AWS 白皮书

部署的最佳做法 WorkSpaces

部署的最佳做法 WorkSpaces: AWS 白皮书

Table of Contents

部署 Amazon 的最佳實踐 WorkSpaces

出版日期：二○二二年六月一日（文件修訂）

摘要

本白皮書概述了部署的一組最佳作法。 WorkSpaces本白皮書涵蓋網路考量、目錄服務及使用者驗證、安全性，以及監控與記錄。

本白皮書還可讓您快速存取相關資訊，適用於網路工程師、目錄工程師或安全工程師。

簡介

Amazon WorkSpaces 是雲中的一種託管桌面計算服務。Amazon WorkSpaces 免除了採購或部署硬體或安裝複雜軟體的負擔，並透過使用 Amazon Web Services (AWS) 命令列界面 (CLI) 或使用應用程式程式設計界面 (API) 按幾下，即可提供桌面體驗。AWS Management Console使用 Amazon WorkSpaces，您可以在幾分鐘內啟動 Microsoft Windows 或 Amazon Linux 桌面，從而使您能夠從現場部署或外部網路安全、可靠且快速地連接和存取桌面軟體。您可以：

- 使用 Directory Service：活動目錄連接器（AD 連接器），充分利用AWS 您現有的內部部署 Microsoft 活動目錄（AD Connector）。
- 將您的目錄擴展到 AWS 雲端。
- 使用 Direc AWS tory Service Microsoft AD 或 Simple AD 建立受管理的目錄，以管理您的使用者和 WorkSpaces.
- 利用內部部署或雲端託管的 RADIUS 伺服器搭配 AD Connector MFA，為您的. WorkSpaces

您可以使用 CLI 或 API 將 Amazon WorkSpaces 的佈建自動化，這可讓您 WorkSpaces 將 Amazon 整合到現有的佈建工作流程中。

為了安全起見，除了 Amazon WorkSpaces 服務提供的整合式網路加密之外，您還可以為您的 WorkSpaces. 請參閱本文件的 WorkSpaces「已加密」一節。

您可以使用現有的內部部署工具，例如 Microsoft 系統中心組態管理員 (SCCM)、傀儡企業或 Ansible 將應用程式部署到您的。 WorkSpaces

以下各節提供有關 Amazon 的詳細資訊 WorkSpaces、說明服務的運作方式、說明啟動服務所需的項目，以及告訴您可以使用哪些選項和功能。

WorkSpaces 要求

Amazon WorkSpaces 服務需要三個元件才能成功部署：

- WorkSpaces 用戶端應用程式 — WorkSpaces 支援 Amazon 的用戶端裝置。請參閱開始使用您的 WorkSpace。

  您也可以使用透過網際網路通訊協定 (PCoIP) 零用戶端的個人電腦進行連線。 WorkSpaces如需可用裝置的清單，請參閱 Amazon 專用的 PCoIP 零用戶端。 WorkSpaces
- 用於驗證用戶並提供訪問權限的 Directory Service WorkSpace-Amazon 目 WorkSpaces 前與AWS 目錄服務和 Microsoft AD 一起使用。您可以將現場部署 AD 伺服器與 AWS Directory Service 搭配使用，以支援 Amazon 現有的企業使用者登入資料 WorkSpaces。
- 要在其中執行 Amazon 的 Amazon 虛擬私有雲 (Amazon VPC) WorkSpaces — Amazon 部署至少需要兩個子網路，因為每個 AWS Directory Service 建構在異地同步備份 WorkSpaces部署中都需要兩個子網路。

網路考量

每個 WorkSpace 都與您用來建立它的特定 Amazon VPC 和 AWS Directory Service 建構相關聯。所有 AWS Directory Service 建構 (簡單 AD、AD Connector 和 Microsoft AD) 都需要兩個子網路才能運作，每個子網路都位於不同的可用區域 (AZ)。子網路與 Directory Service 建構永久關聯，在建立子網路後無法加以修改。因此，在建立目錄服務建構之前，務必先決定正確的子網路大小。在建立子網路之前，請仔細考慮下列事項：

- 隨著時間 WorkSpaces 的推移，您需要多少？
- 預期的增長是多少？
- 您需要容納哪些類型的使用者？
- 您將連接多少 AD 網域？
- 您的企業帳戶位於何處？

Amazon 建議根據您在規劃過程中所需的存取類型和使用者身份驗證來定義使用者群組或角色。當您需要限制對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、路由表和 VPC 安全性群組來區隔和限制存取。每個「AWS Directory Service」建構都使用兩個子網路，並將相同的設定套用至從 WorkSpaces 該建構啟動的所有子網路。例如，您可以使用套用至所有 WorkSpaces 連接至 AD Connector 的安全性群組，以指定是否需要 MFA，或者一般使用者是否可以擁有其 WorkSpace本機系統管理員存取權。

> **Note**
>
> 每個 AD 連接器連接到您現有的企業 Microsoft AD。若要利用此功能並指定組織單位 (OU)，您必須建構 Directory Service，以將使用者角色納入考量。

VPC 設計

本節說明調整 VPC 和子網路大小、流量流程的最佳做法，以及目錄服務設計的影響。

以下是為 Amazon 設計 VPC、子網路、安全群組、路由政策和網路存取控制清單 (ACL) 時需要考慮的一些事項，以 WorkSpaces 便您可以建立擴展、安全性和易於管理的 WorkSpaces 環境：

- VPC — 我們建議您專門針對您的 WorkSpaces 部署使用單獨的 VPC。使用單獨的 VPC，您可以 WorkSpaces 通過創建流量分隔來為您指定必要的控管和安全護欄。
- 目錄服務 — 每個 AWS Directory Service 建構都需要一對子網路，該子網路會在 AZ 之間提供高度可用的目錄服務分割。
- 子網路大小 — WorkSpaces 部署與目錄建構相關聯，並位於與您選擇的相同 VPC 中 AWS Directory Service，但可以位於不同的 VPC 子網路中。一些注意事項：
  - 子網路大小是永久的，無法變更。您應該為 future 的增長留出足夠的空間。
  - 您可以為您選擇的安全性群組指定預設安全性群組 AWS Directory Service。安全性群組會套用至所 WorkSpaces 有與特定 AWS Directory Service 建構相關聯的群組。
  - 您可以有多個 AWS Directory Service 使用相同子網路的執行個體。

設計 VPC 時，請考慮 future 的計劃。例如，您可能想要新增管理元件，例如防毒伺服器、修補程式管理伺服器或 AD 或 RADIUS MFA 伺服器。值得在 VPC 設計中規劃其他可用 IP 位址，以符合此類需求。

有關 VPC 設計和子網路大小的深入指導和考量事項，請參閱 re: Invent 簡報 Amazon.com 如何遷移到 Amazon。 WorkSpaces

網路介面

每個介面都 WorkSpaces 有兩個彈性網路介面 (ENI)、一個管理網路介面 (`eth0`) 和一個主要網路介面 (`eth1`)。 AWS 使用管理網路介面來管理用戶端連線終止的介面。 WorkSpace AWS 使用此介面的私有 IP 位址範圍。若要讓網路路由正常運作，您無法在任何可與 WorkSpaces VPC 通訊的網路上使用此私人位址空間。

如需每個區域使用的私有 IP 範圍清單，請參閱 Amazon WorkSpaces 詳細資訊。

> **Note**
>
> Amazon WorkSpaces 及其相關聯的管理網路界面不駐留在您的 VPC 中，而且您無法在您的虛擬私人雲端中檢視管理網路界面或 Amazon 彈性運算雲端 (Amazon EC2) 執行個體 ID AWS Management Console (請參閱Figure 5Figure 6、和Figure 7)。不過，您可以在主控台中檢視和修改主要網路介面 (`eth1`) 的安全性群組設定。每個界面的主要網路界面都 WorkSpace 會計入您的 ENI Amazon EC2 資源配額中。對於 Amazon 的大型部署 WorkSpaces，您需要透過以下方式開啟支援票證， AWS Management Console 以增加 ENI 配額。

流量

您可以將 Amazon WorkSpaces 流量分解為兩個主要組成部分：

- 客戶端設備和 Amazon WorkSpaces 服務之間的流量。
- Amazon WorkSpaces 服務和客戶網絡流量之間的流量。

下一節將討論這兩個元件。

用戶端裝置至 WorkSpace

無論其位置 (現場部署或遠端)，執行 Amazon 用 WorkSpaces戶端的裝置都會使用相同的兩個連接埠連線至 Amazon WorkSpaces 服務。用戶端使用連接埠 443 (HTTPS 連接埠) 來取得所有驗證和工作階段相關資訊，並使用連接埠 4172 (PCoIP 連接埠)，同時使用具有傳輸控制通訊協定 (TCP) 和使用者資料包通訊協定 (UDP) 的連接埠，以進行像素串流至指定和網路健康狀態檢查。 WorkSpace 兩個連接埠上的流量都經過加密。連接埠 443 流量用於驗證和工作階段資訊，並使用 TLS 來加密流量。像素串流流量使用 AES-256 位元加密，用戶端與`eth0`之間的通訊 WorkSpace，透過串流閘道。您可以在本文件的一安全節中找到更多資訊。

我們會發佈 PCoIP 串流閘道和網路健康狀態檢查端點的每個區域 IP 範圍。您可以將連接埠 4172 上的輸出流量限制從公司網路到 AWS 串流閘道和網路運作狀態檢查端點的連接埠 4172 上的輸出流量，方法是僅允許您使用 Amazon 的特定 AWS 區域。 WorkSpaces如需 IP 範圍和網路運作狀態檢查端點，請參閱 Amazon WorkSpaces PCoIP 閘道 IP 範圍。

Amazon 用 WorkSpaces 戶端具有內建的網路狀態檢查。此實用程序顯示用戶他們的網絡是否可以通過應用程序右下角的狀態指示器支持連接。下圖顯示更詳細的網路狀態檢視，可透過選擇用戶端右上角的 [網路] 來存取。

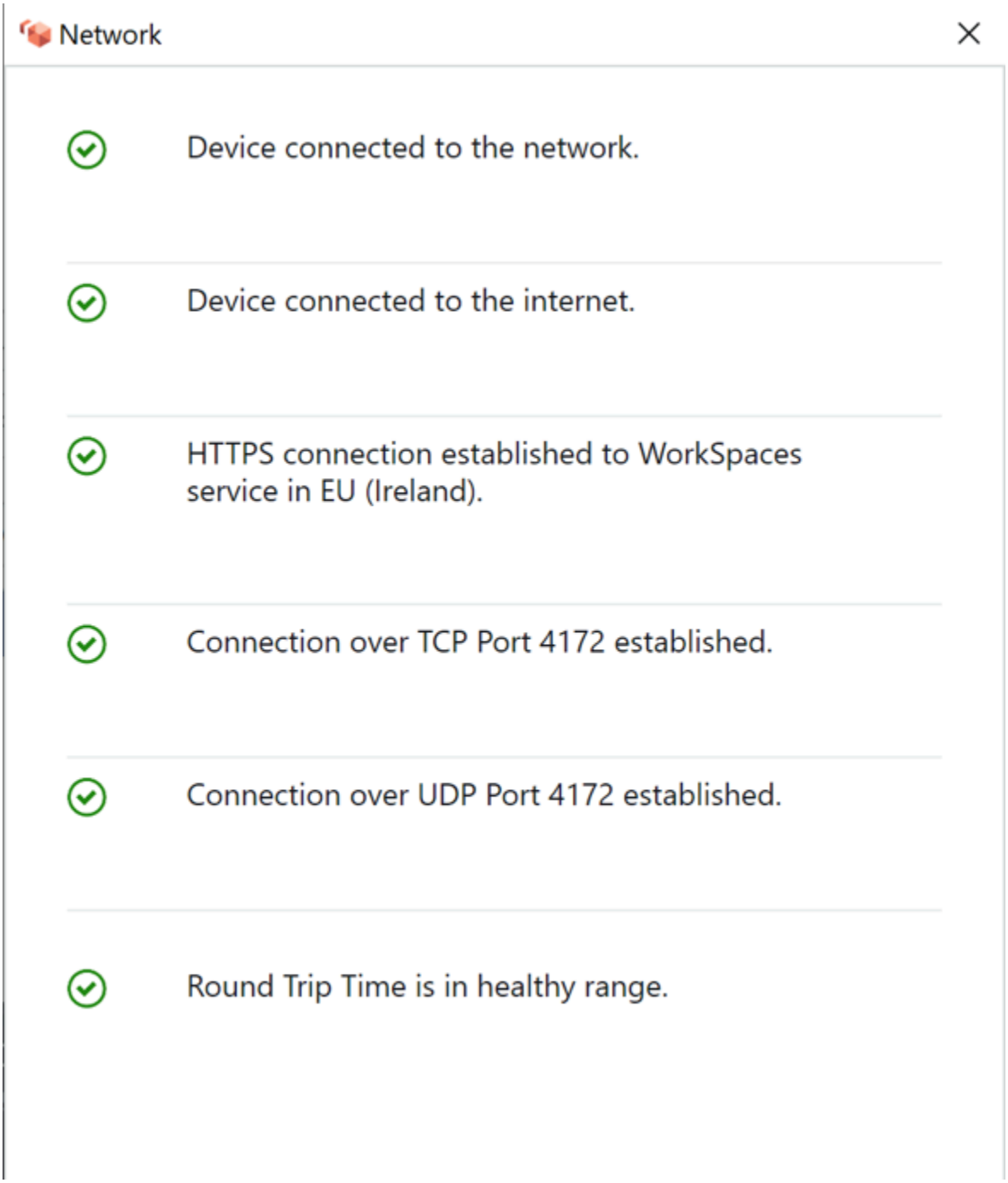

圖 1： WorkSpaces 用戶端：網路檢查

使用者透過提供 Directory Ser WorkSpaces vice 建構 (通常是其公司目錄) 所使用目錄的登入資訊，從其用戶端啟動 Amazon 服務的連線。登入資訊會透過 HTTPS 傳送至所在區域中 Amazon WorkSpaces 服務的身份驗證閘道。 WorkSpace 然後，Amazon WorkSpaces 服務的身份驗證閘道會將流量轉送到與您 WorkSpace相關聯的特定 AWS Directory Service 結構。

例如，使用 AD 連接器時，AD Connector AD Connector 會將驗證要求直接轉送至 AD 服務，而 AD 服務可能位於內部部署或 AWS VPC 中。如需詳細資訊，請參閱本文件的 AD DS 部署案例一節。AD Connector 不會儲存任何驗證資訊，而且它充當無狀態 Proxy。因此，AD 連接器必須具有 AD 伺服器的連線能力。AD Connector 器會使用您在建立 AD 連接器時定義的 DNS 伺服器來決定要連線到哪個 AD Connector。

如果您正在使用 AD Connector，並且已在目錄上啟用 MFA，則會在目錄服務驗證之前檢查 MFA Token。如果 MFA 驗證失敗，使用者的登入資訊就不會轉寄至您的 AWS Directory Service。

一旦使用者通過驗證，串流流量就會開始使用連接埠 4172 (PCoIP 連接埠) 透過 AWS 串流閘道到. WorkSpace 在整個工作階段中，仍會透過 HTTPS 交換工作階段相關資訊。串流流量使用未連接至 VPC 的 WorkSpace (`eth0`上 WorkSpace) 上的第一個 ENI。從串流閘道到 ENI 的網路連線由管理 AWS。如果從串流閘道到串 WorkSpaces 流 ENI 的連線失敗，就會產生 CloudWatch 事件。如需詳細資訊，請參閱本文件的「使用 Amazon 監控或記錄」一 CloudWatch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程度。為確保使用者獲得最佳體驗，我們建議用 WorkSpaces 戶端與您 WorkSpaces 所在 AWS 地區之間的往返時間 (RTT) 少於 100 毫秒 (ms)。通常情況下，這意味著您的 WorkSpaces 客戶距離託管的地區不到 WorkSpace 兩千英里。連線運作 Health 態檢查網頁可協助您判斷連線至 Amazon WorkSpaces 服務的最佳 AWS 區域。

VPC 的 Amazon WorkSpaces 服務

從用戶端到某個連線驗證 WorkSpace 並啟動串流流量後， WorkSpaces 用戶端會顯示連線到虛擬私有雲 (VPC WorkSpace) 的 Windows 或 Linux 桌面平台 (您的 Amazon)，而您的網路應該會顯示您已建立該連線。識別為 WorkSpace`eth1`的主要彈性網路介面 (ENI) 將具有從 VPC 提供的動態主機設定通訊協定 (DHCP) 服務 (通常來自與 AWS Directory Service 相同的子網路) 指派給它的 IP 位址。IP 位址會保 WorkSpace持在的生命週期內 WorkSpace。VPC 中的 ENI 可以存取 VPC 中的任何資源，以及您連接到 VPC 的任何網路 (透過 VPC 對等互連、連線或 VPN AWS Direct Connect 連線)。

ENI 對您網路資源的存取權取決於子網路的路由表和 AWS Directory Service 為每個群組設定的預設安全性群組 WorkSpace，以及您指派給 ENI 的任何其他安全性群組。您可以隨時使用 AWS Management Console 或 AWS CLI將安全群組新增至面對 VPC 的 ENI。如需有關安全性群組的詳細資訊，請參閱您的安全性群組 WorkSpaces。) 除了安全群組之外，您還可以在指定的上使用偏好的主機型防火牆 WorkSpace 來限制對 VPC 內資源的網路存取。

建議您使用 DNS 伺服器 IP 和完全合格的網域名稱來設定 DHCP 選項，這些網域名稱對您的環境有特定權威，然後將這些自訂建立的 DHCP 選項指派給 Amazon 使用的 Amazon VPC。 WorkSpaces根

據預設，Amazon Virtual Private Cloud (Amazon VPC) 使用 AWS DNS 而不是您的目錄服務 DNS。使用 DHCP 選項集將確保適當的 DNS 名稱解析和內部 DNS 名稱伺服器的組態一致，不僅適用於您 WorkSpaces，還可以針對您的部署規劃的任何支援工作負載或執行個體。

套用 DHCP 選項時，與傳統 EC2 執行個體套用方式相比，套用 WorkSpaces DHCP 選項的方式有兩個重要差異：

- 第一個區別是 DHCP 選項 DNS 後綴將如何應用。每個人都 WorkSpace 有為其網路介面卡設定 DNS 設定，並啟用 [附加主要 DNS 尾碼] 和 [附加主要 DNS 尾碼] 選項的 [附加主要和連線特定 DNS 尾碼] 選項的上層尾碼。 WorkSpace 依預設，組態將更新為在您註冊的 AWS Directory Service 中設定的 DNS 尾碼，並與之相關聯的 DNS 尾碼。此外，如果在使用的 DHCP 選項集中配置的 DNS 尾碼不同，它將被添加並應用到任何相關聯的 WorkSpaces。
- 第二個差異是，由於 Amazon WorkSpaces 服務會優先排列已設定目錄的網域控制站 IP 位址，WorkSpace 因此不會套用設定的 DHCP 選項 DNS IP。

或者，您可以設定 Route 53 私有託管區域以支援混合式或分割 DNS 環境，並為您的 Amazon 環 WorkSpaces 境取得適當的 DNS 解析。如需詳細資訊，請參閱 VPC 和混合式 DNS 與使用中目錄的 AWS 混合式雲端 DNS 選項。

> **Note**
>
> 將新的或不同的 DHCP 選項集套用至 VPC 時，每個選項都 WorkSpace 必須重新整理 IP 表格。若要重新整理，您可以執行 ipconfig /更新或重新啟動VPC 中的任何 WorkSpace已更新 DHCP 選項集。如果您正在使用 AD Connector 器，並更新連線 IP 位址/網域控制站的 IP 位址，則必須接著更新. `DomainJoinDNS` WorkSpaces 建議您透過 GPO 執行這項操作。此登錄機碼的路徑為`HKLM:\SOFTWARE\Amazon\Skylight`。如果修改 AD 連接器的 DNS 設定，則不會更新此`REG_SZ`值，且 VPC DHCP 選項組也不會更新此金鑰。

本白皮書「AD DS 部署案例」一節中的圖顯示了描述的流量流量。

如前所述，Amazon WorkSpaces 服務會優先設定 DNS 解析目錄的網域控制站 IP 位址，並忽略 DHCP 選項集中設定的 DNS 伺服器。如果您需要對 Amazon 的 DNS 伺服器設定進 WorkSpaces 行更精細的控制 WorkSpaces，可以在 Amazon 管理指南的 Amazon 更新 DNS 伺服器 WorkSpaces指南 WorkSpaces 中使用說明更新 Amazon 的 DNS 伺服器。

如果您 WorkSpaces 需要解析中的其他服務 AWS，並且使用 VPC 設定的預設 DHCP 選項，則必須將此 VPC 中的網域控制器 DNS 服務設定為使用 DNS 轉送，指向具有 IP 位址位於 VPC CIDR 基礎的

Amazon DNS 伺服器，請使用標準 DNS 轉送 53 路由加上兩個；也就是說，如果您的 VPC CIDR 為 10.0.0/24，請使用路由 53 設定 DNS 轉送一點零點

如果您 WorkSpaces 需要內部部署網路上的資源 DNS 解析，可以使用 Route 53 解析器輸出端點、建立 R oute 53 轉送規則，然後將此規則與需要此 DNS 解析的 VPC 產生關聯。如果您已將網域控制站 DNS 服務上的轉送設定為 VPC 的預設 Route 53 DNS 解析器 (如上一段所述)，您可以在 Amazon Route 53 開發人員指南的解析 VPC 與您的網路指南中找到 DNS 解析程序。

如果您使用的是預設 DHCP 選項集，而且您需要 VPC 中不屬於您 Active Directory 網域一部分的其他主機，才能解析 Active Directory 命名空間中的主機名稱，則可以使用此路由 53 解析器輸出端點，並新增另一個將 Active Directory 網域的 DNS 查詢轉送至 Active Directory DNS 伺服器的路由 53 轉送規則。此路由 53 轉送規則必須與能夠連線到您的 Active Directory DNS 服務的路由 53 解析器輸出端點相關聯，以及您想要啟用以解析 WorkSpaces Active Directory 網域中 DNS 記錄的所有 VPC。

同樣地，Route 53 解析器輸入端點可用於允許從內部部署網路解析 WorkSpaces Active Directory 網域的 DNS 記錄的 DNS 記錄。

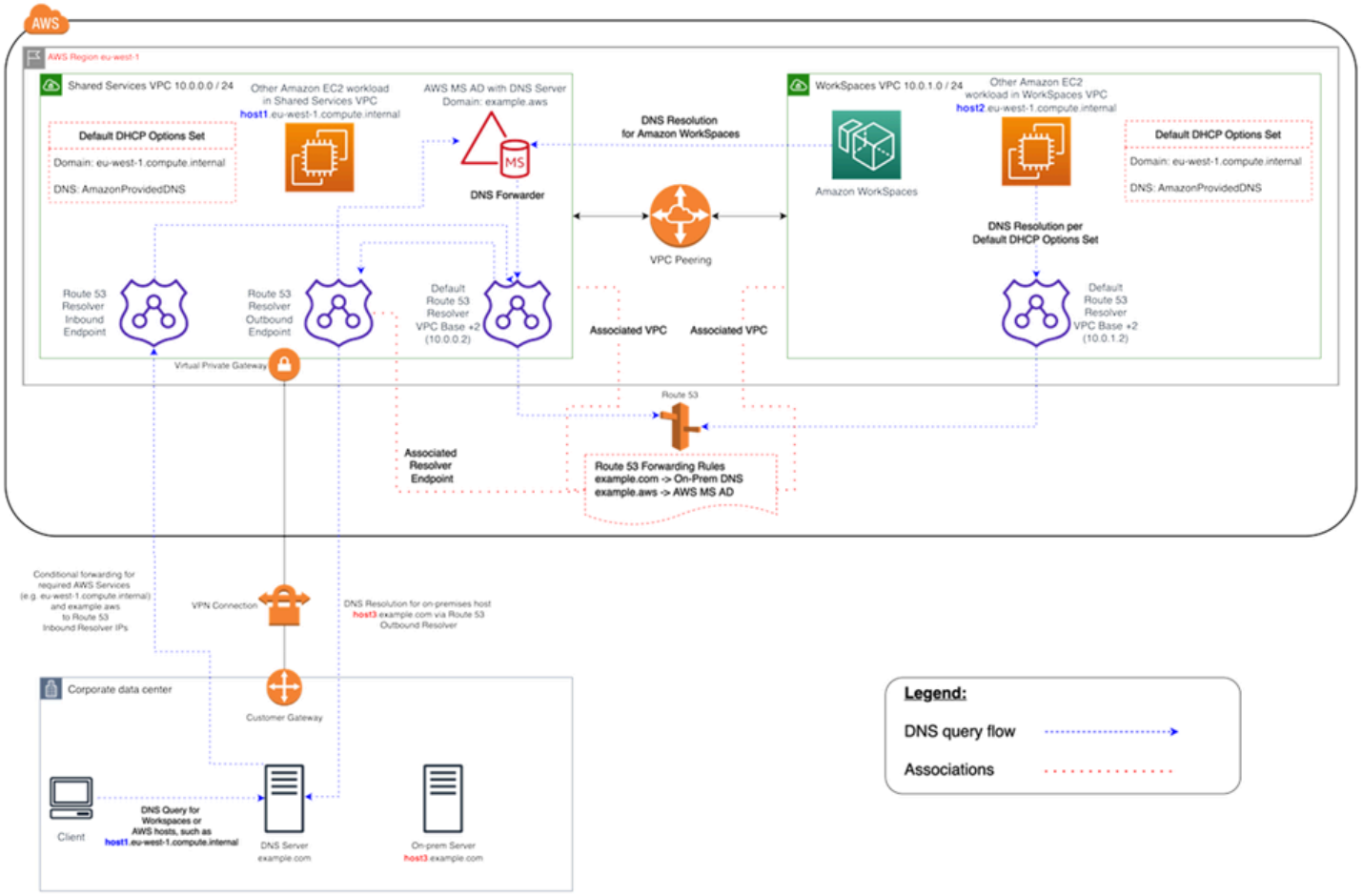

圖 2：路由 53 端點的 WorkSpaces DNS 解析示例

- 您的 Amazon WorkSpaces 將使用 AWS Directory Service for Microsoft Active Directory （AWS Managed Microsoft AD）DNS 服務進行 DNS 解析。 AWS Managed Microsoft AD DNS 服務會解析example.aws網域，並將所有其他 DNS 查詢轉送至 VPC CIDR 基礎 IP 位址 +2 的預設路由 53 DNS 解析程式，以啟用 DNS 解析

  共用服務 VPC 包含一個 Route 53 輸出解析程式端點，該端點與兩個 Route 53 轉送規則相關聯。其中一個規則會將example.com網域的 DNS 查詢轉送至內部部署 DNS 伺服器。第二個規則會將您 AWS Managed Microsoft AD 網域的 DNS 查詢轉送example.aws至共用服務 VPC 中的作用中目錄 DNS 服務。

  使用此架構，您的 Amazon WorkSpaces 將能夠解決以下內容的 DNS 查詢：

  - 您的 AWS Managed Microsoft AD 網域example.aws。
  - 網域中的 EC2 執行個體設定為預設 DHCP 選項 (例如host1.eu-west-1.compute.internal)，以及其他 AWS 服務或端點。
  - 內部部署網域中的主機和服務，例如host3.example.com.
- • 只要 Route 53 轉送規則與兩個 VPC 相關聯 WorkSpaces，共用服務 WorkSpaces VPC (host1.eu-west-1.compute.internalhost2.eu-west-1.compute.internal) 和 VPC () 中的其他 EC2 工作負載可以執行與您相同的 DNS 解析。在這種情況下，example.aws網域的 DNS 解析會透過 VPC CIDR 基礎 IP 位址 +2 的預設 Route 53 DNS 解析器進行，每個已設定和相關聯的 Route 53 轉送規則會透過 Route 53 解析器輸出端點將它們轉送至作用中目錄 DNS 服務。 WorkSpaces
- • 最後，內部部署用戶端也可以執行相同的 DNS 解析，因為內部部署 DNS 伺服器設定了example.aws和eu-west-1.compute.internal網域的條件轉寄站，將這些網域的 DNS 查詢轉寄至 Route 53 解析器輸入端點 IP 位址。

典型組態的範例

假設您有兩種類型的使用者，而您的 AWS Directory Service 會使用集中式 AD 進行使用者驗證的案例：

- 需要從任何地方完整存取權的工作者 (例如，全職員工) — 這些使用者將擁有網際網路和內部網路的完整存取權，而且他們會透過防火牆從 VPC 傳送到內部部署網路。
- 應僅限制從企業網路內部存取的工作者 (例如，承包商和顧問) — 這些使用者限制了透過 Proxy 伺服器存取 VPC 中特定網站的網際網路，並且在 VPC 和內部部署網路中的網路存取權限有限。

您想讓全職員工擁有安裝軟體的本機管理員存取權限，並且想 WorkSpace 要使用 MFA 強制執行雙因素驗證。您還希望允許全職員工訪問互聯網沒有從他們的限制 WorkSpace.

對於承包商，您想要封鎖本機管理員存取，以便他們只能使用特定的預先安裝的應用程式。您想要使用安全性群組來套用限制性網路存取控制。 WorkSpaces您只需要開啟特定內部網站的通訊埠 80 和 443，而且您想要完全封鎖他們對網際網路的存取。

在這個案例中，有兩種完全不同類型的使用者角色具有不同的網路和桌面存取需求。這是管理和配置 WorkSpaces 不同的最佳做法。您將需要創建兩個 AD 連接器，每個用戶角色一個。每個 AD Connector 都需要兩個子網路，這些子網路具有足夠的 IP 位址，以符合 WorkSpaces使用量成長預估值。

> **Note**
>
> 每個 AWS VPC 子網路會耗用五個 IP 位址 (前四個和最後一個 IP 位址) 來進行管理，而且每個 AD Connector 會在持續存在的每個子網路中耗用一個 IP 位址。

此案例的進一步考量如下：

- AWS VPC 子網路應該是私有子網路，以便透過網路位址轉譯 (NAT) 閘道、雲端中的 Proxy NAT 伺服器或透過內部部署流量管理系統路由回路由來控制流量 (例如網際網路存取)。
- 針對綁定到內部部署網路的所有 VPC 流量都有防火牆。
- Microsoft AD 伺服器和 MFA RADIUS 伺服器可能是內部部署 (請參閱本文件中的案例 1：使用 AD Connector 器對內部部署 AD DS 進行 Proxy 驗證) 或部分的 AWS 雲端實作 (請參閱本文件中的案例 2 和案例 3，AD DS 部署案例)。

鑑於所有人 WorkSpaces 都被授予某種形式的互聯網訪問，並且鑑於它們託管在私有子網中，您還必須創建可以通過 Internet 網關訪問 Internet 的公共子網絡。您需要為全職員工提供 NAT 閘道，允許他們存取網際網路，以及供顧問和承包商使用的 Proxy NAT 伺服器，以限制他們對特定內部網站的存取。若要規劃故障、設計高可用性以及限制跨可用區域流量費用，在異地同步備份部署中，您應該在兩個不同的子網路中使用兩個 NAT 閘道和 NAT 或 Proxy 伺服器。您選取做為公用子網路的兩個 AZ 將符合您在具有兩個以上區域的區域中用於 WorkSpaces 子網路的兩個 AZ。您可以將每個 WorkSpaces AZ 的所有流量路由至對應的公有子網路，以限制跨可用區的流量費用，並提供更輕鬆的管理。下圖顯示 VPC 組態。

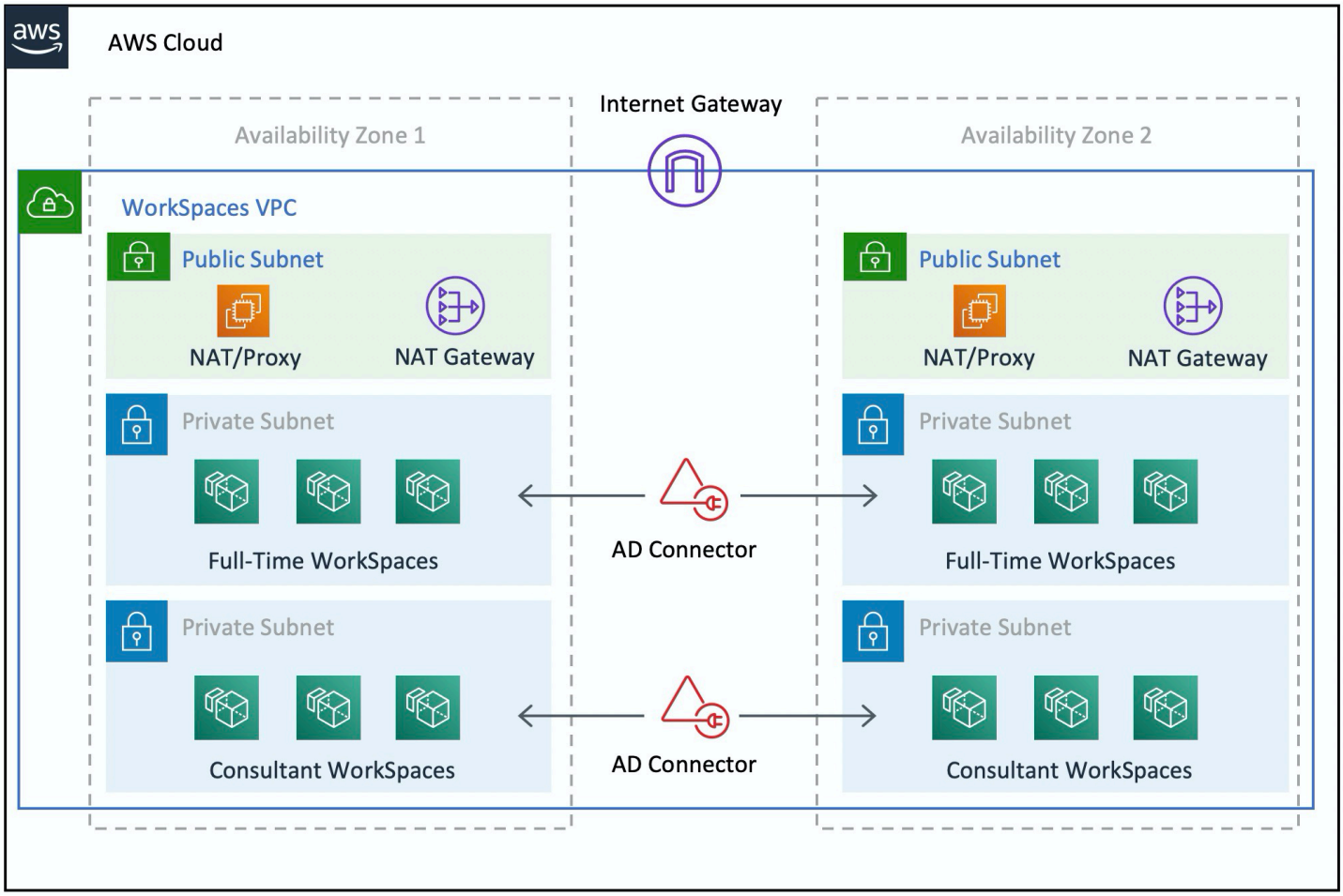

圖 3：高階 VPC 設計

下列資訊說明如何設定兩 WorkSpaces 種不同類型：

若要 WorkSpaces 為全職員工設定：

1. 在 Amazon WorkSpaces 管理主控台中，選擇功能表列上的目錄選項。
2. 選擇託管全職員工的目錄。
3. 選擇本機管理員設定。

啟用此選項後，任何新建立的都 WorkSpace 將具有本機管理員權限。若要授與網際網路存取權，請將 NAT 設定為從您的 VPC 傳出網際網路存取。若要啟用 MFA，您需要指定 RADIUS 伺服器、伺服器 IP、連接埠和預先共用金鑰。

對於全職員工 WorkSpaces，透過 AD Connector 設定套用預設安全性群組， WorkSpace 可以限制為服務台子網路的遠端桌面通訊協定 (RDP)。

若要 WorkSpaces 為承包商和顧問設定：

1. 在 Amazon WorkSpaces 管理主控台中，停用網際網路存取和本機管理員設定。
2. 在「安全性群組設定」區段下新增安全性群組，以針對在該目錄下 WorkSpaces建立的所有新建立強制執行安全性群組。

對於顧問 WorkSpaces，透過 AD Connector 設定將預設的安全性群組套 WorkSpaces 用至與 AD 連接器 WorkSpaces 相關聯的所有項目，將輸出和入站流量限制為。安全性群組可防止從 HTTP 和 HTTPS 流量 WorkSpaces 以外的任何內容的對外存取，以及從內部部署網路中的服務台子網路至 RDP 的輸入流量。

> **Note**
>
> 安全性群組僅適用於 VPC 中的 ENI (在`eth1`上 WorkSpace)，並且不會因為安全性群組而限制 WorkSpace 從用 WorkSpaces 戶端存取。下圖顯示最終的 WorkSpaces VPC 設計。

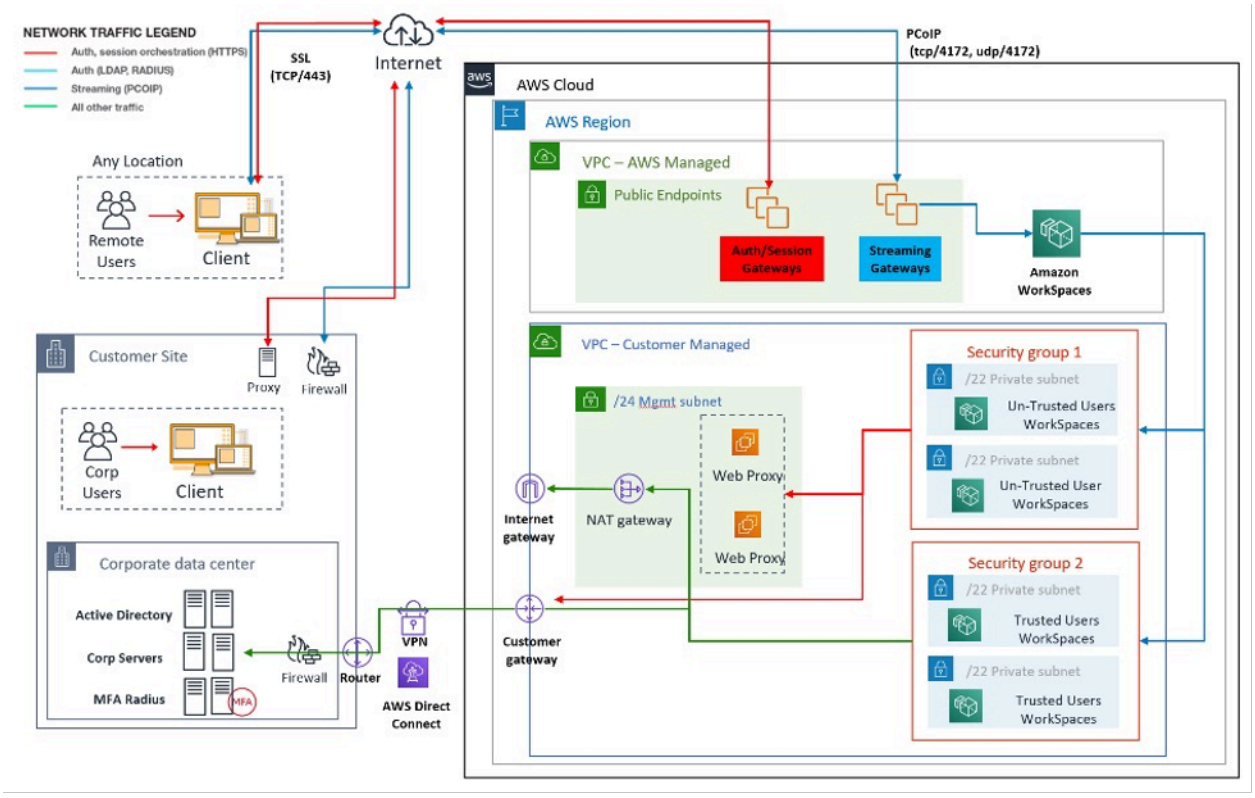

圖 4：使用者角色的 WorkSpaces 設計

AWS Directory Service

如簡介所述， AWS Directory Service 是 Amazon 的核心組成部分 WorkSpaces。使用 AWS Directory Service，您可以使用 Amazon 建立三種類型的目錄 WorkSpaces：

- AWS 管理 Microsoft AD 是一個託管 Microsoft AD，搭載視窗服務器 2012 R2。 AWS 託管 Microsoft AD 提供標準版或企業版。
- S@@ imple AD 是獨立的、與 Microsoft 廣告相容的受管目錄服務，由 Samba 4 提供支援。
- AD Connector 是一種目錄代理，用於將驗證要求和使用者或群組查詢重新導向至您現有的內部部署 Microsoft AD。

下節說明 Amazon WorkSpaces 經紀服務 WorkSpaces與 AWS Directory Service 之間的身份驗證通訊流程、使用 AWS Directory Service 實作的最佳實務，以及進階概念 (例如 MFA)。它還討論了大規模 Amazon WorkSpaces 的基礎設施架構概念、Amazon VPC 上的要求以及 AWS Directory Service，包括與現場部署 Microsoft AD 網域服務 (AD DS) 的整合。

AD DS 部署案例

支援 Amazon WorkSpaces 是 AWS Directory Service，目錄服務的正確設計和部署至關重要。以下六個案例建立在 AWS 快速入門指南中的 Active Directory 網域服務上，並說明與 Amazon 搭配使用時 AD DS 的最佳實務部署選項 WorkSpaces。本文件的「設計考量」一節詳細說明使用 AD Connector 的特定需求和最佳作法 WorkSpaces，這是整體 WorkSpaces設計概念中不可或缺的一部分。

- 案例 1：使用 AD Connector 將驗證代理至內部部署 AD DS — 在這個案例中，網路連線 (VPN/Direct Connect) 會提供給客戶，並透過 AWS Directory Service (AD Connector) 代理至客戶內部部署 AD DS 的所有驗證。
- 案例 2：將內部部署 AD DS 延伸至 AWS (複本) — 這個案例類似於案例 1，但是這裡的客戶 AD DS 複本會與 AD 連接器搭配部署，以減少 AD DS 和 AD DS 通用類別目錄的驗證/查詢要求的延遲。AWS
- 案例 3：在 AWS 雲端中使用 AWS Directory Service 的獨立隔離部署 — 這是一個隔離的案例，不包括回傳給客戶進行驗證的連線。這種方法使用 AWS Directory Service（Microsoft AD）和 AD Connector。雖然這個案例並不依賴客戶的連線來進行驗證，但它確實會在需要透過 VPN 或直 Connect 線時佈建應用程式流量。
- 案例 4： AWS Microsoft AD 和內部部署的雙向傳遞信任 — 這個案例包括 AWS 受管理的 Microsoft AD 服務 (MAD) 與內部部署 Microsoft AD 樹系的雙向傳遞信任。
- 案例 5：使用共用服務 VPC 的 AWS Microsoft AD — 此案例在使用 AD 連接器將輕量型目錄存取通訊協定 (LDAP) 代 AWS 理輕量型目錄存取通訊協定 (LDAP) 使用者驗證請求時，使用受管 Microsoft AD 作為多個 AWS 服務 (Amazon EC2 WorkSpaces、Amazon 等) 的身分識別網域使用。
- 案例 6： AWS Microsoft AD、共用服務 VPC 和單向信任內部部署 AD — 此案例類似於案例 5，但包含使用內部部署單向信任的不同身分識別和資源網域。

當您選取使用中目錄網域服務 (ADDS) 的部署案例時，您需要考量一些事項。本節說明 AD Connector 與 Amazon 的角色 WorkSpaces，並涵蓋選取 ADDS 部署案例時的一些重要考量事項。有關 ADDS 的設計和規劃的進一步指導 AWS，請參閱 Active Directory 域名服務的 AWS 設計和規劃指南。

AWS AD Connector 與 Amazon 的作用 WorkSpaces

AWS AD Connector 是一種 AWS Directory Service，可做為「作用中目錄」的代理服務。它不會儲存或快取任何使用者認證，但會將驗證或查閱要求轉送至您的 Active Directory (內部部署或上)。 AWS除非您正在使用 AWS Managed Microsoft AD，否則它也是註冊您的 Active Directory（現場部署或擴展到 AWS）以與 Amazon WorkSpaces （WorkSpaces）一起使用的唯一方法。

AD Connector 器可以指向您的現場部署作用中目錄、延伸至 AWS (Amazon EC2 上的 AD 網域控制站) 的作用中目錄，或指向 AWS Managed Microsoft AD.

AD Connector 在以下各節中涵蓋的大多數部署案例中扮演著重要的角色。搭配使用 AD Connector 可 WorkSpaces 提供許多好處：

- 當指向您的公司 Active Directory 時，它允許您的使用者使用其現有的企業登入資料登入 WorkSpaces 和其他服務，例如 Amazon WorkDocs。
- 您可以持續套用現有的安全性原則 (密碼到期、帳戶鎖定等)，無論您的使用者正在存取內部部署基礎結構中的資源，或是存取中的資源 AWS 雲端，例如 WorkSpaces.
- AD Connector 可與您現有的 Radius-based MFA 基礎架構進行簡單整合，以提供額外的安全性層。
- 它可以讓您的使用者隔離。例如，它允許設定每個業務單位或角色的數個 WorkSpaces 選項，因為多個 AD 連接器可以指向 Active Directory 的相同網域控制站 (DNS 伺服器)，以進行使用者驗證：
  - 作用中目錄群組原則物件 (GPO) 之目標應用程式的目標網域或組織單位
  - 不同的安全群組來控制流量往返 WorkSpaces
  - 不同的存取控制選項 (允許的用戶端裝置) 和 IP 存取控制群組 (限制對 IP 範圍的存取)
  - 選擇性啟用本機管理員權限
  - 不同的自助權限
  - 選擇性強制執行 Multi-Factor Authentication (MFA)
  - 將您的 WorkSpaces 彈性網路介面 (ENI) 放置到不同的 VPC 或子網路中以進行隔離

如果您達到單一小型或大型 AD 連接器的效能限制，則多個 AD Connector 器也可以支援更多使用者。請參閱的尺寸 AWS Managed Microsoft AD部分以獲取更多詳細信息。

使用 AD 連接器 WorkSpaces 是免費的，只要您在小型 AD 連接器中至少有一個作用中使用 WorkSpaces 者，大型 AD Connector 器中至少有 100 個作用中使用 WorkSpaces 者即可。如需詳細資訊，請參閱目AWS 錄服務定價頁面。

AWS 使用內部部署作用中目錄的網路連結的重要性

WorkSpaces 依賴於連接到您的活動目錄。因此，您的活動目錄的網絡鏈接的可用性是至關重要的。例如，如果您在案例 1 中的網路連結關閉，您的使用者將無法進行驗證，因此將無法使用他們的 WorkSpaces.

如果要使用內部部署 Active Directory 做為案例的一部分，您必須考慮網路連結的復原能力、延遲和流量成本。 AWS在多地區 WorkSpaces 部署中，這可能涉及不同區 AWS 域中的多個網路連結，或是在

它們之間建立了多個 AWS Transit Gateway對等連結，以便將 AD 流量路由到 VPC，並連線到內部部署 AD。這些網路連結考量適用於下列各節中所述的大部分案例，但對於 AD 連接器的 AD 流量，而且 WorkSpaces 需要周遊網路連結才能到達內部部署 Active Directory 的那些案例尤其重要。 情況 1 突出顯示了一些警告。

使用多因素身份驗證 WorkSpaces

如果您打算搭配使用 Multi-Factor Authentication (MFA) WorkSpaces，則必須使用 AWS AD Connector 或 AWS Managed Microsoft AD，因為只有這些服務允許註冊目錄以與 RADIUS 搭配使用 WorkSpaces 和設定。若要放置 RADIUS 伺服器，則適用AWS 使用內部部署作用中目錄的網路連結的重要性本節中涵蓋的網路連結考量。

分隔帳號和資源網域

基於安全性考量或為了更好的管理性，您可能需要將帳號網域與資源網域分開。例如，將 [WorkSpaces 電腦物件] 放入個別的 [資源網域] 中，而 [使用者] 則是 [帳號網域] 的一部分。這樣的實作可用於允許合作夥伴組織管理資源網域中 WorkSpaces使用 AD 群組原則，同時不會放棄控制權或授與帳戶網域的存取權。這可以通過使用兩個活動目錄與配置的活動目錄信任來完成。以下各節將更詳細地介紹這一點：

- 案例 4： AWS Microsoft AD 和內部部署的雙向傳遞信任
- 案例 6： AWS Microsoft AD、共用服務 VPC，以及內部部署的單向信任

大型作用中目錄部署

您必須確保活動目錄站點和服務相應地配置。如果您的 Active Directory 包含大量位於不同地理位置的網域控制站，這一點尤其重要。您的 Windows WorkSpaces 使用標準的 Microsoft 機制來探索他們的網域控制站的作用中目錄網站，它們被指派到。這個 DC 定位器處理程序依賴於 DNS，如果冗長的網域控制站清單具有不特定的優先順序和權重在 DC 定位器處理序的早期階段傳回，可能會顯著延長。更重要的是，如果您「固定」 WorkSpaces 到次最佳的網域控制站，所有後續與此網域控制站的通訊可能會遭受增加的網路延遲和減少頻寬的周遊廣域網路連結時。這會減慢與網域控制站的任何通訊速度，包括處理可能大量的群組原則物件 (GPO)，以及從網域控制站傳輸檔案。視網路拓撲而定，也可能會增加您的網路成本，因為 WorkSpaces 和網域控制站之間交換的資料可能會不必要地周遊較昂貴的網路路徑。如需有關您 VPC 設計的 DHCP 和 DNS 以及使用中目錄網站與服務的指引，請參閱和設計考量章節。VPC 設計

使用 Microsoft Azure 活動目錄或活動目錄域服務 WorkSpaces

如果您打算使用 Microsoft Azure 活動目錄 WorkSpaces，您可以使用 Azure 的 AD Connect 與您的現場部署活動目錄或與您的活動目錄 AWS （ 在 Amazon EC2 上的域控制器 AWS Managed Microsoft AD ）同步您的身份。但是，這將不允許您加入 WorkSpaces 到您的 Azure 活動目錄。如需詳細資訊，請參閱 Microsoft Azure 文件中的 Microsoft 混合身分識別文件。

如果你想要加入您 WorkSpaces 的 Azure 活動目錄，您將需要部署 Microsoft Azure 活動目錄域服務（ Azure AD DS ），建立 AWS 和 Azure 之間的連接，並使用 AWS AD Connector 器指向您的 Azure AD DS 域控制器。如需有關如何設定此項目的詳細資訊，請參閱使用 Azure 作用中目錄網域服務將您新增 WorkSpaces 至 Azure AD 部落格文章。

搭配使用 AWS Directory Service s 時 WorkSpaces，您必須考慮 WorkSpaces部署的大小及其預期成長，才能 AWS Directory Service 適當地調整大小。本節提供調整大小以搭配使 AWS Directory Service 用的指南 WorkSpaces。我們也建議您檢閱 AD Connector 的最佳做法，以及《AWS Directory Service 管理指南》 AWS Managed Microsoft AD各節的最佳做法。

AD Connector 尺寸 WorkSpaces

作用中目錄連接器 (AD Connector) 有兩種大小：小型和大型。雖然沒有強制使用者或連線限制，但我們建議您使用小型 AD Connector，最多可容納 500 WorkSpaces 名授權的使用者，以及最多可容納 5000 WorkSpaces 名獲權使用者的大型 AD Connector。您可以將應用程式負載分散到多個 AD Connector，以根據效能需求進行擴充。例如，如果您需要支援 1500 個 WorkSpaces 使用者，您可以將您的 WorkSpaces 平均分散到三個小型 AD 連接器，每個連接器都支援 500 位使用者。如果所有使用者都位於相同的網域中，AD Connector 器可以全部指向解析您 Active Directory 網域的同一組 DNS 伺服器。

請注意，如果您開始使用小型 AD Connector，且 WorkSpaces 部署隨著時間的推移而成長，您可以提出支援票證，讓 AD Connector 的大小從小變更為大，以處理更多有 WorkSpaces 權使用者。

的尺寸 AWS Managed Microsoft AD

AWS Managed Microsoft AD可讓您以受管理服務的形式執行 Microsoft 活動目錄。啟動服務時，您可以選擇標準版和企業版。標準版適用於擁有最多 5,000 名使用者的中小型企業，最多可支援 30,000 個目錄物件，例如使用者、群組和電腦。企業版最多可支援 500,000 個目錄物件，並提供額外的功能，例如多區域複寫。

如果您需要支援超過 500,000 個目錄物件，請考慮在 Amazon EC2 上部署 Microsoft 活動目錄網域控制器。如需這些網域控制站的大小，請參閱 Microsoft 的使用中目錄網域服務的容量規劃文件。

案例 1 ：使用 AD 連接器對內部部署作用中 Directory Service 的代理驗證

這個案例適用於不想要擴充其內部部署 AD 服務 AWS，或 AD DS 的新部署不是選項的客戶。下圖顯示了高級別，每個組件和用戶身份驗證流程。

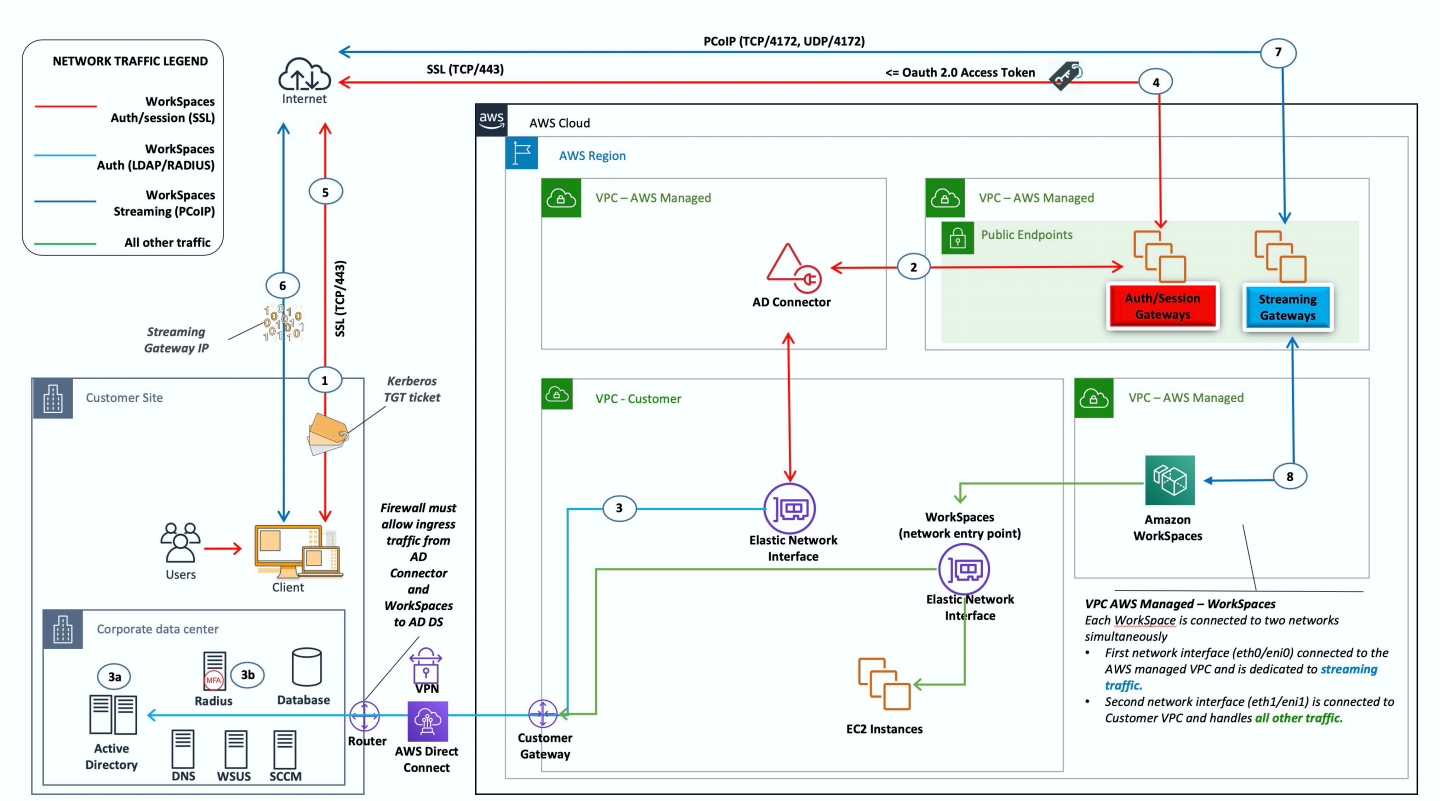

圖 5：AD Connector 到內部部署活動目錄

在這個案例中， AWS Directory Service (AD Connector) 會用於透過 AD 連接器代理至客戶內部部署 AD DS 的所有使用者或 MFA 驗證 (如下圖所示)。如需有關驗證程序所使用之通訊協定或加密的詳細資訊，請參閱本文件的安全章節。

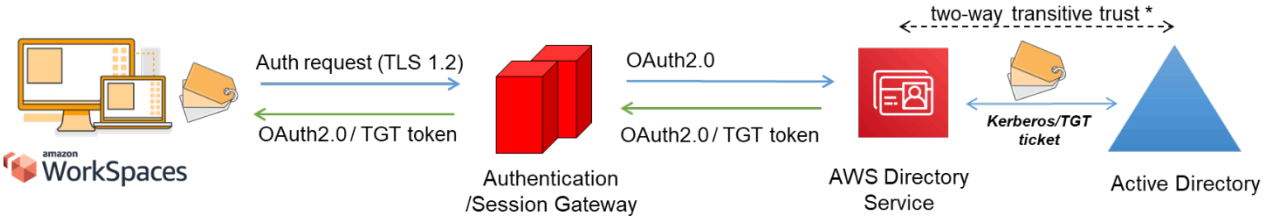

圖 6：透過驗證閘道進行使用者驗證

案例 1 顯示客戶可能已經擁有資源的混合式架構 AWS，以及可透過 Amazon 存取的現場部署資料中心中的資源 WorkSpaces。客戶可以利用現有的內部部署 AD DS 和 RADIUS 伺服器進行使用者和 MFA 驗證。

此架構使用下列元件或建構：

AWS

- Amazon VPC — 建立具有跨兩個 AZ 的至少兩個私有子網路的 Amazon VPC。
- DHCP 選項集 — 建立一個 Amazon VPC 端 DHCP 選項集。這可讓您定義客戶指定的網域名稱和網域名稱伺服器 (DNS) (內部部署服務)。如需詳細資訊，請參閱 DHCP 選項集。
- Amazon 虛擬私有閘道 — 啟用透過 IPSec VPN 通道或 AWS Direct Connect 連線與您自己的網路通訊。
- AWS Directory Service — AD Connector 部署到一對 Amazon VPC 私有子網路中。
- Amazon WorkSpaces — 部署 WorkSpaces 在與 AD Connector 相同的私有子網中。如需詳細資訊，請參閱本文件的 Active Directory：網站與服務一節。

客戶

- 網路連線 — 企業 VPN 或直 Connect 線端點。
- 廣告 DS — 企業廣告 DS.
- MFA（可選）— 公司 RADIUS 服務器。
- 終端使用者裝置 — 用於存取 Amazon 服務的企業或自攜授權 (BYOL) 使用者裝置 (例如 Windows、Mac、iPads、安卓平板電腦、零用戶端和 Chromebook)。 WorkSpaces 如需支援的裝置和 Web 瀏覽器，請參閱此用戶端應用程式清單。

雖然此解決方案對於不想將 AD DS 部署到雲端的客戶來說非常有用，但確實有一些警告：

- 依賴連線 — 如果與資料中心的連線中斷，使用者將無法登入各自的連線 WorkSpaces，而且在 Kerberos /票證授權票證 (TGT) 期間，現有的連線將保持作用中。

- 延遲 — 如果透過連線存在延遲 (VPN 比直 Connect 線更多)，則 WorkSpaces 驗證和任何 AD DS 相關活動 (例如群組原則 (GPO) 強制執行，將會花費更多時間。
- 流量成本 — 所有驗證都必須遍歷 VPN 或直接 Connect 鏈接，因此它取決於連接類型。這可能是從 Amazon EC2 傳出到網際網路的資料傳輸，也可以是資料傳出 (直 Connect)。

> **Note**
>
> AD Connector 是代理服務。它不存儲或緩存用戶憑據。相反地，所有驗證、查詢和管理要求都會由 AD 處理。目錄服務中需要具有委派權限的帳戶，並具有讀取所有使用者資訊並將電腦加入網域的權限。

一般而言，體 WorkSpaces 驗高度依賴於上圖所示的 Active Directory 驗證程序。在此案例中，驗 WorkSpaces 證體驗高度依賴於客戶 AD 和 WorkSpaces VPC 之間的網路連結。客戶應確保鏈接具有高可用性。

案例 2：將內部部署 AD DS 延伸到 AWS (複本)

這個案例類似於案例 1。不過，在這個案例中，客戶 AD DS 的複本會與 AD Connector 一起部署。AWS 如此可減少在 Amazon Elastic Compute Cloud (Amazon EC2) 上執行之 AD DS 的身份驗證或查詢請求的延遲。下圖顯示每個元件和使用者驗證流程的高階檢視。

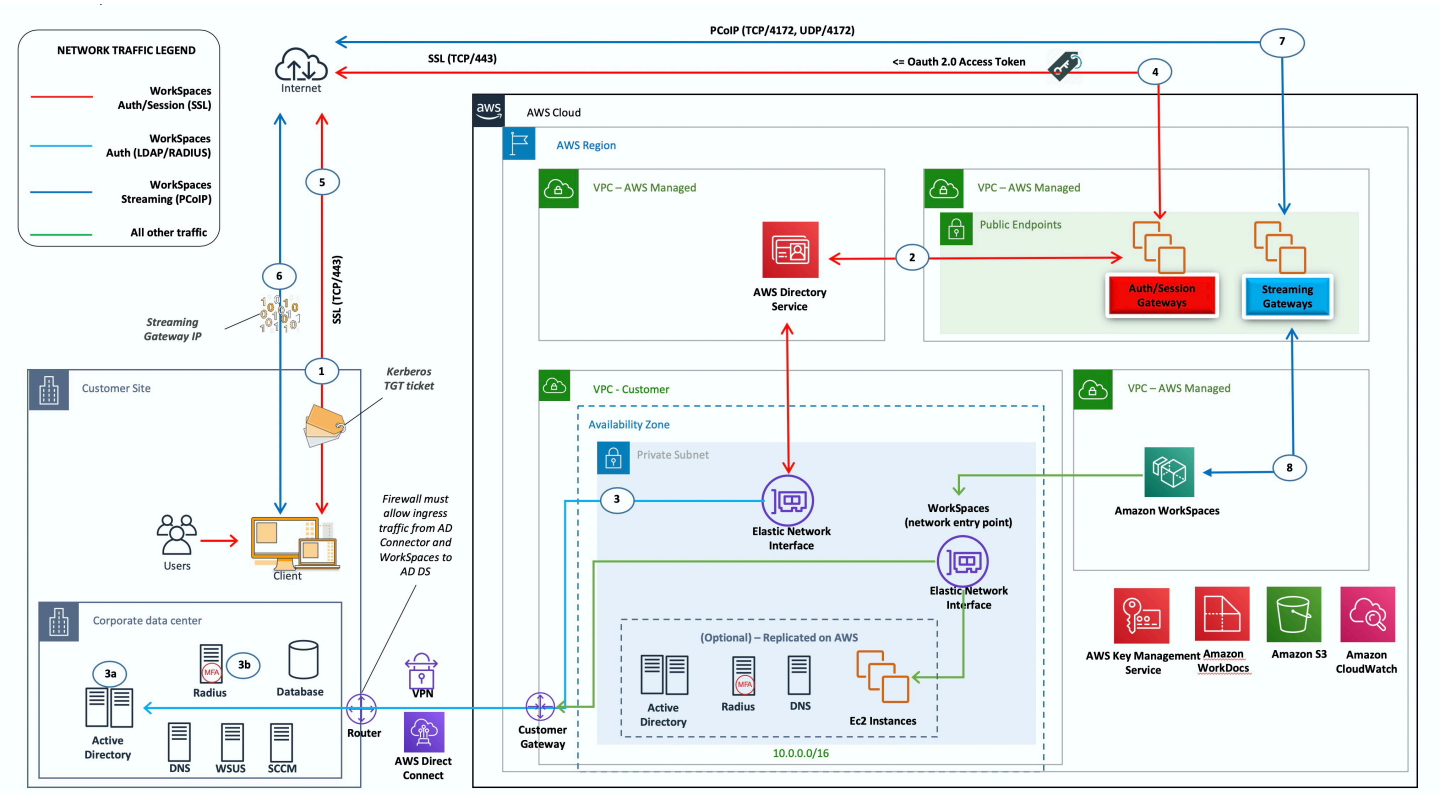

圖 7：將客戶活動目錄域擴展到雲

與案例 1 一樣，AD Connector 用於所有使用者或 MFA 驗證，這些驗證反過來會代理客戶 AD DS (請參閱上圖)。在這個案例中，客戶 AD DS 會部署到 Amazon EC2 執行個體上的 AZ，這些 AZ 在客戶的

現場部署 AD 樹系中被提升為網域控制站，並在 AWS 雲端中執行。每個網域控制站都部署到 VPC 私有子網路中，以使 AD DS 在雲端中具有高可用性。 AWS 如需部署 AD DS 的最佳作法 AWS，請參閱本文件的「設計考量」一節。

WorkSpaces 執行個體部署之後，它們就可以存取雲端架構網域控制站，以取得安全、低延遲的目錄服務和 DNS。所有網路流量 (包括 AD DS 通訊、驗證要求和 AD 複寫) 都是在私有子網路內或跨客戶 VPN 通道或直 Connect 的保護。

此架構使用下列元件或建構：

AWS

- Amazon VPC — 創建具有跨兩個 AZ 至少四個私有子網的 Amazon VPC-兩個用於客戶 AD DS，兩個用於 AD Connector 或 Amazon。 WorkSpaces
- DHCP 選項集 — 建立一個 Amazon VPC 端 DHCP 選項集。這可讓客戶定義指定的網域名稱和 DNSS (AD DS 本機)。如需詳細資訊，請參閱 DHCP 選項集。
- Amazon 虛擬私有閘道 — 啟用透過 IPSec VPN 通道或 AWS Direct Connect 連線與客戶擁有的網路進行通訊。
- Amazon EC2
  - 部署在專用私有 VPC 子網路中 Amazon EC2 執行個體上的客戶公司 AD DS 網域控制站。
  - 專用私有 VPC 子網路中 Amazon EC2 執行個體上 MFA 的客戶 (選用) RADIUS 伺服器。
- AWS 目錄服務 — AD Connector 部署到一對 Amazon VPC 私有子網路中。
- Amazon WorkSpaces — 部署到與 AD Connector 相同的私 WorkSpaces 有子網中。如需詳細資訊，請參閱本文件的 Active Directory：網站與服務一節。

客戶

- 網路連線 — 企業 VPN 或 AWS Direct Connect 端點。
- AD DS — 公司 AD DS (複寫所需)。
- MFA（可選）— 公司 RADIUS 服務器。
- 終端使用者裝置 — 用於存取 Amazon 服務的企業或 BYOL 最終使用者裝置 (例如視窗、蘋果電腦、iPads、安卓平板電腦、零用戶端和 Chromebook)。 WorkSpaces 如需支援的裝置和 Web 瀏覽

器，請參閱用戶端應用程式清單。此解決方案與案例 1 沒有相同的警告。Amazon WorkSpaces 和 AWS Directory Service 不依賴於到位的連接。

- 依賴連線 — 如果與客戶資料中心的連線中斷，使用者可以繼續工作，因為驗證和選用的 MFA 是在本機處理的。
- 延遲 — 複寫流量除外，所有驗證均為本機驗證，且延遲較低。請參閱本文件的「作用中目錄：網站與服務」一節。
- 流量成本 — 在這個案例中，驗證是本機的，只有 AD DS 複寫必須周遊 VPN 或直 Connect 結，以減少資料傳輸。

一般而言，體 WorkSpaces 驗會增強，而且不是與內部部署網域控制站的高度相依性連線，如上圖所示。當客戶想要擴充 WorkSpaces 至數千台桌上型電腦 (特別是與 AD DS 通用類別目錄查詢有關) 時，也會發生這種情況，因為此流量仍保持在本機 WorkSpaces 環境中。

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

這個案例 (如下圖所示) 已在獨立隔離環境中的 AWS 雲端中部署 AD DS。 AWS Directory Service 僅在此案例中使用。客戶可以仰賴 AWS Directory Service 來執行諸如建置高可用性目錄拓撲、監視網域控制站以及設定備份和快照集等工作，而不需要完全管理 AD DS。

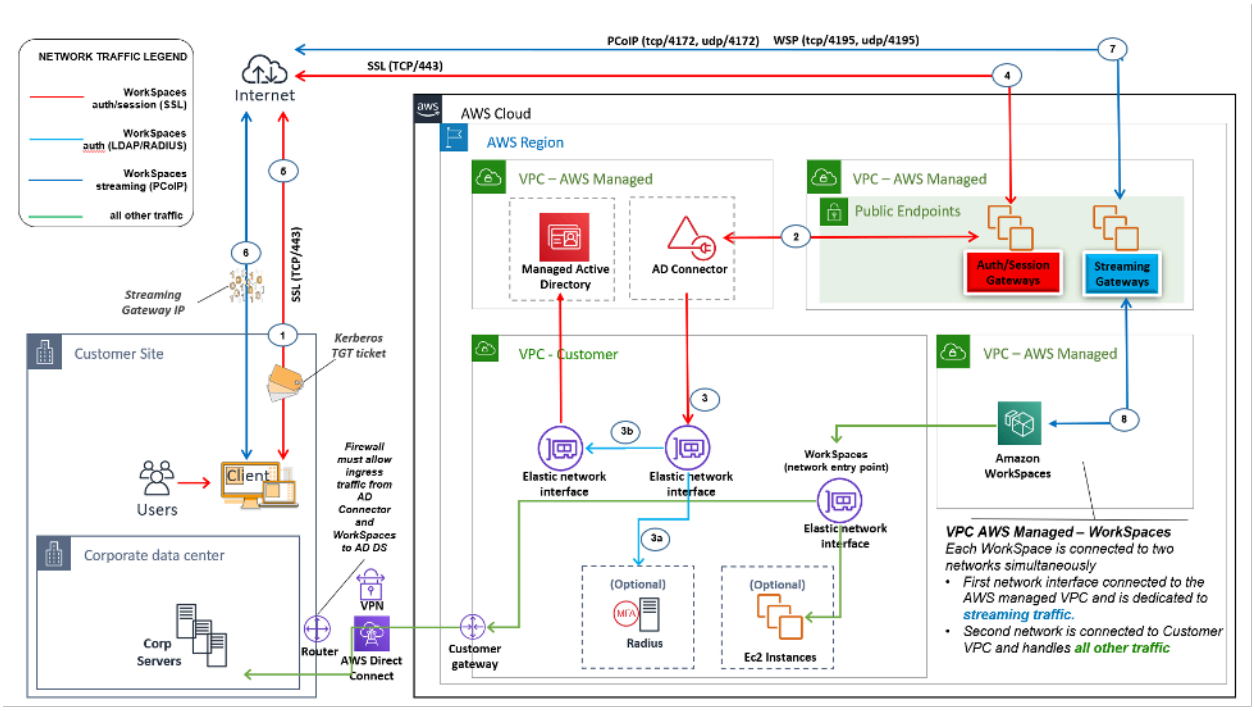

圖 8：僅限雲： AWS 目錄服務（Microsoft AD）

與案例 2 一樣，AD DS (Microsoft AD) 會部署到跨越兩個 AZ 的專用子網路中，讓 AD DS 在雲端中具有高度可用性。 AWS 除了 Microsoft AD，AD Connector（在所有三種情況下）部署用於 WorkSpaces 身份驗證或 MFA。這可確保 Amazon VPC 內的角色或功能分離，這是標準的最佳實務。如需詳細資訊，請參閱本文件的「設計考量」一節。

案例 3 是標準的全包組態，適用於希望 AWS 管理 AWS Directory Service 的部署、修補、高可用性及監視的客戶。由於其隔離模式，該案例也適用於概念驗證、實驗室和生產環境。

除了「 AWS Directory Service」的放置位置之外，此圖還顯示使用者到工作區的流量，以及工作區與 AD 伺服器和 MFA 伺服器的互動方式。

此架構使用下列元件或建構。

AWS

- Amazon VPC — 創建具有跨兩個 AZ 的至少四個私有子網的 Amazon VPC-兩個用於 AD DS Microsoft AD，兩個用於 AD Connector 或. WorkSpaces
- DHCP 選項集 — 建立一個 Amazon VPC 端 DHCP 選項集。這可讓客戶定義指定的網域名稱和 DNS (Microsoft AD)。如需詳細資訊，請參閱 DHCP 選項集。
- 選用：Amazon 虛擬私有閘道 — 啟用透過 IPSec VPN 通道 (VPN) 或 AWS Direct Connect 連線與客戶擁有的網路進行通訊。用於存取內部部署後端系統。
- AWS Directory Service — Microsoft AD 部署到一對專用的 VPC 子網路 (AD DS 受管理服務) 中。
- Amazon EC2 — MFA 的客戶「可選」半徑伺服器。
- AWS 目錄服務 — AD Connector 部署到一對 Amazon VPC 私有子網路中。
- Amazon WorkSpaces — 部署到與 AD Connector 相同的私 WorkSpaces 有子網中。如需詳細資訊，請參閱本文件的 Active Directory：網站與服務一節。

客戶

- 選用：網路連線 — 企業 VPN 或 AWS Direct Connect 端點。
- 終端使用者裝置 — 用於存取 Amazon 服務的企業或 BYOL 終端使用者裝置 (例如視窗、Mac、iPads、安卓平板電腦、零用戶端和 Chromebook)。 WorkSpaces 如需支援的裝置和 Web 瀏覽器，請參閱此用戶端應用程式清單。

就像案例 2 一樣，這個案例不會有依賴客戶內部部署資料中心的連線、延遲或資料傳出成本的問題 (除非在 VPC WorkSpaces 內啟用網際網路存取)，因為根據設計，這是隔離或僅限雲端的案例。

案例 4： AWS Microsoft AD 和內部部署的雙向傳遞信任

這個案例 (如下圖所示) 已在 AWS 雲端部署 AWS Managed AD，其具有對客戶內部部署 AD 的雙向傳遞信任。使用者和 WorkSpaces 在受管理 AD 中建立，並具有 AD 信任，可在內部部署環境中存取資源。

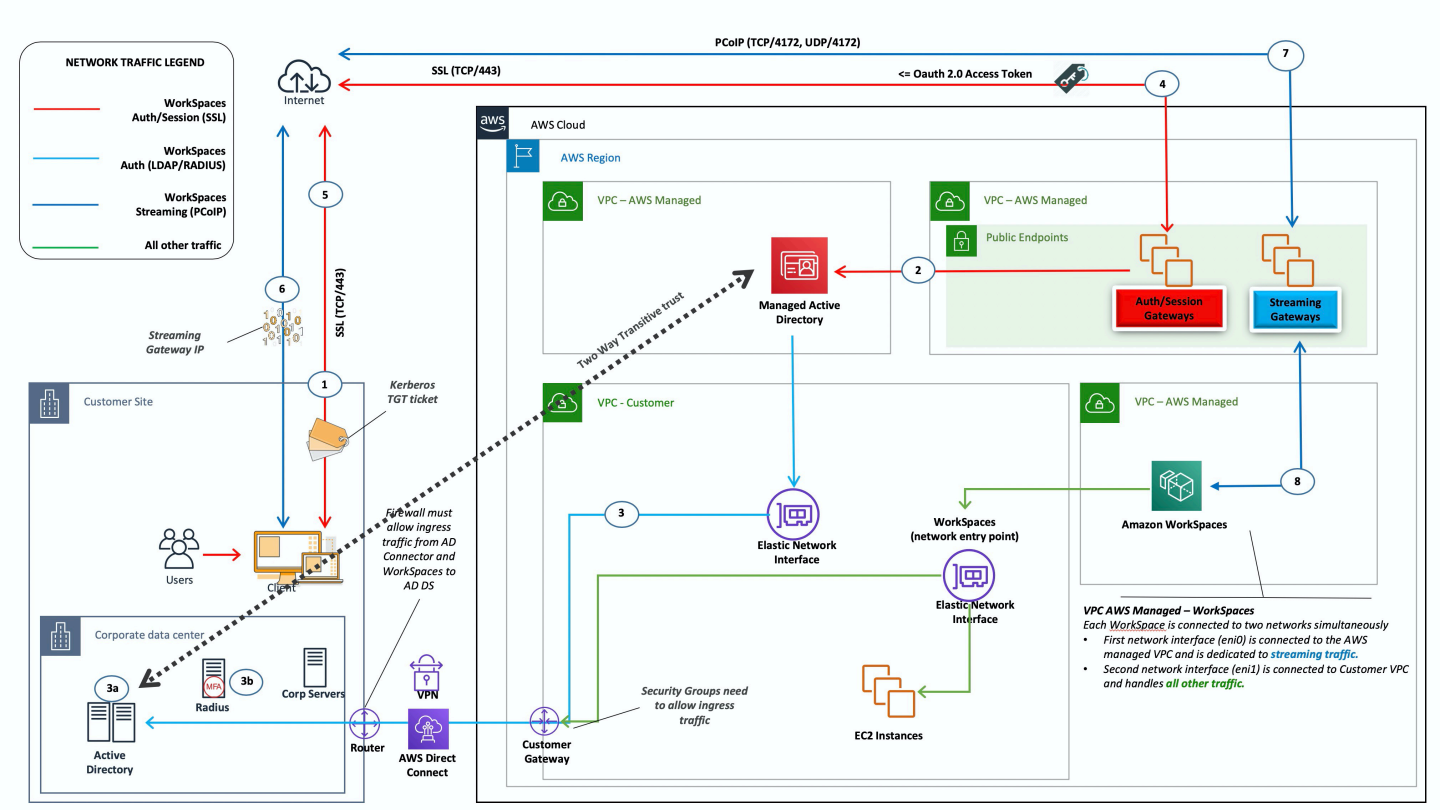

圖 9： AWS Microsoft AD 和內部部署的雙向傳遞信任

與案例 3 一樣，AD DS (Microsoft AD) 會部署到跨越兩個 AZ 的專用子網路中，讓 AD DS 在雲端中具有高度可用性。 AWS

此案例適用於希望擁有完全受控 AWS Directory Service (包括部署、修補、高可用性及監視其 AWS 雲端) 的客戶。這種情況也允許 WorkSpaces 用戶訪問其現有網絡上的 AD 加入資源。這個案例需要有網域信任。安全群組和防火牆規則必須允許兩個作用中目錄之間的通訊。

除了「 AWS Directory Service」的放置之外，上一個圖顯示了從使用者到工作區的流量，以及工作區與 AD 伺服器和 MFA 伺服器的互動方式。

此架構使用下列元件或建構。

AWS

- Amazon VPC — 創建具有跨兩個 AZ 的至少四個私有子網的 Amazon VPC-兩個用於 AD DS Microsoft AD，兩個用於 AD Connector 或. WorkSpaces
- DHCP 選項集 — 建立一個 Amazon VPC 端 DHCP 選項集。這可讓客戶定義指定的網域名稱和 DNS (Microsoft AD)。如需詳細資訊，請參閱 DHCP 選項集。
- 選用：Amazon 虛擬私有閘道 — 啟用透過 IPSec VPN 通道 (VPN) 或 AWS Direct Connect 連線與客戶擁有的網路進行通訊。用於存取內部部署後端系統。
- AWS Directory Service — Microsoft AD 部署到一對專用的 VPC 子網路 (AD DS 受管理服務) 中。

- Amazon EC2 — 客戶可選購 MFA 的半徑伺服器。
- Amazon WorkSpaces — 部署到與 AD Connector 相同的私 WorkSpaces 有子網中。如需詳細資訊，請參閱本文件的 Active Directory：網站與服務一節。

客戶

- 網路連線 — 企業 VPN 或 AWS Direct Connect 端點。
- 終端使用者裝置 — 用於存取 Amazon 服務的企業或 BYOL 終端使用者裝置 (例如視窗、Mac、iPads、安卓平板電腦、零用戶端和 Chromebook)。 WorkSpaces 如需支援的裝置和 Web 瀏覽器，請參閱用戶端應用程式清單。

此解決方案需要連線至客戶內部部署資料中心，才能執行信任程序。如果使用 WorkSpaces者正在使用內部部署網路上的資源，則需要考慮延遲和輸出資料傳輸費用。

案例 5： AWS Microsoft AD 使用共用服務 Virtual Private Cloud (VPC) (VPC)

此案例如下圖所示，已在 AWS 雲端部署 AWS Managed AD，為已在中託管 AWS 或計劃作為更廣泛移轉一部分的工作負載提供驗證服務。最佳做法建議是將 Amazon 放 WorkSpaces 在專用 VPC 中。客戶也應該建立特定的 AD OU 來組織 WorkSpaces 電腦物件。

若要 WorkSpaces 使用主控受管理 AD 的共用服務 VPC 進行部署，請使用在受管理 AD 中建立的 ADC 服務帳戶部署 AD 連接器 (ADC)。服務帳戶需要權限，才能在共用服務受管理 AD 中的 WorkSpaces指定 OU 中建立電腦物件。

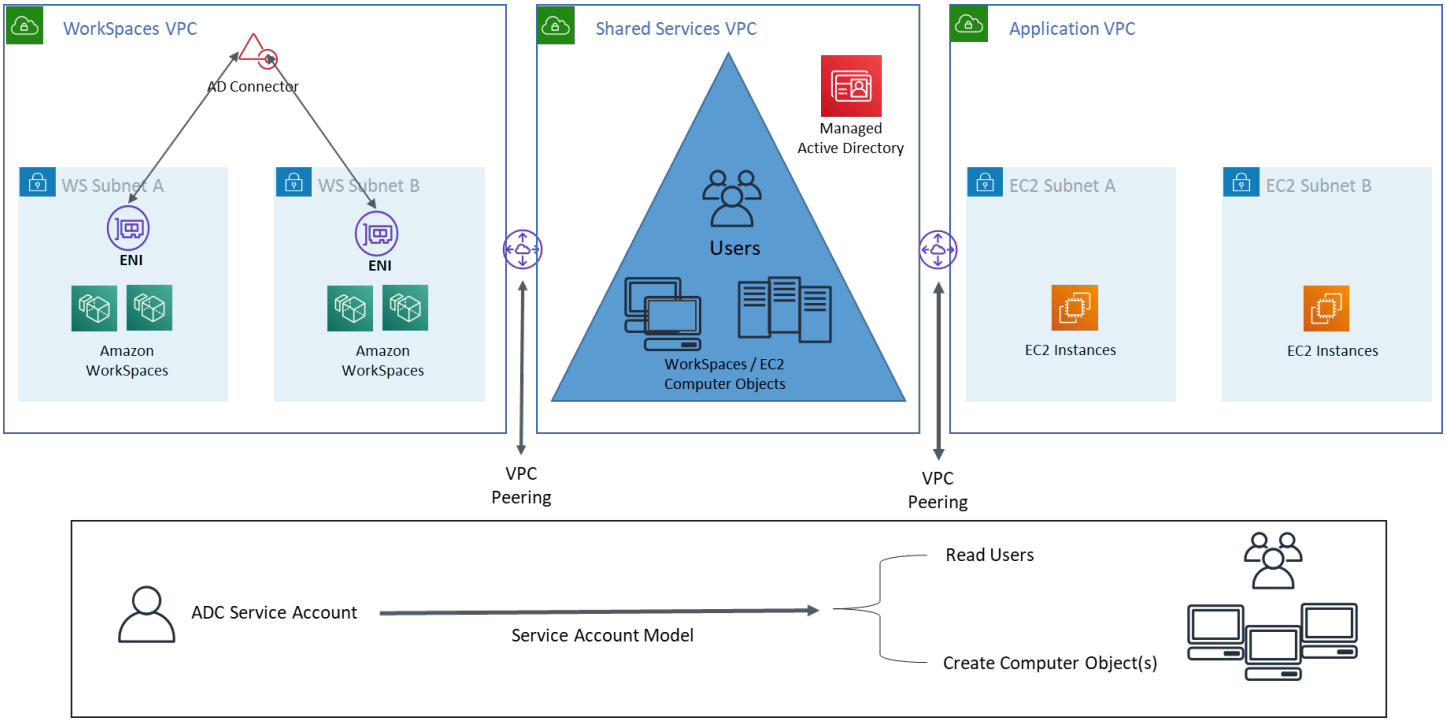

圖 10： AWS Microsoft AD 使用共享服務 VPC

此架構使用下列元件或建構。

AWS

- Amazon VPC — 建立具有跨兩個 AZ 的至少兩個私有子網路的 Amazon VPC (兩個用於 AD Connector 和)。 WorkSpaces
- DHCP 選項集 — 建立一個 Amazon VPC 端 DHCP 選項集。這可讓客戶定義指定的網域名稱和 DNS (Microsoft AD)。如需詳細資訊，請參閱 DHCP 選項集。
- 選用：Amazon 虛擬私有閘道 — 啟用透過 IPSec VPN 通道 (VPN) 或 AWS Direct Connect 連線與客戶擁有的網路進行通訊。用於存取內部部署後端系統。
- AWS Directory Service — Microsoft AD 部署到一對專用的 VPC 子網路 (AD DS 受管理服務)、AD Connector
- AWS 傳@@ 輸道/VPC 對等 — 啟用工作區 VPC 與共用服務 VPC 之間的連線
- Amazon EC2 — 客戶可選購 MFA 的半徑伺服器。

- Amazon WorkSpaces — 部署到與 AD Connector 相同的私 WorkSpaces 有子網中。如需詳細資訊，請參閱本文件的 Active Directory：網站與服務一節。

客戶

- 網路連線 — 企業 VPN 或 AWS Direct Connect 端點。
- 終端使用者裝置 — 用於存取 Amazon 服務的企業或 BYOL 終端使用者裝置 (例如視窗、Mac、iPads、安卓平板電腦、零用戶端和 Chromebook)。 WorkSpaces 如需支援的裝置和 Web 瀏覽器，請參閱用戶端應用程式清單。

案例 6： AWS Microsoft AD、共用服務 VPC，以及內部部署的單向信任

這個案例 (如下圖所示) 會針對使用者使用現有的內部部署 Active Directory，並在 AWS 雲端中引入個別的受管理 Active Directory 來裝載與 WorkSpaces. 這個案例可讓電腦物件和使用中目錄群組原則獨立於公司的使用中目錄進行管理。

當第三方想要代表客戶管理 Windows WorkSpaces 時，這個案例非常有用，因為它允許協力廠商定義和控制與他們相關聯的 WorkSpaces 和政策，而不需要授予第三方對客戶 AD 的存取權。在這個案例中，會建立特定的使用中目錄組織單位 (OU) 來組織共用服務 AD 中的 WorkSpaces 電腦物件。

> **Note**
>
> Amazon Linux WorkSpaces 需要雙向信任才能建立它們。

若要使 WorkSpaces 用來自客戶識別網域的使用者，將 Windows 部署在主控受管理 Active Directory 的共用服務 VPC 中建立的電腦物件，請部署參照公司 AD 的作用中目錄連接器 (ADC)。使用在企業 AD (身分識別網域) 中建立的 ADC 服務帳戶，該帳戶具有委派權限，在組織單位 (OU) 中建立電腦物件，該帳戶是 WorkSpaces 在共用服務受管理 AD 中針對 Windows 設定，且具有公司 Active Directory (身分識別網域) 的讀取權限。

若要確保網域定位器功能能夠驗證身分網域所需 AD 網站中的 WorkSpaces 使用者，請依照 Microsoft 的說明文件，將兩個網域的 Amazon WorkSpaces 子網路 AD 網站命名為相同。最佳做法是將身分識別網域和共用服務網域 AD 網域控制站與 Amazon 位於相同的 AWS 區域 WorkSpaces。

如需設定此案例的詳細指示，請參閱實作指南，以 WorkSpaces 使用 AWS 目錄服務為 Amazon 設定單向信任

在這個案例中，我們會在共用服務 VPC 和內部部署 AD 之間建立單向傳遞信任。 AWS Managed Microsoft AD 圖 11 顯示信任和存取的方向，以及 AWS AD Connector 器如何使用 AD Connector 服務帳戶在資源網域中建立電腦物件。

系統會根據 Microsoft 建議使用樹系信任，以確保盡可能使用 Kerberos 驗證。您從中的資源網域 WorkSpaces 接收群組原則物件 (GPO)。 AWS Managed Microsoft AD此外，您還可以使用您的身份識別域 WorkSpaces 執行 Kerberos 身份驗證。為了可靠地工作，最佳做法是將您的身份域擴展到上面已經解釋的那 AWS 樣。我們建議您查看 WorkSpaces 使用單向信任資源域與 AWS Directory Service 實施指南部署 Amazon 以獲取更多詳細信息。

AD Connector 器和您的 WorkSpaces，都必須能夠與您的身分識別網域和資源網域的網域控制站通訊。如需詳細資訊，請參閱《Amazon WorkSpaces 管理指南》 WorkSpaces中的《IP 位址和連接埠需求》。

如果您使用多個 AD 連接器，最佳做法是讓每個 AD 連接器使用自己的 AD Connector 器服務帳戶。

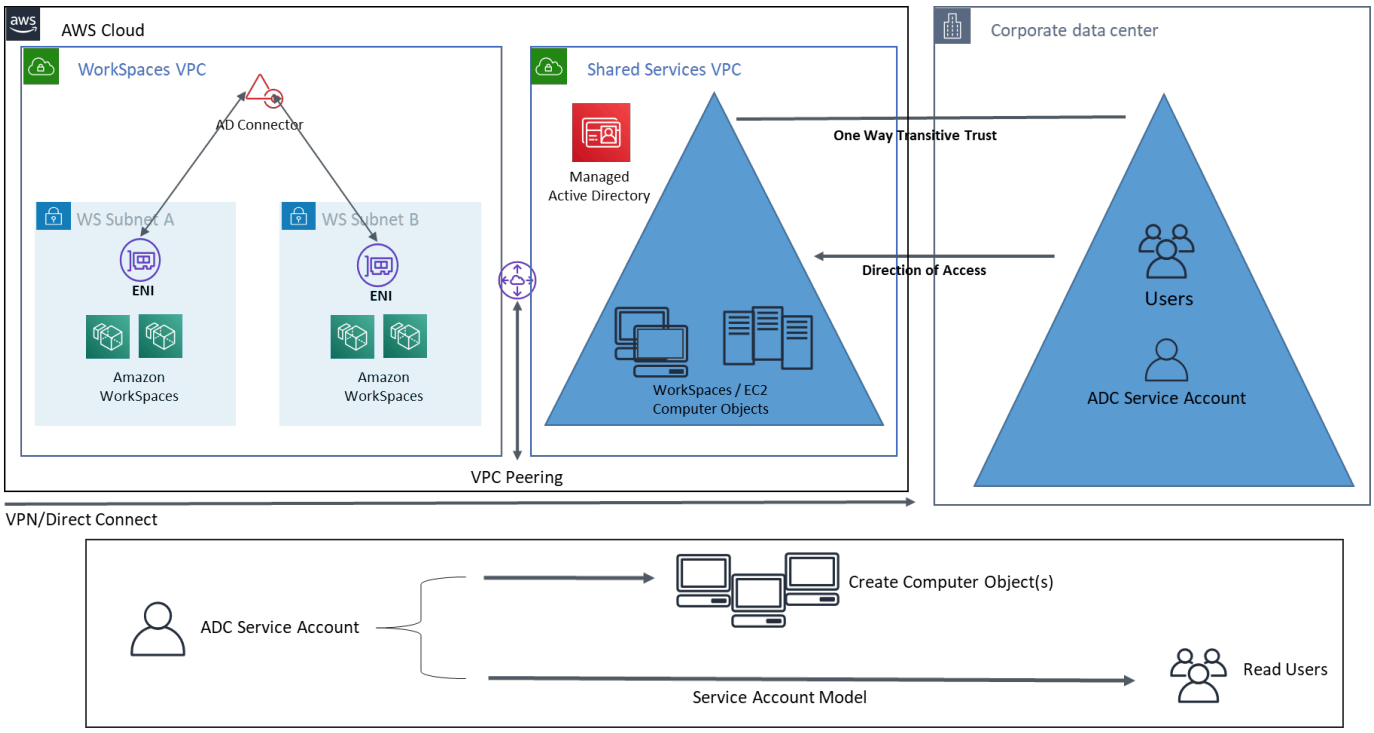

圖 11： AWS Microsoft、共用服務 VPC 和 AD 內部部署的單向信任

此架構使用下列元件或建構：

AWS

- Amazon VPC — 建立具有跨兩個 AZ 至少兩個私有子網路的 Amazon VPC — 兩個用於 AD Connector 和. WorkSpaces
- DHCP 選項集 — 建立一個 Amazon VPC DHCP 選項集。這可讓客戶定義指定的網域名稱和 DNS (Microsoft AD)。如需詳細資訊，請參閱 DHCP 選項集。
- 選用：Amazon 虛擬私有閘道 — 啟用透過 IPSec VPN 通道 (VPN) 或 AWS Direct Connect 連線與客戶擁有的網路進行通訊。用於存取內部部署後端系統。
- AWS Directory Service — Microsoft AD 部署到一對專用的 VPC 子網路 (AD DS 受管理服務)、AD Connector 中。
- 傳@@ 輸道/VPC 對等 — 啟用 Workspace VPC 與共用服務 VPC 之間的連線。
- Amazon EC2 — MFA 的客戶「可選」半徑伺服器。
- Amazon WorkSpaces — 部署到與 AD Connector 相同的私 WorkSpaces 有子網中。如需詳細資訊，請參閱本文件的 Active Directory：網站與服務一節。

客戶

- 網路連線 — 企業 VPN 或 AWS Direct Connect 端點。
- 終端使用者裝置 — 用於存取 Amazon 服務的企業或 BYOL 終端使用者裝置 (例如視窗、Mac、iPads、安卓平板電腦、零用戶端和 Chromebook)。 WorkSpaces 如需支援的裝置和 Web 瀏覽器，請參閱此用戶端應用程式清單。

在 Amazon 使用多區域 AWS 託管活動目錄 WorkSpaces

AWS Directory Service Microsoft 活動目錄（MAD）是一個完全受管的 Microsoft 活動目錄（AD），可以與 Amazon 配對 WorkSpaces。客戶選擇 AWS 受管理的 Microsoft AD，因為它具有內建的高可用性、監控和備份功能。 AWS 管理 Microsoft AD 企業版增加了配置多區域複製的功能。此功能會自動設定區域間的網路連線、部署網域控制站，以及跨多個區域複寫所有 Active Directory 資料，確保駐留在這些區域的 Windows 和 Linux 工作負載能夠以低延遲和高效能連線至 AWS MAD 並使用。複寫的 MAD 區域無法直接註冊 WorkSpaces，但是複寫的 MAD 目錄可以透 WorkSpaces 過將 AD Connector 器 (ADC) 設定為指向複寫的網域控制站來註冊。

使用 MAD 部署 AD 連接器時，最佳做法是為 WorkSpaces 環境中的每個業務單位建立 AD 連接器。這可讓您將每個業務單位與 Active Directory 中的特定組織單位對齊。然後，您可以在組織單位層級指派 AD 群組原則物件，直接與有問題的業務單位一致。

架構

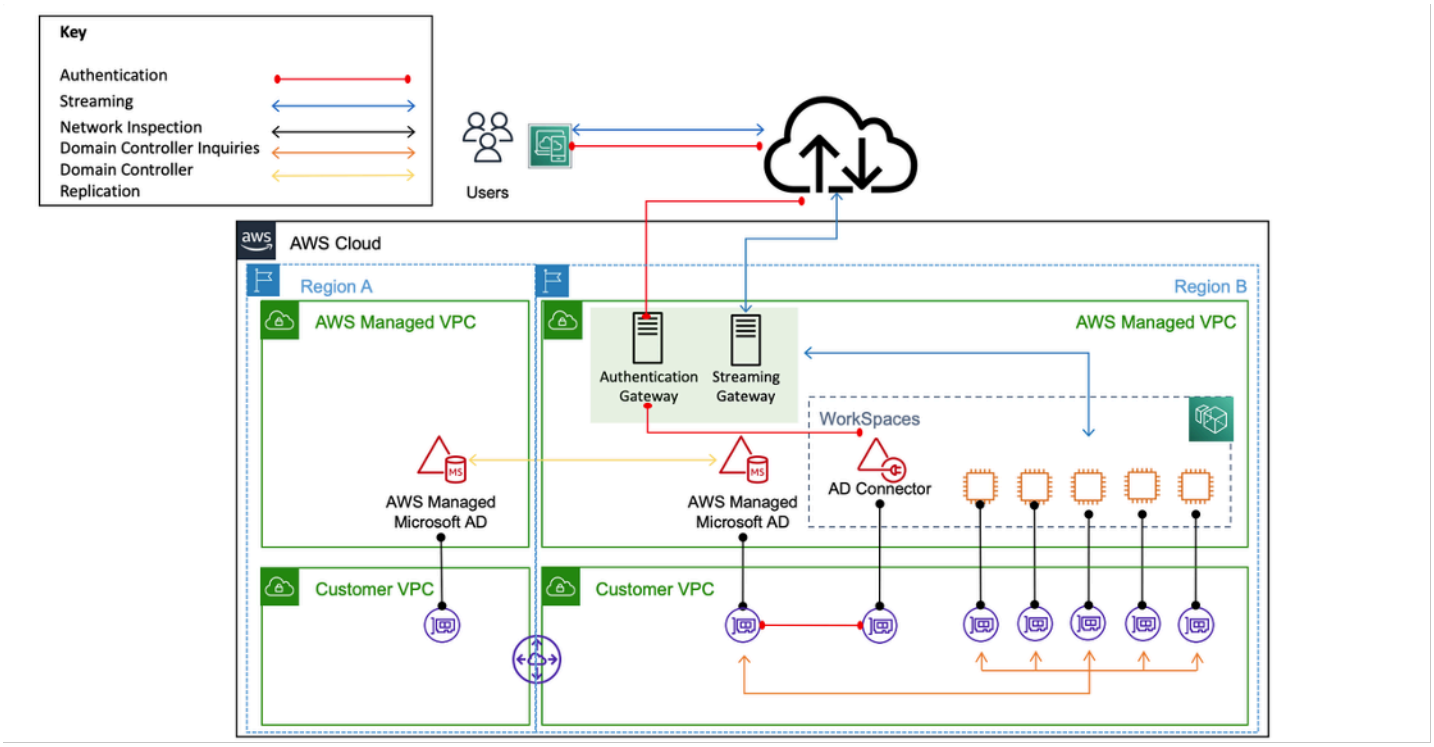

圖 12：將複製的 MAD 區域註冊到的範例架構 WorkSpace

實作

若要註冊複寫的 MAD 區域 WorkSpaces，您必須建立指向您的 MAD 網域控制站 IP 的 AD Connector 器。您可以移至 [AWS Directory Service] 主控台瀏覽窗格，選取 [目錄]，然後選擇正確的目錄識別碼，以尋找您的 MAD 網域控制站 IP 位址。若要建立這些 AD 連接器，請遵循本指南。一旦他們被創建，你可以註冊它們 WorkSpaces。在新區域 WorkSpaces 中部署之前，請確定您已更新 VPC DHCP 選項集。

設計考量

在 AWS 雲端中的功能性 AD DS 部署需要對使用中目錄概念和特定 AWS 服務有很好的了解。本節討論部署適用於 Amazon 之 AD DS 時的主要設計考量事項 WorkSpaces、 AWS Directory Service 的 VPC 最佳實務、DHCP 和 DNS 需求、AD Connector 細節以及 AD 網站和服務。

VPC 設計

如先前在本文件的「網路考量」一節中所討論，先前針對案例 2 和 3 所述，客戶應在 AWS 雲端中部署 AD DS 到跨兩個 AZ 的專用子網路組合，並與 AD Connector 或 WorkSpaces 子網路分開。此建構提供對 AD DS 服務的高可用性、低延遲存取 WorkSpaces，同時維持 Amazon VPC 中角色或功能分離的標準最佳實務。

下圖顯示將 AD DS 和 AD Connector 分離為專用的私有子網路 (案例 3)。在此範例中，所有服務都位於相同的 Amazon VPC 中。

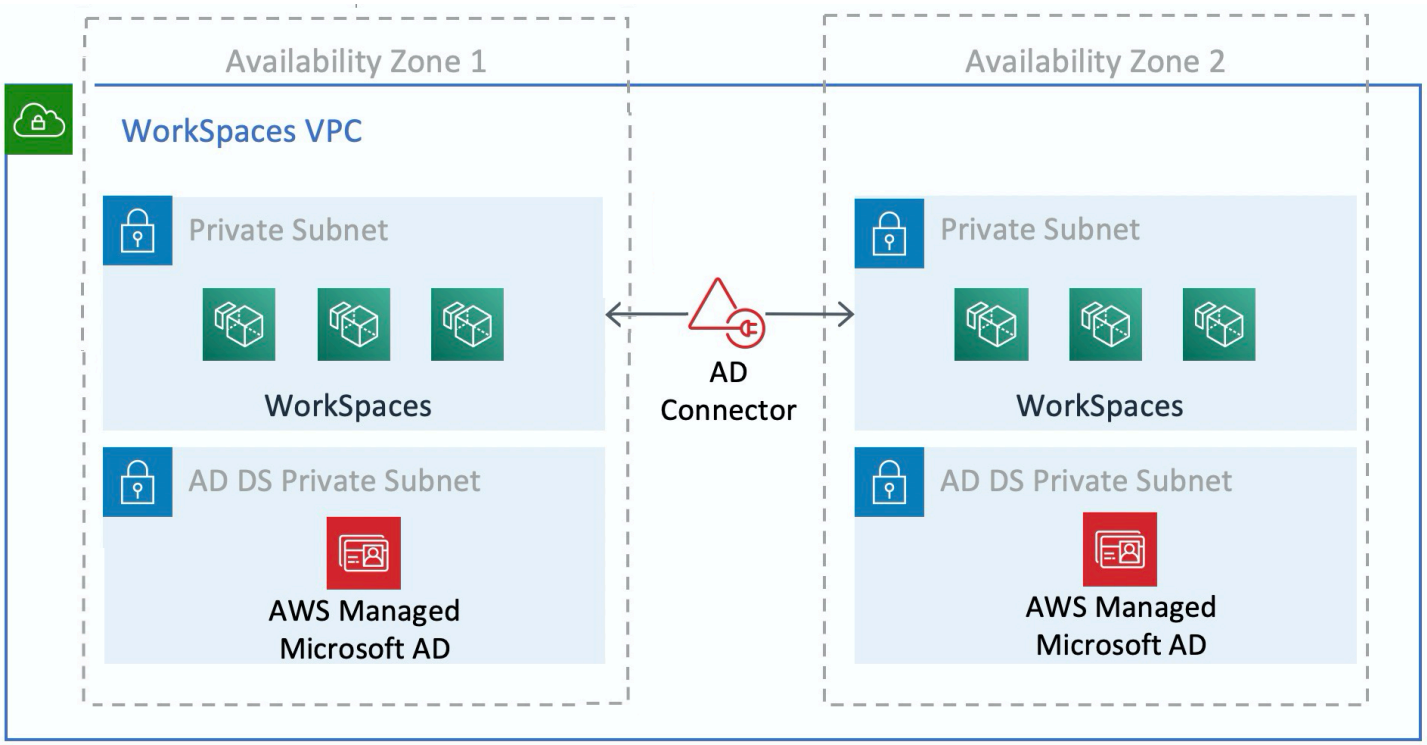

圖 13：廣告 DS 網路分離

下圖顯示與案例 1 類似的設計；不過，在此案例中，現場部署部分位於專用 Amazon VPC 中。

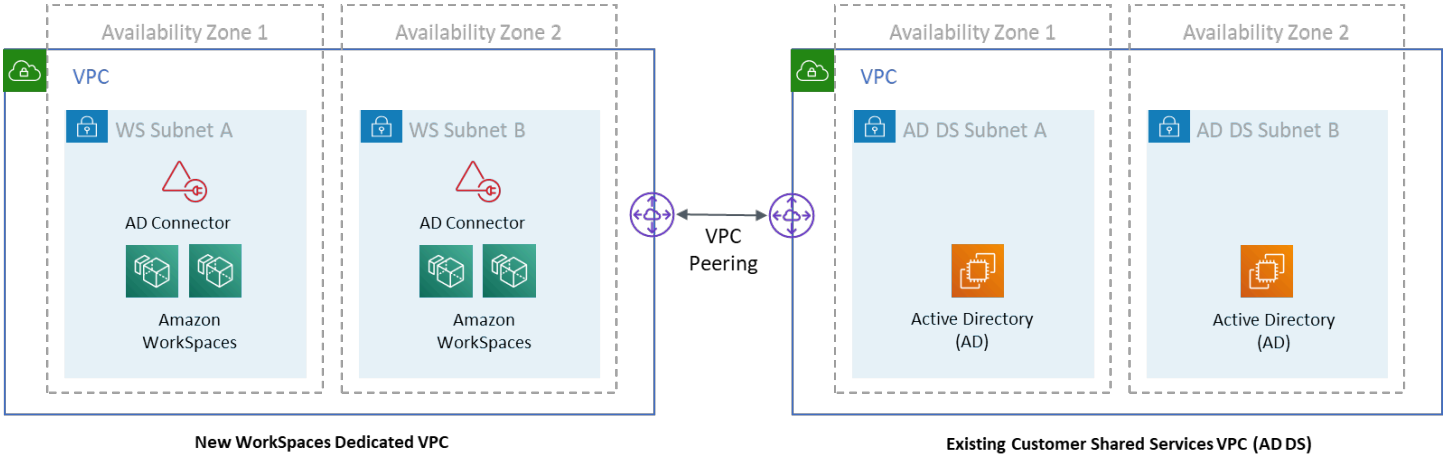

圖 14：專用 WorkSpaces VPC

> **Note**
>
> 對於擁有使用 AD DS 的現有 AWS 部署的客戶，建議他們在專用 VPC WorkSpaces 中找到它們，並使用 VPC 對等互連進行 AD DS 通訊。

除了為 AD DS 建立專用的私人子網路之外，網域控制站和成員伺服器還需要數個安全性群組規則，以允許服務的流量，例如 AD DS 複寫、使用者驗證、Windows Time 服務和分散式檔案系統 (DFS)。

> **Note**
>
> 最佳做法是將必要的安全性群組規則限制為 WorkSpaces私有子網路，而在案例 2 的情況下，允許內部部署進出 AWS 雲端的雙向 AD DS 通訊，如下表所示。

表 1 — 往來雲端的 AWS 雙向 AD DS 通訊

通訊協定	連線埠	使用	目的地
TCP	53、八八、一三五、一三九、 445、464、636	驗證（主要）	活動目錄（私有數據中心或 Amazon EC2）*

通訊協定	連線埠	使用	目的地
TCP	49152 — 65535	RPC 高端口	活動目錄（私有數據中心或 Amazon EC2）**
TCP	3268-3269	信託	活動目錄（私有數據中心或 Amazon EC2）*
TCP	9389	遠程 Microsoft 視窗 PowerShell （可選）	活動目錄（私有數據中心或 Amazon EC2）*
UDP	五十八、一二三、一三七、一三八 389、445、	驗證（主要）	活動目錄（私有數據中心或 Amazon EC2）*
UDP	1812	驗證 (MFA) (選擇性)	半徑 (私有資料中心或 Amazon EC2) *

如需詳細資訊，請參閱 Windows 的使用中目錄和作用中目錄網域服務連接埠需求和服務概觀和網路連接埠需求

如需實作規則的 step-by-step 指引，請參閱 Amazon 彈性運算雲端使用者指南中的〈將規則新增至安全群組〉。

VPC 端設計：DHCP 和 DNS

使用 Amazon VPC 時，依預設會為您的執行個體提供動態主機設定通訊協定 (DHCP) 服務。依預設，每個 VPC 都提供內部網域名稱系統 (DNS) 伺服器，可透過無類別網域間路由 (CIDR) +2 位址空間存取，並透過預設 DHCP 選項集指派給所有執行個體。

在 Amazon VPC 內使用 DHCP 選項集來定義範圍選項，例如網域名稱或應透過 DHCP 傳遞給客戶執行個體的名稱伺服器。客戶 VPC 擬私人雲端中 Windows 服務的正確功能取決於此 DHCP 範圍選項。在先前定義的每個案例中，客戶都會建立並指派自己的範圍，以定義網域名稱和名稱伺服器。WorkSpaces 如此可確保已加入網域的 Windows 執行個體，或設定為使用 AD DNS。

下表是一組自訂 DHCP 範圍選項的範例，必須為 Amazon WorkSpaces 和 AWS 目錄服務建立這些選項才能正常運作。

表 2 — 自訂 DHCP 範圍選項集

參數	值
Name tag (名稱標籤)	創建鍵 = 名稱和值設置為特定字符串的標籤 範例：
網域名稱	example。com
Domain name servers (網域名稱伺服器)	DNS 伺服器位址，以逗號分隔 範例：192.0.2.10、192.0.2.21
NTP servers (NTP 伺服器)	將此欄位保留空白
NetBIOS name servers (NetBIOS 名稱伺服器)	輸入與網域名稱伺服器相同的逗號分隔 IP 範例：192.0.2.10、192.0.2.21
NetBIOS node type (NetBIOS 節點類型)	2

如需有關建立自訂 DHCP 選項集並將其與 Amazon VPC 產生關聯的詳細資訊，請參閱 Amazon V irtual Private Cloud 使用者指南中的使用 DHCP 選項集。

在案例 1 中，DHCP 範圍會是內部部署 DNS 或 AD DS。但是，在案例 2 或 3 中，這將是本機部署的目錄服務（Amazon EC2 上的 AD DS 或 AWS 目錄服務：Microsoft AD）。建議您將常駐在 AWS 雲端中的每個網域控制站都是通用類別目錄和目錄整合的 DNS 伺服器。

活動目錄：網站和服務

對於案例 2，網站和服務是 AD DS 正確功能的關鍵元件。站台拓撲控制相同站台內及跨站台界限的網域控制站之間的 AD 複寫。在案例 2 中，至少存在兩個站台：現場部署和雲端 WorkSpaces 中的 Amazon。

定義正確的站台拓撲可確保用戶端相似性，表示用戶端 (在本例中為 WorkSpaces) 會使用其慣用的本機網域控制站。

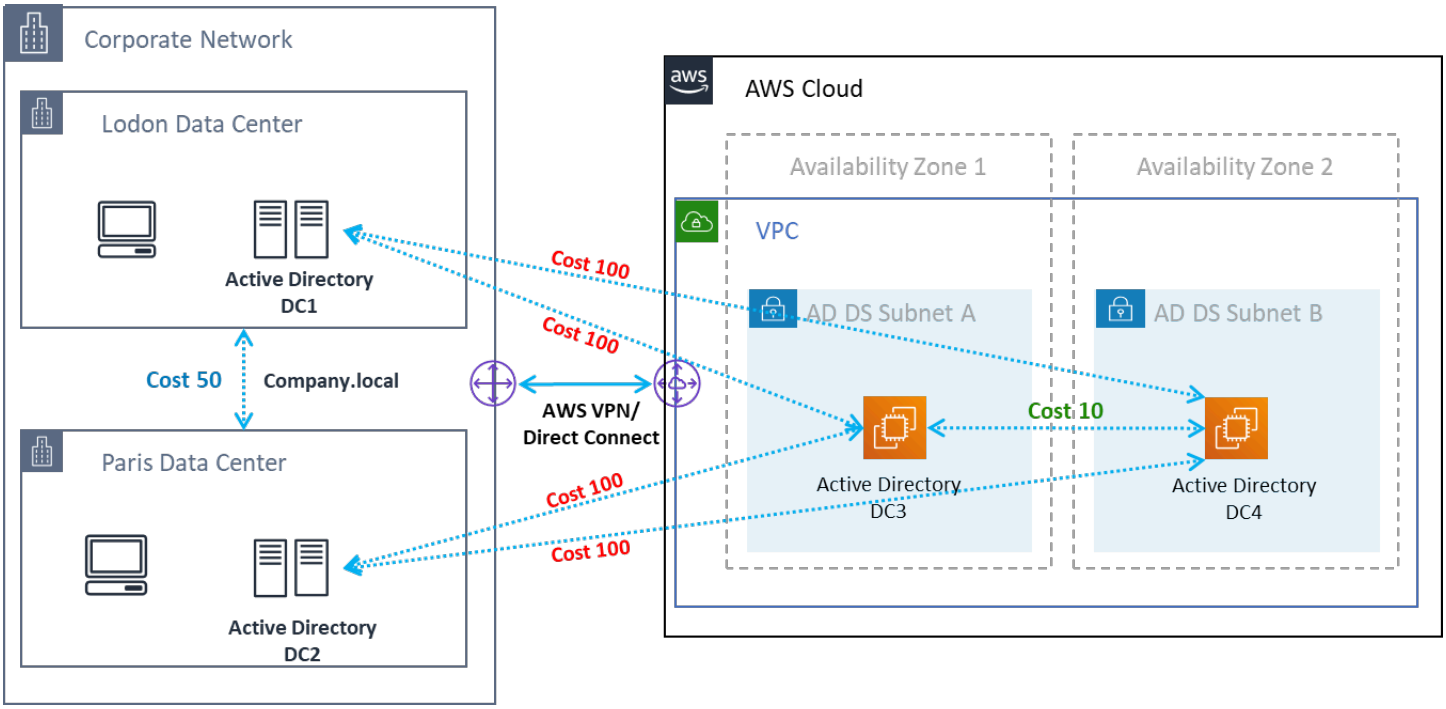

圖 15：活動目錄站點和服務：用戶端親和性

最佳做法：為內部部署 AD DS 和 AWS 雲端之間的網站連結定義高成本。下圖是指派給站台連結的成本範例 (成本 100)，以確保與站台無關的用戶端相似性。

這些關聯有助於確保流量 (例如 AD DS 複寫和用戶端驗證) 會使用最有效率的網域控制站路徑。在案例 2 和 3 的情況下，這有助於確保降低延遲和交叉連結流量。

通訊協定

Amazon WorkSpaces 串流通訊協定 (WSP) 是雲端原生串流通訊協定，可在全球距離和不可靠的網路中提供一致的使用者體驗。WSP 通 WorkSpaces 過卸載指標分析，編碼，編解碼器使用和選擇來分離協議。WSP 使用連接埠 決定是否使用 WSP 通訊協定時，應在部署之前回答幾個關鍵問題。請參閱下面的決策矩陣：

問題	WSP	PCoIP
確定的 WorkSpaces 用戶是否需要雙向音頻/視頻？	•	
零客戶端是否會用作遠程端點（本地設備）？		•

問題	WSP	PCoIP
視窗或 macOS 是否會用於遠端端點？	•	•
Ubuntu 18.04 會用於遠端端點嗎？		•
用戶會 WorkSpaces 通過網絡訪問訪問 Amazon 嗎？		•
是否需要工作階段前或工作階段中的智慧卡支援 (PIC/CAC)？	•	
WorkSpaces 將在中國 (寧夏) 地區使用嗎？		•
是否需要智慧卡預先驗證或工作階段中的支援？	•	
終端使用者是否使用不可靠、高延遲或低頻寬的連線？	•	

先前的問題對於確定應使用的協議至關重要。您可以在這裡檢閱有關建議通訊協定使用案例的其他資訊。您也可以稍後使用 Amazon WorkSpaces Migrate 功能變更使用的通訊協定。有關使用此功能的更多信息，可以在這裡查看。

WorkSpaces 使用 WSP 部署時，應將 WSP 閘道新增至允許清單，以確保服務的連線能力。此外，連接到 WorkSpaces 使用 WSP 的用戶，往返時間（RTT）應小於 250 毫秒，以獲得最佳性能。與 250 毫秒至 400 毫秒之間 RTT 的連線將會降級。如果使用者的連線持續降級，建議盡可能 WorkSpaces 在最接近終端使用者的服務支援區域部署 Amazon。

Multi-Factor Authentication (MFA)

實作 MFA 需 WorkSpaces 要將 Amazon 設定為使用中目錄連接器 (AD Connector 器) 或 AWS 受管 Microsoft AD (MAD) 做為其 Directory Service，並具有可由 Directory Service 存取網路的 RADIUS 伺服器。簡單的活動目錄不支持 MFA。

請參閱上一節，說明 AD 的 Active Directory 和目錄服務部署考量，以及每個案例中的 RADIUS 設計選項。

MFA — 雙因素身份驗證

啟用 MFA 之後，使用者必須向用 WorkSpaces 戶端提供其使用者名稱、密碼和 MFA 代碼，以便對其各自 WorkSpaces 的桌面進行驗證。

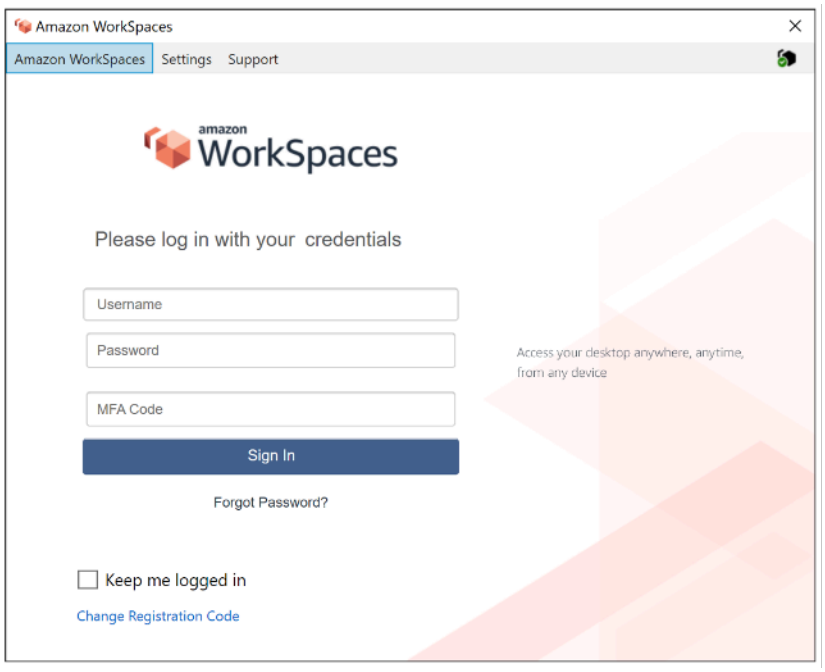

圖 16：已啟用 MFA 的 WorkSpaces 用戶端

> **Note**
>
> AWS Directory Service 不支援選擇性的每個使用者或內容化 MFA：這是每個目錄的全域設定。如果需要選擇性的「每位使用者」MFA，使用者必須由 AD Connector 隔開，它可以指向相同的來源 Active Directory。

WorkSpaces MFA 需要一個或多個 RADIUS 伺服器。通常，這些是您可能已經部署的現有解決方案，例如 RSA 或金雅拓。或者，RADIUS 伺服器也可以部署在 EC2 執行個體上的 VPC 中 (有關架構選項，請參閱本文件的 AD DS 部署案例一節)。如果您正在部署新的 RADIUS 解決方案，則存在多種實作，例如 FreeRADIUS，以及 SaaS 產品，例如雙核心安全性或 Okta MFA。

最佳做法是利用多個 RADIUS 伺服器，以確保您的解決方案能夠抵禦故障。為 MFA 設定 Directory Service 時，您可以使用逗號分隔多個 IP 位址 (例如 192.0.0.0,192.0.0.12) 來輸入多個 IP 位址。目錄

服務 MFA 功能會嘗試指定的第一個 IP 位址，並將移至第二個 IP 位址，如果第一個 IP 位址無法建立網路連線。高可用性架構的 RADIUS 組態對於每個解決方案集來說都是獨一無二的，但過度建議是將 RADIUS 功能的基礎執行個體置於不同的可用區域。其中一個設定範例是雙核心安全性，對於 Okta MFA，您可以用相同的方式部署多個 Okta RADIUS 伺服器代理程式。

如需啟用 MFA AWS Directory Service 的詳細步驟，請參閱 AD Connector 和AWS 受管理的 Microsoft AD。

災難恢復/業務持續性

WorkSpaces 跨區域重新導向

Amazon WorkSpaces 是為客戶提供遠端桌面存取的區域服務。視業務持續性和災難復原需求 (BC/DR) 而定，有些客戶需要順暢的容錯移轉至另一個提供 WorkSpaces 服務的區域。此 BC/DR 需求可以使用 WorkSpaces 跨區域重新導向選項來完成。它可讓客戶使用完整網域名稱 (FQDN) 作為 WorkSpaces 註冊碼。

一個重要的考慮因素是決定應該在什麼時候重新導向到容錯移轉區域。此決定的準則應根據您的公司原則，但應包括復原時間目標 (RTO) 和復原點目標 (RPO)。Well-Architected 的 WorkSpaces 架構設計應包括服務失敗的可能性。正常業務運營復原的時間容忍度也將納入決策。

當您的使用者以 FQDN 作為其註 WorkSpaces 冊碼登入時，會解析 DNS TXT 記錄，其中包含連線識別碼，決定使用者將被導向至 WorkSpaces 的已註冊目錄。然後，系統會根據與傳回的連線識別碼相關聯的已註冊目錄來呈現 WorkSpaces 用戶端的登入登入頁面。這可讓系統管理員根據 FQDN 的 DNS 原則，將其使用者導向至不同的 WorkSpaces目錄。假設可從用戶端機器解析私有區域，此選項可與公用或私有 DNS 區域搭配使用。跨區域重新導向可以是手動或自動化的。這兩種容錯移轉都可以透過將包含連線識別碼的 TXT 記錄變更為指向所需目錄來達成。

在開發 BC/DR 策略時，請務必考慮使用者資料，因為 WorkSpaces 跨區域重新導向選項不會同步處理任何使用者資料，也不會同步您的映像檔。 WorkSpaces 您在不同區 AWS 域的 WorkSpaces 部署是獨立的實體。因此，您必須採取其他措施，以確保您的 WorkSpaces 使用者可以在重新導向至次要區域時存取其資料。有許多選項可用於使用者資料複寫 WorkSpaces，例如 Windows FSx (DFS 共用)，或協力廠商公用程式來同步區域之間的資料磁碟區。同樣地，您必須確保您的次要區域能夠存取所需的 WorkSpaces 影像，例如跨區域複製影像。如需詳細資訊，請參閱 Amazon WorkSpaces 管理指南 WorkSpaces中的 Amazon 跨區域重新導向和圖中的範例。

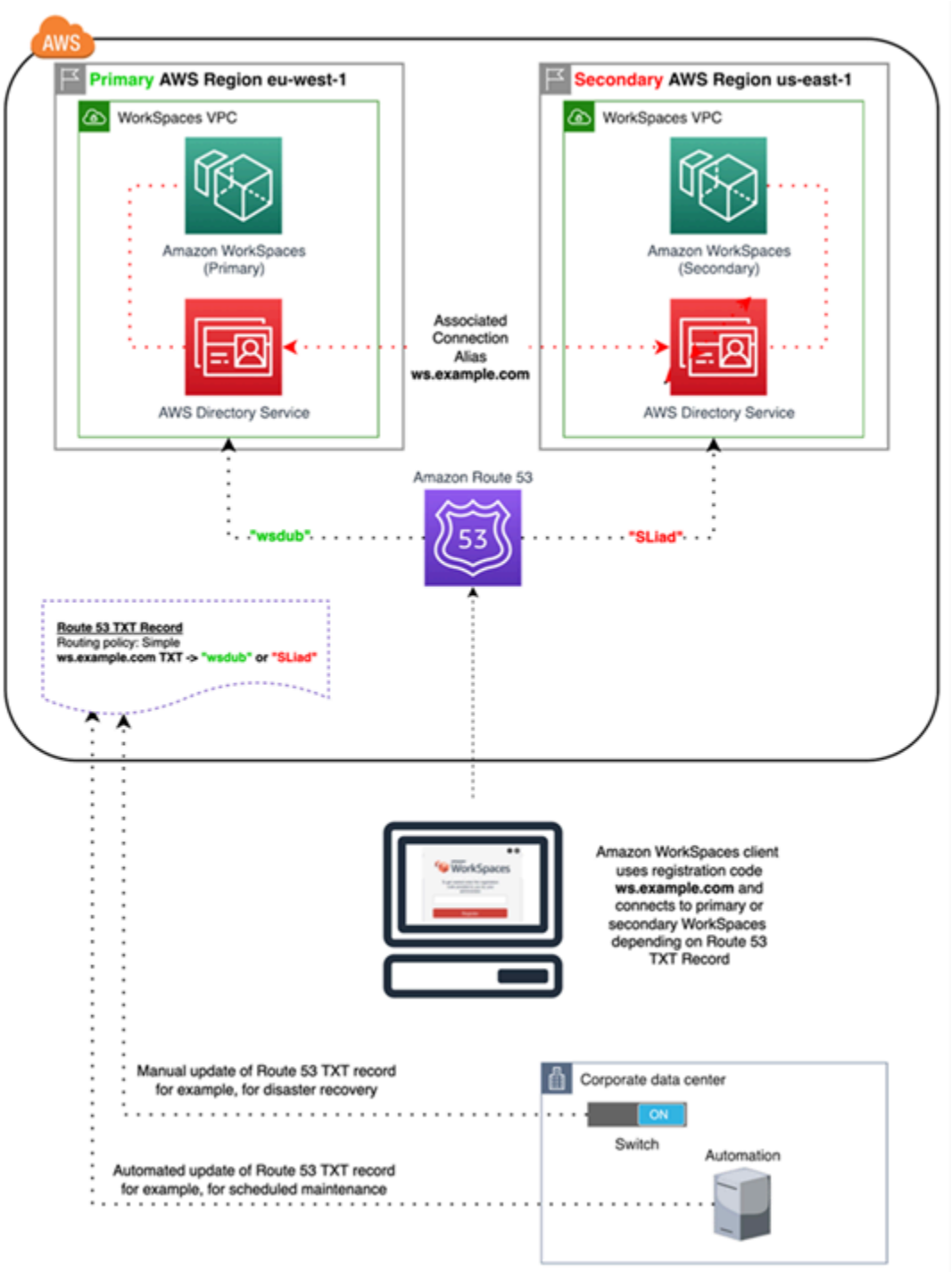

圖 17：使用 Amazon 路線 53 的 WorkSpaces 跨區域重定向示例

WorkSpaces 介面 VPC 人雲端端點 (AWS PrivateLink) — API 呼叫

上支援 Amazon WorkSpaces 公用 API AWS PrivateLink。 AWS PrivateLink 通過減少數據暴露在公共互聯網上，從而提高與雲端應用程序共享數據的安全性。 WorkSpaces 您可以使用介面端點來保護

VPC 內的 API 流量，介面端點是一種 elastic network interface，該介面具有來自子網路 IP 位址範圍的私有 IP 位址，可做為目標至受支援服務之流量的進入點。這使您可以使用私有 IP 地址來私有訪問 WorkSpaces API 服務。

PrivateLink 搭配 WorkSpaces 公用 API 使用也可讓您將 REST API 安全地公開給僅在 VPC 內的資源，或透 AWS Direct Connect過.

您可以限制對所選 Amazon VPC 和 VPC 端點的存取，並使用資源特定政策啟用跨帳戶存取。

請確定與端點網路介面關聯的安全群組允許端點網路介面和 VPC 中與服務通訊的資源之間的通訊。如果安全群組限制來自 VPC 資源的傳入 HTTPS 流量 (連接埠 443)，您可能無法透過端點網路介面傳送流量。界面端點僅支援 TCP 流量。

- 端點僅支援 IPv4 流量。
- 當您建立端點時，可以將端點政策連接至閘道端點，以控制存取您要連線的服務。
- 每個 VPC 可建立的端點數量都有配額。
- 僅在相同區域內支援端點。您無法在 VPC 和不同地區的服務之間建立端點。

建立通知以接收介面端點事件的警示 — 您可以建立通知以接收介面端點上發生的特定事件的警示。若要建立通知，您必須建立 Amazon SNS 主題與通知的關聯。您可以訂閱 SNS 主題，在端點事件發生時收到電子郵件通知。

為 Amazon 建立 VPC 端點政策 WorkSpaces — 您可以為 Amazon 的 Amazon VPC 端點建立政策，以指定 WorkSpaces 以下內容：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

將私人網路 Connect 到 VPC — 若要透過 VPC 呼叫 Amazon WorkSpaces API，您必須從 VPC 內的執行個體進行連線，或使用 Amazon 虛擬私人網路 (VPN) 或將私人網路連線到 VPC。 AWS Direct Connect如需 Amazon VPN 的相關資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的 VPN 連線。若要取得有關的資訊 AWS Direct Connect，請參閱《使用指南》中的AWS Direct Connect 〈建立連接〉。

如需透過 VPC 介面端點使用 Amazon WorkSpaces API 的詳細資訊，請參閱 Amazon WorkSpaces 中的基礎設施安全。

智慧卡支援

智能卡支持可用於 Microsoft 視窗和 Amazon Linux WorkSpaces。透過共用存取卡 (CAC) 和個人身分驗證 (PIV) 提供的智慧卡支援，可透過 Amazon WorkSpaces 使用 WorkSpaces 串流通訊協定 (WSP) 獨家提供。WSP 上的智慧卡支援可 WorkSpaces 提供更高的安全性狀態，以智慧卡讀卡機的形式驗證組織核准的端點與特定硬體連線的使用者。首先要熟悉可用於智慧卡的支援範圍，並決定智慧卡在現有和 future WorkSpaces 部署中的運作方式非常重要。

最佳作法是判斷需要哪種類型的智慧卡支援、工作階段前驗證或工作階段內驗證。工作階段前驗證僅在撰寫本文時提供 AWS GovCloud (美國西部)、美國東部 (維吉尼亞北部)、美國西部 (奧勒岡)、歐洲 (愛爾蘭)、亞太區域 (東京) 和亞太區域 (雪梨)。工作階段內智慧卡驗證通常可以考量一些考量，例如：

- 您的組織是否擁有與 Windows 作用中目錄整合的智慧卡基礎結構？
- 您的線上憑證狀態通訊協定 (OCSP) 回應程式公用網際網路可存取嗎？
- 主體別名 (SAN) 欄位中是否使用使用者主要名稱 (UPN) 簽發的使用者憑證？
- 有關會話中和會話前部分的更多考量事項。

透過群組原則啟用智慧卡支援。最佳做法是將 WSP 的 Amazon WorkSpaces 群組原則管理範本新增至 Amazon WorkSpaces 目錄使用的 Active Directory 網域的中央存放區。將此政策套用至現有 Amazon WorkSpaces 部署時，所有部署 WorkSpaces 都需要群組原則更新和重新開機，變更才能對所有使用者生效，因為它是以電腦為基礎的政策。

根 CA

Amazon 用 WorkSpaces 戶端和使用者的可攜性本質需要將第三方根 CA 憑證從遠端傳遞到使用者用來連接 Amazon 的每個裝置的受信任根憑證存放區。 WorkSpacesAD 網域控制站和具有智慧卡的使用者裝置必須信任根 CA。如需有關確切需求的詳細資訊，請檢閱 Microsoft 提供的啟用協力廠商 CA 所提供的準則。

在 AD 網域加入的環境中，這些裝置會透過群組原則散發根 CA 憑證來滿足此需求。在從 non-domain-joined 裝置使用 Amazon 用 WorkSpaces 戶端的案例中，必須決定第三方根 CA 的替代交付方法，例如 Intune。

工作階段中

在 Amazon WorkSpaces 使用者工作階段啟動之後，工作階段內身份驗證可簡化和保護應用程式身份如前所述，Amazon 的預設行為 WorkSpaces 會停用智慧卡，且必須透過群組原則啟用。從 Amazon

WorkSpaces 管理的角度來看，傳遞身份驗證的應用程式特別需要進行設定 (例如 Web 瀏覽器)。AD 連接器和目錄不需要變更。

最常見的應用需要在會話中的身份驗證支持是通過 Web 瀏覽器，如火狐瀏覽器和谷歌瀏覽器。火狐瀏覽器需要有限的配置，以支持會話中的智能卡。Amazon Linux WSP WorkSpaces 需要為火狐瀏覽器和谷歌瀏覽器在會話中智能卡支持額外的配置。

最佳做法是確保在進行故障排除之前，先將根 CA 載入使用者的個人憑證存放區，因為 Amazon WorkSpaces Client 可能沒有本機電腦的許可。此外，在疑難排解智慧卡的任何可疑工作階段中驗證問題時，請使用 OpenSC 識別智慧卡裝置。最後，建議使用線上憑證狀態通訊協定 (OCSP) 回應程式，透過憑證撤銷檢查來改善應用程式驗證的安全性狀態。

會前

Support 工作階段前驗證功能需要 Windows WorkSpaces 用戶端 3.1.1 及更新版本，或 macOS WorkSpaces 用戶端版本 3.1.5 及更新版本。使用智慧卡進行工作階段前驗證與標準驗證有根本不同，要求使用者透過插入智慧卡和輸入 PIN 碼的組合進行驗證。使用此驗證類型時，使用者工作階段的持續時間受 Kerberos 票證的存留期限制。完整的安裝指南可以在這裡找到。

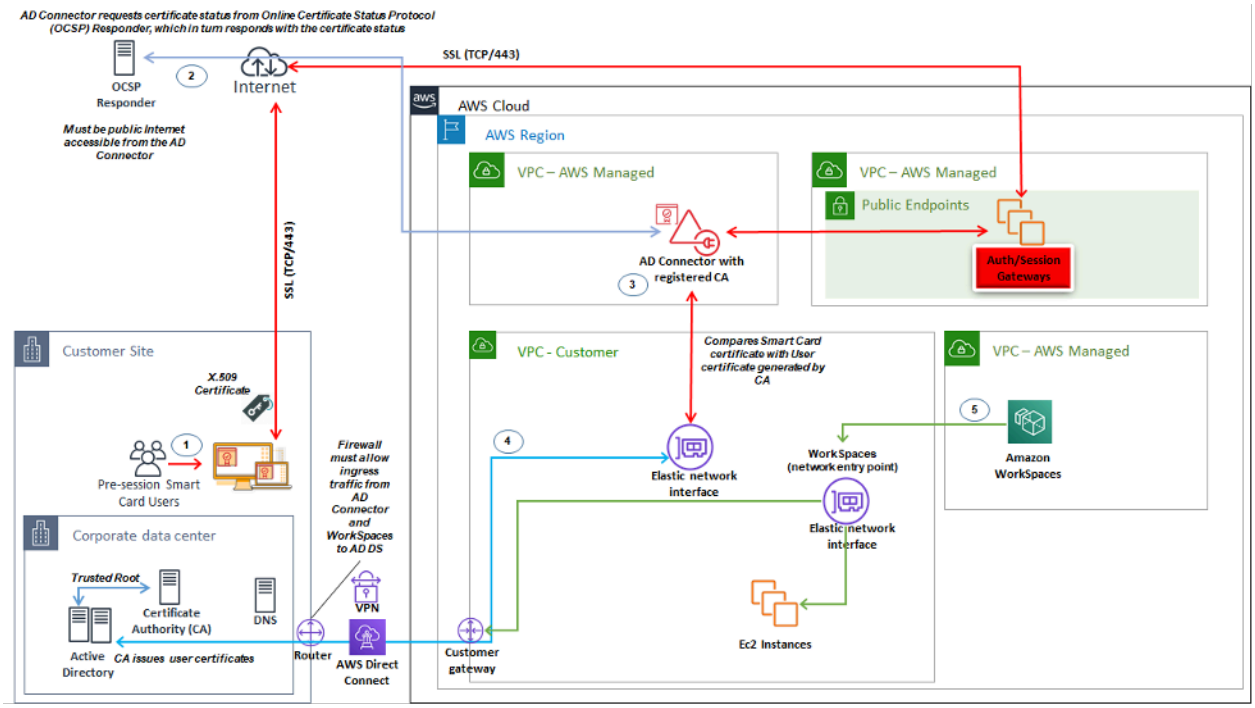

圖 18：工作階段前驗證概觀

1. 用戶打開 Amazon WorkSpaces 客戶端，插入智能卡，然後輸入他們的 PIN。Amazon 用 WorkSpaces 戶端會使用 PIN 碼來解密 X.509 憑證，此憑證是透過身份驗證閘道代理到 AD Connector 的憑證。
2. AD Connector 會根據目錄設定中指定的可公開存取的 OCSP 回應程式 URL 來驗證 X.509 憑證，以確保憑證尚未撤銷。
3. 如果憑證有效，Amazon 用 WorkSpaces 戶端會提示使用者再次輸入 PIN 碼以將 X.509 憑證和 Proxy 解密至 AD Connector 接器，以繼續進行驗證程序，然後將其與 AD 連接器的根憑證和中繼憑證進行驗證。
4. 成功比對憑證的驗證之後，AD Connector 會使用 Active Directory 來驗證使用者，並建立 Kerberos 票證。
5. Kerberos 票證會傳遞給使用者的 Amazon， WorkSpace 以驗證並開始 WSP 工作階段。

OCSP 回應程式必須可公開存取，因為連線是透過 AWS 管理網路而非客戶管理網路執行，因此在此步驟中沒有路由到私人網路。

不需要輸入使用者名稱，因為提供給 AD Connector 的使用者憑證會在憑證的 userPrincipalName (SAN) 欄位中包含使用者的 subjectAltName (UPN)。最佳做法是自動化所有需要使用智慧卡工作階段前驗證的使用者，將 AD 使用者物件更新為使用憑證中預期的 UPN 進行驗證 PowerShell，而不是在 Microsoft 管理主控台中個別執行此操作。

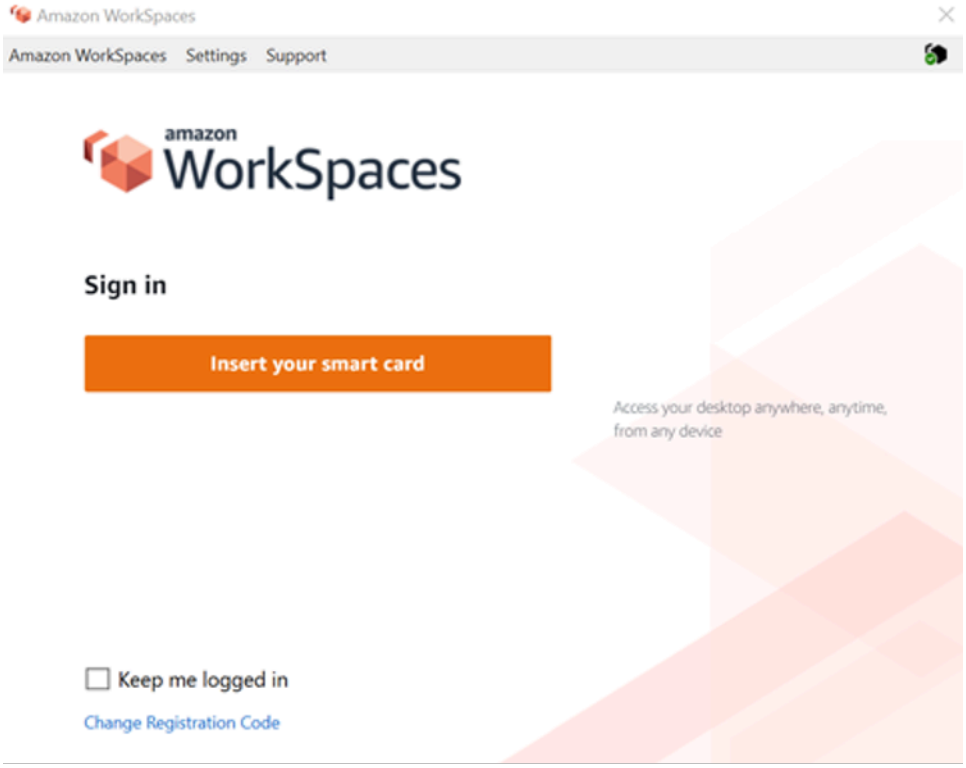

圖 19： WorkSpaces 登錄控制台

用戶端部署

Amazon 用 WorkSpaces 戶端 (3.X+ 版本) 使用標準化的組態檔案，管理員可利用這些檔案來預先配置其使用者的用戶端。 WorkSpaces 您可以在以下網址找到兩個主要組態檔案的路徑：

作業系統	組態檔案路徑
Windows	C:\Users\USERNAME\AppData\ 本地\ Amazon Web Services\ Amazon WorkSpaces
macOS	/用戶/用戶名/庫/應用程序Support /亞馬遜網絡服務/Amazon WorkSpaces
Linux 系統 (Ubuntu 18.04)	/家/聯絡/本地/共享/亞馬遜網絡服務/亞馬Amazon/ WorkSpaces

在這些路徑中，您將找到兩個配置文件。第一個配置文件是 UserSettings .json，它將設置諸如當前註冊，代理配置，日誌級別以及保存註冊列表的能力之類的內容。第二個配置文件是 RegistrationList .json。此檔案將包含用戶端用來對應至正確 WorkSpaces 目錄的所有 WorkSpaces 目錄資訊。預先設定 RegistrationList .json 會填入使用者用戶端內的所有註冊碼。

> **Note**
>
> 如果您的使用者執行的是用 WorkSpaces 戶端版本 2.5.11，proxy.cfg 將用於用戶端代理伺服器設定，而 client_settings.ini 會設定記錄檔層級以及儲存註冊清單的能力。默認代理設置將使用操作系統中設置的內容。

由於這些檔案是標準化的，因此管理員可以下載用WorkSpaces 戶端、設定所有適用的設定，然後將相同的組態檔推送給所有使用者。若要讓設定生效，必須在設定新組態之後啟動用戶端。如果您在用戶端執行時變更組態，則用戶端內不會設定任何變更。

可以為 WorkSpaces 使用者設定的最後一個設定是 Windows 用戶端 auto 更新。這不是通過配置文件進行控制，而是通過 Windows 註冊表進行控制。當新版本的用戶端出現時，您可以建立登錄機碼來略過該版本。這可以通過在以下路徑中創建一個字符串註冊表項名稱 SkipThisVersion ，該字符串註冊

表項名稱設置為完整版本號：計算機\ HKEY_CURRENT_USER\ 軟件\ Amazon Web Services。LLC \ Amazon WorkSpaces\ WinSparkle 此選項也適用於 macOS；但是，配置位於 plist 文件中，需要特殊的軟件才能編輯。如果您仍然想執行此操作，可以通過在 com.amazon.workspaces 域中添加 SU SkippedVersion 條目來完成：/用戶/用戶名/庫/首選項

Amazon WorkSpaces 端點選擇

為您的端點選擇 WorkSpaces

Amazon WorkSpaces 為從 Windows 桌面到 iPads 和 Chromebook 的多個端點設備提供支持。您可以從 Amazon 工作區網站下載可用的 Amazon WorkSpaces 客戶端。為使用者選擇正確的端點是一項重要決定。如果您的使用者需要使用雙向音訊/視訊，而且將會使用 WorkSpaces串流通訊協定，他們必須使用 Windows 或 macOS 用戶端。對於所有用戶端，請確保已明確設定 Amazon 的 IP 位址和連接埠需求中列出 WorkSpaces的 IP 地址和連接埠，以確保用戶端可以連線到服務。以下是一些可協助您選擇端點裝置的其他考量事項：

- 視窗 — 若要使用視窗 Amazon 用 WorkSpaces 戶端，4.x 用戶端必須執行需要 64 位元 Microsoft 視窗 8.1、視窗 10 桌面。使用者可以只為其使用者設定檔安裝用戶端，而不需要在本機電腦上的管理權限。系統管理員可以使用群組原則、Microsoft 端點管理員組態管理員 (MEMCM) 或環境中使用的其他應用程式部署工具，將用戶端部署到受管理的端點。Windows 用戶端最多支援四個顯示器，最大解析度為 3840x2160。
- macOS — 若要部署最新的 macOS Amazon WorkSpaces 用戶端, macOS 的設備必須運行 macOS 10.12 (塞拉利昂) 或更高版本. WorkSpaces 如果端點執行 OSX 10.8.1 或更新版本，您可以部署舊版 WorkSpaces 用戶端以連線到 PCoIP。macOS 用戶端最多可支援兩部 4K 解析度顯示器或四部解析度螢幕。
- Linux — Amazon WorkSpaces 用戶端需要執行 64 位元的 Ubuntu 18.04 (AMD64)。如果您的 Linux 端點未執行此作業系統版本，則不支援 Linux 用戶端。在部署 Linux 用戶端或向使用者提供其註冊碼之前，請確定您已在 WorkSpaces 目錄層級啟用 Linux 用戶端存取，因為預設會停用此功能，且在啟用之前，使用者將無法從 Linux 用戶端連線。Linux 用戶端最多可支援兩個 4K 解析度監視器或四台解析度監視器。
- iPad — Amazon WorkSpaces iPad 用戶端應用程式支援 PCoIP WorkSpaces。支持的 iPads 是 iPad 或更高版本與 iOS 8.0 或更高版本，iPad 視網膜與 iOS 8.0 及更高版本，iPad 迷你與 iOS 8.0 及更高版本，和 iPad 臨與 iOS 9.0 及更高版本。確定使用者連線的裝置符合這些準則。iPad 用戶端應用程式支援許多不同的手勢。(請參閱支援手勢的完整清單。) Amazon WorkSpaces iPad 客戶端應用程序還支持快速點 GT 和 PadPoint 鼠標。 ProPoint不支援快速點追蹤點 PenPoint 和滑 GoPoint 鼠。

- 安卓/Chromebook — 當您希望部署 Android 設備或 Chromebook 作為終端用戶的終端時，必須考慮一些考慮因素。請確定連線 WorkSpaces 的使用者為 PCoIP WorkSpaces，因為這個用戶端只支援 PCoIP。 WorkSpaces此用戶端僅支援單一顯示器。如果使用者需要多重監視器支援，請使用不同的端點。如果要部署 Chromebook，請確保您部署的模型支持安裝 Android 應用程序。只有安卓用戶端才支援完整功能支援，而不支援舊版 Chromebook 用戶端。這通常只是 2019 年之前製造的 Chromebook 的考慮因素。只要 Android 運行操作系統 4.4 及更高版本，就可以為平板電腦和手機提供 Android 支持。但是，建議安卓設備運行操作系統 9 或更高版本，以使用最新的 WorkSpace 安卓客戶端。如果您的 Chromebook 執行的是 3.0.1 或更高版本的用 WorkSpaces 戶端，您的使用者現在可以利用自助服務功能。WorkSpaces 此外，身為系統管理員，您可以使用受信任裝置憑證來限制對具有有效憑證之受信任裝置的 WorkSpaces 存取。
- 網頁存取 — 使用者可以使用網頁瀏覽器 WorkSpaces 從任何位置存取其 Windows。這非常適合必須使用鎖定裝置或限制性網路的使用者。使用者可以造訪網站以存取其工作資源，而不是使用傳統的遠端存取解決方案及安裝適當的用戶端應用程式。使用者可以利用 WorkSpaces 網頁存取連線至 WorkSpaces 執行 non-graphics-based視窗 10 或具有桌面體驗的視窗伺服器 2016 或視窗伺服器 2016。使用者必須使用 Chrome 53 或更新版本，或火狐 49 或更新版本進行連線。對於基於 WSP WorkSpaces，用戶可以利用 WorkSpaces Web 訪問連接到基於 Windows 的非圖形。 WorkSpaces 這些用戶必須使用 Microsoft 邊緣 91 或更高版本或谷歌瀏覽器 91 或更高版本連接。支援的最低螢幕解析度為 960 x 720，支援的最大解析度為 2560 x 1600。不支援多個監視器。為了獲得最佳的使用者體驗，建議使用者盡可能使用作業系統版本的用戶端。
- PCoIP 零用戶端 — 您可以將 PCoIP 零用戶端部署到已指派或將要指派 P WorkSpaces CoIP 的終端使用者。TerA2 零用戶端的韌體版本必須為 6.0.0 或更新版本，才能直接連線至. WorkSpace 若要在 Amazon 上使用多重要素身份驗證 WorkSpaces，TerA2 零用戶端裝置必須執行韌體版本 6.0.0 或更新版本。零客戶端硬件的 Support 和故障排除應該與製造商完成。
- 伊格爾作業系統 — 只要韌體版本為 11.04.280 或以上，您就可以在端點裝置上使用 IGEL WorkSpaces 作業系統來連接 PCoIP。支援的功能符合目前現有 Linux 用戶端的功能。在部署 IGEL OS 客戶端或向用戶提供註冊碼之前，請確保您在 WorkSpaces 目錄級別啟用 Linux 客戶端訪問，因為默認情況下禁用，並且在啟用 IGEL OS 客戶端之前，用戶將無法從 IGEL OS 客戶端進行連接。LGel 作業系統用戶端最多支援兩個 4K 解析度顯示器或四個 WUXGA (1920x1200) 解析度顯示器。

網頁存取用戶端

Web Access 用戶端專為鎖定的裝置而設計，無需部署用戶端軟體 WorkSpaces 即可存取 Amazon。只有在 Amazon WorkSpaces 為 Windows 作業系統 (OS) 的設定中才建議使用 Web 存取用戶端，並且用於有限的使用者工作流程，例如信息亭環境。大多數使用案例都受益於 Amazon 用 WorkSpaces

戶端提供的功能集。只有在裝置和網路限制需要替代連線方法的特定使用案例時，才建議使用 Web Access 用戶端。

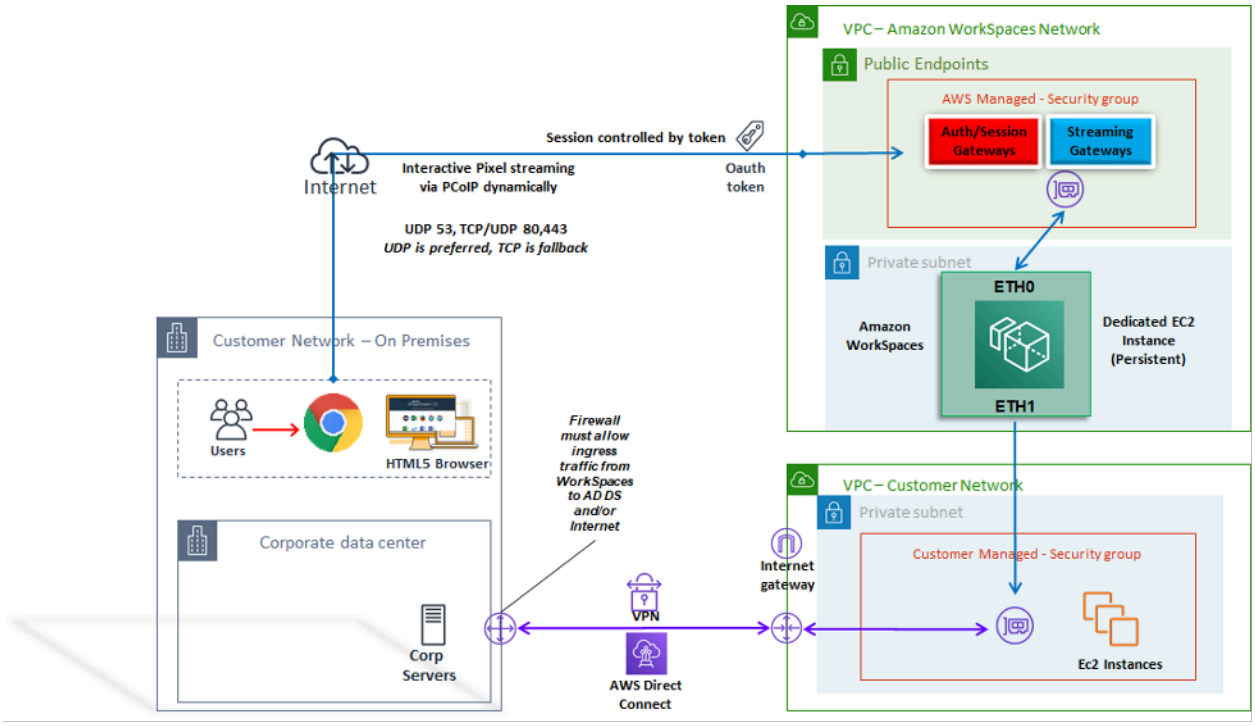

圖 20：Web 訪問客戶端體系結構

如圖所示，Web Access 用戶端有不同的網路需求，將工作階段串流給使用者。網頁存取可供 WorkSpaces 使用 PCoIP 或 WSP 通訊協定的視窗使用。在閘道上 WorkSpaces 進行驗證和註冊時，需要使用 DNS 和 HTTP/HTTPS。若要 WorkSpaces 使用 WSP 通訊協定，需要開啟到 WSP 閘道 IP 位址範圍的 UDP/TCP 4195 的直接連線。串流流量不會像使用完整 Amazon WorkSpaces 用戶端一樣分配給固定連接埠；而是動態分配。UDP 最適合串流流量；不過，當 UDP 受到限制時，網頁瀏覽器會回復為 TCP。在 TCP/UDP 連接埠 4172 遭封鎖且因組織限制而無法解除封鎖的環境中，Web 存取用戶端會為使用者提供替代的連線方法。

依預設，Web 存取用戶端會在目錄層級停用。若要讓使用者 WorkSpaces 透過網頁瀏覽器存取其 Amazon，請使用更新目錄設定，或以程式設計方式使用 WorkspaceAccessProperties API 修改 DeviceTypeWeb 為允許。 AWS Management Console 此外，系統管理員必須確定群組原則設定不會與登入需求衝突。

Amazon WorkSpaces 標籤

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
```

```
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.

Tag restrictions
```

- 每一資源標籤數上限：50
- 索引鍵長度上限：127 個 Unicode 字元
- 數值長度上限：255 個 Unicode 字元
- 標籤金鑰與值皆區分大小寫。允許的字元包括可用 UTF-8 表示的英文字母、空格和數字，還有以下特殊字元：+ - = . _ : / @。不可使用結尾或前方空格。
- 請勿在標籤名稱或值中使用 aws: 或 aws: 工作區:前置詞，因為它們已保留供使用。 AWS 您不可編輯或刪除具有這些字首的標籤名稱或值。

您可以標記的資源

- 您可以在建立下列資源時將標籤新增至下列資源： WorkSpaces、匯入的映像和 IP 存取控制群組。
- 您可以將標籤新增至下列類型的現有資源： WorkSpaces、已註冊的目錄、自訂服務包、映像和 IP 存取控制群組。

使用成本配置標記

若要在 Cost Explorer 中檢視 WorkSpaces 資源標籤，請依照《 AWS Billing and Cost Management 與成本管理使用者指南》中的〈啟動使用者定義的成本配置標籤〉中的指示，啟動您套用至 WorkSpaces 資源的標籤。

雖然標籤會在啟用後 24 小時顯示，但與這些標籤相關聯的值可能需要四到五天才會顯示在 Cost Explorer 中，才會在 Cost Explorer 中顯示並提供成本資料，但已標記的 WorkSpaces 資源必須在該期間產生費用。Cost Explorer 只會顯示標籤向前啟動時的成本資料。目前沒有可用的歷史資料。

管理標籤

若要使用更新現有資源的標籤 AWS CLI，請使用建立標籤和刪除標籤指令。對於批量更新和自動執行大量 WorkSpaces 資源的任務，Amazon 新 WorkSpaces增了對 AWS Resource Groups 標籤編輯器的支援。 AWS Resource Groups 標籤編輯器可讓您新增、編輯或刪除標 AWS 籤以 WorkSpaces 及其他 AWS 資源。

Amazon WorkSpaces 服務配額

Service Quotas 可讓您輕鬆查詢特定配額的值，也稱為限制。您也可以查詢特定服務的所有配額。

若要檢視您的配額 WorkSpaces

1. 瀏覽至「Ser vice Quotas」主控台。
2. 在左側導覽窗格中，選擇 [AWS 服務]。
3. WorkSpaces從列表中選擇 Amazon，或在預先輸入的搜索字段 WorkSpaces中輸入 Amazon。
4. 若要檢視有關配額的其他資訊，例如其說明和 Amazon 資源名稱 (ARN)，請選擇配額名稱。

Amazon WorkSpaces 提供您可在指定區域的帳戶中使用的不同資源，包括映像 WorkSpaces、服務包、目錄、連線別名和 IP 控制群組。建立 Amazon Web Services 帳戶時，會針對您可以建立的資源數量設定預設配額 (也稱為限制)。

您可以使用「Service Quotas」主控台來檢視預設的「Service Quotas」，或要求增加可調配額的配額。

如需詳細資訊，請參閱 Service Quotas 使用者指南中的檢視服務配額和要求增加配額。

自動化 Amazon WorkSpaces 部署

使用 Amazon WorkSpaces，您可以在幾分鐘內啟動 Microsoft Windows 或 Amazon Linux 桌面平台，並從現場部署或外部網路安全、可靠且快速地連接並存取桌面軟體。您可以將 Amazon 的佈建自動化，以 WorkSpaces 便 WorkSpaces將 Amazon 整合到現有的佈建工作流程中。

常用 WorkSpaces 自動化方法

客戶可以使用多種工具來快速 WorkSpaces 部署 Amazon。這些工具可用來簡化管理 WorkSpaces、降低成本，並啟用可快速擴充和移動的敏捷環境。

AWS CLI 和 API

您可以使用 Amazon WorkSpaces API 操作來安全且大規模地與服務互動。所有公用 API 都可與 AWS CLI SDK 和工具一起使用 PowerShell，而私有 API (例如映像建立) 只能透過 AWS Management Console. 考慮 Amazon 的營運管理和業務自助服務時 WorkSpaces，請考慮 WorkSpaces API 確實需要技術專業知識和安全許可才能使用。

您可以使用 AWS SDK 進行 API 呼叫。AWS Windows 工具 PowerShell和 PowerShell 核心 AWS 工具是建立在 AWS SDK 為 .NET 公開的功能上的 PowerShell 模組。這些模組可讓您從命令列對 AWS 資源執行指 PowerShell 令碼作業，並與現有工具和服務整合。例如，API 呼叫可讓您透過與 AD 整合， WorkSpaces 根據使用者的 AD 群組成員資格佈建和解除委任，藉此自動管理 WorkSpaces 生命週期。

AWS CloudFormation

AWS CloudFormation 可讓您在文字檔案中建立整個基礎結構的模型。此範本會成為您基礎結構的單一事實來源。這可協助您將整個組織中使用的基礎結構元件標準化，達到組態合規性並加快疑難排解速度。

AWS CloudFormation 以安全、可重複的方式佈建您的資源，讓您能夠建置和重建基礎架構和應用程式。您可以用 CloudFormation 來委託和解除委任環境，當您有許多要以可重複的方式建立和解除委任的帳戶時，這非常有用。在考慮 Amazon 的營運管理和業務自助服務時 WorkSpaces，請考慮這確AWS CloudFormation實需要技術專業知識和安全許可才能使用。

自助 WorkSpaces 入口

客戶可以使用建置在 WorkSpaces API 命令和其他 AWS 服務上建立 WorkSpaces 自助式入口網站。這有助於客戶簡化大規模部署和回收 WorkSpaces 的流程。使用入 WorkSpaces 口網站，您可以讓您的員工 WorkSpaces 透過整合式核准工作流程佈建自己的工作流程，而每個請求都不需要 IT 介入。如此可降低 IT 營運成本，同時協助終端使用者 WorkSpaces 更快速地開始使用。額外的內建核准工作流程可簡化企業的桌上型電腦核准程序。專用入口網站可提供佈建 Windows 或 Linux 雲端桌面的自動化工具，讓使用者能夠重建、重新啟動或移轉 WorkSpace，並提供密碼重設的功能。

在本文件的「進一步閱讀」一節中，參考了建立自助服務 WorkSpaces 入口網站的引導範例。 AWS 合作夥伴透過提供預先設定的 WorkSpaces AWS Marketplace管理入口網站

與企業 IT 服務管理整合

隨著企業大規模採用 Amazon WorkSpaces 作為虛擬桌面解決方案，因此需要實作 IT 服務管理 (ITSM) 系統或與之整合。ITSM 整合允許用於佈建和作業的自助服務供應項目。Ser vice Catalog 可讓您集中管理常用部署的 AWS 服務和佈建的軟體產品。此服務可協助您的組織達成一致的治理與合規性需求，同時讓使用者僅部署所需的核准 AWS 服務。Service Catalog 可用於 WorkSpaces 從 IT 服務管理工具 (例如. ServiceNow

WorkSpaces 部署自動化最佳做法

您應該考慮選擇和設計 WorkSpaces 部署自動化的良好架構原則。

- 自動化設計 — 在流程中提供盡可能少的人工介入，以實現可重複性和擴展性的設計。
- 成本最佳化設計 — 透過自動建立和回收 WorkSpaces，您可以減少提供資源所需的管理工作，並移除閒置或未使用的資源，從而產生不必要的成本。
- 提高效率的設計 — 最大限度地減少創建和終止所需的資源 WorkSpaces。在可能的情況下，為企業提供 Tier 0 自助服務功能，以提高效率。
- 彈性設計 — 建立一致的部署機制，可處理多個案例，並且可以使用相同的機制進行擴充 (使用標記的使用案例和設定檔識別碼進行自訂)。
- 生產力設計 — 設計您的 WorkSpaces 操作，以允許正確的授權和驗證來添加或刪除資源。
- 可擴展性設計 — Amazon WorkSpaces 使用的 pay-as-you Go 模型可以根據需要建立資源來節省成本，並在不再需要資源時將其移除。
- 安全性設計 — 設計您的 WorkSpaces 操作，以允許正確的授權和驗證來添加或刪除資源。
- 支援能力設計 — 設計您的 WorkSpaces 作業，以允許非侵入性的支援與復原機制和程序。

Amazon WorkSpaces 修補和就地升級

透過 Amazon WorkSpaces，您可以使用現有的第三方工具來管理修補和更新，例如 Microsoft 系統中心組態管理員 (SCCM)、傀儡企業或 Ansible。就地部署安全性修補程式通常會維持每月一次的修補週期，並提供額外的程序來進行升級或快速部 但是，在就地作業系統升級或功能更新的情況下，通常需要特別考量。

WorkSpace 維護

Amazon WorkSpaces 有一個預設維護時段，在此期間 WorkSpace 安裝 Amazon WorkSpaces 代理程式更新和任何可用的作業系統更新。 WorkSpaces 在排程的維護時段期間，使用者連線將無法使用。

- AlwaysOn WorkSpaces 默認維護時間是 00h00 到 04h00，在的時區，每個星期日早上 WorkSpace。

- 依預設會啟用時區重新導向，而且可覆寫預設視窗以符合使用者的本機時區。
- 您可以 WorkSpaces使用群組原則停用 Windows 的時區重新導向。您可以使用 PCoIP 代理程式連續值 WorkSpaces來停用 Linux 的時區重新導向。

- AutoStop WorkSpaces 每月自動啟動一次以安裝重要更新。從每月的第三個星期一開始，最多兩週，維護窗口每天從 00h00 到 05h00 開放，在該地區的時區。 AWS WorkSpace WorkSpace 可以在維護窗口中的任何一天進行維護。

- 雖然您無法修改用於維護的時區 AutoStop WorkSpaces，但您可以停用您的維護時段 AutoStop WorkSpaces。

- 可以根據您偏好的排程來設定手動維護時段，方法是將狀態設定 WorkSpace 為 ADMIN_VIATION。

- 該 AWS CLI 命令modify-workspace-state可用於將 WorkSpace 狀態修改為「管理員 _ 維護」。

Amazon WorkSpaces

如需在 Amazon Linux WorkSpaces 自訂映像上管理更新和修補程式的考量、先決條件和建議模式，請參閱白皮書 WorkSpaces 為 Linux 映像準備 Amazon 的最佳實務。

Linux 修補的先決條件和考量

- Amazon Linux 儲存庫託管在 Amazon Simple Storage Service (Amazon S3) 貯體中，可透過可透過公用網際網路存取的端點或私有端點進行存取。如果您的 Amazon Linux WorkSpaces 沒有網際網路存取權限，請參閱這個程序，讓更新可供存取：如何在執行 Amazon Linux 1 或 Amazon Linux 2 的 EC2 執行個體上更新 yum 或安裝沒有網際網路存取的套件？
- 您無法設定 Linux 的預設維護時段 WorkSpaces。如果需要自訂此視窗，則可以使用手動維護程序。

Amazon 視窗修補

默認情況下，您的 Windows 配 WorkSpaces 置為從 Windows 更新接收更新，這需要從您的 WorkSpaces VPC 訪問互聯網。若要設定您自己的 Windows 自動更新機制，請參閱 Windows 伺服器更新服務 (WSUS) 和組態管理員的文件。

Amazon 視窗就地升級

- 如果您打算從 Windows 10 建立映像檔 WorkSpace，請注意，已從舊版升級 (Windows 功能/版本升級) 的 Windows 10 系統上不支援建立映像檔。不過， WorkSpaces 映像建立和擷取處理作業支援 Windows 累積或安全性更新。

- 自訂 Windows 10 自攜授權 (BYOL) 映像檔應以虛擬機器上最新受支援的 Windows 版本開頭，作為 BYOL 匯入程序的來源：如需進一步的詳細資訊，請參閱 BYOL 匯入文件。

就地升級的必要條件

- 如果您已使用作用中目錄群組原則或 SCCM 延遲或暫停 Windows 10 升級，請啟用 Windows 10 的作業系統升級。 WorkSpaces
- 如果 WorkSpace 是 AutoStop WorkSpace，請將 AutoStop 時間變更為至少三個小時，以配合升級時段。
- 就地升級程序會建立預設使用者 (C:\Users\Default) 的複本，以重新建立使用者設定檔。請勿使用預設的使用者設定檔進行自訂。建議改為透過群組原則物件 (GPO) 對使用者設定檔進行任何自訂。透過 GPO 進行的自訂可以輕鬆修改或復原，而且較不容易發生錯誤。
- 就地升級程序只能備份並重新建立一個使用者設定檔。如果磁碟機 D 上有多個使用者設定檔，請刪除您所需以外的其他設定檔。

視窗就地升級考量

- 就地升級程序會使用兩個登錄指令碼 (enable-inplace-upgrade.ps1 和更新 pvdrivers.ps1) 來對您 WorkSpaces 進行必要的變更，並啟用 Windows 更新程序執行。這些更改涉及在驅動器 C 而不是驅動器 D 上創建臨時用戶配置文件。如果驅動器 D 上已經存在用戶配置文件，則該原始用戶配置文件中的數據保留在驅動器 D 上。
- 部署就地升級之後，您必須將使用者設定檔還原至 D 磁碟機，以確保您可以重建或移轉您的 WorkSpaces，並避免使用者 shell 資料夾重新導向的任何潛在問題。您可以使用 PostUpgradeRestoreProfileOnD 登錄機碼來執行此操作，如 BYOL 升級參考頁面所述。

Amazon WorkSpaces 語言包

提供 Windows 10 桌面體驗的 Amazon WorkSpaces 套裝軟體支援英文 (美國)、法文 (加拿大)、韓文和日文。不過，您可以為西班牙文、義大利文、葡萄牙文以及更多其他語言選項加入其他語言套件。如需詳細資訊，請參閱如何使用英文以外的用戶端語言建立新的 Windows WorkSpace 映像？ 。

Amazon WorkSpaces 檔案管理

Amazon 透過將所有設定檔寫入重新導向至單獨的 Amazon 彈性區塊存放區 (Amazon EBS) 磁碟區，將使用者設定檔 WorkSpaces 與基本作業系統 (OS) 區隔開來。在 Microsoft 視窗中，使用者設定檔

儲存在 D:\Users\username 。在 Amazon Linux 中，用戶配置文件存儲在 /home 中。EBS 磁碟區會每 12 小時自動擷取一次。快照會自動存放在受 AWS 管 S3 儲存貯體中，以便在重建或還原 Amazon WorkSpace 時使用。

對於大多數組織而言，每 12 小時自動快照功能優於現有的桌上型電腦部署，不備份使用者設定檔。但是，客戶可能需要對使用者設定檔進行更精細的控制；例如 WorkSpaces，從桌面移轉到新的 OS/AWS 區域、支援 DR 等。Amazon 提供了用於設定檔管理的替代方法 WorkSpaces。

文件夾重定

雖然資料夾重新導向是虛擬桌面基礎設施 (VDI) 架構中常見的設計考量，但這並不是最佳實務，甚至不是 Amazon 設 WorkSpaces 計的常見需求。原因是 Amazon WorkSpaces 是持久的桌面即服務 (DaaS) 解決方案，應用程式和使用者資料立即可用。

在特定情況下，需要使用者殼層資料夾的資料夾重新導向 (例如，D:\Users\username\Desktop 重新導向至\\ Server\ RedirectionShare $\ 使用者名稱\ Desktop)，例如嚴重損壞修復 (DR) 環境中的使用者設定檔資料的立即復原點目標 (RPO)。

最佳實務

以下列出可靠的資料夾重新導向的最佳作法：

- 在 Amazon WorkSpaces 推出的同一 AWS 區域和 AZ 中託管 Windows 文件服務器。
- 確定 AD 安全性群組輸入規則包含 Windows 檔案伺服器安全性群組或私人 IP 位址；否則請確定內部部署防火牆允許相同的 TCP 和 UDP 連接埠型流量。
- 確保 Windows 檔案伺服器安全群組輸入規則包含所有 Amazon WorkSpaces 安全群組的 TCP 445 (SMB)。
- 為 Amazon WorkSpaces 用戶創建 AD 安全組，以授權用戶訪問 Windows 文件共享。
- 使用 DFS 命名空間 (DFS-N) 和 DFS 複寫 (DFS-R) 來確保您的 Windows 檔案共用具有敏捷性，不會與任何特定的 Windows 檔案伺服器繫結在一起，而且所有使用者資料都會在 Windows 檔案伺服器之間自動複製。
- 在 Windows 檔案總管中瀏覽網路共用時，將「$」附加至共用名稱的末尾，以隱藏共用主機使用者資料。
- 依照 Microsoft 針對重新導向的資料夾指引建立檔案共用：使用離線檔案部署資料夾重新導向。請仔細遵循安全性權限和 GPO 組態的指引。
- 如果您的 Amazon WorkSpaces 部署是使用自有授權 (BYOL)，您還必須依照 Microsoft 的指示指定停用離線檔案：停用個別重新導向資料夾上的離線檔案。

- 如果您的 Windows 檔案伺服器是 Windows Server 2016 或更新版本，請安裝並執行重複資料刪除 (通常稱為「刪除重複資料」)，以減少儲存體耗用量並最佳化成本。請參閱安裝並啟用重複資料刪除和執行重複資料刪除。
- 使用現有的組織備份解決方案來備份 Windows 檔案伺服器檔案共用。

要避免的事情

- 請勿使用只能透過廣域網路 (WAN) 連線存取的 Windows 檔案伺服器，因為 SMB 通訊協定並非針對此用途而設計。
- 請勿使用用於主目錄的相同 Windows 檔案共用，以減少使用者意外刪除其使用者殼層資料夾的機會。
- 為了方便檔案還原，建議您啟用磁碟區陰影複製服務 (VSS)，但這並不會移除備份 Windows 檔案伺服器檔案共用的需求。

其他考量

- 適用於 Windows 檔案伺服器的 Amazon FSx 提供 Windows 檔案共用的受管服務，並簡化資料夾重新導向 (包括自動備份) 的操作開銷。
- 如果沒有現有的組織備份解決方案，可用AWS Storage Gateway 於 SMB 檔案共用來備份您的檔案共用。

設定檔設定

群組原則

企業 Microsoft Windows 部署中常見的最佳作法是透過群組原則物件 (GPO) 和群組原則喜好設定 (GPP) 設定來定義使用者環境設定。快速鍵、磁碟機對應、登錄機碼和印表機等設定是透過群組原則管理主控台定義的。透過 GPO 定義使用者環境的好處包括但不限於：

- 集中式組態管理
- AD 安全性群組成員資格或 OU 放置定義的使用者設定
- 防止刪除設定
- 首次登入時自動建立設定檔和個人化
- 易於 future 的更新

> **Note**
>
> 請遵循 Microsoft 最佳化群組原則效能的最佳作法。

不得使用互動式登入橫幅群組原則，因為 Amazon 不支援這些原則 WorkSpaces。橫幅會透過 AWS 支援請求呈現在 Amazon WorkSpaces 用戶端上。此外，不得透過群組原則封鎖卸除式裝置，因為 Amazon 需要卸除式裝置 WorkSpaces。

GPO 可以用來管理視窗 WorkSpaces。如需詳細資訊，請參閱管理您的視窗 WorkSpaces。

Amazon WorkSpaces 卷

每個 Amazon WorkSpaces 執行個體都包含兩個磁碟區：作業系統磁碟區和一個使用者磁碟區。

- Amazon 視窗 WorkSpaces — C：\ 驅動器用於操作系統（OS），D：\ 驅動器是用戶卷。使用者設定檔位於使用者磁碟區 (AppData、[文件]、[圖片]、[下載] 等) 上。
- Amazon Linux WorkSpaces — 使用 Amazon Linux 時 WorkSpace，系統磁碟區 (/dev/xvda1) 會掛載為根資料夾。使用者磁碟區適用於使用者資料和應用程式；/dev/xvdf1 掛載為 /home。

對於作業系統磁碟區，您可以為此磁碟機選取 80 GB 或 175 GB 的起始大小。對於使用者磁碟區，您可以選取 10 GB、50 GB 或 100 GB 的起始大小。根據需要，兩個磁碟區的大小最多可增加到 2TB；不過，若要將使用者磁碟區增加到 100 GB 以上，作業系統磁碟區必須為 175 GB。每個磁碟區每六小時只能執行一次音量變更。如需有關修改 WorkSpaces 磁碟區大小的其他資訊，請參閱《管理指南》的 WorkSpace〈修改〉一節。

WorkSpaces 磁碟區最佳實踐

規劃 Amazon 部 WorkSpaces 署時，建議考量 OS 安裝、就地升級以及將新增至作業系統磁碟區映像的其他核心應用程式的最低需求。對於使用者磁碟區，建議從較小的磁碟配置開始，並視需要增加使用者磁碟區大小。最小化磁碟區的大小可降低執行 WorkSpace.

> **Note**
>
> 雖然可以增加磁碟區大小，但無法減小磁碟區大小。

Amazon WorkSpaces 日誌

在 Amazon WorkSpaces 環境中，可擷取許多日誌來源，以便對問題進行疑難排解並監控整體 WorkSpaces 效能。

Amazon WorkSpaces 用戶端 3.x 在每個 Amazon WorkSpaces 用戶端上，用戶端日誌位於以下目錄中：

- 視窗 — % 本地應用程序數據 %\ Amazon Web Services\ Amazon\ 日誌 WorkSpaces
- macOS-〜/庫/「應用程序 Support」/「Amazon Web Services」/「Amazon」/日誌 WorkSpaces
- Linux (Ubuntu 18.04 或更高版本) — /選擇/工作空間客戶端/工作空間客戶端

有許多實例可能需要從客戶端的 WorkSpaces 會話診斷或調試詳細信息。透過將「-l3」新增至工作區可執行檔，也可以啟用進階用戶端記錄檔。例如：

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

Amazon WorkSpaces 服務

Amazon WorkSpaces 服務與 Amazon CloudWatch 指標， CloudWatch 事件和 CloudTrail. 此整合可讓效能資料和 API 呼叫登入中央 AWS 服務。

管理 Amazon WorkSpaces 環境時，持續監控某些 CloudWatch 指標以確定整體環境健康狀態非常重要。指標

雖然 Amazon 還有其他 CloudWatch 指標可用 WorkSpaces (請參閱監控您的 WorkSpaces 使用 CloudWatch 指標)，但下列三個指標將有助於維護 WorkSpace執行個體的可用性：

- 不健康 — 傳回不健康狀態 WorkSpaces 的數目。
- SessionLaunchTime— 啟動 WorkSpaces 工作階段所需的時間。
- InSessionLatency— 用 WorkSpaces 戶端與之間的往返時間 WorkSpace。

如需有關 WorkSpaces 記錄選項的詳細資訊，請參閱使用記錄 Amazon WorkSpaces API 呼叫 CloudTrail。額外的 CloudWatch 事件將協助擷取使用者工作階段的用戶端 IP、使用者連線至 WorkSpaces 工作階段時，以及連線期間使用的端點。所有這些詳細資料都有助於在疑難排解工作階段期間隔離或找出使用者回報的問題。

> **Note**
>
> 某些 CloudWatch 量度僅適用於 AWS 受管理 AD。

適用於 Amazon 的 Linux 容器和視窗子系統 WorkSpaces

容器和 Amazon WorkSpaces

希望透過 Amazon WorkSpaces 為容器工作負載提供服務的客戶通常會處理最終使用者運算。儘管可能，但這不是首選或建議的解決方案。強烈建議希望釋放容器潛在成本和營運節省的客戶，以評估 Amazon 彈性容器服務 (Amazon ECS) 和/或 Amazon Elastic Kubernetes Service (Amazon EKS)。

在客戶需求要求使用 Amazon 啟用容器的情況下 WorkSpaces，已經發布了可以使用 Docker 的技術操作指南。客戶應該知道這需要其他尾隨服務，並且與解耦的原生容器服務相比，成本和複雜性會增加。

視窗子系統

隨著 Windows 服務器 2019 作為 Amazon 的基礎操作系統的推出 WorkSpaces，客戶一直渴望實施適用於 Linux 的 Windows 子系統（WSL），特別是 WSL2。由於 WSL2 會叫用虛擬機器 (Hyper-V) 來執行其功能，因此無法在由虛擬機器管理程式管理的 Amazon WorkSpaces 上執行。 AWS 客戶應該知道由於這個原因，只有 WSL1 可用，並了解 WSL1 和 WSL2 之間的差異。

Amazon WorkSpaces 遷移

Amazon WorkSpaces 遷移功能可讓您將使用者磁碟區資料帶入新的服務包。您可以使用此功能來：

- 將您 WorkSpaces 從視窗 7 體驗遷移到視窗 10 桌面體驗。
- 從 PCoIP 移轉 WorkSpace 至 WorkSpaces 串流通訊協定 (WSP)。 WorkSpace
- WorkSpaces 從一個公用或自訂套裝軟體移轉至另一個公用套裝軟體。例如，您可以從已啟用 GPU 的 (圖形和 GraphicsPro) 服務包移轉至未啟用 GPU 的服務包，反之亦然。

移轉程序

透過 WorkSpaces 移轉，您可以指定目標 WorkSpaces 服務包。移轉程序會重新建立 WorkSpace使用目標套裝軟體映像中的新根磁碟區，以及從最新的原始使用者磁碟區快照重新建立使用者磁碟區。移轉期間會產生新的使用者設定檔，以提高相容性。舊使用者設定檔中無法移至新設定檔的資料會儲存在 .NotMigration 資料夾中。

移轉期間，會保留使用者磁碟區 (磁碟機 D) 上的資料，但是根磁碟區 (C:\ 磁碟機) 上的所有資料都會遺失。這表示不會保留任何已安裝的應用程式、設定和登錄變更。舊的使用者設定檔資料夾會以重新命名。 NotMigrated 后綴，并創建一個新的用戶概況。

每個遷移程序最多需要一個小時 WorkSpace。此外，如果移轉工作流程無法完成程序，服務會在移轉前自動復原 WorkSpace 至其原始狀態，將任何資料遺失風險降至最低。

任何指派給原始標籤的標籤 WorkSpace 都會在移轉期間結轉。會保留的執行模式。 WorkSpace 移轉後會 WorkSpace 有新的 WorkSpace ID、電腦名稱和 IP 位址。移轉程序

您可以 WorkSpaces 透過 Amazon 主 WorkSpaces 控台、 AWS CLI 使用遷移工作區命令或 Amazon WorkSpaces API 進行遷移。所有遷移要求都會排入佇列，而且如果有太多遷移要求，服務會自動調節遷移要求的總數。移轉限制

- 您無法遷移至公用或自訂 Windows 7 桌面體驗套件。
- 您無法移轉至 BYOL 視窗 7 套裝軟體。
- 您 WorkSpaces 只能將 BYOL 移轉至其他 BYOL 服務包。
- 您無法將從公用或自訂套裝軟體 WorkSpace 建立的套裝軟體移轉至 BYOL 套裝軟體。
- 目前 WorkSpaces 不支援移轉 Linux。
- 在支援多種語言的 AWS 地區中，您可以在語言服務包 WorkSpaces 之間進行遷移。

- 來源和目標套件必須不同。但是，在支援多種語言的地區中，只要語言不同，您就可以移轉至相同的 Windows 10 服務包。) 如果您想要 WorkSpace 使用相同的套裝軟體重新整理，請 WorkSpace改為重建。
- 您無法 WorkSpaces 跨區域移轉。
- WorkSpaces 當它們處於「管理 _ 維護」模式時，無法進行移轉。

成本

在進行遷移的月份，系統會針對新的和原始版本按比例分配的金額向您收取費用。 WorkSpaces舉例來說，如果您在 5 月 10 日將 WorkSpace A 移轉至 WorkSpace B，我們會在 5 月 1 日至 5 月 10 日期間向您收取 WorkSpace A 費用，而且在 5 月 11 日至 5 月 30 日期間會向您收取 WorkSpace B 費用。

WorkSpaces 移轉最佳做法

在移轉之前 WorkSpace，請執行下列動作：

- 將磁碟機 C 上的所有重要資料備份到另一個位置。遷移期間，磁碟機 C 上的所有資料都會清除。
- 請確定要移轉 WorkSpace 的時間至少為 12 小時，以確保已建立使用者磁碟區的快照。在 Amazon WorkSpaces 主控台的 Migrate WorkSpaces 頁面上，您可以參考上次快照的時間。遷移期間，最後一次快照之後建立的任何資料都會遺失。
- 若要避免潛在的資料遺失，請確定您的使用者已登出其 WorkSpaces，並在遷移程序完成之前不要重新登入。
- 請確定 WorkSpaces 您要移轉的狀態為 [可用]、[已停止] 或 [錯誤]。
- 確保您有足夠的 IP 地址供 WorkSpaces您正在遷移。在移轉期間，將為 WorkSpaces.
- 如果您使用指令碼進行移轉 WorkSpaces，請一次以不超過 25 WorkSpaces 個批次的方式移轉指令碼。

Well-Architected 的框架

AWS Well-Architected 可協助雲端架構師為其應用程式和工作負載建置安全、高效能、彈性和高效率的基礎架構。本文說明在雲端中設計和執行工作負載的關鍵概念、設計原則和架構最佳實務。它基於五個關鍵支柱：

- 操作效能
- 安全
- 可靠性
- 效能效率
- 成本最佳化

建構 Amazon WorkSpaces 環境時，請務必評估這些關鍵支柱以確定成熟度部署層級，並探索可與 Amazon WorkSpaces 搭配使用的其他功能。雖然有 AWS Well-Architect 架構的整體指引，但下列提供了一些關鍵問題，這些問題可以包含在 WorkSpaces 部署的規劃階段，以確保五個支柱中的每一個都被考慮。

一般

- 這個項目的業務驅動力是什麼？

操作效能

- 如何隔離使用者和不同管理員群組之間的存取控制？

安全

1. 運作時應考慮哪些安全性和合規性要求？ WorkSpaces
2. 路由至外部 IP 位址是否有任何限制？
3. 是否允許所需的 WorkSpaces 連接埠通過企業防火牆？
4. 此部署是否會使用多重要素驗證？
5. 你今天有多少用戶身份和授權請求？

可靠性

1. 桌上型電腦的資料保留原則為何？
2. 一般使用者資料的復原點目標 (RPO) 是什麼？
3. 一般使用者資料的復原時間目標 (RTO) 是什麼？

成本最佳化

1. WorkSpaces 捆綁包的尺寸是否適合用戶案例和應用程序？
2. 用戶每月消耗的時間是否 WorkSpaces 超過 82 小時？

雖然上述問題並不構成應考慮的項目的詳盡清單，但它們提供了一些總體指導來協助您進行 Well-Architected 的 Amazon 部署。 WorkSpaces

安全

本節說明如何在使用 Amazon WorkSpaces 服務時使用加密來保護資料。它描述了傳輸中和靜態加密，以及使用安全群組來保護對 WorkSpaces. 本節也提供如何使用受信任的裝置和 IP 存取控制群組 WorkSpaces 來控制終端裝置存取的資訊。

您可以在本節中找到有關 AWS Directory Service 中驗證 (包括 MFA 支援) 的其他資訊。

傳輸中加密

Amazon WorkSpaces 使用加密技術來保護不同通訊階段 (傳輸中) 的機密性，並保護靜態資料 (加密 WorkSpaces)。下列各節說明 Amazon 傳輸 WorkSpaces 中使用之加密各階段的程序。

如需有關靜態加密的資訊，請參閱本文件的 WorkSpaces「已加密」一節。

註冊和更新

桌面用戶端應用程式會與 Amazon 通訊，以便使用 HTTPS 進行更新和註冊。

認證階段

桌面用戶端會透過將身分證明傳送至驗證閘道來初始化驗證。桌面用戶端與驗證閘道之間的通訊使用 HTTPS。在此階段結束時，如果驗證成功，則驗證閘道會透過相同的 HTTPS 連線將 OAuth 2.0 權杖傳回至桌面用戶端。

> **Note**
>
> 桌面用戶端應用程式支援使用 Proxy 伺服器進行連接埠 443 (HTTPS) 流量，以進行更新、註冊和驗證。

從用戶端收到身分證明後，驗證閘道會將驗證要求傳送至「 AWS Directory Service」。從驗證閘道到 AWS Directory Service 的通訊是透過 HTTPS 進行的，因此不會以純文字傳輸使用者身份證明。

驗證 — 作用中目錄連接器 (ADC)

AD Connector 使用 Kerberos 建立與內部部署 AD 的驗證通訊，因此它可以繫結至 LDAP 並執行後續 LDAP 查詢。ADC 中的用戶端 LDAPS 支援也可用來加密 Microsoft AD 和 AWS 應用程式之間的查詢。在實作用戶端 LDAPS 功能之前，請檢閱用戶端 LDAPS 的先決條件。

AWS Directory Service 也支援使用 TLS 的 LDAP。任何時候都不會以純文字傳輸使用者認證。為了提高安全性，您可以使用 VPN 連線將 WorkSpaces VPC 與內部部署網路 (AD 所在位置) 連線。使用 AWS 硬體 VPN 連線時，客戶可以使用標準 IPSEC (網際網路金鑰交換 (IKE) 和 IPSEC SA) 與 AES-128 或 AES-256 對稱加密金鑰、SHA-1 或 SHA-256 設定完整性雜湊，以及 DH 群組 (2,14-18、22、23 和 24 (第一階段)，設定傳輸中的加密；第一階段 1,2,5、14-18、22、23 和 24 (第 2 階段)。

經紀人階段

收到 OAuth 2.0 權杖後 (從身份驗證閘道，如果身份驗證成功)，桌面用戶端會使用 HTTPS 查詢 Amazon WorkSpaces 服務 (代理連線管理員)。桌面用戶端會傳送 OAuth 2.0 權杖來驗證本身，因此用戶端會接收串流閘道的端點資訊。 WorkSpaces

流媒體階段

桌面用戶端要求開啟包含串流閘道的 PCoIP 工作階段 (使用 OAuth 2.0 權杖)。此工作階段已經過 AES-256 加密，並使用 PCoIP 連接埠進行通訊控制 (4172/TCP)。

串流閘道會使用 OAuth2.0 權杖，透過 HTTPS 從 Amazon WorkSpaces 服務要求使用者特定 WorkSpaces 資訊。

串流閘道也會從用戶端接收 TGT (使用用戶端使用者的密碼加密)，並透過使用 Kerberos TGT 傳遞，閘道會使用使用者擷取的 Kerberos TGT 在上 WorkSpace啟動 Windows 登入。

WorkSpace 然後會使用標準 Kerberos 驗證，向設定的 AWS Directory Service 起始驗證要求。

成功登入 WorkSpace 之後，PCoIP 串流便會啟動。連線是由 TCP 4172 連接埠上的用戶端啟動，其傳回流量位於連接埠 UDP 4172 上。此外，透過管理介面，串流閘道與 WorkSpaces 桌上型電腦之間的初始連線是透過 UDP 55002。(請參閱 Amazon 的 IP 位址和連接埠需求文件 WorkSpaces。 初始輸出 UDP 連接埠是 55002。) 使用連接埠 4172 (TCP 和 UDP) 的串流連線會使用 AES 128 位元和 256 位元加密，但預設為 128 位元加密。客戶可以使用適用於視窗的 PCoIP 特定 AD 群組原則設定，或使用適用於 Amazon Linux 的 PCOIP 代理程式 .conf 檔案 WorkSpaces，將其主動變更為 256 位元。WorkSpaces如需 Amazon 群組原則管理的詳細資訊 WorkSpaces，請參閱文件。

網路介面

每個 Amazon 都 WorkSpace 有兩個網路界面，稱為主要網路界面和管理網路界面。

主要網路介面提供客戶 VPC 內部資源的連線能力，例如 AWS Directory Service、網際網路和客戶企業網路的存取。您可以將安全性群組附加至此主要網路介面。從概念上講，安全性群組會根據部署範圍 (安全性群組和 ENI WorkSpaces 安全性群組) 來區分連接到此 ENI。

管理網路介面

管理網路介面無法透過安全性群組控制；不過，客戶可以使用主機型防火牆 WorkSpaces 來封鎖連接埠或控制存取。我們不建議在管理網路介面上套用限制。如果客戶決定新增以主機為基礎的防火牆規則來管理此界面，則應開啟一些連接埠，以便 Amazon WorkSpaces 服務可以管理. WorkSpace 如需詳細資訊，請參閱《Amazon 工作區管理指南》中的網路界面。

WorkSpaces 安全性群組

系統會針對每個 AWS Directory Service 建立一個預設安全性群組，並自動附加至屬於 WorkSpaces 該特定目錄的所有安全性群組。

與許多其他 AWS 服務一樣，Amazon WorkSpaces 使用安全組。當您向 WorkSpaces 服務註冊目錄時，Amazon WorkSpaces 會建立兩個 AWS 安全群組。一個用於目錄控制器目錄控制器，另一個用於目錄目錄 _ 工作空 WorkSpaces 間成員。請勿刪除這些安全性群組中的任何一個，否則您 WorkSpaces 將會受到損害。根據預設，「 WorkSpaces 成員」安全性群組的出口開放時間為 0.0.0.0/0。您可以將預設 WorkSpaces安全性群組新增至目錄。將新的安全性群組與目錄產生關聯之後，您啟動 WorkSpaces 的新 WorkSpaces 目錄或重新建立的現 WorkSpaces 有安全性群組將會有新的安全性群組。您也可以將這個新的預設安全性群組新增至現有的安全性群組， WorkSpaces 而無需重建 將多個安全性群組與 WorkSpaces 目錄相關聯時，請將每個安全群組中的規則 WorkSpaces彙總為單一規則集。建議盡可能緊縮您的安全群組規則。如需有關安全群組的詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 安全群組。

如需將安全性群組新增至 WorkSpaces 目錄或現有目錄的詳細資訊 WorkSpace，請參閱WorkSpaces 管理指南。

有些客戶想要限制 WorkSpaces 流量可以輸出的連接埠和目的地。若要限制來自的輸出流量 WorkSpaces，您必須確定您保留服務通訊所需的特定連接埠；否則，您的使用者將無法登入其 WorkSpaces。

WorkSpaces 在 WorkSpace 登入期間，使用客戶 VPC 中的彈性網路介面 (ENI) 與網域控制站通訊。若要允許您的使用者 WorkSpaces 成功登入他們，您必須允許下列連接埠存取您的網域控制站，或包括 _WorkSpacesMembers 安全性群組中的網域控制站的 CIDR 範圍。

- TCP/UDP 53 - DNS

- TCP/UDP 88 - Kerberos 身分驗證
- 接口 389-LDAP
- TCP/UDP 445 - SMB
- TCP 3268-3269 - 通用類別
- 密碼變更
- TCP 139 - Netlogon
- UDP 137-138 - Netlogon
- UDP 123 - NTP
- 適用於 RPC 的暫時連接埠

如果您 WorkSpaces 需要存取其他應用程式、網際網路或其他位置，則必須在 _WorkSpacesMembers 安全性群組中以 CIDR 標記法允許這些連接埠和目的地。如果您未新增這些連接埠和目的地，WorkSpaces 將無法連接到上述連接埠以外的任何連接埠。根據預設，新的安全性群組沒有輸入規則的最後一個考量。因此，直到您將傳入規則新增到安全群組之前，來自其他主機的流量都無法傳入您的執行個體。只有在您想要限制輸出規則，或將輸入規則鎖定為只有應具有存取權的資源或 CIDR 範圍時，才需要執行上述步驟。 WorkSpaces

> **Note**
>
> 修改後，新關聯的安全性群組只會附加至 WorkSpaces 建立或重建。

ENI 安全性群組

由於主要網路介面是一般 ENI，因此可以使用不同的 AWS 管理工具進行管理。如需詳細資訊，請參閱彈性網路介面。導覽至 WorkSpace IP 位址 (在 Amazon WorkSpaces 主控台的 WorkSpaces 頁面中)，然後使用該 IP 位址做為篩選器來尋找對應的 ENI (在 Amazon EC2 主控台的「網路界面」區段中)。

一旦找到 ENI，就可以由安全群組直接管理。手動將安全群組指派給主要網路界面時，請考慮 Amazon 的連接埠需求 WorkSpaces。如需詳細資訊，請參閱《Amazon 工作區管理指南》中的網路界面。

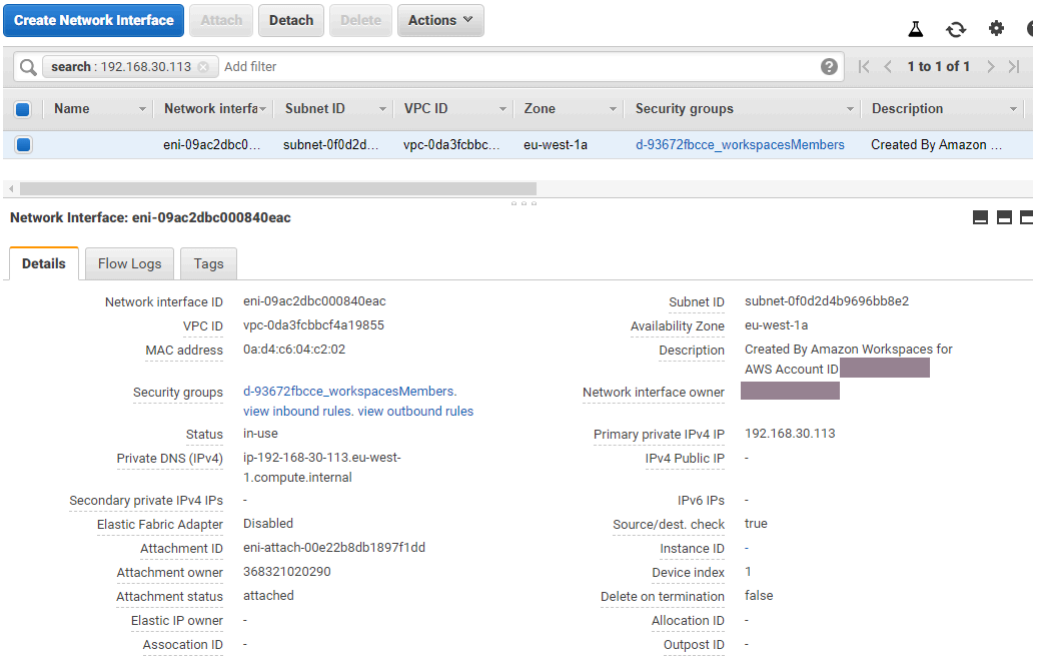

圖 21：已啟用 MFA 的 WorkSpaces 用戶端

網路存取控制清單 (ACL)

由於管理另一個防火牆的複雜性增加，因此網路 ACL 通常用於非常複雜的部署中，通常不會做為最佳作法。當網路 ACL 連接到 VPC 中的子網路時，將其功能集中在 OSI 模型的第 3 層 (網路)。由於 Amazon WorkSpaces 是在目錄服務上設計的，因此必須定義兩個子網路。網路 ACL 會與目錄服務分開管理，而且網路 ACL 很可能只指派給其中一個「指派的子網路 WorkSpaces」。

當需要無狀態防火牆時，網路 ACL 是安全性的最佳作法。確保在每個子網路基礎上驗證超出預設設定的網路 ACL 所做的任何變更，這是最佳作法。如果網路 ACL 未如預期般執行，請考慮使用 VPC 流量記錄檔來分析流量。

AWS Network Firewall

AWS Network Firewall 提供的功能超越原生安全群組和網路 ACL 提供的功能，但需要付費。當客戶要求能夠提高網路連線的安全性時，例如 HTTP 網站的伺服器名稱檢查 (SNI)、入侵偵測和防範，以及網域名稱的允許和拒絕清單時，他們便可在網站上找到替代防火牆。 AWS Marketplace部署這些防火牆的複雜性面臨的挑戰，超越標準 EUC 系統管理員所熟練的挑戰。 AWS Network Firewall 提供原生 AWS 體驗，同時啟用第 3 層到第 7 層保護。如果組織不具備任何其他方法 (可傳輸至雲端的第三方防火牆的現有內部部署授權，或排除管理防火牆的個別團隊) 以涵蓋所有 EUC 網路保護，則搭配 NAT 閘道使 AWS 用 Network Firewall 是最佳作法。NAT 閘道也是免費的 AWS Network Firewall。

AWS Network Firewall 的部署是圍繞現有 EUC 設計而設計的。單一虛擬私人雲端設計可實現簡化的架構，其中包含防火牆端點的子網路，以及個別的網際網路輸出路由考量，而多個 VPC 設計則可受益於具有防火牆和 Transit Gateway 端點的整合式檢測 VPC。

設計方案

案例 1：基本執行個體鎖定

預設的「 WorkSpaces 安全群組」不允許任何流量輸入，因為安全群組預設為拒絕且可設定狀態。這表示不需要設定額外的設定來進一步保護 WorkSpaces 執行個體本身的安全。考慮允許所有流量的出站規則，以及是否適合用例。例如，最好將連接埠 443 的所有輸出流量拒絕到任何位址，以及符合連接埠使用案例的特定 IP 範圍，例如 LDAP 389、LDAPS 636、SMB 445 等；雖然請注意環境的複雜性可能需要多個規則，因此可以透過網路 ACL 或防火牆裝置提供更好的服務。

案例 2：輸入例外

雖然這不是一個恆定的要求，但有時可能會啟動網絡流量輸入到 WorkSpaces. 例如，在 WorkSpaces 用戶端無法連線時分類執行個體需要替代的遠端連線。在這些情況下，最好是暫時向客戶 ENI 的安全性群組啟用輸入 TCP 3389。 WorkSpace

另一個案例是由集中式執行個體起始的清查或自動化功能執行命令的組織指令碼。您可以永久設定來自輸入特定集中式執行個體的該連接埠上的流量，但最佳做法是在連接至目錄組態的其他安全性群組上執行此作業，因為它可套用至 AWS 帳戶中的多個部署。

最後，有些網路流量並非以狀態為基礎，而且需要在輸入例外狀況中指定暫時連接埠。如果查詢和指令碼失敗，最佳作法是在判斷連線失敗的根本原因時，至少暫時允許暫時連接埠。

情境 3：單次 VPC 檢測

簡化的部署 WorkSpaces (例如沒有擴展計劃的單一 VPC) 不需要單獨的 VPC 進行檢查，因此可以透過 VPC 對等互連來簡化與其他 VPC 的連線。不過，對於防火牆端點而言，必須建立個別的子網路，並使用設定至這些端點的路由，以及網際網路閘道 (IGW) 輸出路由，否則不需要設定。如果所有子網路都使用整個 VPC CIDR 區塊，則現有部署可能沒有可用的 IP 空間。在這些情況下，案例 4 可能會提供更好的效果，因為部署已經超出其初始設計的擴展。

案例 4：集中檢查

通常在一個 AWS 區域中的多個 EUC 部署中優先使用，以簡化 AWS 網路防火牆的可設定狀態和無狀態規則的管理。由於此設計需要使用 Transit Gateway 附件，以及只能透過這些附件設定的檢查路由，

因此現有的 VPC 對等方式將會取代為 Transit Gateway。此組態也會行使更大程度的控制，並提供超越預設 WorkSpaces 體驗的安全性。

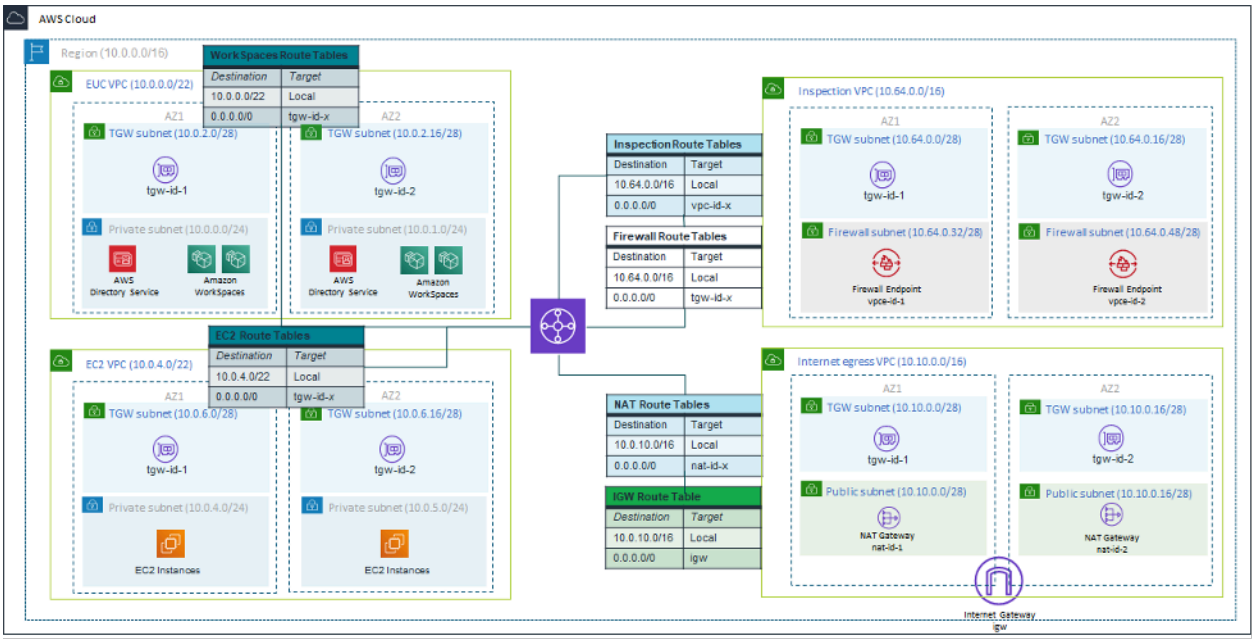

圖 22：使用 Transit Gateway 附件的範例架構

加密 WorkSpaces

每個 Amazon WorkSpace 都佈建了一個根磁碟區 (C: 磁碟機適用於 Windows WorkSpaces，Amazon Linux 的根目錄 WorkSpaces) 和一個使用者磁碟區 (D: 磁碟機適用於視窗 WorkSpaces，/home 用於 Amazon Linux WorkSpaces)。加密 WorkSpaces 功能可以加密一個或兩個磁碟區。

會加密哪些資料？

儲存在靜態的資料、磁碟輸入/輸出 (I/O) 到磁碟區，以及從加密磁碟區建立的快照都會加密。

何時會發生加密？

啟動 (建立) 時， WorkSpace 應指定 a 的加密 WorkSpace。 WorkSpaces 磁碟區只能在啟動時加密：啟動後，無法變更磁碟區加密狀態。下圖顯示了 Amazon 主 WorkSpaces 控台頁面，用於在新的啟動期間選擇加密 WorkSpace。

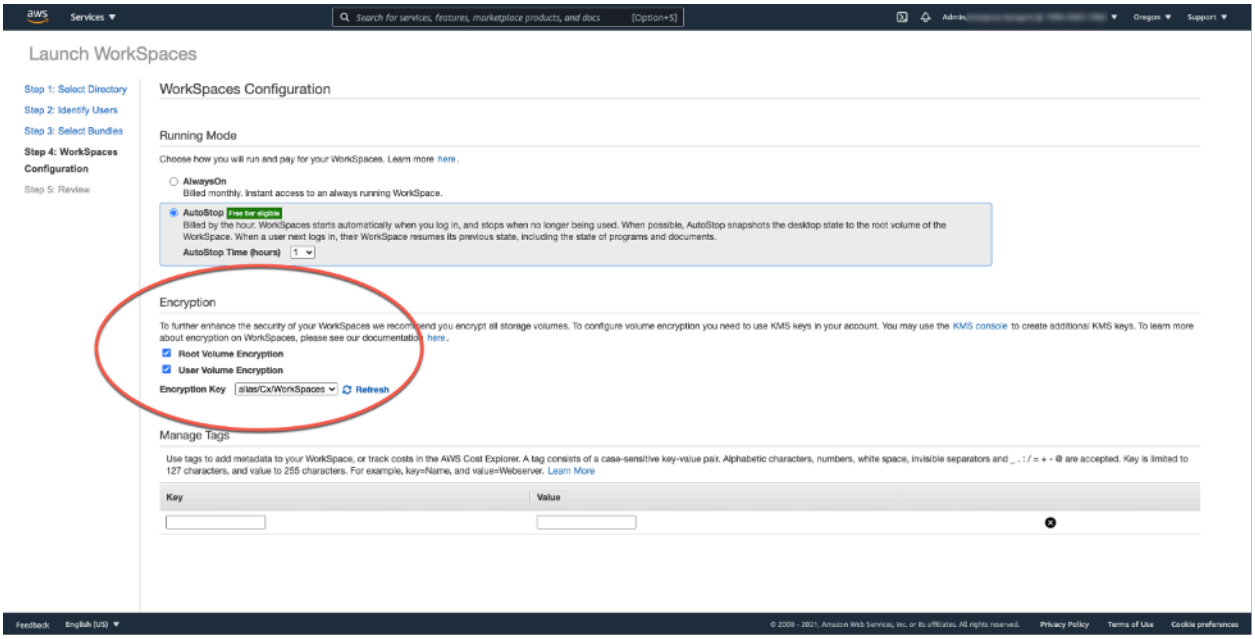

圖 23：加密 WorkSpace 根磁碟區

新的 WorkSpace 加密方式如何？

客戶可以從 Amazon WorkSpaces 主控台 WorkSpaces 選擇「加密」選項 AWS CLI，或者在客戶啟動新功能時使用 Amazon WorkSpaces API 來選擇「加密」選項 WorkSpace。

為了加密卷，Amazon WorkSpaces 使用 CMK 從 AWS Key Management Service （ AWS KMS ）。第一次在「區域」中啟動時，會建立預設 AWS KMS CMK。 WorkSpace （ CMK 有一個區域範圍。 ）

客戶也可以建立由客戶管理的 CMK，以便搭配加密使用。 WorkSpacesCMK 用於加密 Amazon WorkSpaces 服務用來加密每個 WorkSpace 磁碟區的資料金鑰。（從嚴格意義上說，將加密卷的是 Amazon EBS ）。如需目前的 CMK 限制，請參閱AWS KMS 資源配額。

> **Note**
>
> 不支援從加密 WorkSpace 建立自訂映像檔。此外，在 WorkSpaces啟用根磁碟區加密的情況下啟動，最多可能需要一個小時才能佈建。

如需 WorkSpaces 加密程序的詳細說明，請參閱 Amazon 如何 WorkSpaces 使用 AWS KMS。考慮如何監控 CMK 的使用情況，以確保正確服務加密 WorkSpace 的請求。如需有關 AWS KMS 金鑰和資料金鑰的其他資訊，請參閱AWS KMS 頁面。

存取控制選項和受信任的裝置

Amazon 為客戶 WorkSpaces 提供管理可存取哪些用戶端裝置的選項 WorkSpaces。客戶只能限 WorkSpaces 制對受信任裝置的存取。 WorkSpaces 可以使用數字證書從 macOS 和 Microsoft 視窗 PC 訪問。它還可以允許或阻止訪問 iOS，安卓，Chrome 操作系統，Linux 和零客戶端，以及 WorkSpaces Web 訪問客戶端。有了這些功能，它可以進一步改善安全狀態。

新部署已啟用存取控制選項，讓使用者可 WorkSpaces 從 Windows、MacOS、iOS、安卓、ChromeOS 和零用戶端上的用戶端存取他們的使用者。對於新 WorkSpaces 部署，預設不會啟用使用 Web 存取或 Linux 用 WorkSpaces 戶端的存取，因此需要啟用。

如果從受信任的裝置 (也稱為受管理裝置) 存取公司資料有限制，則可以將 WorkSpaces 存取限制在具有有效憑證的受信任裝置。啟用此功能後，Amazon WorkSpaces 會使用憑證型身份驗證來判斷裝置是否受信任。如果用 WorkSpaces 戶端應用程式無法驗證裝置是否受信任，則會封鎖嘗試登入或從裝置重新連線。

受信任的裝置支援適用於下列用戶端：

- 在谷歌播放 Amazon WorkSpaces Android 客戶端應用程序，在 Android 和 Android 兼容的 Chrome 操作系統設備上運行
- 在 WorkSpaces macOS 設備上運行的 Amazon macOS 客戶端
- 在 WorkSpaces 視窗設備上運行的 Amazon 視窗客戶端

如需控制可存取哪些裝置的詳細資訊 WorkSpaces，請參閱限制對受信任裝置的 WorkSpaces 存取。

> **Note**
>
> 受信任裝置的憑證僅適用於 Amazon WorkSpaces 視窗、macOS 和安卓用戶端。此功能不適用於 Amazon WorkSpaces 網路存取用戶端或任何第三方用戶端，包括但不限於 Terdici PCoIP 軟體和行動用戶端、Terdici PCoIP 零用戶端、RDP 用戶端和遠端桌面應用程式。

IP 存取控制群組

使用以 IP 位址為基礎的控制群組，客戶可以定義和管理受信任 IP 位址的群組，並允許使用者 WorkSpaces 只有在連線到受信任的網路時才能存取。此功能可協助客戶更好地控制其安全狀態。

您可以在 WorkSpaces 目錄層級新增 IP 存取控制群組。有兩種方法可以開始使用 IP 存取控制群組。

- IP 存取控制頁面 — 您可以從 WorkSpaces 管理主控台在 IP 存取控制頁面上建立 IP 存取控制群組。您可以輸入可存取的 IP 位址或 IP 範圍，將規則新增至這些群組。 WorkSpaces 然後可以將這些群組新增至 [更新詳細資料] 頁面上的目錄中。
- 工作區 API — WorkSpaces API 可用於建立、刪除和檢視群組；建立或刪除存取規則；或從目錄新增和移除群組。

如需將 IP 存取控制群組與 Amazon WorkSpaces 加密程序搭配使用的詳細說明，請參閱[您的 IP 存取控制群組 WorkSpaces]。

使用 Amazon 監控或記錄 CloudWatch

監控網路、伺服器和記錄檔是任何基礎結構不可或缺的一部分。部署 Amazon 的客戶 WorkSpaces 需要監控其部署，特別是個人的整體健康狀態和連線狀態 WorkSpaces。

Amazon CloudWatch 指標 WorkSpaces

CloudWatch 的指標旨在 WorkSpaces 為管理員提供更多有關個人整體健全狀況和連線狀態的深入資訊 WorkSpaces。指標可以針對指定目錄中組織 WorkSpaces 中的所有人使用 WorkSpace，或彙總量度。

與所有指標一樣，這些 CloudWatch 指標可在 AWS Management Console (如下圖所示) 檢視、透過 CloudWatch API 存取，並由 CloudWatch 警示和協力廠商工具進行監控。

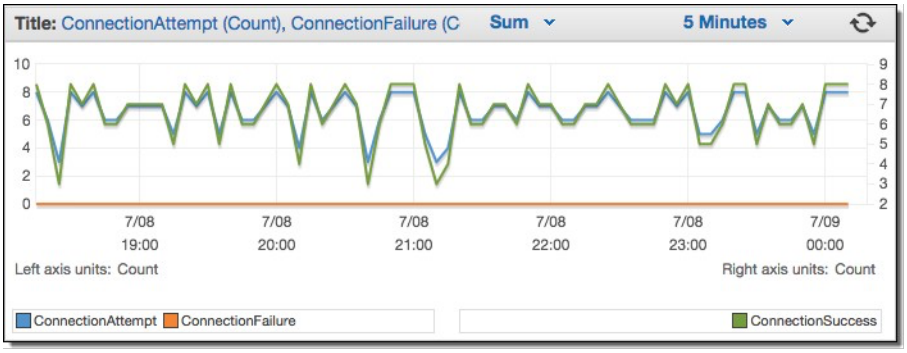

圖 24： CloudWatch 量度： ConnectionAttempt / ConnectionFailure

依預設，會啟用下列量度，且無需額外費用即可使用：

- 可用 — 回 WorkSpaces應狀態檢查的會計入此測量結果中。
- 不健康 — WorkSpaces 不回應相同狀態檢查的情況會計入此量度中。

- ConnectionAttempt— 對 a 進行的連線嘗試次數 WorkSpace。
- ConnectionSuccess— 成功嘗試連線的次數。
- ConnectionFailure— 失敗的連線嘗試次數。
- SessionLaunchTime— 用 WorkSpaces 戶端所測量的啟動工作階段所花費的時間。
- InSessionLatency— WorkSpaces 客戶端和客戶之間的往返時間 WorkSpaces，由客戶測量和報告。
- SessionDisconnect— 使用者啟動和自動關閉的工作階段數目。

此外，也可以建立警報，如下圖所示。

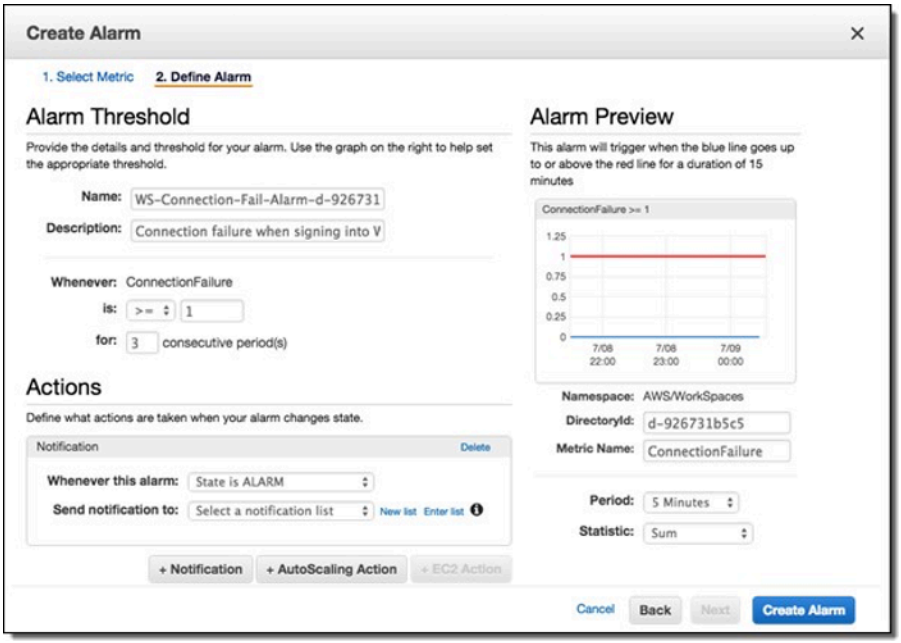

圖 25：為 WorkSpaces 連接錯誤創建 CloudWatch 警報

Amazon CloudWatch 活動 WorkSpaces

Amazon Events 的 CloudWatch 事件可用於檢視、搜尋、下載、封存、分析和回應成功登入 WorkSpaces。此服務可以監控用戶端 WAN IP 位址、作業系統、 WorkSpaces ID 和目錄識別碼資訊，以供使用者登入 WorkSpaces。例如，它可以將事件用於以下目的：

- 將 WorkSpaces 登入事件儲存或封存為記錄檔以供日 future 參考、分析記錄檔以尋找病毒碼，並根據這些病毒碼採取處理行動。
- 使用 WAN IP 位址判斷使用者從何處登入，然後使用原則讓使用者只能存取符合「事件」類型「存取 WorkSpaces 」(CloudWatch Event) 類型存取準則的檔案或資料。WorkSpaces

- 使用政策控制來封鎖來自未經授權的 IP 位址對檔案和應用程式的存取。

如需有關如何使用 CloudWatch 事件的詳細資訊，請參閱 Amazon CloudWatch 事件使用者指南。若要進一步了解的 CloudWatch 事件 WorkSpaces，請參閱 WorkSpaces 使用 Cloudwatch 事件監控您的事件。

YubiKey 支持 Amazon WorkSpaces

為了增加額外的安全層，客戶通常會選擇使用多重要素驗證來保護工具和網站的安全性。有些顧客選擇使用 Yubic YubiKey o 這樣做。Amazon 同時 WorkSpaces 支持一次性密碼（OTP）和 FIDO U2F 身份驗證協議。 YubiKeys

Amazon WorkSpaces 目前支援 OTP 模式，管理員或最終使用者不需要其他步驟即可使 YubiKey 用 OTP。用戶可以將其連接 YubiKey 到他們的計算機上，確保鍵盤集中在 WorkSpace （特別是在需要輸入 OTP 的字段中），並觸摸上的金色觸點YubiKey。 YubiKey 將自動輸入 OTP 到選定的字段中。

為了使用 FIDO U2F 模式與 YubiKey 和 WorkSpaces，需要額外的步驟。確保您的使用者獲得下列其中一種支援的 YubiKey 模型，以便透 WorkSpaces過下列方式使用 U2F 重新導向：

- YubiKey 4
- YubiKey 5 近場通訊
- YubiKey 5 納米
- YubiKey 5C
- YubiKey 5C 納米
- YubiKey 5 近場通訊

若要啟用 YubiKey U2F 的 USB 重新導向

PCoIP 的 USB 重新導向預設為停用 WorkSpaces；若要搭配使用 U2F 模式 YubiKeys，您必須啟用它。

1. 請確定您已為 PCoIP (32 位元) 安裝最新的WorkSpaces群組原則系統管理範本，或是 PCoIP (64 位元) 的WorkSpaces群組原則系統管理範本。
2. 在加入目錄的目 WorkSpaces 錄管理 WorkSpace 或 Amazon EC2 執行個體上，開啟群組原則管理工具 (gpmc.msc)，然後瀏覽至 P CoIP 工作階段變數。
3. 若要允許使用者覆寫您的設定，請選擇可重新定義的管理員預設值。否則，請選擇「不可覆寫的管理員預設值」。

4. 開啟在 PCOIP 工作階段中啟用/停用 USB 設定。
5. 選擇啟用，然後選擇確定。
6. 開啟設定 PCoIP USB 允許和不允許的裝置規則設定。
7. 選擇啟用，然後在輸入 USB 授權表格 (最多十個規則) 之下，設定您的 USB 裝置允許清單規則。
   a. 授權規則 - 110500407。此值是廠商 ID (VID) 與產品 ID (PID) 的組合。VID/PID 組合的格式為`1xxxxyyyy`，其`xxxx`中是十六進位格式的 VID，而且`yyyy`是十六進位格式的 PID。在這個範例中，1050 是 VID，而 0407 是 PID。如需更多 YubiKey USB 值，請參閱 YubiKeyUSB 識別碼值。
8. 在 [輸入 USB 授權表格 (最多十個規則)] 下，設定您的 USB 裝置封鎖清單規則。
   a. 針對取消授權規則，設定空字串。這表示只允許授權清單中的 USB 裝置。

> **Note**
>
> 您最多可以定義 10 個 USB 授權規則和最多 10 個 USB 取消授權規則。使用垂直列 (|) 字元來分隔多個規則。如需有關授權/取消授權規則的詳細資訊，請參閱適用於 Windows 的 PCoIP 標準代理程式

9. 選擇 確定。
10. 群組原則設定變更會在下一次群組原則更新之後以 WorkSpace 及 WorkSpace 工作階段重新啟動之後生效。若要套用群組政策變更，請執行下列其中一項：
    a. 重新啟動 WorkSpace （在 Amazon WorkSpaces 控制台中，選擇 WorkSpace，然後選擇操作，重新啟動 WorkSpaces）。
    b. 在系統管理命令提示字元中，輸入強制。
11. 設定生效後，除非透過 USB 裝置規則設定設定限制， WorkSpaces 否則所有支援的 USB 裝置都可以重新導向至。

啟用 YubiKey U2F 的 USB 重定向後，您可以使用您的 YubiKey Fido U2F 模式。

成本最佳化

自助 WorkSpace 管理功能

在 Amazon 中 WorkSpaces，可以為使用者啟用自助 WorkSpace 管理功能，讓他們能夠更好地控制自己的體驗。允許使用者自助服務功能可以減少 Amazon 的 IT 支援人員工作量 WorkSpaces。啟用自助服務功能後，使用者可以直接從 Amazon 的 Windows、macOS 或 Linux 用戶端執行下列一或多項任務 WorkSpaces：

- 在他們的客戶端上快取其憑證。這可讓使用者重新連線至他們， WorkSpace 而無需重新輸入其認證。
- 重新啟動他們 WorkSpace。
- 增加其上的根磁碟區和使用者磁碟區的大小 WorkSpace。
- 變更其運算類型 (套件) WorkSpace。
- 切換它們的運行模式 WorkSpace。
- 重建他們的 WorkSpace.

允許使用者使用其的 [重新啟動] 和 [重建] 選項，沒有持續的成本影響 WorkSpaces。使用者應該注意，他們的重建 WorkSpace 會導 WorkSpace致他們在一個小時內無法使用，因為重建程序會發生。

增加磁碟區大小、變更運算類型以及切換執行模式的選項可能會產生額外費用 WorkSpaces。最佳做法是啟用自助服務，以減少支援團隊的工作負載。在工作流程處理中，應允許額外成本項目的自助服務，以確保已獲得額外費用的授權。這可以通過專用的自助服務門戶進行 WorkSpaces，或通過與現有的信息技術服務管理（ITSM）服務集成，例如ServiceNow。

如需詳細資訊，請參閱啟用使用者的自助式 WorkSpace 管理功能。如需為使用者自助服務啟用結構化入口網站的範例，請參閱使 WorkSpaces 用自助入口網站自動化 Amazon。

Amazon WorkSpaces 成本優化

Amazon 成 WorkSpaces 本優化器解決方案會分析您所有的 Amazon WorkSpaces 用量資料。根據您的使用情況，它會自動轉換 WorkSpace 為最具成本效益的計費選項（每小時或每月）。此解決方案可協助您監控使 WorkSpace 用情況並最佳化成本，並使用 AWS CloudFormation 自動佈建和設定必要的 AWS 服務，以便每 24 小時分析使用量並轉換個別服務 WorkSpaces。最新版本 2.4 為客戶提供了在現有 VPC 中部署解決方案的靈活性，並為區域和終止配置可選項。此外，還改善了計費小時計算的準確性， WorkSpaces 並增強了報告中繼資料。如果您之前已部署此解決方案的舊版 (v2.2.1 或更低版

本)，請依照更新堆疊文件更新 Amazon WorkSpaces Cost Optimizer CloudFormation 堆疊，以取得解決方案架構的最新版本。

的執行模式會 WorkSpace 決定其立即可用性和計費。以下是當前正在運行的 WorkSpaces 運行模式：

AlwaysOn— 支付固定的月費無限使用時使用 WorkSpaces. 此模式最適合使用其 WorkSpace 作為主要桌面並且始終需要立即存取正 WorkSpace 在執行的桌面的使用者。

AutoStop— 按小時付 WorkSpaces 款時使用。使用此模式時，請在指定的閒置時間後 WorkSpaces 停止，並儲存應用程式和資料的狀態。若要設定自動停止時間，請使用 AutoStop 時間 (小時)。這種模式是最好的誰只需要兼職訪問他們的用戶 WorkSpaces.

最佳做法是監控使用情況，並使用 Amazon WorkSpaces 成本優化器等解決方案將 Amazon 的運行模式設置為最具 WorkSpaces 成本效益的模式。此解決方案會部署 Amazon CloudWatch 事件規則，該規則每 24 小時叫用一個AWS Lambda函數。

該解決方案可以在達到閾值後的任何一天將個人 WorkSpaces 從小時計費模式轉換為每月計費模式。如果解決方案將每小時計費轉換為每月計費，則該解決方案在下個 WorkSpace 月開始之前不會將計費轉換 WorkSpace 回小時計費，且僅在使用量低於閾值時才會轉換回小時計費。不過，帳單模式可以隨時使用 AWS Management Console 或 Amazon WorkSpaces API 手動變更。解決方案的 AWS CloudFormation 範本包含可執行這些轉換的參數，並允許以乾式執行模式執行解決方案，以提供建議的報告。

選擇退出標籤

若要防止解決方案在計費模型 WorkSpace 之間轉換，請 WorkSpace 使用標籤鍵 Skip_Convert 和任何標籤值將資源標籤套用至。此解決方案將記錄標記 WorkSpaces，但不會轉換標記 WorkSpaces。您可以隨時移除標籤，以繼續自動轉換 WorkSpace。如需詳細資訊，請參閱 Amazon WorkSpaces 成本最佳化器。

選擇在地區

根據預設，此解決方案會掃描同一 AWS 帳戶 WorkSpaces 中在 Amazon WorkSpaces 註冊的目錄，以監控所有可用 AWS 區域。您可以在「AWS 地區清單」輸入參數中提供您要監視的 AWS 區域 (以逗號分隔) 清單，以限制要監視的區域。

在現有 VPC 中部署

此解決方案需要 VPC 才能執行 ECS 工作。依預設，解決方案會建立新的 VPC，但您可以在現有的 VPC 中部署，方法是提供子網路 ID 和安全群組識別碼做為輸入參數的一部分。您目前的子網路具有通往網際網路的 ECS 任務的路由，以提取公用 Amazon ECR 儲存庫中託管的 Docker 映像檔。

未使用的終止 WorkSpaces

此解決方案允許您 WorkSpaces 在滿足所有條件的當月的最後一天終止未使用的狀態。您可以透過將TerminateUnusedWorkSpaces輸入參數變更為 CloudFormation 樣板來選擇加入此功能。最佳做法是在乾運行模式下運行此功能幾個月，然後檢查每月報告以查看 WorkSpaces 標記為終止。

Amazon Amazon Connect 優化 WorkSpaces

客服中心專員的最終使用者體驗必須是首要任務，因為如果他們的音訊降級，它會為他們所服務的客戶帶來不良的通話體驗。在遠端桌面平台中執行客服中心解決方案時，當語音流量沒有優先於網路連線時，音訊效能會在某些可測量的規模上受到影響。此影響是因為音訊從音訊端點流至虛擬工作階段，然後透過串流通訊協定進行壓縮，以傳送給使用者。這種額外的路由會導致音訊因網路瓶頸而降低效能。

避免這種行為的一種方法是將音頻分割出會話，這意味著當音頻流保持在會話之外時，所有聯繫中心代理的資源都保持在會話中。此分割可讓音訊從音訊端點直接串流至使用者，而所有其他呼叫資源 (包括代理程式正在檢視的 PII) 仍保留在安全的工作階段中。這種音頻優化被認為是最佳實踐，因為它可以確保客戶的通話體驗盡可能好。

Amazon Connect 提供串流 API，可讓管理員自訂其聯絡人控制面板 (CCP) 以符合其業務需求。管理員擁有的其中一個選項是控制自訂 CCP 是否可以接收通話的音訊。這些設定可讓我們設定分割的 CCP；在工作階段外使用的純音訊 CCP，以及在工作階段中使用無媒體的 CCP。管理員設定了這些自訂 CCP 之後，就可以利用 Amazon Connect 音訊最佳 WorkSpaces化。由於 CCP 是在瀏覽器內傳遞的，因此此設定可讓系統管理員將其僅限音訊的 CCP URL 提供給目錄。 WorkSpaces設定完成後，當 WorkSpaces Connect 聯絡中心代理程式成功驗證給他們時 WorkSpaces， WorkSpaces 用戶端會自動在代理程式的本機預設瀏覽器中開啟提供的純音訊 CCP URL。此動作可讓音訊直接流向代理程式的本機電腦，而無媒體 CCP 則會處理安全工作階段中的其他所有項目。 WorkSpaces

架構圖

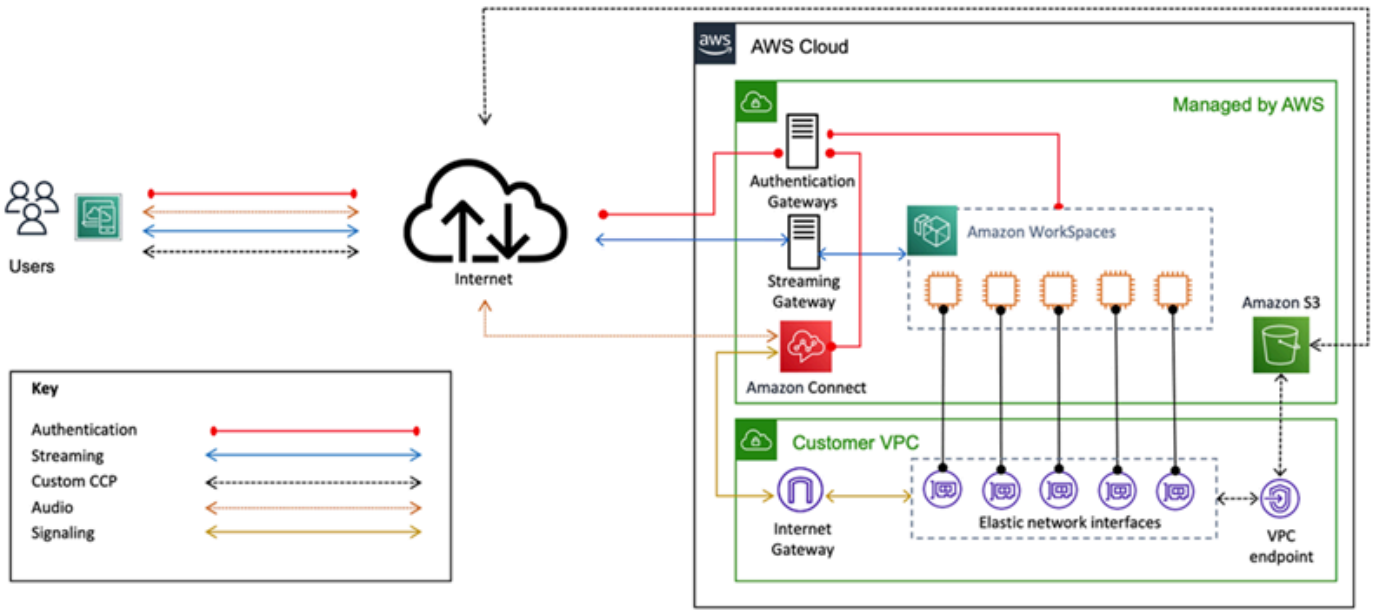

圖 26 — Amazon Connect 和 WorkSpaces 架構圖

疑難排解

您可以在 Amazon WorkSpaces 管理指南的「用戶端和管理員疑難排解」頁面上找到常見的管理和用戶端問題，例如您的裝置無法連線到 WorkSpaces 註冊服務或無法連線到 WorkSpace 具有互動式登入橫幅的錯誤訊息。

主題

- AD Connector 無法連接到活動目錄
- 疑難排解 WorkSpace 自訂映像檔建立錯誤
- 疑難排解 WorkSpace 標示為狀況不良的 Windows
- 收集用於偵錯的 WorkSpaces 支援記錄檔服務包
- 如何檢查到最近 AWS 地區的延遲

AD Connector 無法連接到活動目錄

若要讓 AD Connector 連接到內部部署目錄，內部部署網路的防火牆必須對 VPC 中兩個子網路的 CIDR 開放特定連接埠。請參閱案例 1：使用 AD Connector 對內部部署 Active Directory Service 進行代理驗證。若要測試是否符合這些條件，請執行下列步驟。

若要測試連線：

1. 在 VPC 中啟動 Windows 執行個體，並透過 RDP 與其連線。其餘步驟會在 VPC 執行個體上執行。
2. 下載並解壓縮DirectoryServicePortTest測試應用程式。源代碼和 Microsoft Visual Studio 項目文件包括修改測試應用程序，如果需要的話。
3. 從 Windows 命令提示字元中，使用下列選項執行 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>— 完全合格的域名，用於測試樹系和域功能級別。如果域名被排除，則不會測試功能級別。

< 伺服器 IP 位址 > — 內部部署網域中網域控制站的 IP 位址。連接埠會根據此 IP 位址進行測試。如果排除 IP 位址，則不會測試連接埠。

此測試會判斷是否要從 VPC 開啟至網域的必要連接埠。測試應用程式也會驗證最低樹系和網域功能層級。

疑難排解 WorkSpace 自訂映像檔建立錯誤

如果 Windows 或 Amazon Linux WorkSpace 已經啟動並進行了自定義，則可以從中創建自定義映像 WorkSpace。自訂映像包含的作業系統、應用程式軟體和設定 WorkSpace。

檢閱需求以建立視窗自訂映像檔，或檢閱建立 Amazon Linux 自訂映像檔的需求。建立映像檔需要符合所有必要條件，才能開始建立映像。

若要確認 Windows WorkSpace 符合建立映像檔的需求，建議您執行影像檢查程式。Image Checker 會針對建立映像的 WorkSpace 時間執行一系列測試，並提供如何解決找到的任何問題的指導。如需詳細資訊，請參閱安裝和設定影像檢查程式。

WorkSpace 通過所有測試後，會出現「驗證成功」消息。您現在可以建立自訂套裝軟體。否則，請解決導致測試失敗和警告的任何問題，並重複執行 Image Checker 的程序，直到 WorkSpace 通過所有測試為止。必須先解決所有失敗和警告，才能建立影像。

如需詳細資訊，請遵循解決影像檢查程式偵測到的問題的提示。

疑難排解 WorkSpace 標示為狀況不良的 Windows

Amazon WorkSpaces 服務會 WorkSpace 透過傳送狀態請求來定期檢查 a 的運作狀態。如果未及時收到來自的回應， WorkSpace 就會標示為「 WorkSpace 不健康」。這個問題的常見原因是：

- 上的應用程式 WorkSpace 正在阻止 Amazon WorkSpaces 服務和 WorkSpace.
- 上的 CPU 使用率很高 WorkSpace。
- 的電腦名稱 WorkSpace 已變更。
- 回應 Amazon 服務的代理程式或 WorkSpaces 服務未處於執行中狀態。

下列疑難排解步驟可能會恢復 WorkSpace 到健全狀態：

- 首先， WorkSpace從 Amazon WorkSpaces 控制台重新啟動。如果重新啟動 WorkSpace 無法解決問題，請使用 RDP，或 WorkSpace 使用 SSH 連接到 Amazon Linux。
- 如果不同的 WorkSpace 通訊協定無法存取，請 WorkSpace從 Amazon WorkSpaces 主控台重建。
- 如果無法建立 WorkSpaces 連線，請確認下列事項：

驗證 CPU 使用率

使用 [開啟工作管理員] 判斷 CPU 使用率 WorkSpace 是否高。如果是，請嘗試下列任一疑難排解步驟來解決問題：

1. 停止任何耗用大量 CPU 的服務。
2. 將大小調整 WorkSpace 為大於目前使用的運算類型。
3. 重新啟動 WorkSpace.

> **Note**
>
> 若要診斷高 CPU 使用率，以及如果上述步驟無法解決 CPU 使用率過高的問題，請參閱如何在 CPU 未限制時診斷 EC2 Windows 執行個體上的 CPU 使用率過高？

驗證的電腦名稱 WorkSpace

如果工作區的電腦名稱已變更，請將其變更回原始名稱：

1. 打開 Amazon WorkSpaces 控制台，然後展開不健康 WorkSpace 以顯示詳細信息。
2. 複製電腦名稱。
3. Connect 到使 WorkSpace 用 RDP。
4. 開啟命令提示字元，然後輸入 hostname 以檢視目前的電腦名稱。
   a. 如果名稱與步驟 2 中的「電腦名稱」相符，請跳至下一個疑難排解區段。
   b. 如果名稱不相符，請輸入 sysdm.cpl 以開啟系統內容，然後依照本節中的其餘步驟執行。
5. 選擇 [變更]，然後貼上步驟 2 中的 [電腦名稱]。
6. 出現提示時，請輸入網域使用者認證。
7. 確認處SkyLightWorkspaceConfigService於執行中狀態
   a. 在服務中，確認 WorkSpace服務處SkyLightWorkspaceConfigService於執行中狀態。如果不是，請啟動服務。

驗證防火牆規則

確認 Windows 防火牆和正在執行的任何協力廠商防火牆具有允許下列連接埠的規則：

- 連接埠 4172 上的輸入 TCP：建立串流連線。
- 連接埠 4172 上的輸入 UDP：串流使用者輸入。
- 連接埠 8200 上的輸入 TCP：管理和設定 WorkSpace.
- 連接埠 55002 上的輸出 UDP：PCoIP 串流。

如果防火牆使用無狀態篩選，請開啟暫時連接埠 49152-65535 以允許回傳通訊。

如果防火牆使用可設定狀態篩選，則暫時連接埠 55002 已開啟。

收集用於偵錯的 WorkSpaces 支援記錄檔服務包

疑難排解 WorkSpaces 問題時，必須從受影響的記錄檔服務包以 WorkSpace 及安裝 WorkSpaces 用戶端的主機收集記錄服務包。記錄檔有兩種基本類別：

- 伺服器端記錄檔：在這個案例中 WorkSpace 是伺服器，因此這些是存在於 WorkSpace 本身的記錄檔。
- 用戶端記錄檔：記錄使用者用來連線到 WorkSpace.

- 只有 Windows 和 macOS 用戶端會在本機寫入記錄檔。
- 零用戶端和 iOS 用戶端不會記錄。
- Android 日誌在本地存儲上進行加密，並自動上傳到 WorkSpaces 客戶端工程團隊。只有該團隊可以查看 Android 設備的日誌。

WSP 伺服器端記錄檔

所有 WSP 元件都會將其記錄檔寫入兩個資料夾中的其中一個：

- 主要位置：`C:\ProgramData\Amazon\WSP\`和 `C:\ProgramData\NICE\dcv\log\`
- 封存位置：`C:\ProgramData\Amazon\WSP\TRANSMITTED\`

變更視窗上的記錄檔詳細程度

您可以設定記錄詳細程度層級群組原則設定，以大規模設定 WSP Windows WorkSpaces 的記錄檔詳細程度層級。

若要變更個人的記錄檔詳細程度 WorkSpaces，請使用 Windows 登錄編輯程式設定機h_log_verbosity_options碼：

1. 以管理員身分開啟 Windows 登錄編輯程式。
2. 導覽至 \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon。
3. 如果WSP金鑰不存在，請按一下滑鼠右鍵，然後選擇「新增」>「機碼」並命名WSP。
4. 導覽至 \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP。
5. 如果該h_log_verbosity_options值不存在，請按一下滑鼠右鍵，然後選擇「新增」> DWORD 並將其h_log_verbosity_options命名。
6. 按一下新 h_log_verbosity_options DWORD，然後根據所需的詳細程度等級，將「值」變更為下列其中一個數字：
   - 0 — 錯誤
   - 1 — 警告
   - 。2-信息。
   - 3 — 除錯
7. 選擇 OK (確定) 並關閉 Windows 登錄編輯程式。
8. 重新啟動 WorkSpace.

PCoIP 伺服器端記錄檔

所有 PCoIP 元件都會將其記錄檔案寫入下列其中一個資料夾：

- 主要位置：C:\ProgramData\Teradici\PCoIPAgent\logs
- 封存位置：C:\ProgramData\Teradici\logs

有時候， AWS Support 在處理複雜問題時，必須將 PCoIP Server 代理程式置於詳細記錄模式。若要啟用此功能：

1. 開啟下列登錄機碼：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP \pcoip_admin_defaults
2. 在pcoip_admin_defaults索引鍵中，建立下列 32 位元 DWORD：pcoip.event_filter_mode
3. 將的值設定pcoip.event_filter_mode為「3」(十二月或十六進位)。

作為參考，這些是可以在此 DWORD 中定義的日誌閾值。

- 0 — (重要)
- 1 — (錯誤)
- 2 — (資訊)
- 3 — (除錯)

如果 `pcoip_admin_default` DWORD 不存在，則預設為2記錄層級。建議在 DWORD 不再需要詳細記錄檔之後，將值還原2至 DWORD，因為它們會大得多，而且會不必要地消耗磁碟空間。

WebAccess 伺服器端記

對於 PCoIP 和 WSP（ 1.0 以上版本） WorkSpaces， WorkSpaces 網頁存取用戶端會使用 STXHD 服務。 WorkSpaces Web 存取的記錄會儲存在`C:\ProgramData\Amazon\Stxhd\Logs`。

對於 WSP (2.0 版以上) WorkSpaces， WorkSpaces 網頁存取的記錄會儲存在。`C:\ProgramData\Amazon\WSP\`

用戶端記錄

這些記錄檔來自使用者連線的用 WorkSpaces 戶端，因此記錄檔位於使用者的電腦上。視窗和 Mac 的記錄檔位置如下：

- Windows: `"%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"`
- macOS：`~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs`
- Linux: `~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs`

若要協助疑難排解使用者可能遇到的問題，請啟用可在任何 Amazon 用 WorkSpaces 戶端上使用的進階記錄功能。每個後續的用戶端工作階段都會啟用進階記錄，直到停用為止。

1. 連線到之前 WorkSpace，一般使用者應該啟用其用 WorkSpaces 戶端的進階記錄。
2. 然後，最終用戶應該像往常一樣連接，使用他們的 WorkSpace，並嘗試重現問題。
3. 進階記錄會產生包含診斷資訊和偵錯層級詳細資料 (包括詳細效能資料) 的日誌。

此設定會一直保留到明確關閉為止。使用者成功重現詳細登入的問題之後，應停用此設定，因為它會產生大型記錄檔。

適用於 Windows 的自動化伺服器端記錄檔

此指`Get-WorkSpaceLogs.ps1`令碼有助於快速收集的伺服器端記錄檔服務包 AWS Support。可以 AWS Support 通過在支持案例中請求腳本來請求腳本：

1. 使用用戶端或 WorkSpace 使用遠端桌面通訊協定 (RDP) Connect 線至。
2. 啟動管理命令提示符（以管理員身份運行）。
3. 使用下列命令，從命令提示字元啟動指令碼：

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. 指令碼會在使用者的桌面上建立記錄服務包。

   該腳本創建一個包含以下文件夾的 zip 文件：

   - Ç-包含從程序文件的文件, 程序文件 (x86), ProgramData, 和視窗有關天窗, EC2Config, 圖表, 事件查看器, 和 Windows 日誌 (豹和其他人).
   - CLIxml — 包含 XML 檔案，這些檔案可以使用`Import-CliXML`互動式篩選匯入。請參閱匯入檔案。
   - Config — 每次執行的檢查的詳細記錄
   - ScriptLogs— 有關指令碼執行的記錄檔 (與調查無關，但對於偵錯指令碼的作用很有用)。
   - tmp — 暫存資料夾 (應該是空的)。
   - 追蹤 — 在記錄收集期間完成的封包擷取。

如何檢查到最近 AWS 地區的延遲

連線運作 Health 態檢查網站可快速檢查是否 WorkSpaces 可以連線到所有使用 Amazon 的必要服務。它還對可用 Amazon WorkSpaces 的每個 AWS 區域進行性能檢查，並讓用戶知道哪一個最快。

結論

隨著組織努力提高敏捷性、更妥善保護資料並協助員工提高生產力，因此終端使用者運算發生了策略性轉變。雲計算已經實現的許多好處也適用於最終用戶計算。透過使用 Amazon 將 Windows 或 Linux 桌面移至 AWS 雲端 WorkSpaces，組織可以在新增員工時快速擴展規模、透過將資料保留在裝置之外來改善安全狀態，以及為員工提供可攜式桌面，並使用他們選擇的裝置隨時隨地存取。

Amazon WorkSpaces 旨在整合到現有的 IT 系統和程序中，而本白皮書描述了執行此操作的最佳實務。遵循本白皮書中指導方針的結果是符合成本效益的雲端桌面部署，可隨著您的企業在 AWS 全球基礎架構上安全地擴充。

貢獻者

本文件的貢獻者包括：

- 安德魯·摩根，EUC 解決方案架構師，Amazon Web Services
- 唐·斯科特, 歐盟資深專業顧問, Amazon Web Services
- 克勞斯·貝克爾，歐盟資深專家解決方案架構師，Amazon Web Services
- 納維羅馬吉，首席解決方案架構師，Amazon Web Services
- 羅伯特噴泉, EUC 專業顧問, Amazon Web Services
- 斯蒂芬·斯特勒，資深歐盟解決方案架構師，Amazon Web Services

深入閱讀

如需其他資訊，請參閱：

- Amazon WorkSpaces 管理指南
- Amazon WorkSpaces 開發指南
- Amazon WorkSpaces 客戶
- 管理 Amazon Linux 2 Amazon WorkSpaces 與 AWS OpsWorks 木偶企業
- 定制 Amazon Linux WorkSpace
- 如何使用用戶端 LDAPS 改善 AWS Directory Service 中的 LDAP 安全性
- 搭配 Amazon 使用 Amazon CloudWatch 活動 WorkSpaces 並 AWS Lambda 獲得更高的機隊能見度
- Amazon 如何 WorkSpaces 使用 AWS KMS
- AWS CLI 指令參考 — WorkSpaces
- 監控 Amazon WorkSpaces 指標
- MATE 桌面環境
- 疑難排解 AWS Directory Service 的管理
- Amazon WorkSpaces 管理問題疑難
- 疑難排解 Amazon WorkSpaces 客戶
- WorkSpaces 使用自 Amazon 服務入口網站自動化

文件修訂

若要收到有關此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
次要更新	更新 AD 目錄服務、災難復原/業務持續性和跨區域重新導向的內容。添加 WorkSpaces 和 Amazon Connect 音頻優化。格式化的次要更新。	2022 年 5 月 26 日
次要更新	修復非包容性語言。	2022 年 4 月 6 日
白皮書已更新	已更新內容	2022 年 3 月 24 日
白皮書已更新	更新了 AWS Network Firewall、MAD 複製目錄、Sup YubiKey port、容器、W SLV1、智慧卡 Support、WorkSpaces 服務配額和受信任裝置的內容。	2021 年 12 月 20 日
白皮書已更新	更新了 WorkSpaces 串流通訊協定、智慧卡驗證、圖表、用戶端部署、終端裝置選擇和 Web 存取的內容	2021 年 4 月 28 日
白皮書已更新	已更新內容	2020 年 12 月 1 日
白皮書已更新	自首次發布以來更新內容並添加了新的圖表。	2020 年 5 月 1 日
初次出版	首次出版。	二○一六年七月一日

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。 AWS AWS 產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。客戶的責任和責任由 AWS 協議控制，本文件不屬於與客戶之間 AWS 的任何協議的一部分，也不會修改。 AWS

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的AWS 詞彙表。

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。