運用 Amazon Web Services 更新您的 Microsoft 應用程式，因應現今需求

如何開始著手進行

2016 年 3 月

注意

本文件資訊僅供參考，其內容為文件發佈日當時 AWS 的最新產品項目與實務方法，如有變更，恕不另行通知。客戶需自行獨立評估本文件資訊，任何 AWS 產品或服務皆以「現狀」提供，不包含任何明示或暗示性保證。本文件不提供任何來自 AWS、其附屬公司、供應商或授權人之任何保證、表示、契約承諾、條件或擔保。AWS 對其客戶的責任與義務由 AWS 協議進行控管，本文件並非 AWS 與其客戶之間的任何協議的一部分，也並非修改上述協議。

目錄

摘要

雲端是現今大多數企業 IT 策略的核心。許多企業發現，採用精心規劃的「直接遷移」模式轉移至雲端，能夠立即獲得回報。本白皮書適用於以 Microsoft 作業環境為主的組織決策者和 IT 專業人員。他們想採用雲端式 IT 架構，且為因應現今需求，須全面更新那些目前以 Microsoft Windows Server 和 Microsoft SQL Server 建置的關鍵業務應用程式。本白皮書說明透過 Amazon Web Services (AWS) 更新應用程式的效益，以及如何開始著手進行。

為什麼要針對現今需求更新應用程式？

對許多 IT 組織而言，針對現今需求來更新應用程式是一項重大的計畫，這主要有下列幾項原因：

- **移除舊的過時軟體**

  避免花費時間及成本維護舊的過時軟體和不支援的版本 (Windows Server 2003、SQL Server 2003 和 SQL Server 2005)，也可免除與效能及可靠性相關的挑戰。

- **DevOps 策略**

  目地為善用新的 DevOps 與應用程式生命週期管理方法。透過轉移至新的應用程式交付平台，公司可加快創新的速度。

- **行動性提案**

  當使用者改用行動裝置時，對 IT 服務的使用量可能會急遽暴增。如果應用程式沒有準備好因應，會帶來可擴充性方面的挑戰。

- **新產品的推出**

  新產品的推出，可能會造成對 IT 服務的需求急遽暴增。相依的基礎應用程式 (包括 Microsoft SQL Server 和 Microsoft SharePoint) 必須具備所需的規模，才能支援新產品的推出。

- **併購 (M&A) 活動**

  在進行併購時，工作會越來越複雜。在多次併購後，公司可能會有數百個 SharePoint 站點、多個 Exchange 執行個體，以及數不清的 SQL Server 資料庫。簡化不同應用程式的管理，經常是艱鉅的任務。

為什麼要在 AWS 上執行 Microsoft 應用程式？

在最近的一項調查中[1]，國際數據資訊公司 (IDC) 的報告指出，有 50% 的受訪者使用 AWS 來支援其生產力應用程式 (例如 Microsoft 所提供的產品)。而在這些受訪者中，有 65% 表示已計畫增加使用 AWS，他們願意將現有的應用程式轉移至 AWS，或是擴充已經在 AWS 上執行的應用程式。很顯然，客戶已經開始更新自己的 Microsoft 應用程式，以因應現今的需求。

適用於企業應用程式的 AWS

客戶可在 AWS 雲端中，執行 Microsoft Windows Server 上所建置的企業應用程式，以改善其安全機制、應用程式效能及可靠性。例如，客戶可在 33 個 AWS 可用區域的任一區中，部署能夠從全世界各地存取的 SharePoint 環境，只要幾小時就能完成。為了簡化工作，客戶可以使用 AWS 工具，這些工具整合了 Microsoft 的管理與存取控制應用程式，例如 System Center 和 Active Directory。客戶也可使用 AWS CloudFormation 範本，以可靠的方式重複部署應用程式。

適用於 LOB 應用程式與資料庫的 AWS

事業單位 (LOB) 業主正在執行的應用程式涵蓋各領域，包括石油與天然氣探勘、零售銷售點 (POS)、金融、健康照護、保險、製藥、媒體和娛樂。為了加快建置時間並簡化工作，客戶可以開啟預先設定好的 Amazon Machine Image (AMI) 範本，此範本包含了完全相容的 Microsoft Windows Server 與 Microsoft SQL Server 授權。

適用於開發人員的 AWS

在 AWS 上進行開發工作的客戶可使用 Microsoft 開發工具，包括 Visual Studio、PowerShell 和 .NET Developer Center。這些工具如果能結合 AWS CodeDeploy、AWS Elastic Beanstalk (Elastic Beanstalk) 和 AWS OpsWorks 所具備的可擴充性與彈性，客戶就能夠在更低風險的情況下，以更快的速度完成開發工作，並在 AWS 上部署程式碼。

[1] http://www.idc.com/getdoc.jsp?containerId=256654

我可以在 AWS 上執行哪些 Microsoft 應用程式？

我們的客戶已經成功將幾乎所有的 Microsoft 應用程式部署到 AWS 雲端上，包括：

- Microsoft Windows Server
- Microsoft SQL Server
- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft Dynamics CRM 與 Dynamics AX、Dynamics ERP
- Microsoft SharePoint Server
- Microsoft System Center
- 商務用 Skype (前身為 Microsoft Lync)
- Microsoft Project Server
- Microsoft Visual Studio Team Foundation Server
- Microsoft BizTalk Server
- Microsoft Remote Desktop Services

我該如何開始？

如果是企業，第一步驟就是先判斷在超過 50 種 AWS 服務中，要使用哪些來執行應用程式更新計劃。下列圖表為企業 IT 組織一般功能與 AWS 方案的對照圖。本白皮書說明了此對照圖中的重要服務，以及這些服務如何用來執行 Microsoft 應用程式更新計劃。

圖 1：企業 IT 與 Amazon Web Services 的概念對照圖

安全性與存取

> 我們與 AWS 合作，開發出一項安全模型，能夠讓我們更安全地在 AWS 中運作，而且甚至比自己資料中心的運作還安全。
>
> — Capital One 資訊長 Rob Alexander

現今越來越關切與注重安全性，大多數客戶也開始選擇能夠確保合規和降低管理風險的服務。AWS 雲端中也同樣採用傳統資料中心的安全隔離模式，包括實體安全性、網路分隔、伺服器硬體及儲存隔離。AWS 已通過 ISO 27001 認證，並獲得支付卡產業 (PCI) 資料安全標準 (DSS) 的 Level 1 服務供應商認證。AWS 每年都會接受服務機構內部控制 (SOC) 第 1 類稽核，也已成功獲得美國聯邦政府系統的中級評等，以及美國國防部資訊保證認證與驗證流程 (DICAP) 中的國防部 (DOD) 系統 Level 2 認證。

如果企業想尋找一套適合的安全性與權限服務，AWS 虛擬私有網路、AWS Direct Connect 和 AWS Directory Service 皆為可考慮的選項。Amazon Virtual Private Cloud (Amazon VPC) 可讓客戶將 AWS 資源啟動至已定義的虛擬網路。此虛擬網路非常近似於現場部署資料中心的傳統網路，卻可提供 AWS 可擴展基礎架構的效益。

AWS Direct Connect 透過私有的 1 GB 或 10 GB 乙太網路光纖纜線，將組織的內部網路連結至 AWS。纜線的一端連結至資料中心的路由器，另一端則連結至 AWS Direct Connect 的路由器。建立此加密連線後，客戶即可繞過網路路徑上的網際網路服務供應商，建立直接連結 AWS 雲端 (例如，連結至 Amazon Elastic Compute Cloud (Amazon EC2) 和 Amazon Simple Storage Service (Amazon S3) 與 Amazon VPC 的虛擬介面。

AWS Directory Service 是一項託管服務，能夠讓客戶輕鬆將 AWS 服務連結至現有的現場部署 Microsoft Active Directory (透過 AD Connector 的使用)，或是在 AWS 雲端中建立並運作新的目錄(透過使用 Simple AD 和AWS Directory Service for Microsoft Active Directory)。

透過伺服器端和用戶端同時加密的選項，可針對傳送中 (透過 SSL) 和靜態的資料，提供資料加密服務。AWS Certificate Manager (ACM)、AWS Key Management Service (AWS KMS) 和 AWS CloudHSM 可搭配使用，以確保提供金鑰與憑證管理服務，進而安全產生、儲存和管理資料加密所使用的加密金鑰。

最後，AWS WAF 提供了 web 應用程式的防火牆服務，能夠保護這些應用程式免於受到常見的網路攻擊，不會影響到應用程式的可用性、安全性或消耗過多資源。

運算：在 EC2 執行個體上運作的 Windows Server

> 我們沒時間重新設計應用程式，AWS 雲端可讓我們在 Windows Server 2003、各種 Microsoft SQL Server 及 Oracle 資料庫和穩定耐用的 Citrix 環境上，執行舊版 32 位元應用程式。
>
> — Hess 首席架構師 Jim McDonald

制定安全策略後，就要針對需更新的應用程式，檢視支援這些應用程式的基礎架構。

Amazon EC2 是一項 web 服務，提供可調整大小的運算容量，以用來建置和託管軟體系統。設計執行於 Amazon EC2 上的 Windows 應用程式時，客戶可根據各種需求，計劃如何快速部署並快速縮減運算與儲存資源。當客戶在 EC2 執行個體上執行 Windows Server 時，不必像針對現場部署的 Windows Server 一樣佈建確切的硬體系統套件、虛擬化資源、軟體和儲存空間。客戶反而可以專注於使用各種雲端資源，來改善 Windows 應用程式的可擴充性與整體效能。啟動執行 Windows Server 的 Amazon EC2 執行個體後，此執行個體就會像執行 Windows Server 的傳統伺服器一樣運作。例如，無論 Windows Server 是部署於現場或 Amazon EC2 執行個體上，皆可執行 web 應用程式、進行批次處理，或管理需要大量運算的應用程式。客戶可使用遠端桌面協定，從遠端直接存取 Windows Server 執行個體，輕鬆進行管理。客戶可針對單一 Windows Server 執行個體執行 PowerShell 程式碼，也可針對整個伺服器群組，使用 Amazon EC2 Run Command。

針對 Amazon EC2 所建置的應用程式，依隨需模式使用底層的運算基礎架構。這些應用程式會隨需取用資源 (例如儲存空間和運算能力) 執行工作，並在完成時釋出資源。此外，這些應用程式也常在工作完成後自行終止。在運作期間，這些應用程式可根據需要的資源，彈性進行擴充或縮減。Elastic Load Balancing 會自動將傳入的應用程式資料分送給雲端中的多個 Amazon EC2 執行個體。這可讓客戶達成更高層的應用程式容錯能力，無縫提供所需的負載平衡能力，以分配應用程式傳輸資料。

Auto Scaling 可讓客戶密切跟隨應用程式的需求曲線來進行調整，不需事先以手動方式來佈建容量。例如，客戶可設定條件，一旦 Amazon EC2 群組的平均使用率高，即可在 Auto Scaling 群組中遞增加入新的 Amazon EC2 執行個體；同樣地，客戶也可設定條件，一旦 CPU 使用率低，即可遞減移除相同數量的執行個體。

資料庫：在 Amazon RDS 或 Amazon EC2 上運作的 SQL Server

> Amazon Relational Database Service (Amazon RDS) 可讓我們的 DBA 團隊減少花在處理日常維護作業的時間，將時間拿來研究如何加強系統。Elastic Load Balancing 功能也讓我們不需再使用昂貴複雜的負載平衡器，但仍能保有必要的功能。
>
> — Kaplan 技術服務總監 Chad Marino

進行更新規劃的另一個重要建構模塊，就是資料庫服務的選擇。客戶如果想要針對雲端中所部署的 SQL Server 進行管理、擴充和調整，可以使用 Amazon RDS，或是在 Amazon EC2 上執行 SQL Server。

客戶如果希望讓 AWS 來處理 SQL Server 資料庫的日常管理工作，則可選擇 Amazon RDS，因為此項服務可讓客戶輕鬆設定、操作和擴充雲端中的關聯式資料庫。Amazon RDS 會針對 SQL Server 資料庫自動進行安裝、磁碟規劃佈建與管理、修補程式、版本小幅升級、失效執行個體的更換，以及備份和復原。Amazon RDS 也可針對多個可用區域 (Multi-AZ) 自動進行同步複寫，打造出由 AWS 完全管理且具備高度可用性及可擴展性的環境。這能讓使用者專注於更高階的工作 (例如結構描述最佳化、查詢調校，以及應用程式開發)，而省去維護和操作資料庫的一般性工作。Amazon RDS for SQL Server 支援 Windows 身份驗證機制，讓客戶能夠更輕鬆地針對 SQL Server 執行個體存取並管理 Amazon RDS。

Amazon RDS for SQL Server 支援 Microsoft SQL Server Express、Web、Standard 和 Enterprise 版本。客戶不需另外購買授權，即可使用 SQL Server Express，此軟體適合小型工作負載或概念驗證的部署。SQL Server Web Edition 最適合開放給公有與網際網路存取的 web 工作負載。SQL Server Standard Edition 適合大多數的 SQL Server 工作負載，可採用 Multi-AZ 模式部署。SQL Server Enterprise Edition 是功能最豐富的 SQL Server，也可採用 Multi-AZ 模式部署。

管理服務：Amazon CloudWatch、AWS CloudTrail、Run Command

> CSS 自動啟動執行個體的方式，將啟動專案的時間縮短了約 75%。之前需要花四天完成的工作，現在只需要一天。我們不用一直從頭開始重新建置 web 和資料庫伺服器，只需複製並重複使用映像就能完成。
>
> — Unilever 企業架構師 Nick Morgan

AWS 為企業提供了一套完備的管理服務：

- **Amazon CloudWatch**：客戶可以使用 Amazon CloudWatch，針對 AWS 上正在執行的 AWS 資源和應用程式，進行即時監控。CloudWatch 警示功能會根據客戶所制定的規則來發送通知，並自動對所監控的資源進行變更。
- **AWS CloudTrail**：客戶可運用 AWS CloudTrail 來監控其雲端中的 AWS 部署，針對其帳戶中所進行的 AWS API 呼叫動作取得歷程記錄，包括透過 AWS 管理主控台所進行的 API 呼叫動作、AWS SDK、命令列工具，以及高階的 AWS 服務。客戶也可得知，哪些使用者和帳戶針對支援 CloudTrail 的服務，呼叫了 AWS API，以及進行呼叫的來源 IP 位址和呼叫的時間。CloudTrail 可使用 API 來整合至應用程式，以自動建立組織的追蹤記錄、查看追蹤記錄的狀態，並控制管理員開啟和關閉 CloudTrail 登入的方式。

- **Amazon EC2 Run Command**：用來自動進行常見的管理工作，例如套用至數百個虛擬機器的修補程式管理或組態更新，客戶可使用 Amazon EC2 Run Command，這項功能提供了簡單的方法來執行 PowerShell 程式碼。Run Command 已經與 AWS Identity and Access Management (IAM) 解決方案整合，以確保管理員只能存取自己所負責機器的更新內容。所有的更新皆透過 AWS CloudTrail 進行稽核。

適用於 Microsoft System Center 的 AWS 外掛程式 可擴充現有 System Center 系統的功能，以搭配 Microsoft System Center Operations Manager 和 Microsoft System Center Virtual Machine Manager 使用。安裝完成後，客戶可使用熟悉的 System Center 介面，針對 AWS 雲端中的 Microsoft Windows Server 資源以及現場佈署的 Windows Server，來檢視和管理 Amazon EC2。

運用 AWS Marketplace 完成解決方案

客戶經常會有自己偏好的獨立軟體廠商 (ISV)，為其提供專門的軟體解決方案，以增強安全性、商業智慧和儲存等機制。AWS Marketplace 是一個線上商店，讓客戶能夠輕鬆搜尋、採購和部署自己所需的軟體和服務，以建置解決方案和執行其業務。AWS Marketplace 提供超過 2,600 家廠商的清單，涵蓋超過 35 種類別，客戶只要按幾下按鈕，就能在線上接受使用者合約、選擇定價選項，以及自動部署軟體與相關的 AWS 資源，簡化了客戶的軟體授權與採購作業。AWS Marketplace 也可每月定期提供一張發票，詳細列舉業務軟體和 AWS 資源的使用與計費，為客戶簡化發票單據作業。AWS Marketplace 上顯示了各種方案，由 SAP、Tableau、NetApp、Trend Micro、F5 Networks 和其他許多廠商提供。客戶可透過 Marketplace 的合作夥伴來存取 Microsoft 應用程式，例如 Microsoft Windows Server、Microsoft SQL Server 和自訂 AMI 的 Microsoft SharePoint。

授權選項

客戶可選擇在 AWS 雲端中使用新的或現有的 Microsoft 軟體授權。如果是新的應用程式，客戶可購買已包含授權的 Amazon EC2 或 Amazon RDS 執行個體。如此一來，客戶即可直接從 AWS 取得完全符合的 Windows Server 和 SQL Server 新授權。客戶可採用「隨收隨付」的模式來使用這些授權，不需付出前期成本或長期投資。客戶可選擇 AMI 只安裝於 Microsoft Windows Server，或同時預先安裝的 Windows Server 和 Microsoft SQL Server。客戶存取授權 (CAL) 也包含其中。

已經購買 Microsoft 軟體的客戶，可選擇「使用自有授權 (BYOL)」選項，在 Microsoft 的授權行動性 (Microsoft License Mobility) 政策的軟體保證 (Software Assurance) 中，允許使用此種授權。Microsoft 的授權行動性 (License Mobility) 方案，可讓已經擁有 Windows Server 或 Microsoft SQL Server 授權的客戶，在 Amazon EC2 和 Amazon RDS 上執行自己部署的應用程式。微軟大量授權 (VL) 的客戶如果擁有 Microsoft 軟體保證 (Microsoft Software Assurance) 合約所涵蓋的 Windows Server 和 SQL Server 授權 (目前包括 Standard 和 Enterprise 版本)，即可受惠於此選項。

如果客戶的授權合約需要控制處理器插槽、核心或每一 VM 的層級，則可使用 Amazon EC2 專用主機，此主機提供了硬體，可用來記錄授權的使用狀況和妥適性，並向 Microsoft 或獨立軟體廠商 (ISV) 呈報。

結論

本白皮書說明了透過 Amazon Web Services (AWS) 來更新應用程式的效益，以及如何開始著手進行。文中將說明您如何能受惠於運作企業應用程式、事業單位 (LOB) 和資料庫應用程式，以及如何使用 AWS 平台，為您的更新計劃開發新的應用程式。以上是我們建議的 AWS 服務，皆能讓您開始在 AWS 上使用符合現今需求的應用程式。