄

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5 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：將您的現場部署 Oracle 資料庫遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

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

經常用於經常性問題的解決方案，其中解決方案具有反生產力、無效或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

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

人工智慧 (AI)

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

人工智慧操作 (AIOps)

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

非對稱加密

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

原子性、一致性、隔離性、耐久性 (ACID)

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

屬性型存取控制 (ABAC)

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

授權資料來源

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

可用區域

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

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

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

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

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

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

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

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

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

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上為資訊編製索引的 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，以及透過核准的程序，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。

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 遷移策略相關的詳細資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

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

冷快取

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

冷資料

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

電腦視覺 (CV)

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。

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

數位分身

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

維度資料表

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

災難

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

災難復原 (DR)

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

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

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。對於需要特定格式、推理或網域知識的任務，少量的提示可以有效。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，以及自然語言的交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

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

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

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

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程會被視為舊版，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、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

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

高可用性 (HA)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統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。

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、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在操作時強化和改善自身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。

成員帳戶

除了屬於組織一部分的管理帳戶 AWS 帳戶 之外的所有 AWS Organizations。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)

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，請參閱此詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

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

現代化準備程度評定

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

單一應用程式 (單一)

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

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

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

可變基礎設施

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

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

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

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

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

操作水準協議 (OLA)

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

操作整備審查 (ORR)

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

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造業中，整合 OT 和資訊技術 (IT) 系統是工業 4.0 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱操作整合指南。

組織追蹤

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。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，並改善查詢效能。

預防性控制

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

委託人

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

依設計的隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

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

主動控制

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

產品生命週期管理 (PLM)

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

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

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

擬匿名化

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

發佈/訂閱 (pub/sub)

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

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

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

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強產生。

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、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 Rs。

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 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 秘密中的什麼內容？。

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。

SIEM

請參閱安全資訊和事件管理系統。

單點故障 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

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

SPOF

請參閱單一故障點。

星狀結構描述

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

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作

為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

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

系統提示

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

T

標籤

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

目標變數

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

任務清單

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

測試環境

請參閱 環境。

訓練

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

傳輸閘道

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

主幹型工作流程

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

受信任的存取權

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

調校

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

雙比薩團隊

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

U

不確定性

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

也稱為繁重工作，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

危及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，並防止資料遭到刪除或修改。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瑕疵或漏洞。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。