部署 Amazon WorkSpaces 的最佳實務

網路存取、目錄服務及安全性

2016 年 7 月

注意

本文件資訊僅供參考。其內容為文件發佈當日時，AWS 最新的產品內容及實務，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之保證。本文並不構成 AWS、其附屬公司、供應商或授權人所做出的任何保證、表示、契約承諾、條件或擔保。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

目錄

摘要

本白皮書概述部署 Amazon WorkSpaces 的各種最佳實務。白皮書的內容涵蓋網路方面的考量、目錄服務和使用者身分驗證、安全性，以及監控和記錄。

本文件分成四大類，方便讀者快速取得相關資訊。本文件適用於網路工程師、目錄工程師或安全工程師。

簡介

Amazon WorkSpaces 是雲端中的受管桌面運算服務。Amazon WorkSpaces 免除了採購、部署硬體或安裝複雜軟體的負擔，只要在 AWS 管理主控台進行幾次按鍵操作、使用 AWS 命令列介面 (CLI) 或是使用 API 就能達成桌面體驗。Amazon WorkSpaces 讓您在幾分鐘內就能啟動桌面，提供安全、可靠、迅速的現場部署或外部網路連線環境，讓您放心存取桌面軟體。您可以：

- 透過 AWS Directory Service：AD Connector 運用現有的現場部署 Microsoft Active Directory (AD)。
- 將目錄延伸到 AWS 雲端。
- 運用 AWS Directory Service：Microsoft AD 或 Simple AD，建置受管目錄來管理您的使用者和 WorkSpaces。

此外，您還可以利用現場部署或雲端託管的 RADIUS 伺服器搭配 AD Connector，為 WorkSpaces 提供 Multi-Factor Authentication (MFA)。

使用 CLI 或 API，自動化完成 Amazon WorkSpaces 的佈建工作，並將 Amazon WorkSpaces 整合到您現有的佈建流程中。

為了安全起見，除了 WorkSpaces 服務提供的整合式網路加密之外，您還可以為 WorkSpaces 啟用靜態加密 (請參閱「安全性」一節的加密的 WorkSpaces)。

您可以使用包括像是 Microsoft System Center Configuration Manager (SCCM) 這類現有的現場部署工具將應用程式部署到 WorkSpaces，或是利用 Amazon WorkSpaces Application Manager (Amazon WAM) 進行部署。

以下各節將詳細說明 Amazon WorkSpaces、服務運作方式、啟動服務的需求，以及可供使用的選項和功能。

WorkSpaces 需求

Amazon WorkSpaces 服務需要有三項元件才能成功部署：

- **WorkSpaces 用戶端應用程式**。Amazon WorkSpaces 支援的用戶端裝置。完整清單請參閱這裡：Supported Platforms and Devices。

  您也可以使用 Personal Computer over Internet Protocol (PCoIP) 極簡型用戶端 (Zero Client) 連線到 WorkSpaces。如需可用裝置的清單，請參閱 PCoIP Zero Clients for Amazon WorkSpaces。

- **目錄服務，負責驗證使用者身分並讓使用者存取 WorkSpace**。Amazon WorkSpaces 目前採用 AWS Directory Service 和 Active Directory。您可以使用現場部署的 Active Directory 伺服器搭配 AWS Directory Service，透過 WorkSpaces 上支援現有的企業使用者登入資料。

- **Amazon 虛擬私有雲端 (Amazon VPC)，供您執行 Amazon WorkSpaces**。每一個 WorkSpaces 部署最少需要兩個子網路，因為每一個 AWS Directory Service 結構在異地同步備份部署中都需要兩個子網路。

網路方面的考量

每一個 WorkSpace 都會與用來建立它的特定 Amazon VPC 和 AWS Directory Service 結構建立關聯。所有 AWS Directory Service 結構 (Simple AD、AD Connector 和 Microsoft AD) 都需要有兩個分別位於不同可用區域的子網路才能運作。子網路永久隸屬於 Directory Service 結構，而且在建立 AWS Directory Service 之後就無法修改。因此，在您建立 Directory Services 結構前，就必須先決定適當的子網路規模。建立子網路之前，請仔細考量下列事項：

- 隨著時間增加，您會需要多少個 WorkSpaces？預期的增加幅度為何？
- 需要容納哪些類型的使用者？
- 要連線到多少個 Active Directory 網域？
- 企業使用者帳戶位於何處？

Amazon 建議您在規劃時，依據需要的存取類型和使用者身分驗證來定義使用者群組或角色。在您需要限制特定應用程式或資源的存取時，這些問題的答案很有幫助。已定義的使用者角色可協助您使用 AWS Directory Service、網路存取控制清單、路由表及 VPC 安全群組來分隔和限制存取。每個 AWS Directory Service 結構都會使用兩個子網路，並且將相同的設定套用至由該結構啟動的所有 WorkSpaces。例如，若安全群組已套用至連接 AD Connector 的所有 WorkSpaces，則可指定是否需要 MFA 驗證，或者最終使用者是否能在自己的 WorkSpace 上擁有本機管理員存取權。

> **注意** 每個 AD Connector 都連線到一個 Microsoft Active Directory 組織單位 (OU)。您必須建構自己的 Directory Service，並將使用者角色納入考量才能利用這項功能。

本節旨在說明設定 VPC 和子網路規模的最佳實務、流量，以及目錄服務設計上的隱憂。

VPC 設計

以下提供幾項考量，可供您在設計 VPC、子網路、安全群組、路由政策及 Amazon WorkSpaces 的網路 ACL 時參考，協助打造出方便擴展、安全且容易管理的 WorkSpaces 環境：

- **VPC**。建議您使用 WorkSpaces 部署專用的個別 VPC。使用個別的 VPC 就能建立分流，為您的 WorkSpaces 指定必要的控管和安全防護機制。
- **目錄服務**。每一個 AWS Directory Service 結構都需要一對子網路，在 Amazon AZ 之間分別提供高可用性的目錄服務。
- **子網路規模**。WorkSpaces 部署與目錄結構關係密切，並且與您選擇的 AWS Directory Service 位於相同的 VPC 子網路中。以下是幾項考量：
  - 子網路規模為永久設定且無法變更，因此應保留足夠空間以因應未來成長。
  - 您可以為選定的 AWS Directory Service 指定預設安全群組；這個安全群組會套用到與特定 AWS Directory Service 結構相關聯的所有 WorkSpaces。
  - 您可以讓多個 AWS Directory Service 使用相同子網路。

設計 VPC 時務必將未來的計畫納入考量。例如，您可能想要加入管理元件，像是防毒伺服器、修補程式管理伺服器，或是 Active Directory 或 RADIUS MFA 伺服器。因此在 VPC 設計中可規劃額外的可用 IP 地址來因應這類需求。

如需有關 VPC 設計和子網路規模的深入指導和考量，請參閱 **re:Invent** 簡報 How Amazon.com is Moving to Amazon WorkSpaces。

網路介面

每個 WorkSpace 都有兩個彈性網路界面 (ENI)，即一個管理網路介面 (eth0) 及一個主要網路介面 (eth1)。AWS 運用管理網路介面管理 WorkSpace；這是做為用戶端連線終端的介面。AWS 針對這個介面採用私有 IP 地址範圍。為使網路路由正常運作，這個私有地址空間無法在任何能與 WorkSpaces VPC 通訊的網路上使用。

如需各區域所使用的私有 IP 範圍清單，請參閱 Amazon WorkSpaces Details。

> **注意** Amazon WorkSpaces 與其相關的管理網路介面並非位於您的 VPC 中，而且您無法在您的 AWS 管理主控台中檢視管理網路介面或 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體 ID (請參閱圖 4、圖 5 和 圖 6)。不過，您可以在 AWS 管理主控台中檢視和修改主要網路介面 (eth1) 的安全群組設定。此外，每個 WorkSpace 的主要網路介面都會計入您的 ENI Amazon EC2 資源上限。如果是大型 WorkSpaces 部署，便需要透過 AWS 管理主控台提出支援請求，才能提高 ENI 上限。

流量

您可以將 Amazon WorkSpaces 流量分成兩個主要元素：

- 用戶端裝置與 Amazon WorkSpace 服務之間的流量
- Amazon WorkSpace 服務與客戶網路流量之間的流量

下一節會討論這兩個元素。

用戶端裝置到 WorkSpace

執行 Amazon WorkSpaces 用戶端的裝置無論位於何處 (現場部署或遠端)，都會使用兩個相同的連接埠連線到 WorkSpaces 服務。用戶端在連接埠 443 上使用 https 進行所有身分驗證及處理工作階段相關的資訊，並且使用連接埠 4172 (PCoIP 連接埠) 搭配 TCP 與 UDP 處理導向特定 WorkSpace 的像素串流，以及進行網路運作狀態檢查。這兩個連接埠上的流量都會經過加密。連接埠 443 的流量用於處理身分驗證和工作階段資訊，並且利用 TLS 將流量加密。像素串流的流量則透過串流閘道，對用戶端和 WorkSpace 的 etho 之間的通訊採用 AES 256 位元加密。本文件後續的安全性一節中，將提供更多相關資訊。

我們會發佈 PCoIP 串流閘道的各區域 IP 範圍，以及網路運作狀態檢查端點。只要將連接埠 4172 上的對外流量侷限在使用 Amazon WorkSpaces 的特定 AWS 區域，就可以限制連接埠 4172 上從企業網路到 AWS 串流閘道和網路運作狀態檢查端點的對外流量。有關 IP 範圍和網路運作狀態檢查端點，請參閱 Amazon WorkSpaces PCoIP Gateway IP Ranges。

Amazon WorkSpaces 用戶端擁有內建的網路狀態檢查功能。這個公用程式會以應用程式右下角的狀態指示燈，告知使用者網路是否支援連線。選取用戶端右下方的 **[Network]** 即可存取有關網路狀態的詳細視圖，結果如圖 1 所示。

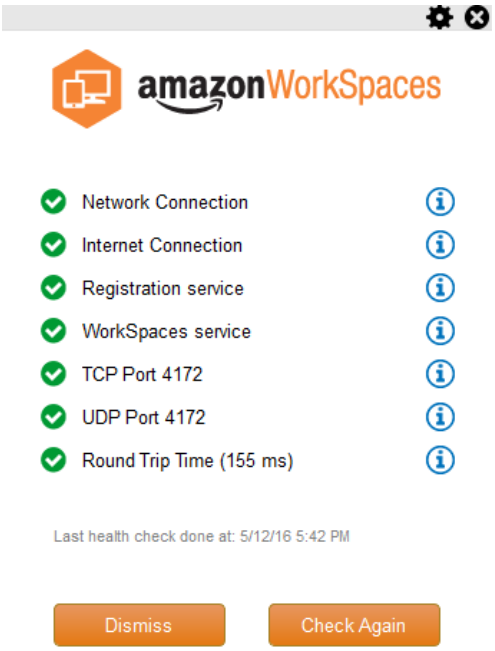

圖 1：WorkSpaces 用戶端 – 網路檢查

使用者對 Directory Service 結構所使用的目錄 (通常是公司目錄) 提供自己的登入資訊，從自己的用戶端啟動連線至 WorkSpaces 服務。登入資訊是透過 https 傳送至 WorkSpace 所在區域中，Amazon WorkSpaces 服務的身分驗證閘道。Amazon WorkSpaces 服務的身分驗證閘道接著將流量轉送至與您的 WorkSpace 相關的特定 AWS Directory Service 服務結構。例如，使用 AD Connector 時，AD Connector 會將身分驗證要求直接轉送至您的 Active Directory 服務，該服務可能是現場部署或位於 AWS VPC 中 (請參閱 AD DS 部署案例)。AD Connector 不會儲存任何身分驗證資訊，而是做為單純的無狀態代理。因此，AD Connector 必須擁有可連線至 Active Directory 伺服器的能力。AD Connector 會使用您建立 AD Connector 時定義的 DNS 伺服器，來決定要連線的 Active Directory 伺服器。

如果您使用 AD Connector 並且在目錄上啟用 MFA，則在進行目錄服務身分驗證之前，會先檢查 MFA 符記。若 MFA 驗證失敗，使用者的登入資訊將不會轉送到您的 AWS Directory Service。

使用者通過身分驗證後，串流流量就會在連接埠 4172 (PCoIP 連接埠) 上開始出現，並透過 AWS 流量閘道傳送至 WorkSpace。整個工作階段的工作階段相關資訊仍是透過 https 進行交換。串流流量會利用 WorkSpace 上未連線到您的 VPC 的第一個 ENI (WorkSpace 上的 eth0)。從串流閘道至 ENI 的網路連線是由 AWS 管理。若串流閘道至 WorkSpaces 串流 ENI 的連線失敗，就會產生 CloudWatch 事件 (請參閱本白皮書的使用 Amazon CloudWatch 監控或記錄一節)。

Amazon WorkSpaces 服務和用戶端之間傳送的資料量取決於像素活動的層級。為確保使用者獲得最佳體驗，建議 WorkSpaces 用戶端與 WorkSpaces 所在 AWS 區域之間的往返時間 (RTT) 小於 100 毫秒。這表示在正常情況下，WorkSpaces 用戶端距離託管 WorkSpace 的區域小於兩千英哩。我們提供 Connection Health Check 網頁供您參考，以便決定連線取得 Amazon WorkSpaces 服務的最佳 AWS 區域。

Amazon WorkSpaces 到 VPC

用戶端到 WorkSpace 的連線經過驗證且串流流量起始之後，您的 WorkSpaces 用戶端將會顯示 Windows 桌面 (您的 WorkSpace) 已連線到 VPC，而且網路應顯示您已建立該連線。WorkSpace 主要 ENI (標識為 eth1) 的 IP 地址會是由您 VPC 所提供的動態主機設定通訊協定 (DHCP) 服務所指派，通常是來自與 AWS Directory Service 相同的子網路。在 WorkSpace 的使用期間，這個 IP 地址會持續供 WorkSpace 使用。VPC 中的 ENI 能夠存取 VPC 中的所有資源，以及連線到 VPC 的所有網路 (透過 VPC Peering、AWS Direct Connect 連線或 VPN 連接)。

ENI 對網路資源的存取權是取決於 AWS Directory Service 為每一個 WorkSpace 設定的預設安全群組（請至此處了解更多有關安全群組的資訊），以及您指派至 ENI 的任何其他安全群組。您可以利用 AWS 管理主控台或 CLI，自行決定將安全群組加入面向 VPC 的 ENI。除了安全群組之外，您還可以在特定 WorkSpace 上使用慣用的主機型防火牆來限制對 VPC 內資源的網路存取權。

本白皮書後續 AD DS 部署案例 中的 圖 4 將呈現上述流量。

典型設定範例

試想，有兩種類型的使用者，而且 AWS Directory Service 使用集中式 Active Directory 來進行使用者身分驗證：

- **需要在任何地點都具有完整存取權的工作者**（例如，全職員工）。這些使用者將具備網際網路和內部網路的完整存取權，並且通過防火牆從 VPC 連線至現場部署的網路。
- **只能從公司網路內部存取且存取權受限的工作者**（例如，承包商和顧問）。這些使用者可透過 VPC 中的代理伺服器 (連線至特定網站) 對網際網路進行有限的存取，而且對於 VPC 中網路和現場部署網路的存取皆受限。

您想讓全職員工擁有對於各自 WorkSpace 的本機管理員存取權，以便安裝軟體，並且想使用 MFA 強制執行雙重身分驗證。也想讓全職員工能從自己的 WorkSpace 存取網際網路而不會受到限制。

對於承包商，您想要封鎖本機管理存取權，僅允許他們使用預先安裝的特定應用程式。您想透過這些 WorkSpace 的安全群組來套用嚴苛的網路存取控制。您需要只針對特定內部網站開放連接埠 80 和 443，而且想要封鎖其網際網路的存取權。

在這種情況下，有兩種完全不同的使用者角色，其對網路和桌面存取權也有不同的需求。這是以不同的方式管理和設定 WorkSpace 的最佳實務。若要達成這項目標，您需要建立兩個 AD Connector，每種使用者角色各一個。每個 AD Connector 都需要兩個子網路，並且擁有足夠的 IP 地址能夠因應您估計的 WorkSpace 使用量成長。

> **注意** 每個 AWS VPC 子網路會使用五個 IP 地址 (前四個和最後一個 IP 地址) 進行管理，而且每個 AD Connector 會在本身所在的每個子網路中使用一個 IP 地址。

以下是這種情況下的進一步考量：

- AWS VPC 子網路應為私有子網路，如此一來，類似網際網路存取的流量才能透過 NAT 閘道、雲端的 Proxy-NAT 伺服器控制，或透過現場部署流量控制系統路由回傳。
- 所有傳送至現場部署網路的 VPC 流量都設有防火牆。
- Microsoft Active Directory 伺服器和 MFA RADIUS 伺服器為現場部署 (請參閱 案例 1：使用 AD Connector 代理對現場部署 AD DS 的身分驗證)，或屬於 AWS 雲端實作的一部分 (請參閱案例 2 和 3，AD DS 部署案例)。

假設所有 WorkSpaces 都將獲得某種形式的網際網路存取權，並且託管於私有子網路上，則您也需要建立公有子網路，以便透過網際網路閘道存取網際網路。您需要 NAT 閘道，讓全職員工存取網際網路，還需要 Proxy-NAT 伺服器，提供顧問和承包商只能進入特定內部網站的有限存取權。為了因應故障而進行規劃、做出高可用性的設計，以及限縮跨 AZ 流量的費用，您應在異地同步備份部署的兩個不同子網路中設置兩個 NAT 閘道和 NAT 或代理伺服器。您選擇做為公有子網路的兩個 AZ，必須符合您在擁有兩個以上 AZ 的區域中針對 WorkSpaces 子網路所使用的兩個 AZ。您可以將所有流量從各個 WorkSpaces AZ 路由傳送到對應的公有子網路，藉此限縮跨 AZ 流量的費用，並簡化管理工作。圖 2 說明 VPC 設定。

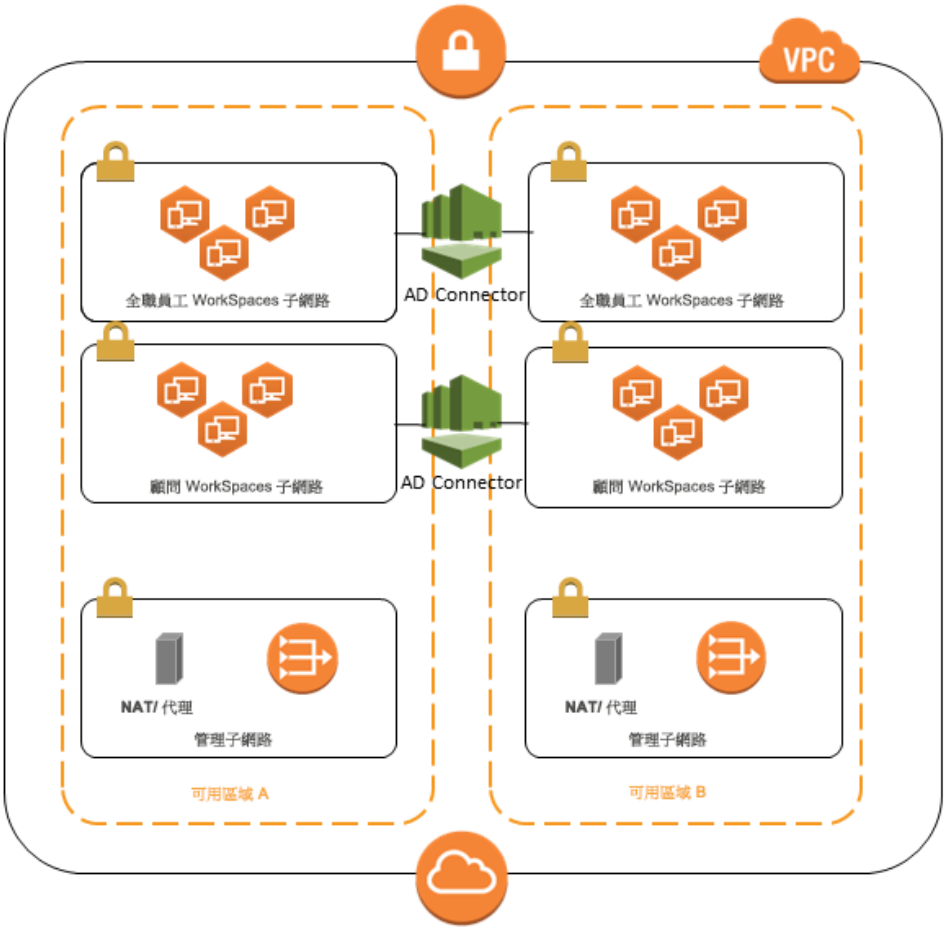

圖 2：高階 VPC 設計

以下資訊說明如何設定前述兩種不同的 WorkSpace。

- **全職員工**：在 Amazon WorkSpaces 管理主控台中的選單列上，選取 **[Directories]** 選項，選取主管全職員工的目錄，然後選取 **[Local Administrator Setting]**。啟用這個選項後，所有新建立的 WorkSpace 都將擁有本機管理員權限。若要授與網際網路存取權，您應為 VPC 對外網際網路存取設定網路位址轉譯 (NAT)。若要啟用 MFA，您需要指定 RADIUS 伺服器、伺服器 IP、連接埠及預先共用金鑰。

  如果是全職員工的 WorkSpace，傳入 WorkSpace 流量會透過 AD Connector 設定套用預設安全群組，限制為從 Helpdesk 子網路到遠端桌面協定 (RDP)。

- **承包商和顧問**：在 Amazon WorkSpaces 管理主控台中停用 **[Internet Access]** 和 **[Local Administrator Setting]**。然後在 **[Security Group]** 設定區段下方加入安全群組，對所有在該目錄下新建立的 WorkSpaces 強制執行安全群組。

  若是顧問的 WorkSpaces，可透過 AD Connector 將預設安全群組套用至與該 AD Connector 相關的所有 WorkSpaces，藉此限制 WorkSpaces 的對外和對內流量。安全群組可避免從 WorkSpaces 對外存取 HTTP 和 HTTPS 流量以外的任何流量，以及將目標為 RDP 的對內流量限於來自現場部署網路的 Helpdesk 子網路。

注意 安全群組只會套用到 VPC 內的 ENI (WorkSpace 上的 eth1)，從 WorkSpaces 用戶端存取 WorkSpace 並不會因為安全群組而受限。圖 3 顯示先前所述的 WorkSpaces VPC 最終設計。

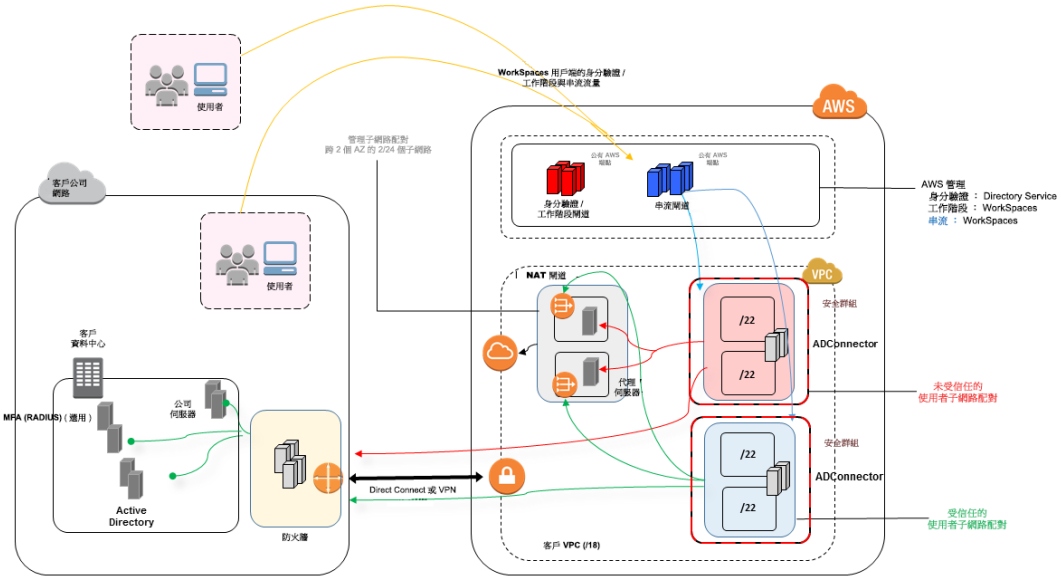

圖 3：採用典型使用者的 WorkSpaces 設計

AWS Directory Service

如「簡介」中所提到，Amazon WorkSpaces 是以 AWS Directory Service 為強化基礎。您可以使用 AWS Directory Service 建立三種類型的目錄。其中兩種存在 AWS 雲端中：

- 適用於 Microsoft Active Directory (Enterprise Edition) (或稱為 **Microsoft AD**) 的 AWS Directory Service，這是由 Windows Server 2012 R2 提供支援的受管 Microsoft Active Directory。
- **Simple AD** 是與 Microsoft Active Directory 相容的獨立受管目錄服務，由 Samba 4 提供。

第三種 **AD Connector** 是目錄閘道，可讓您代理對現有的現場部署 Microsoft Active Directory 提出的身分驗證要求及使用者或群組查詢。

下一節將說明 Amazon WorkSpaces 中介服務與 AWS Directory Service 之間身分驗證的通訊流程、透過 AWS Directory Service 實作 WorkSpaces 的最佳實務，以及一些進階概念，像是 MFA。另外我們也會討論大規模 Amazon WorkSpaces 的基礎設施架構概念、Amazon VPC 的相關需求，以及 AWS Directory Service，包括與現場部署 Microsoft Active Directory Domain Services (AD DS) 整合。

AD DS 部署案例

Amazon WorkSpaces 是以 AWS Directory Service 為強化基礎，而正確設計和部署目錄服務也都十分關鍵。以下三個案例是以 *Microsoft Active Directory Domain Services* 快速入門指南為基礎所建置，詳細說明了 AD DS 的最佳實務部署選項，其中特別強調與 WorkSpaces 的整合。本章第 *設計考量* 節深入探討針對 WorkSpaces 使用 AD Connector 的特殊需求和最佳實務，這是 WorkSpaces 整體設計概念的一部分。

- **案例 1：使用 AD Connector 代理對現場部署 AD DS 的身分驗證。**在此案例中，客戶有現成的網路連線 (VPN/Direct Connect (DX)) 可使用，而所有身分驗證都是經由 AWS Directory Service (AD Connector) 代理，對客戶現場部署 AD DS 進行。
- **案例 2：將現場部署 AD DS 延伸到 AWS (複本)。**此案例類似案例 1，但是會將客戶 AD DS 複本部署到 AWS 並結合 AD Connector，藉此減少對 AD DS 和 AD DS 通用類別目錄提出身分驗證/查詢要求時發生延遲的情況。

- **案例 3：在 AWS 雲端使用 AWS Directory Service 的獨立隔離部署。**這是隔離的案例，不包括與客戶連線進行身分驗證。此方法使用 AWS Directory Service (Microsoft AD) 和 AD Connector。雖然此案例不倚賴與客戶連線進行身分驗證，但確實會針對需要透過 VPN 或 DX 的應用程式流量進行佈建。

案例 1：使用 AD Connector 代理對現場部署 AD DS 的身分驗證

此案例適用於不想將現場部署 AD DS 延伸到 AWS 或是不考慮部署新的 AD DS 的客戶。圖 4：AD Connector 連線至現場部署 Active Directory 提供每一個元件的高階描述，並說明使用者身分驗證流程。

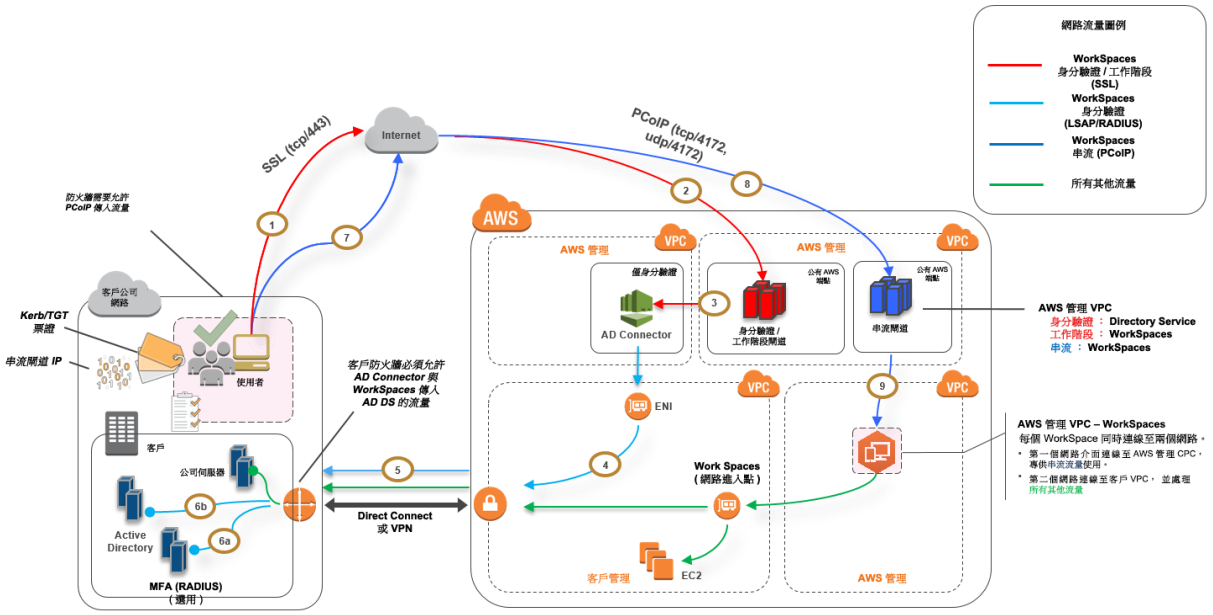

圖 4：AD Connector 連線至現場部署 Active Directory

在此案例中，所有透過 AD Connector 代理、對客戶現場部署 AD DS 進行的使用者或 MFA 身分驗證，都是使用 AWS Directory Service (AD Connector) (圖 5)。如需身分驗證程序所使用通訊協定或加密的詳細資訊，請參閱本白皮書的安全性一節。

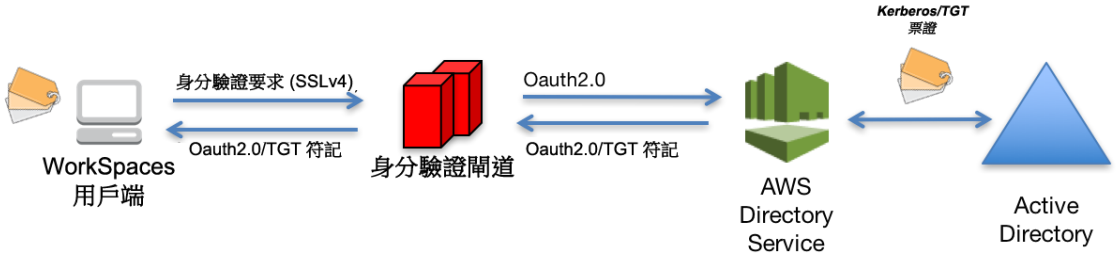

圖 5：透過驗證閘道進行使用者身分驗證

案例 1 採用混合架構，使用者的 AWS 中可能已有資源，而且可透過 WorkSpaces 存取的現場部署資料中心內可能也有資源。使用者可以利用自己現有的現場部署 AD DS 和 RADIUS 伺服器進行使用者和 MFA 身分驗證。

此架構使用以下元件或結構。

Amazon Web Services：

- **Amazon VPC**：建立 Amazon VPC，當中至少包含兩個私有子網路且橫跨兩個可用區域。
- **DHCP 選項組**：建立 Amazon VPC DHCP 選項組。這樣就可定義使用者指定的網域名稱和網域名稱伺服器 (DNS) (現場部署服務)。(如需詳細資訊，請參閱 DHCP 選項組。)
- **Amazon 虛擬私有閘道**：能夠經由 IPsec VPN 通道或 AWS Direct Connect 連線與您本身的網路通訊。
- **AWS Directory Service**：AD Connector 部署到一組 Amazon VPC 私有子網路中。
- **Amazon WorkSpaces**：WorkSpaces 與 AD Connector 部署在相同的私有子網路中 (請參閱 設計考量，AD Connector)。

客戶：

- **網路連線**：企業 VPN 或 Direct Connect 端點。
- **AD DS**：企業 AD DS。
- **MFA (選用)**：企業 RADIUS 伺服器。
- **最終使用者裝置**：企業或 BYOL 最終使用者裝置 (例如 Windows、Mac、iPad 或 Android 平板電腦、極簡型用戶端、Chromebook)，用來存取 Amazon WorkSpaces 服務 (請參閱支援的平台和裝置)。

雖然此解決方案對於不想要將 AD DS 部署到雲端的客戶來說十分理想，但是也有些缺點。

- **倚賴連線**：如果與資料中心的連線中斷，使用者就無法登入自己的個別 WorkSpaces，而且現有連線會在 Kerberos/TGT 存留期間保持作用狀態。

- **延遲**：如果連線時發生延遲 (使用 VPN 比使用 DX 更常遇到這種情況)，WorkSpaces 身分驗證和任何 AD DS 相關活動 (像是強制實施群組政策 (GPO)) 將耗費更長時間。
- **流量費用**：所有身分驗證都必須周遊 VPN 或 DX 連結，因此取決於連線類型。一種是資料從 Amazon EC2 傳出至網路，一種是資料傳出 (DX)。

> **注意** AD Connector 是代理服務。它不會儲存或快取使用者登入資料。所有身分驗證、查詢和管理要求都是另外由您的 Active Directory 處理。目錄服務中需要具有委託權限的帳戶，並且有權讀取所有使用者資訊並將電腦加入網域。

如需有關如何在目錄中針對 AD Connector 設定使用者的詳細資訊，請參閱委託連線權限。

一般而言，WorkSpaces 體驗高度倚賴 圖 4 中顯示的第 5 項。

案例 2：將現場部署 AD DS 延伸到 AWS (複本)

此案例類似案例 1，但是在案例 2 中會將客戶 AD DS 複本部署到 AWS 並結合 AD Connector。如此可減少對 AD DS 提出身分驗證或查詢要求時發生延遲的情況。圖 6 提供每一個元件的高階視圖並說明使用者身分驗證流程。

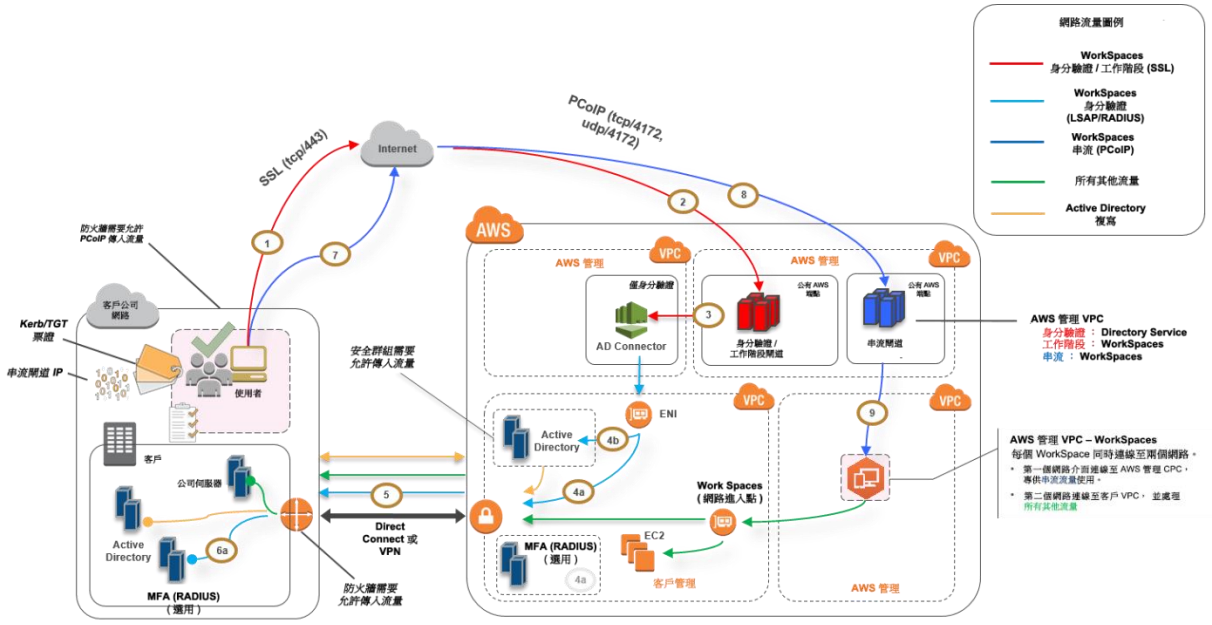

圖 6：將客戶 Active Directory Domain 延伸到雲端

如同案例 1，所有使用者或 MFA 身分驗證都是使用 AD Connector，接著再代理至客戶 AD DS (圖 5)。在案例 2 中，客戶 AD DS 會部署到客戶現場部署 Active Directory 樹系中提升為網域控制器，並於 AWS 雲端執行的 Amazon EC2 執行個體上的可用區域。每個網域控制器都會部署到 VPC 私有子網路中，以便在 AWS 雲端提供高可用性的 AD DS。如需在 AWS 雲端中部署 AD DS 的最佳實務，請參閱本白皮書後續的「設計考量」。

部署 WorkSpaces 執行個體後，它們就能存取雲端型網域控制器並使用安全、低延遲的目錄服務和 DNS。包括 AD DS 通訊、身分驗證要求及 Active Directory 複寫在內的所有網路流量，無論是在私有子網路內或是在客戶 VPN 通道或 DX 上，都會受到妥善的保護。

此架構使用以下元件或結構。

Amazon Web Services：

- **Amazon VPC**：建立 Amazon VPC，當中至少包含四個私有子網路且橫跨兩個可用區域 (兩個用於客戶 AD DS，兩個用於 AD Connector 或 WorkSpaces)。

- **DHCP 選項組**：建立 Amazon VPC DHCP 選項組。這樣您就可定義使用者指定的網域名稱和 DNS (區域 AD DS)。如需詳細資訊，請參閱 DHCP 選項組。
- **Amazon 虛擬私有閘道**：能夠經由 IPsec VPN 通道或 AWS Direct Connect 連線與您自己的網路通訊。
- **Amazon EC2**：

— 客戶企業 AD DS 網域控制器，部署於專用私有 VPC 子網路中的 Amazon EC2 執行個體上。

— 用於 MFA 的客戶「選用」RADIUS 伺服器。

- **AWS Directory Services**：AD Connector 部署到一組 Amazon VPC 私有子網路中。
- **Amazon WorkSpaces**：WorkSpaces 與 AD Connector 部署在相同的私有子網路中 (請參閱 設計考量，AD Connector)。

客戶：

- **網路連線**：企業 VPN 或 AWS Direct Connect 端點。
- **AD DS**：企業 AD DS (複寫所需)。
- **MFA「選用」**：企業 RADIUS 伺服器。
- **最終使用者裝置**：企業或 BYOL 最終使用者裝置 (例如 Windows、Mac、iPad 或 Android 平板電腦、極簡型用戶端、Chromebook)，用來存取 Amazon WorkSpaces 服務 (請參閱支援的平台和裝置)。

此解決方案並沒有案例 1 所附帶的缺點。因此 WorkSpaces 和 AWS Directory Service 不需倚賴既有的連線。

- **對連線的倚賴**：如果與客戶資料中心的連線中斷，最終使用者仍可繼續工作，因為身分驗證和「選用」MFA 會在本機上處理。
- **延遲**：除了複寫流量以外 (請參閱*設計考量：*AD DS 站點與服務)，所有身分驗證都在本機上進行且低延遲。
- **流量費用**：在此案例中，身分驗證是在本機上進行，只有 AD DS 複寫需要周遊 VPN 或 DX 連結，因此減少了資料傳輸。

一般而言，WorkSpaces 體驗因此獲得提升，而且不會高度倚賴 圖 6 中顯示的第 5 項。當您想要將 WorkSpaces 擴展到數千個桌面時感受更深，尤其是與 AD DS 通用類別目錄查詢相關時更是如此，因為此流量會保持在 WorkSpaces 環境內。

案例 3：在 AWS 雲端使用 AWS Directory Service 的獨立隔離部署

如圖 7 中所示，此案例將 AD DS 部署到 AWS 雲端獨立的隔離環境中。AWS Directory Service 只在此案例中使用。您不必自行管理 AD DS 的一切，可以仰賴 AWS Directory Service 為您完成像是建置高可用性目錄拓撲、監控網域控制器，以及設定備份和快照等工作。

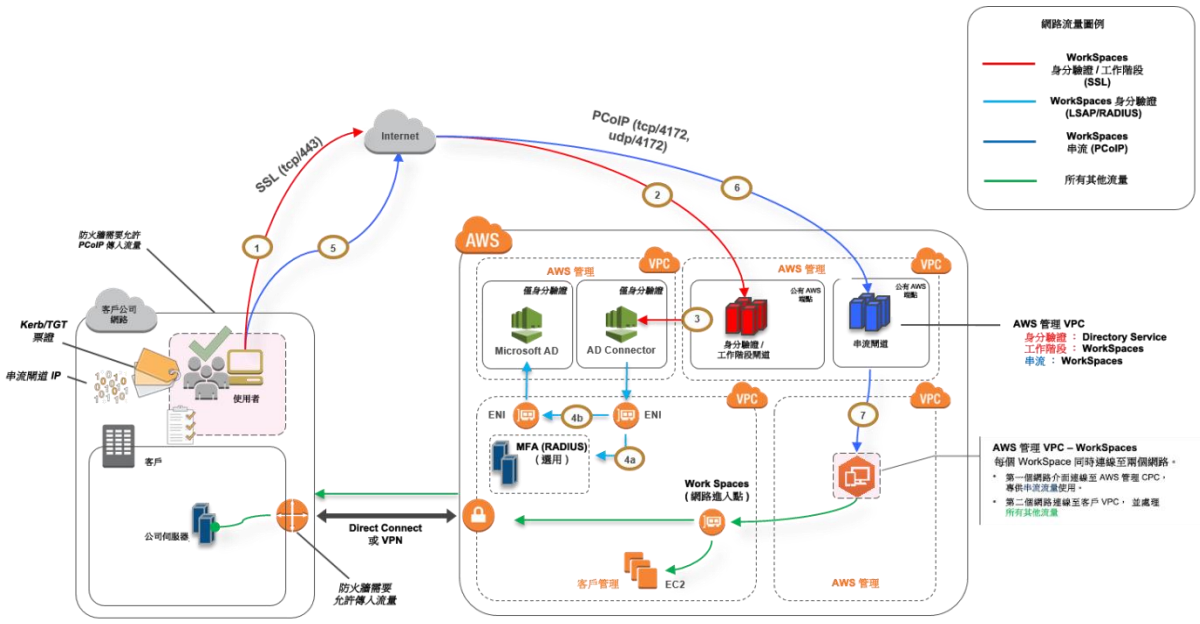

圖 7：僅限雲端 - AWS Directory Services (Microsoft AD)

如同案例 2，AD DS (Microsoft AD) 會部署到橫跨兩個可用區域的專用子網路中，以便在 AWS 雲端提供高可用性的 AD DS。除了 Microsoft AD 之外，另外還會部署 AD Connector (三個案例皆相同) 用於 WorkSpaces 身分驗證或 MFA。如此可確保 Amazon VPC 內的角色或功能有所區分，這是標準的最佳實務 (請參閱 *設計考量*：分割網路一節)。

案例 3 是標準的全含式組態，對於想要使用 AWS 管理部署、修補、高可用性及監控 AWS Directory Service 的客戶而言最為理想。由於它本身為隔離模式，因此除了生產環境之外，此案例也適用於概念驗證和實驗室環境。

除了 AWS Directory Service 的配置之外，圖 7 還會說明從使用者到工作空間的流量流程，以及工作空間如何與 AD 伺服器和 MFA 伺服器互動。

此架構使用以下元件或結構。

Amazon Web Services：

- **Amazon VPC**：建立 Amazon VPC，當中至少包含四個私有子網路且橫跨兩個可用區域 (兩個用於 AD DS *Microsoft AD*，兩個用於 AD Connector 或 WorkSpaces)。「*角色區分*」。
- **DHCP 選項組**：建立 Amazon VPC DHCP 選項組。這樣您就可定義使用者指定的網域名稱和 DNS (Microsoft AD)。如需詳細資訊，請參閱 DHCP 選項組。
- **選用：Amazon 虛擬私有閘道**：能夠經由 IPsec VPN 通道 (VPN) 或 AWS Direct Connect 連線與您自己的網路通訊。用於存取現場部署的後端系統。
- **AWS Directory Service**：Microsoft AD 部署到一組專用的 VPC 子網路中 (AD DS 受管服務)。
- **Amazon EC2**：用於 MFA 的客戶「選用」RADIUS 伺服器。
- **AWS Directory Services**：AD Connector 部署到一組 Amazon VPC 私有子網路中。
- **Amazon WorkSpaces**：WorkSpaces 與 AD Connector 部署在相同的私有子網路中 (請參閱 設計考量，AD Connector)。

客戶：

- **選用：網路連線**：企業 VPN 或 AWS Direct Connect 端點。
- **最終使用者裝置**：企業或 BYOL 最終使用者裝置 (例如 Windows、Mac、iPad 或 Android 平板電腦、極簡型用戶端、Chromebook)，用來存取 Amazon WorkSpaces 服務 (請參閱支援的平台和裝置)。

就像案例 2，此解決方案不需倚賴與客戶現場部署的資料中心連線，也沒有延遲或資料傳出費用的問題 (除非在 VPC 內啟用 WorkSpaces 的網際網路存取)，因為它的原始設計就是隔離或僅限雲端的案例。

設計考量

為使 AWS 雲端中的 AD DS 部署正常運作，需要充分了解 Active Directory 概念與特定 AWS 服務。本節旨在討論針對 WorkSpaces 部署 AD DS 時的重要設計考量、AWS Directory Service 的 VPC 最佳實務、DHCP 和 DNS 需求、AD Connector 詳細規格，以及 Active Directory 站點與服務。

VPC 設計

依照我們在本文件的網路考量一節中所討論，以及前面有關案例 2 和 3 的記載資料，您應將 AWS 雲端中的 AD DS 部署到橫跨兩個可用區域的一組專用私有子網路中，並且與 AD Connector 或 WorkSpaces 子網路隔離。此結構可為 WorkSpaces 提供高可用性、低延遲的 AD DS 存取，同時維持標準最佳實務，也就是將 Amazon VPC 內的角色或功能加以區分。

圖 8 顯示將 AD DS 和 AD Connector 分配到專用的私有子網路 (案例 3)。此範例中的所有服務都位於相同的 Amazon VPC 中。

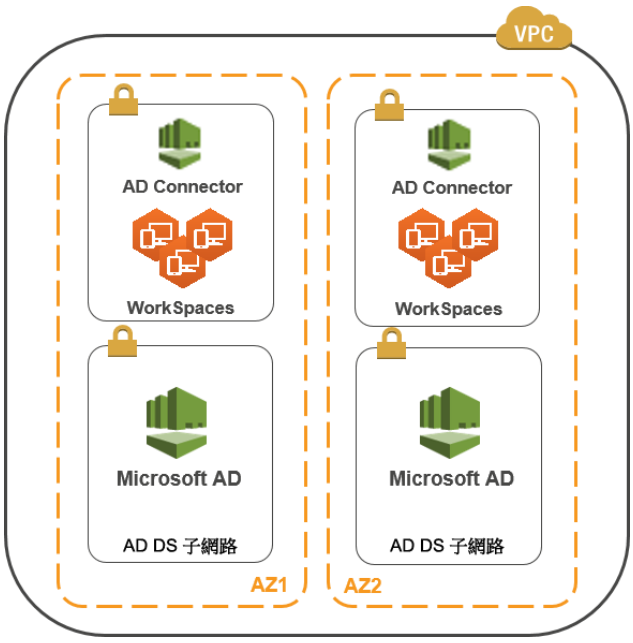

圖 8：AD DS 網路隔離

圖 9 顯示的設計類似案例 1，不過此案例的現場部署部分位於專用的 Amazon VPC 中。

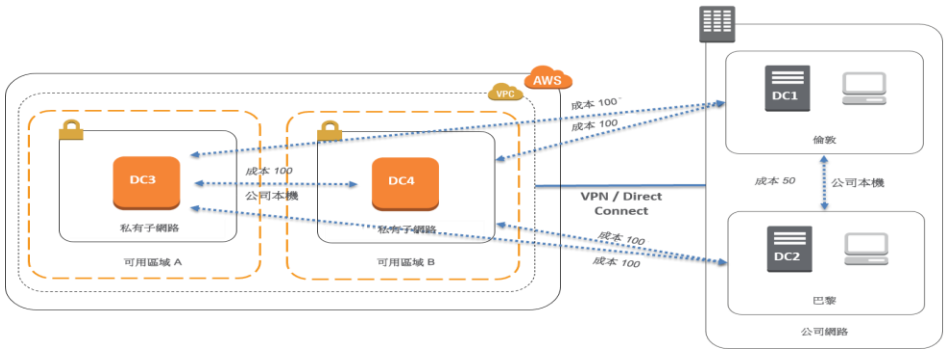

圖 9：專用 WorkSpaces VPC

> **注意** 若客戶擁有使用 AD DS 的現成 AWS 部署，建議您將 WorkSpaces 放置在專用的 VPC 中，並且使用 VPC Peering 進行 AD DS 通訊。

除了為 AD DS 建立專用的私有子網路之外，網域控制器和成員伺服器還需要數項安全群組規則才能允許像是 AD DS 複寫、使用者身分驗證、Windows 時間服務及分散式檔案系統 (DFS) 這類服務的流量。

> **注意** 最佳實務是將必要的安全群組規則限於 WorkSpaces 私有子網路，以及在案例 2 中，允許現場部署與 AWS 雲端之間的雙向 AD DS 通訊，如下表所示。

通訊協定	連接埠	用途	目的地
tcp	53, 88, 135, 139, 389, 445, 464, 636	驗證 (主要)	Active Directory (私有資料中心或 EC2)*
tcp	49152 – 65535	RPC 高速連接埠	Active Directory (私有資料中心或 EC2)**
tcp	3268-3269	信任	Active Directory (私有資料中心或 EC2)*
tcp	9389	遠端 Microsoft Windows PowerShell (選用)	Active Directory (私有資料中心或 EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	驗證 (主要)	Active Directory (私有資料中心或 EC2)*
udp	1812	驗證 (MFA) (選用)	RADIUS (私有資料中心或 EC2)*

* 請參閱 Active Directory 和 Active Directory Domain Services 連接埠需求

**請參閱 Windows 服務概觀和網路連接埠需求

如需實作規則的逐步指導方針，請參閱《*Amazon Elastic Compute Cloud 使用者指南*》中的新增規則至安全群組。

VPC 設計：DHCP 和 DNS

在 Amazon VPC 中，DHCP 是預設提供給您的執行個體使用的服務。根據預設，每個 VPC 都會提供內部 DNS 伺服器，可經由無類別網域間路由選擇 (CIDR) +2 地址空間存取，並且透過預設 DHCP 選項組指派至所有執行個體。

DHCP 選項組在 Amazon VPC 內用來定義範圍選項，像是應透過 DHCP 交給執行個體的網域名稱或名稱伺服器。VPC 內 Windows 服務的功能是否正常，取決於此 DHCP 範圍選項，而且您需要正確設定此選項。在先前定義的各案例中，您會建立並指派自己的範圍來定義您的網域名稱和名稱伺服器。這樣可確保加入網域的 Windows 執行個體或 WorkSpaces 會設定為使用 Active Directory DNS。下表示範一組自訂的 DHCP 範圍選項，必須建立這些選項才能讓 WorkSpaces 和 AWS Directory Services 正常運作。

參數	值
名稱標籤	建立標籤，其中鍵值 = **name** 及 **value** 設定為特定字串 範例：exampleco.com
網域名稱	exampleco.com
網域名稱伺服器	DNS 伺服器地址，以逗號分隔 範例：10.0.0.10, 10.0.1.10
NTP 伺服器	此欄留白
NetBIOS 名稱伺服器	依照網域名稱伺服器輸入相同的逗號分隔 IP 範例：10.0.0.10, 10.0.1.10
NetBIOS 節點類型	2

如需建立自訂 DHCP 選項組並將它與您的 Amazon VPC 建立關聯的詳細資訊，請參閱《*Amazon 虛擬私有雲端使用者指南*》中的使用 DHCP 選項組。

在案例 1 中，DHCP 範圍會是現場部署 DNS 或 AD DS。不過在案例 2 或 3 中，此範圍會是部署在本機上的目錄服務 (Amazon EC2 上的 AD DS 或 AWS Directory Services：Microsoft AD)。建議您將位於 AWS 雲端的每一個網域控制器都設為通用類別目錄及目錄整合的 DNS 伺服器。

Active Directory：站點與服務

對於案例 2 來說，站點與服務是 AD DS 功能是否正常的關鍵元件。站點拓撲負責控制同一站點內及跨站點邊界的網域控制器之間的 Active Directory 複寫。案例 2 中至少有兩個站點存在，也就是現場部署和雲端中的 AWS WorkSpaces。定義正確的站點拓撲可確保用戶端親和性，也就是說，用戶端 (此處是指 WorkSpaces) 使用自己慣用的區域網域控制器。

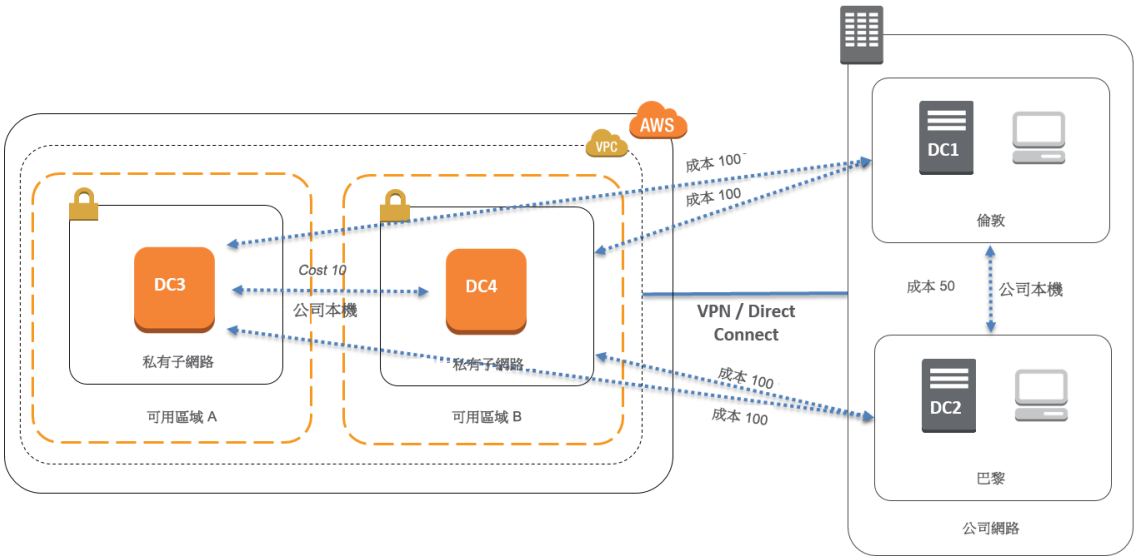

圖 10：Active Directory 站點與服務：用戶端親和性

最佳實務 定義現場部署 AD DS 與 AWS 雲端之間站點連結的高成本。圖 10 舉例說明指派給站點連結的成本 (成本 100)，以確保獨立於站點的用戶端親和性。

這些關聯讓像是 AD DS 複寫及用戶端身分驗證等流量能確實使用最有效率的網域控制器路徑。在案例 2 和 3 的情況下，則有助於降低延遲和交互連結流量。

Multi-Factor Authentication (MFA)

要實作 MFA，WorkSpaces 基礎設施必須使用 AD Connector 做為 AWS Directory Service，且必須配備 RADIUS 伺服器。本文件未討論 RADIUS 伺服器的部署，但先前的 AD DS 部署案例章節已詳述 RADIUS 在各案例下的配置。

MFA – 雙重身分驗證

Amazon WorkSpaces 可透過 AWS Directory Service：AD Connector 支援 MFA 與*客戶所擁有的* RADIUS 伺服器。啟用後，使用者必須提供 WorkSpaces 用戶端的**使用者名稱**、**密碼**和 **MFA 代碼**，以驗證其各自的 WorkSpaces 桌面。

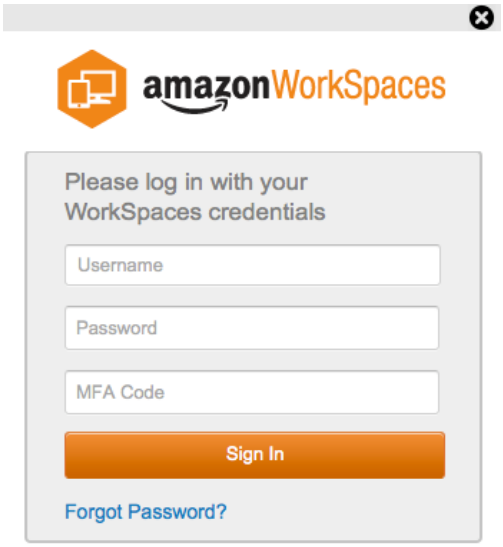

圖 11：啟用 MFA 的 WorkSpaces 用戶端

硬性規定 實作 MFA 身分驗證需使用 AD Connector。AD Connector 不支援選擇性「依使用者」的 MFA，因為這是全域依附於 AD Connector 的設定。如果您需要選擇性「依使用者」的 MFA，必須用 AD Connector 區隔使用者。

WorkSpaces MFA 需要一或多個 RADIUS 伺服器。這些通常是現有的解決方案，例如 RSA，或可將伺服器部署在 VPC 內 (請參閱 AD DS 部署案例)。如果要部署新的 RADIUS 解決方案，目前業界內也有多個實作可選，例如 FreeRADIUS，以及類似 Duo Security 的雲端服務。

如需取得利用 Amazon WorkSpaces 實作 MFA 必要條件清單，請參閱 *Amazon WorkSpaces Administration Guide* 中的 Preparing Your Network for an AD Connector Directory。設定 AD Connector 使用 MFA 的流程如 *Amazon WorkSpaces Administration Guide* 的 Managing an AD Connector Directory: Multi-factor Authentication 中所述。

安全性

本小節說明使用 Amazon WorkSpaces 服務時如何利用加密功能來保護資料。在此說明傳輸中加密、靜態加密，以及如何利用安全群組保護對 WorkSpaces 的網路存取。有關身分驗證的詳細資訊 (包括 MFA 支援)，可在 AWS Directory Service 一節中找到。

傳輸中加密

Amazon WorkSpaces 在通訊 (傳輸) 的不同階段使用密碼編譯來保護資料的機密性，同時也會保護靜態資料 (加密的 WorkSpaces)。Amazon WorkSpaces 在傳輸各階段所使用的加密程序如下列各節所述。關於靜態加密的資訊，請參閱本白皮書後續的加密 WorkSpaces 一節。

註冊和更新

桌面用戶端應用程式使用 https 與 Amazon 進行通訊，以便更新和註冊。

身分驗證階段

桌面用戶端會傳送登入資料至身分驗證閘道以啟動身分驗證。桌面用戶端與身分驗證閘道之間使用 https 進行通訊。此階段結束時，如果身分驗證成功，身分驗證閘道將透過相同的 https 連線傳回 OAuth 2.0 符記給桌面用戶端。

> **注意** 桌面用戶端應用程式支援在連接埠 443 (HTTPS) 流量上使用代理伺服器進行更新、註冊及身分驗證。

收到用戶端的登入資料後，身分驗證閘道將傳送身分驗證要求至 AWS Directory Service。身分驗證閘道是透過 HTTPS 與 AWS Directory Service 通訊，不會以純文字傳輸使用者登入資料。

身分驗證— AD Connector

AD Connector 使用 Kerberos 建立與現場部署 AD 的驗證通訊，因此其將繫結於 LDAP 並執行後續的 LDAP 查詢。此時 AWS Directory Service 並不支援 LDAP with TLS (LDAP)。但是絕對不會傳送純文字的使用者登入資料。為提高安全性，可透過 VPN 連接利用現場部署網路 (AD 所在處) 連接 WorkSpaces VPC。使用 AWS 硬體 VPN 連接時，會設定傳輸中加密，使用的是標準 IPSEC (IKE 與 IPSEC SA)，含有 AES-128 或 AES-256 對稱加密金鑰、完整性雜湊的 SHA-1 或 SHA-256，以及使用 PFS 的 DH 群組 (階段 1 為 2、14-18、22、23 與 24；階段 2 為 1、2、5、14-18、22、23 與 24)。

代理人階段

接收 OAuth 2.0 符記 (如果身分驗證成功會由身分驗證閘道傳出) 之後，桌面用戶端將使用 HTTPS 向 Amazon WorkSpaces 服務 (Broker Connection Manager) 查詢。桌面用戶端會傳送 OAuth 2.0 符記以進行自我驗證，因此用戶端將接收到 WorkSpaces 串流閘道的端點資訊。

串流階段

桌面用戶端要求 (使用 OAuth 2.0 符記) 透過串流閘道開啟 PCoIP 工作階段。此工作階段以 aes256 加密，並使用 PCoIP 連接埠進行通訊控制 (亦即 4172/tcp)。

串流閘道將利用 OAuth2.0 符記透過 https 向 WorkSpaces 服務要求使用者專屬的 WorkSpaces 資訊。

串流閘道同時也會從用戶端接收 TGT (使用用戶端使用者的密碼加密)，且閘道將利用 Kerberos TGT 傳遞，使用使用者所擷取到的 Kerberos TGT 在 WorkSpace 上啟動 Windows 登入。

接著 WorkSpace 會使用標準 Kerberos 身分驗證，向設定的 AWS Directory Service 啟動身分驗證要求。

成功登入 WorkSpace 之後，PCoIP 便開始串流。連線由用戶端在連接埠 tcp 4172 上啟動，傳回流量則使用連接埠 udp 4172。串流閘道與 WorkSpaces 桌面透過 UDP 55002 在管理介面上建立初始連接。(請參閱 Amazon Workspaces 說明文件 Amazon WorkSpaces Details。初始的對外 UDP 連接埠為 55002。) 使用連接埠 4172 (tcp 與 udp) 的串流連線，是以 AES 128 與 256 位元密碼加密，預設為 128 位元。您可主動透過 PCoIP 專用 Active Directory GPO (pcoip.adm) 將此設定變更為 256 位元。

網路介面

每個 Amazon WorkSpace 都有兩個網路介面，分別稱為主要網路介面和管理網路介面。

主要網路介面可連線至 VPC 內的資源，例如存取 AWS Directory Service、網際網路和企業網路。您可將安全群組連接到此主要網路介面 (如同您處理 ENI 的方式)。就概念而言，會根據部署範圍將連接到此 ENI 的安全群組因區分為：WorkSpaces 安全群組與 ENI 安全群組。

管理網路介面

您無法透過安全群組控制管理網路介面，但可在 WorkSpace 上利用主機型防火牆來封鎖連接埠或控制存取。不建議將限制套用於管理網路介面。如果您決定要新增主機型防火牆規則來管理此介面，必須讓幾個連接埠保持開啟，如此 WorkSpaces 服務才能依照 Amazon WorkSpaces Administration Guide 的定義來管理 WorkSpace 的狀態與存取情形。

WorkSpaces 安全群組

預設的安全群組是依照 AWS Directory Service 建立，並自動連接至該特定目錄下的所有 WorkSpaces。

如同任何其他的安全群組，您也可修改 WorkSpaces 安全群組的規則。結果將在變更套用後立即生效。

此外，透過變更 WorkSpaces 安全群組的關聯，也可變更連接至 AWS Directory Service 的預設 WorkSpaces 安全群組。

> **注意** 新建立關聯的安全群組只會連接至修改後所建立或重建的 WorkSpaces。

ENI 安全群組

主要網路介面為一般的 ENI，因此您可用不同的 AWS 管理工具來管理其設定 (請參閱 Elastic Network Interfaces (ENI))。請特別找出 WorkSpace IP (在 Amazon WorkSpaces 主控台的 WorkSpaces 頁面上)，接著使用該 IP 地址做為篩選條件，找出對應的 ENI (在 Amazon EC2 主控台的 Network Interfaces 區段)。

找到 ENI 之後，便能直接在該處管理安全群組。手動指派安全群組至主要網路介面時，請考量 Amazon WorkSpaces 的連接埠需求，如 Amazon WorkSpaces Details *所述*。

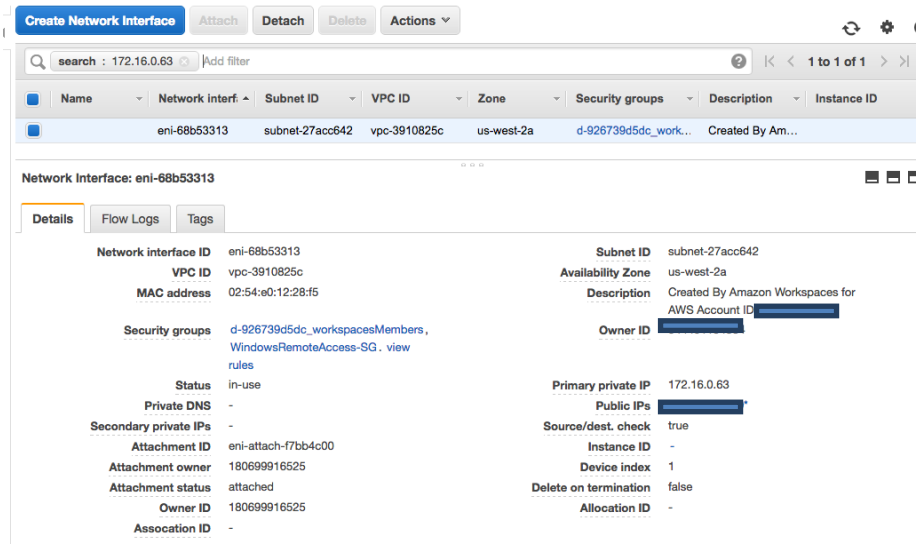

圖 12：管理安全群組關聯

加密的 WorkSpaces

每個 Amazon WorkSpace 均佈建根磁碟區 (C: 磁碟機) 和使用者磁碟區 (D: 磁碟機)。加密 WorkSpaces 功能可讓您加密任一磁碟區或同時加密兩個磁碟區。

哪些資料有加密保護？

靜態儲存的資料、對磁碟區的磁碟 I/O，及加密磁碟區所建立的快照全都會加密。

何時執行加密？

您應在啟動 (建立) WorkSpace 時指定 WorkSpace 的加密。WorkSpaces 磁碟區只能在啟動時加密：啟動後便無法再變更磁碟區的加密狀態。圖 13 顯示 Amazon WorkSpaces 主控台頁面，可在啟動新的 WorkSpace 時選擇加密。

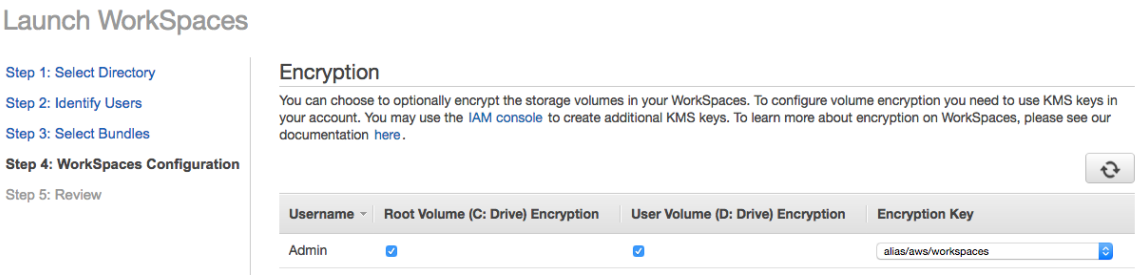

圖 13：加密 WorkSpaces 磁碟區

新的 WorkSpace 如何加密？

您可從 Amazon WorkSpaces 主控台或 AWS CLI 選擇 Encrypted WorkSpaces 選項，或在啟動新 WorkSpace 時使用 Amazon WorkSpaces API。

加密磁碟區時，Amazon WorkSpaces 使用 AWS Key Management Service (KMS) 的客戶主金鑰 (CMK)。預設的 AWS KMS CMK 會在於某地區 (CMK 有其區域範圍) 首次啟動 WorkSpace 時建立。您也可建立客戶管理的 CMK，以用於加密 WorkSpaces。CMK 用於加密資料金鑰，Amazon WorkSpaces 服務再利用該金鑰來加密磁碟區 (嚴格來說，將由 Amazon Elastic Block Store (Amazon EBS) 服務加密磁碟區)。每個 CMK 皆可用來加密最多 30 個 WorkSpaces 的金鑰。

> **注意** 目前不支援從加密的 WorkSpace 建立自訂映像。此外，在啟用根磁碟區加密下啟動的 WorkSpaces 最長可能需要一個小時才可完成佈建。

如需 WorkSpaces 加密流程的詳細說明，請參閱 Overview of Amazon WorkSpaces Encryption Using AWS KMS。如需 AWS KMS 客戶主金鑰與資料金鑰的詳細資訊，請參閱 AWS Key Management Service Concepts。

使用 Amazon CloudWatch 監控或記錄

監控是網路、伺服器或日誌等基礎設施不可或缺的一項功能。部署 Amazon WorkSpaces 的客戶需要監控其部署，尤其是要留意各個 WorkSpaces 的整體運作與連線狀態。

適用於 WorkSpaces 的 Amazon CloudWatch 指標

WorkSpaces 的 CloudWatch 指標可讓管理員深入檢視各個 WorkSpaces 的整體運作與連線狀態。指標將依各 WorkSpace 提供，或針對組織特定目錄內所有的 WorkSpaces 匯總提供 (*AD Connector，請參閱身分*)。

跟所有的 CloudWatch 指標一樣，這些指標均可在 AWS 管理主控台 (圖 13) 內檢視、透過 CloudWatch API 存取，以及經由 CloudWatch 警示與第三方工具進行監控。

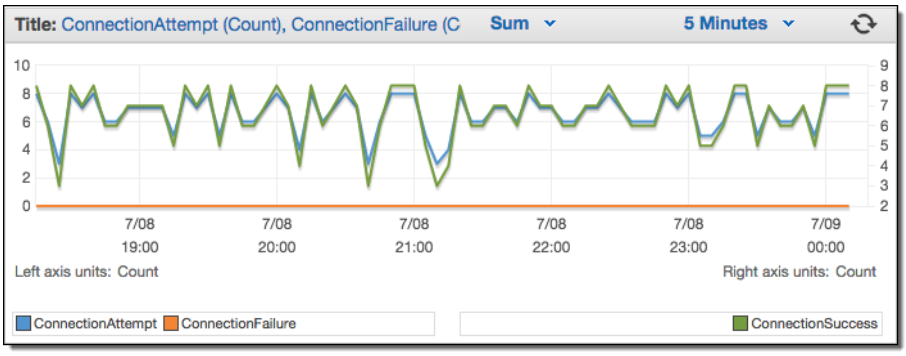

圖 14：CloudWatch 指標 – ConnectionAttempt/ConnectionFailure

根據預設，下列指標為啟用狀態且免費提供使用：

- **Available**：回應狀態檢查的 WorkSpaces 會計入此指標。
- **Unhealthy**：未回應同一狀態檢查的 WorkSpaces 會計入此指標。
- **ConnectionAttempt**：嘗試連線到 WorkSpace 的次數。
- **ConnectionSuccess**：嘗試連線且成功的次數。
- **ConnectionFailure**：嘗試連線卻失敗的次數。
- **SessionLaunchTime**：啟動工作階段所花的時間，從 WorkSpaces 用戶端測量。

- **InSessionLatency**：往返 WorkSpaces 用戶端與 WorkSpaces 的時間，從用戶端測量及回報。
- **SessionDisconnect**：由使用者啟動且自動關閉的工作階段數目。

此外，也可建立警示，如圖 15 所示。

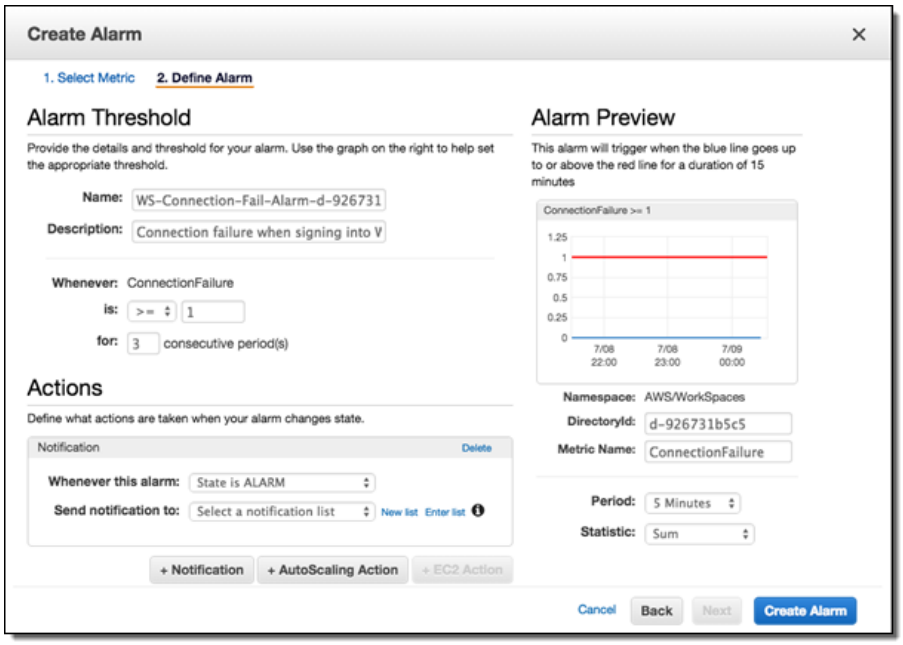

圖 15：建立 WorkSpaces 連線錯誤的 CloudWatch 警示

故障診斷

「我看到下列錯誤訊息：『裝置無法連線至 WorkSpaces 註冊服務』或『無法連線至有互動式登入橫幅的 WorkSpace』」的這類常見管理與用戶端問題可在 *Amazon WorkSpaces Administration Guide* 的 Client 與 Admin 故障診斷頁面上找到。

AD Connector 無法連線至 Active Directory

若要讓 AD Connector 連線至現場部署目錄，現場部署網路的防火牆必須有特定連接埠開放給 VPC 中兩個子網路的 CIDR 使用 (請參閱 AD Connector)。若要測試是否符合這些條件，請執行下列步驟。

驗證連線

1. 在 VPC 中啟動 Windows 執行個體，並透過 RDP 與其連線。其餘步驟將在 VPC 執行個體中執行。
2. 下載並解壓縮 DirectoryServicePortTest 測試應用程式。其中包含原始碼與 Visual Studio 專案檔，您可視需要修改測試應用程式。
3. 在 Windows 命令提示下，運用下列選項執行 DirectoryServicePortTest 測試應用程式：

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
"53,88,135,139,389,445,464,636,49152" -udp "53,88,123,137,138,389,445,464"
<domain_name>
```

<domain_name>

完全合格的網域名稱，用於測試樹系與網域的功能層級。如果排除網域名稱，便不會測試其功能層級。

<server_IP_address>

現場部署網域中網域控制器的 IP 地址。連接埠將針對此 IP 地址進行測試。如果排除 IP 地址，便不會測試連接埠。

這會決定 VPC 是否向網域開放必要連接埠。測試應用程式將驗證樹系與網域的最低功能層級。

如何檢查最近的 AWS 區域的延遲

Amazon WorkSpaces 於 2015 年 10 月推出了 Connection Health Check 網站。此網站可快速檢查您是否取得使用 WorkSpaces 需要的所有服務。此外也會對 WorkSpaces 運作的各個 AWS 區域執行效能檢查，讓使用者知道哪個區域使用起來速度最快。

結論

我們發現，組織不斷致力於提升靈敏度、改善資料保護，以及幫助工作者提升生產力，因此最終使用者運算也隨之發生策略性的變動。許多經由雲端運算實現的優勢也可發揮在最終使用者運算上。將桌面轉移到包含 Amazon WorkSpaces 的 AWS 雲端後，組織便能隨工作者數量的增加而快速擴展，不必將資料存入裝置即強化自身安全狀態，同時為工作者提供可攜式的桌面，讓他們透過任何裝置、從任何位置進行存取。

Amazon WorkSpaces 的設計可整合至現有的 IT 系統與流程，而本白皮書說明了進行整合的最佳實務。只要遵照本白皮書中的準則，便能以符合成本效益的方式完成雲端桌面的部署，隨著您事業的成長在 AWS 全球基礎架構上不斷擴展。

作者群

協力完成本文件的個人如下：

- Justin Bradley，Amazon Web Services 解決方案架構師
- Mahdi Sajjadpour，AWS 專業服務資深顧問
- Mauricio Munoz，Amazon Web Services 解決方案架構師

深入閱讀

如需其他協助，請參考以下資源：

- Troubleshooting AWS Directory Service Administration Issues
- Troubleshooting Amazon WorkSpaces Administration Issues
- Troubleshooting Amazon WorkSpaces Client Issues
- Amazon WorkSpaces Administration Guide
- Amazon WorkSpaces Developer Guide
- Supported Platforms and Devices
- How Amazon WorkSpaces Uses AWS KMS
- AWS CLI Command Reference – workspaces
- Monitoring Amazon WorkSpaces Metrics